Introducción

La tecnología Blockchain es ante todo una problemática de actividad. Hay muchas tecnologías en el ámbito técnico que podrían competir con las tecnologías Blockchain. Sin embargo, al incorporar los límites de actividad, muy pronto las alternativas se convierten en ineficaces, demasiado costosas o su implementación es compleja.

En este apartado, presentamos un modelo para evaluar la conveniencia de la tecnología, y un proceso de aprovechamiento de los casos de uso. Basándonos en un enfoque genérico e industrial, cubrimos los proveedores principales, así como los casos de uso en varios sectores. A continuación, proponemos un proceso de creación de blockchain específico, de gobernanza y de modelo económico subyacente.

# ¿Cuándo utilizar la tecnología?

Hay varias maneras de considerar los casos de uso de una blockchain. Después de reflexionar sobre el asunto, hemos decidido empezar en este capítulo con la lógica por su vertiente de actividad en lugar de hacerlo por su vertiente técnica.

En función de las necesidades, tendremos tendencia a tomar una solución antes que otra.

Se pueden considerar cuatro casos genéricos, donde cada uno añade una capa de complejidad.

* Necesidad de almacenar y hacer un seguimiento de los datos (caso básico).
* Necesidad, además, de que uno o varios terceros recuperen o completen información.
* Necesidad de que ninguna de las partes tomadoras controle toda la información. Entonces hay que delegarla a un tercero.
* En caso de ausencia de un tercero de confianza, todos deben poder leer y escribir en una base de datos mientras sigue siendo digna de confianza para todas las partes interesadas.

El primer caso se puede resolver mediante una base de datos local de confianza. La gestión de esta base de datos, su coste, así como su alimentación son competencia de la empresa que la necesita. Este es el caso clásico de las PYME que gestionan su stock.

El segundo caso necesita una base de datos gestionada por una sola entidad. Los derechos de acceso son limitados a una determinada cantidad de actores con normas de acceso y de uso muy restrictivas. Este es el modelo que habitualmente implantan las grandes empresas para captar datos de terceros asociados con una restricción legal. Una vez más, la empresa propietaria de la base de datos soporta la gestión y el coste. Varias partes comparten la alimentación y la calidad de los datos es un reto importante y costoso, es más frecuente que sea gestionada en el intermediario de contratos que en su uso.

El tercer caso de uso exige que todas las partes tomadoras tengan acceso limitado al dato, excepto un tercero de confianza. Este tercero de confianza se ocupa íntegramente de la gestión de la base de datos. En el sector bancario, este suele ser el caso de las cámaras de compensación. Una entidad realiza la transferencia de fondos a cambio de un activo subyacente si y solo si se reúnen las condiciones. Esta base de datos centralizada gestionada por un tercero representó la última tecnología durante muchos años. Con frecuencia, la estructura de coste se comparte bajo modalidades muy variables (por ejemplo: según el uso o en función del tamaño de la empresa).

En muchos casos, el tercero de confianza no existe o no es necesariamente apropiado por muchos motivos.

Esto es muy habitual, especialmente en el marco de la empresa extendida. En este caso concreto, la blockchain o la lógica de los registros distribuidos, (es decir, Blockchain sin algoritmo de consenso) es especialmente adecuada.

La figura siguiente representa esta relación.

Diagrama

Descripción generada automáticamente

*Soluciones técnicas de almacenamiento de datos en función del caso de uso*

Vamos a centrarnos en las obligaciones que hacen que el uso de un tercero de confianza sea poco apropiado. Las empresas se enfrentan a obligaciones de gestión cada vez más fuertes. El ecosistema en el que navegan se ha hecho cada vez más complejo durante las últimas décadas. Internamente se han realizado muchas mejoras. En cambio, la interacción con las empresas socias parece haber tenido menos éxito. Por un lado, en la era de los datos, las empresas no están listas para dar su información gratis a un tercero. Por otro lado, la confianza no existe forzosamente entre actores. Por fin, las obligaciones legales impiden los intercambios de un determinado tipo entre actores. Por ejemplo, las leyes antimonopolio y la ley LOPDGDD 2018 pueden hacer que los actores se pongan nerviosos en el intercambio de datos que pueden llevar a cabo.

Blockchain no resuelve todas las dificultades, pero es especialmente adecuada cuando se necesita:

* certificar un dato o auditarlo;
* interactuar con empresas externas de manera eficaz, como si se tratara de datos internos de la empresa;
* reconciliar datos entre al menos dos sistemas de información. Esto implica una verificación de la veracidad y de la consistencia de los datos;
* implicar a numerosos actores en una misma temática, que no están necesariamente en la misma empresa.

La figura que aparece más abajo incluye estos elementos.

Por supuesto, la finalidad es hacer que las interacciones entre los participantes sean más fluidas mientras se respeta la legislación local. Blockchain no puede gestionar este último punto, pero sí puede hacerse mediante la gobernanza que la rodea. Por lo tanto, la meta de los técnicos no es implementar las normas impuestas por los propietarios del producto.

Diagrama

Descripción generada automáticamente

*Razones para usar una Blockchain*

Durante los últimos años, ha surgido un marco general de los distintos proyectos alrededor de blockchain. Varias cuestiones críticas representadas en la siguiente figura retoman estos elementos. Las primeras problemáticas están relacionadas con la pertinencia de la tecnología en el contexto. Específicamente, blockchain es adecuada cuando hay múltiples actores en un contexto de desconfianza contenida.

En segundo lugar, muchas normas que tratan sobre la gobernanza son verdaderos puntos de bloqueo. Es necesario que las partes tomadoras no deseen pasar por un tercero de confianza en concreto, que se pongan de acuerdo sobre los derechos de acceso y que haya un auténtico interés (p. ej.: técnico o económico) que les invitará a converger hacia normas de uso de la blockchain. Estas normas incluyen los derechos de acceso, el proceso de validación para dar los accesos y el uso de los datos en el contexto de una aplicación blockchain. Estas normas afectan tanto a los que tienen acceso a la blockchain, de qué manera, que a los usos de los datos en sí mismos.

Por lo tanto, es muy importante, en la primera etapa, encontrar los socios idóneos. Este punto específico relativo a la gobernanza se tratará en el párrafo correspondiente en esta sección.

Diagrama

Descripción generada automáticamente

*Metodología para identificar la conveniencia de usar una blockchain*

Una vez planteado el cuadro general, podemos analizar el proceso de diseño.

# El proceso de diseño: identificación de los casos de uso

El proceso de diseño es fundamental antes de cualquier ejecución. Durante los últimos cuatro años, se han llevado a cabo múltiples intentos en muchas empresas de muchos sectores. Generalmente, se han realizado a nivel de PoC (*Proofs of Concepts*, Pruebas de conceptos) y han sido iniciadas por personas con un perfil informático de los departamentos de innovación, pero pocas veces han llegado a producción.

En 2018 hubo novedades, la tecnología maduró, especialmente en el segmento de las blockchains privadas, y muchos casos de uso encontraron su camino a producción. La cuestión del valor de la aplicación de la tecnología se plantea más que nunca. Esta pasa por un proceso de creación, una valoración de las ganancias y de los costes, y finalmente las etapas de ejecución.

## **1. Búsqueda del valor**

La búsqueda del valor es un pilar fundamental para cualquier proyecto que tenga el objetivo de resolver un problema. Surgen dos filosofías, por un lado las blockchains públicas, y por otro lado las blockchains privadas o de consorcio.

El planteamiento de blockchain pública tiende a buscar la liberación de todos los sistemas de información y convertirse en el «back-end» universal. El planteamiento privado o de consorcio tiende a acoplarse a un sistema de información existente o a sustituirlo parcialmente cuando este último no existe, como si fuera una capa superior informática transversal interempresarial.

Aquí debajo, proponemos un planteamiento de valoración de las ganancias y de los costes de un proyecto blockchain que es suficientemente general para que un responsable de toma de decisiones pueda hacer una planificación.

### a. Metodología y valoración de las ganancias y de los costes

Una gran cantidad de empresas ofrecen sesiones de diseño. Hay varios métodos, algunos muy innovadores. Empíricamente, el más prolífico consiste en reunir a un grupo operativo en un seminario.

Al principio, se les presenta blockchain con sus ventajas e inconvenientes. Luego, los actores alrededor de la mesa interactúan para presentar los casos de uso en los que creen que podría ayudarles la tecnología. Se intercambian notas adhesivas según el sistema Agile, una idea por nota, y resulta ser muy eficaz para la recopilación de ideas.

Es indispensable establecer algunas buenas prácticas para obtener el máximo valor de estos seminarios:

* Hacer que interactúe y participe personal operativo y expertos en el tema.
* Favorecer el intercambio y el debate con amabilidad y sin temor a la jerarquía.
* Limitar los perfiles informáticos en esta etapa para incrementar la creatividad.

La última mención está destinada a favorecer el surgimiento de ideas. A menudo, el intercambio Agile© combinado con el enfoque blockchain es muy distinto de los planteamientos habituales de los grandes grupos. Por otro lado, se corre el riesgo de que el debate se incline rápidamente hacia problemas técnicos, que no son el objetivo de este tipo de seminarios.

Al final de este primer encuentro, una parte importante del trabajo consiste en analizar el valor, la viabilidad y poner desarrollos en marcha. Sin embargo, la experiencia ha demostrado que limitarse a un único departamento de una empresa (p. ej.: departamento de logística o de compras) no siempre es lo mejor. Es preferible repetir el ejercicio en varios departamentos de una empresa. En efecto, teniendo en cuenta el valor transversal del planteamiento de la herramienta blockchain, surgen problemáticas similares o complementarias. La mayoría de las veces, los casos de uso que aportan más valor tienen lugar en:

* la optimización del ecosistema;
* la reducción de riesgo;
* la creación de valores nuevos.

Por ejemplo, en la optimización del ecosistema se vuelven a encontrar la reducción de la reintroducción entre sistemas gracias a una continuidad digital entre empresas, el acceso al dato en tiempo real o incluso la reducción de los intermediarios.

La figura siguiente retoma los elementos de valor identificados. Estos elementos solo son válidos si se trata de una blockchain con acceso limitado (p.ej.: blockchain denominada privada o de consorcio), con la propiedad Turing completo (que permite realizar todo tipo de objetos con un lenguaje de programación). Este último punto vuelve a dar la posibilidad de crear cualquier forma de objeto en el sentido informático del término.

En el caso de las blockchains públicas, la comprobación es más moderada por el momento. Los motivos surgen principalmente de la volatilidad de la criptomoneda, la sostenibilidad del modelo de negocio de los proveedores de solución blockchain o incluso de la gestión de la seguridad.

Tabla

Descripción generada automáticamente

*Los pilares de valor de Blockchain*

Si tomamos como base estos generadores de valor, es posible aplicar un planteamiento de proyecto clásico de ganancias frente a costes. La figura de la página siguiente retoma un modelo sencillo de valoración de las ganancias estimadas.

Para un caso de uso dado, muchos equipos utilizan KPI (indicadores de rendimiento). Es muy frecuente que estos KPI ya existan, y se trata de reutilizarlos. Es una buena práctica contar con la ayuda de un controlador de gestión para evaluar el impacto económico de las ganancias asociadas.

En algunos casos, se pueden crear KPI nuevos. En efecto, tratándose de un sistema informático conectado con procesos interempresariales nuevos, las ganancias pueden cubrir procesos que, considerados individualmente, tienen un coste pequeño, pero que, considerados en un ecosistema toman una dimensión completamente diferente.

Tabla

Descripción generada automáticamente

*Modelo de valoración de un proyecto Blockchain*

Respecto a la estimación de los costes, dependen de la ambición del proyecto. Sin embargo, se constata que los proyectos blockchain de tipo privado tienen un coste global un 10 % superior a un proyecto digital más clásico. Esto se explica por la adición de la tecnología específica, y probablemente por una multiplicación de las soluciones de almacenamiento en la nube, allí donde antes era suficiente con una sola base de datos. Sin embargo, a nivel de una empresa, donde los costes son potencialmente compartidos entre los actores de la blockchain, el coste marginal es manifiestamente más bajo. Compartir costes depende de la cantidad de participantes, de la gobernanza y del modelo de negocio que se deriva. No hay una norma fija. Las empresas tampoco comunican obligatoriamente la cantidad de actores, porque la implementación tiene un impacto importante en la eficiencia de las empresas. Por otro lado, hay que respetar las normas de confidencialidad.

Los proyectos de blockchains públicas tienen resultados en las inversiones más variables. En efecto, la blockchain ya está implementada, en teoría, es posible conectarse directamente. En la práctica, aparecen numerosas limitaciones técnicas, con aspectos tanto de la actividad como informáticos que a menudo no se han evaluado correctamente.

En los proyectos registrados en Europa, se observa que el método de trabajo más utilizado es el método Agile©. Actualmente, es difícil evaluar el índice de éxito de los proyectos en España.

Para hacernos una idea, podemos tomar como referencia el informe de Deloitte (K. Edelman, 2017), que estudia de manera extensiva los proyectos blockchain disponibles en la plataforma colaborativa GitHub (GitHub es una solución de trabajo colaborativa en Internet para los desarrolladores. La herramienta permite almacenar código informático). Los buscadores han contabilizado 86 034. Esto representa un aumento medio de más de 8600 proyectos al año, con un aumento exponencial de 26 885 proyectos en 2016. Si se considera que un proyecto se ha modificado al menos una vez durante los últimos seis meses, entonces solo se mantiene de manera activa un 8 % de los proyectos identificados. La vida media de un proyecto es de 1,2 años. La figura que aparece más abajo, procedente del informe Deloitte, analiza el crecimiento de los proyectos en GitHub desde 2009 hasta mediados de 2017, por tipología de actores: empresas y particulares.

Es importante tener en cuenta que, durante la segunda mitad de 2017, y hasta mediados de 2018, una explosión de la cantidad de proyectos basados en ICO (captación de fondos a base de criptomoneda) hizo aumentar la cantidad de proyectos de manera significativa, pero no forzosamente su supervivencia.

Gráfico

Descripción generada automáticamente

*Proyectos nuevos en GitHub por tipo de autor entre enero de 2009 y junio de 2017*

Con nuestros propios medios, y por lo tanto no las mismas herramientas y la misma metodología que la consultoría Deloitte, hemos contabilizado unos 48 000 proyectos de blockchain en el mundo a principios de 2019. Esta cantidad no tiene en cuenta los proyectos privados que se ocultan de manera predeterminada. En cambio, el índice de supervivencia ha bajado al 7 %. Además, allí donde los perfiles estadounidenses emitían los proyectos de manera masiva, observamos que los países asiáticos tomaron la delantera a principios de 2019, con China en primera posición.

Como ya hemos mencionado antes, 2017 y 2018 fueron testigos de un gran aumento de los lanzamientos de proyectos blockchain. Un mecanismo denominado ICO (*Initial Coin offering*, Oferta inicial de monedas) permitió recaudar fondos privados para financiar los distintos proyectos. Estas captaciones de fondos representan un sector infinitesimal de los proyectos blockchain.

En 2017, la recaudación media de fondos era de 8 millones de euros, frente a 4 millones en 2018. Estas medias ocultan variaciones importantes en función de las pretensiones del proyecto y del territorio.

Por ejemplo:

* Mil millones de euros para Telegram;
* 500 millones de euros para EOS (alcanzó 4000 millones de euros con el aumento temporal de las criptomonedas);
* 230 millones de euros para Tezos.

A título comparativo, una blockchain muy conocida como Ethereum «solo» recaudó 15 millones de euros. Sin embargo, estas inversiones proceden de inversores privados, la mayoría particulares. También, si hacemos la audaz apuesta de decir que el coste de un proyecto es igual a la recaudación de fondos menos el 30 % de margen comercial habitual, un proyecto de blockchain cuesta de media entre 2,8 y 5,6 millones de euros.

El informe de la consultora Deloitte (L. Pawczuk, 2018), que analiza las inversiones previstas por grandes empresas de todo el mundo en blockchain, parece corroborar esta hipótesis. El cuestionario basado en el estudio se ha enviado a 1000 responsables de toma de decisiones colocados en empresas que generan más de 500 millones de dólares de ingresos.

Gráfico, Gráfico de barras

Descripción generada automáticamente

*Inversiones previstas en 2019 para blockchain*

En la figura superior podemos observar que la mitad de las empresas consultadas pensaban invertir entre uno y cinco millones de dólares en 2019. 40 % planeaban invertir más de 5 millones. Podemos obtener los importes en euros consultando el tipo de cambio vigente entre el euro y el dólar.

Considerando las cantidades comprometidas, el año 2019 parecía bendecir las transiciones a producción. Una vez abordada la noción de valor y de costes, se plantea la cuestión de los plazos de ejecución y del impacto de la tecnología.

### b. Estimación del impacto y de los plazos de ejecución de la tecnología

Un proyecto blockchain influye en el funcionamiento de un ecosistema. La innovación procede del planteamiento técnico y de proceso. Muy a menudo, hay metodologías de trabajo internas que se aplican en función de las limitaciones. Sin embargo, los procesos de trabajo entre empresas no están escritos, son poco conocidos e influyen de manera significativa en los métodos de trabajo internos.

Muchas empresas utilizan un planteamiento cliente-proveedor en silos, con los consiguientes juegos de poder. En el marco de un proyecto blockchain, este intercambio sufre una fuerte perturbación. Por ejemplo, una cierta cantidad de tareas de poco valor añadido se pueden automatizar, como la coordinación de planificaciones entre múltiples actores. Actualmente, una tarea de este tipo exige muchos recursos humanos solo para ponerse de acuerdo sobre fechas de entrega y de introducción en producción.

Gracias a la implantación de una blockchain, es posible certificar que una acción se ha realizado de manera correcta y con una calidad dada. Ya no es posible jugar en la zona gris (p. ej.: documento enviado, factura pagada, etc.). Este cambio de desafíos tiene un profundo impacto en el conjunto de las partes. Por otro lado, ya no es necesario pasar por una lógica «bajo-alto-bajo». Por ejemplo, un proveedor debe pasar por el cliente para comunicar una modificación a otro proveedor durante un cambio que impacte en el conjunto de los actores. Esta estructura de pasarela consume tiempo y es una fuente de múltiples anomalías y retrasos. El planteamiento de blockchain puede resolver una parte de estos problemas compartiendo el dato entre actores, sin el intermediario del cliente. Este intercambio se puede llevar a cabo de manera legal y respetando la legislación antimonopolio.

Igualmente, para garantizar un impacto positivo y un retorno de la inversión, una comunidad de actores comprometidos prima sobre el esfuerzo tecnológico. La parte más pesada del trabajo consiste en identificar las pérdidas de eficiencia y el proceso de puesta en común.

Asimismo, si tradicionalmente un proyecto digital consiste en un 60 % de desarrollo y un 40 % de gestión, el planteamiento blockchain puede cambiar esta norma. De esta manera, el proyecto tiene más posibilidades de culminar con retorno de la inversión positivo.

A pesar de las problemáticas internas, el mercado parece despegar. En función de las fuentes, la inversión mundial en las empresas emergentes basadas en blockchain oscilaba entre 600 y 1300 millones de euros en 2016 (L. Aré, 2016). Por el contrario, en 2018, las tres mayores recogidas de fondos privados en las blockchains públicas ya representaban 1700 millones de euros. Además, los fondos de capital riesgo especializados en las empresas emergentes blockchain invirtieron 1300 millones entre enero y junio de 2018 (Rowley, 2018). El sector se estima en 20 000 millones de euros de aquí a 2024 (L. Aré, 2016).

Ahora, el foco se centra en la rentabilidad y el futuro de los proyectos.

Según un estudio realizado por IBM (IBM, 2016) en 2016 sobre 200 bancos y 200 instituciones de mercados financieros, un 52 % de los bancos y un 57 % de las instituciones consideraban que la falta de retorno sobre la inversión de los proyectos blockchain es una barrera a la puesta en marcha de blockchain. Sin embargo, casi dos terceras partes contemplaban una puesta en producción dentro de tres años.

Su observación se confirma en un informe de Deloitte (L. Pawczuk, 2018) que presenta la parte de los proyectos blockchain en producción o previstos para entrar en producción entre 2018 y 2019 en siete países.

Gráfico, Gráfico de barras

Descripción generada automáticamente

*Proyectos blockchain en producción o planificados para entrar en producción en 2019*

Podemos observar que en Francia, casi el 86 % de sus proyectos blockchain han llegado a producción. Sin lugar a dudas, 2018 fue testigo del final de los proyectos en formato Proof of Concept y el inicio de los MVP (*minimum viable product*, Producto mínimo viable). Una tendencia observada en todo el mundo, a excepción de los Estados Unidos. En efecto, el mismo estudio explica que un 30 % de las empresas estadounidenses tienen dificultades para encontrar el caso de uso.

Los proyectos mencionados abarcan los sectores de la automoción, energético (gaz y petróleo), médico, bancario, alimentario, tecnológico y servicios públicos, por ejemplo. Los tres primeros estiman en más del 70 % que la tecnología va a transformar en gran medida la organización del sector durante los tres próximos años. Para las otras industrias, las cifras oscilan entre el 64 % y el 46 %.

Estos resultados coinciden con otro estudio realizado por la misma consultoría en asociación con la EFMA (*European Financial Management Association*, Asociación europea de Gestión Financiera) en 2016 a cerca de 3000 instituciones financieras. Se les preguntó a los responsables de toma de decisiones cómo se transformaría su sector.

Puede ver los resultados en la figura que aparece aquí debajo.

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

*Estimación del impacto de la tecnología Blockchain en el sector financiero. Fuente: Deloitte, EFMA, 2016*

Se constata que menos del 10 % de los responsables de toma de decisiones estiman que la tecnología del registro descentralizado no tendrá ningún impacto o este será despreciable, para cualquier actividad o en el sector donde trabajan.

En 2016, solo el 30 % de los actores encuestados estimaban que la tecnología estaría lista en un plazo de dos años, es decir, en 2018. La mayoría parecía estar de acuerdo en un plazo de dos a cinco años, como en la figura que aparece aquí debajo.

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

*Estimación del período de incubación antes de un uso de la tecnología en el sector financiero. Fuente: Deloitte, EFMA, 2016*

Retrospectivamente, el pronóstico es concluyente. En el aspecto técnico, las blockchains como Hyperledger han pasado de algunas decenas de transacciones a más de 3500 por segundos con latencias inferiores al segundo y una escalabilidad que supera los 100 nudos de red (E. Androulaki, 2018). Sin embargo, aunque la tecnología puede usarse en producción, todavía no permite una eficiencia comparable a la de las bases de datos clásicas durante los picos de carga (N. Qassim, 2018). Según el personal operativo, a principios de 2019 sus expectativas estaban más dirigidas a problemas de seguridad que a problemas de eficiencia.

A finales de 2016, IBM ya había invertido más de 200 millones de euros en esta tecnología, es decir, un poco más del equivalente a mil empleos a tiempo completo. Esto significa que la técnica, bajo reserva de inversiones de investigación, no es una barrera tan fuerte como se preveía.

Respecto a las blockchains públicas, el protocolo Lightning está en vías de implementación en la red Bitcoin, con el objetivo de aumentar la velocidad de procesamiento de las transacciones. Ethereum y las tecnologías públicas no se quedan atrás, aunque su perímetro de aplicación se considera reducido teniendo en cuenta las imposiciones técnicas más estrictas.

De manera paralela, la investigación sobre el tema se multiplicó por diez entre 2014 y 2016 (L. Aré, 2016), luego aún se cuadriplicó entre 2016 y 2018.

Así, parece evidente que la tecnología se desarrolla y tendrá un impacto significativo. La principal dificultad consiste en identificar cuándo y desde cuándo los proyectos recuperan sus gastos.

Según múltiples estudios disponibles y los correspondientes Corda e IBM, el futuro de los proyectos de blockchains privadas parece oscilar entre 3 y 5 años para producir lo fundamental de su valor. No hemos encontrado documentación estadística sobre las blockchains públicas. Si algunas han podido encontrar su caso de uso, muchas todavía lo están buscando.

Para terminar, los problemas actuales a los que se enfrentan las organizaciones están asociados con un método de pensamiento concreto. Para que un proyecto blockchain tenga éxito, parece necesario reformular el problema. Después, se encontrarán soluciones nuevas. Entonces la cuestión se plantea sobre los desafíos, más que sobre su resolución. La tecnología es una oportunidad fantástica para no buscar más soluciones en silo, sino en grupo y así encontrar el retorno de la inversión. Entonces se trata de identificar los factores que permitirían acelerar, o ralentizar el desarrollo y la adopción del registro descentralizado en el sector.

### c. Motivaciones y obstáculos para la adopción de la tecnología

Múltiples elementos pueden acelerar el ritmo de adopción o, al mismo tiempo, frenarlo. Hay varios puntos de vista posibles para realizar un análisis completo.

Los elementos motrices alegados presentados en la figura de la página siguiente durante el estudio no son competencia de la técnica (Deloitte, EFMA, 2016), sino de aplicaciones en el sentido económico del término. El estudio muestra características económicas interesantes.

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

*Motores de la adopción de la tecnología Blockchain en el sector financiero. Fuente: Deloitte, EFMA, 2016*

En primer lugar, casi el 40 % de los encuestados están motivados para la conquista de mercados nuevos, frente al 20 % que la consideran un medio de reducir costes. El miedo parece representar una parte pequeña de la motivación. De lo que se deriva que el entusiasmo está claramente asociado con la búsqueda de mercados nuevos, de manera similar a los inicios de Internet o del smartphone.

A nivel global, los equipos operativos están entusiasmados por el planteamiento de blockchain. Les evita operaciones manuales de reintroducción, crea los vínculos inexistentes entre aplicaciones y favorece los intercambios productivos entre actores. Su enfoque positivo se debe especialmente a una promesa de captación de información a la que todavía no tienen acceso y que necesitan para aumentar la eficiencia.

Además de las motivaciones, los obstáculos también son importantes para desbloquear los fondos necesarios.

La figura siguiente representa los distintos factores mencionados, como los problemas de seguridad o la ausencia de supervisión de la red. Estas críticas ya se habían mencionado antes de la adopción masiva de la industria informática en la gestión de transacciones.

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

*Obstáculos a la adopción de la tecnología Blockchain en el sector financiero. Fuente: Deloitte, EFMA, 2016*

Sin embargo, el factor preponderante en los primeros desarrollos y en el paso a la fase industrial para ser el relacionado con la normativa. El sector financiero está inundado de normas y reglamentos destinados a garantizar la seguridad del sistema financiero, pilar de las sociedades capitalistas. También, no es sorprendente que casi la mitad de las personas encuestadas estimen que la dificultad principal a su nivel gira entorno a la incertidumbre jurídica.

Aquí hay que leer un mensaje sólido destinado a las administraciones estáticas, y más especialmente al cuerpo legislativo. A nivel de España, así como de la Unión europea, se plantea la cuestión de cómo legislar sobre esta nueva tecnología. Toda la dificultad reside en la necesidad de proteger a los ciudadanos por un lado, mientras se evita asfixiar a las aplicaciones potenciales que podrían dar muchos puntos de crecimiento a las economías desarrolladas. Parece que se debería apostar por la vía jurídica anglosajona. Más precisamente, parece importante enviar un mensaje claro a los que quieren desarrollar la tecnología creando un marco global, para luego precisar de manera progresiva las normativas legales. Por ejemplo, sabemos que la tecnología ya puede aplicarse para validar las transacciones financieras entre dos partes dentro de un banco.

Sin embargo, las leyes exigen que algunos de estos controles sean realizados por personas con cualificaciones precisas. Suavizar al menos uno de estos perímetros de manera experimental podría ser una solución para crear la confianza entre los bancos, el cuerpo normativo y los profesionales de blockchain.

Además de este estudio, la práctica ha hecho aflorar familias de obstáculos que no son evidentes a simple vista, y difícilmente aparecen en los estudios. El impacto de la tecnología implica nuevas organizaciones. Un obstáculo importante consiste en agrupar y dirigir un proyecto entre empresas. Paradójicamente, las partes tomadoras más reticentes y escépticas son los departamentos informáticos de los grandes grupos. La elección de la tecnología y de la implementación escapa a su control en beneficio de una gobernanza compartida. Por otro lado, hay pocos expertos en blockchain. Por eso el desafío es doble: cualificación y control.

La segunda familia de obstáculos es a nivel de la estructura organizativa y financiera que sostiene un proyecto blockchain. Una cierta cantidad de grandes grupos funcionan por silos, es decir, por campo de especialización. Aunque las necesidades concuerdan entre departamentos, los enfoques transversales no suelen dar frutos, porque es difícil asignar en qué departamento recae un gasto transversal. El problema se complica con dos actores externos en la empresa que tienen intereses divergentes. En el marco de un proyecto entre empresas, el proceso de captación de las necesidades debe realizarse en el seno de una iniciativa financiada (p. ej.: una asociación con intereses económicos o una sociedad por acciones simplificada). Esto implica un sobrecoste que no estaba necesariamente considerado en el lanzamiento del proyecto. Por último, un problema nada despreciable, la incomprensión de las leyes antimonopolio y su escaso conocimiento puede hacer que un ecosistema de actores se muestre reticente a reunirse en torno a un proyecto común. Otro obstáculo que se empieza a observar: el planteamiento blockchain puede transformar profundamente los intereses de los proveedores frente a los de sus clientes. Pueden favorecer sus necesidades allí donde primarían las del cliente.

Para concluir, ante todo, la búsqueda de valor se encuentra en un ecosistema antes que en una empresa. El proceso de valorización es afín a los métodos tradicionales, pero debe estar sujeto a una revisión de los desafíos para tener en cuenta un porvenir más amplio que el de una empresa en concreto.

Los costes no son sensiblemente superiores a un planteamiento digital clásico y a menudo se compensan porque se comparte el coste total. Las ganancias, en cambio, son poco conocidas, con retornos de la inversión inciertos, probablemente vinculados a una manera nueva de ver un proyecto. La tecnología tiende a estar lista para su uso en producción, como se explica en el siguiente apartado.

## **2. Realización: POC, MVP y hackathons**

Una vez establecido el caso de uso, surge la cuestión de la realización. Actualmente, hay más de 2000 tecnologías distintas, con características particulares. Los lenguajes de programación difieren sustancialmente con la mayoría de los lenguajes que todavía no son dominantes (p. ej.: Plutus, Solidity, RIDE).

Sin embargo, en la práctica, pocas tecnologías están realmente maduras y listas para usarse en producción. En lo que concierne a la blockchain pública, el mercado de las aplicaciones sigue estando en pañales, a pesar de los cientos de miles de aplicaciones disponibles. Por ejemplo, las aplicaciones más populares difícilmente sobrepasan los 3000 miembros. No es fácil encontrarlas e integrarlas en soluciones clásicas (p. ej.: página de Internet) y mucho menos hacerlas trabajar en conjunto.

Las soluciones de blockchains privadas o de consorcio han visto una mejora continua de sus características durante el año pasado y son firmes candidatas en la realización de Proofs of Concepts y mucho más.

En este apartado, presentamos las distintas etapas de desarrollo para obtener valor de los proyectos blockchains lo más rápido posible.

### a. Las POC: evaluación de las hipótesis

La etapa de creación ha permitido identificar una determinada cantidad de casos de uso. La dificultad es conocer la viabilidad, crear indicadores de rendimiento y formar los equipos en la nueva tecnología.

Ahora más que nunca, los proyectos blockchain exigen una recopilación de necesidades y una lista de desafíos precisos a resolver. El valor de la PoC se constata en una lógica de ecosistema, más que en el logro técnico en un puesto de trabajo aislado. Es necesario detectar obligaciones reales, tanto en el plano técnico como funcional.

En el plano funcional, se recomienda en gran medida empezar con al menos un socio externo. Se trata de innovación conjunta, ya sea con el cliente o con un proveedor, antes de empezar a escribir el código. El esqueleto de un proceso debe estar definido con antelación, para facilitar la etapa de integración de la innovación en los sistemas ya existentes. Después de las observaciones según la experiencia de los desarrolladores, la PoC no ha tenido éxito en algunos casos porque habían descuidado esta etapa, y los actores que utilizarían la herramienta no estaban involucrados. Los factores principales que se deben considerar incluyen:

* la definición del campo de acción del caso de uso de la PoC en función de la concepción final objetivo. Esto incluye la definición de los socios;
* compartir el conocimiento de la tecnología (evangelización) y lo que puede hacer;
* la definición de las responsabilidades de cada socio o parte tomadora;
* la implantación de procesos de convergencia de decisiones y de priorización de las funciones.

En el aspecto técnico, hay que validar etapas críticas. Las que aparecen a continuación se encuentran entre las más importantes:

* la viabilidad técnica;
* la alimentación del dato, al menos manual;
* la aplicación del proceso de trabajo;
* la gestión del aislamiento de los datos y de la confidencialidad minimalista;
* el servicio de seguridad, al menos elemental.

El caso de uso permitirá identificar qué tecnología será necesaria, y no a la inversa. Empezar por una tecnología puede implicar costes adicionales importantes durante el paso a la etapa MVP (*minimum viable product*).

La fase de los indicadores es un ejercicio delicado con nuevas tecnologías. Considerarlos en esta fase, incluso al final, es un desafío difícil de identificar.

Por el momento, el coste medio observado de una PoC oscila entre 50 000 y 75 000 €. Los más ambiciosos pueden alcanzar los 150 000 €. No parece haber una constante para el mecanismo de gastos.

La consultora Deloitte realizó un estudio para evaluar en qué fase se encontraban las empresas en 2016. Un 43 % de los encuestados respondió que consideraban estar en fase de aprendizaje, mientras que un 28 % todavía no había empezado a estudiar el tema (Deloitte, EFMA, 2016). En cambio, en 2018, casi tres cuartas partes de las personas encuestadas habían pasado a producción o pensaban hacerlo durante el año siguiente, como puede verse en la figura que aparece más arriba.

La PoC afecta tanto a las blockchains públicas como a las privadas. La figura que aparece aquí debajo muestra la tipología de uso.

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

*Categorías de blockchains preferidas por el sector financiero. Fuente: Deloitte, EFMA, 2016*

Podemos observar una preferencia mayoritaria por las blockchains privadas de consorcio; una minoría desea utilizar una blockchain pública. Hay varios motivos detrás de este entusiasmo. En primer lugar, una blockchain privada se considerada menos propensa al pirateo y a las manipulaciones de criptomonedas que una blockchain pública. Después, como se utiliza la misma norma en el sector mediante un consorcio, se resuelve el problema de interoperabilidad entre las blockchains. Cabe recordar que, en 2019, no hay ningún método para fusionar dos blockchains basadas en sistemas distintos.

Los resultados de las blockchains privadas, propiedad de una empresa, se defienden de la misma manera. Una quinta parte de las empresas que respondieron al cuestionario era optimistas en cuanto a la viabilidad de esta solución. Es probable que esté relacionado con la etapa de experimentación. Crear su propia blockchain, privada o pública, es accesible y permite un avance rápido del proyecto, algo que no sucede cuando se crea una blockchain de consorcio. Se pueden ocultar flujos en la blockchain, como desean algunas instituciones. Si hay soluciones de blockchains donde los importes también están ocultos, como Monero, actualmente no es una práctica generalizada. Monero es una criptomoneda protegida, privada y casi imposible de rastrear. Sin embargo, no hay ningún medio de convertir divisas clásicas en Moneros. Sus usuarios deben pasar de manera sistemática por el protocolo Bitcoin, y por lo tanto por las plataformas Bitcoin.

Los motivos para elegir una cadena Bitcoin se resumen en el hecho de que funciona. Los postulados teóricos también consideran que todo el mundo podría, o incluso debería, funcionar en una sola blockchain. Entonces se evitarían de facto los problemas de fusión de las blockchains. También consideran que evolucionarán las imposiciones técnicas vinculadas al protocolo. Frente a los debates tumultuosos y encendidos sobre las bifurcaciones (*forks*), algunas evoluciones corren el riesgo de ser comprometidas. En efecto, todos los sectores no tienen las mismas necesidades. Pero sobre todo, la motivación fundamental de esta elección, más allá de algunas imposiciones técnicas, es que esta blockchain funciona y que ha hecho pruebas.

Cuando la etapa PoC da frutos, se puede plantear pasar a MVP.

### b. Los MVP: think big, begin small

El MVP es una etapa que transforma la experimentación en un auténtico proyecto. Se requieren innovaciones muy numerosas en esta etapa. Una vez más, las mayores innovaciones no son técnicas, sino más bien funcionales.

La tecnología aporta muchas promesas y es importante canalizar el esfuerzo en una comunidad con una gran cantidad de actores.

Los desafíos son especialmente importantes en el marco de una blockchain de consorcio, porque los métodos de trabajo tienden a recibir un fuerte impacto. La gobernanza se vuelve crítica, al igual que el modelo de pago, de valoración de gestión del dato, etc. La primera dificultad consiste en identificar a qué rama vincular un proyecto blockchain. ¿Es un proyecto técnico o funcional? ¿Se va a calificar en una sección logística, de compras o calidad, por ejemplo? ¿Hay que crear un segmento nuevo en la empresa o se puede vincular de manera transversal a varias unidades de negocio?

Vincular los proyectos a ámbitos técnicos acelera en teoría el proceso de desarrollo y la realización. Sin embargo, los proyectos tienden a convertirse en productos técnicos que responden a problemáticas internas. Esto conduce a fracasos, según dos responsables de toma de decisiones en banca de inversión entrevistados. Los proyectos blockchain tienen una dimensión transversal en la empresa dentro de un ecosistema de actores. Requiere que sus actores tengan una disposición mental particular.

Vincular los proyectos a una sola división de actividad tiene la ventaja de centrarse en el valor del producto y facilitar la dirección en las instancias existentes. A cambio, la interacción con los otros departamentos es muy complicada, y no es viable el paso en todas las instancias.

Los responsables de la toma de decisiones raramente desean vincular el proyecto a una entidad transversal nueva y las organizaciones casi nunca lo hacen, porque la dirección y la justificación presupuestaria son complejas.

Uno de los planteamientos más prometedores actualmente consiste en crear un programa que entra en una instancia de gobernanza lo más transversal posible dentro de una empresa.

En el sector bancario, sería por ejemplo la gestión de riesgos. Cuando se reúne, esta instancia tiene la misión de comunicar los elementos de proyectos. La consulta con el experto es puntual y la organización de tipo matricial.

Estas cuestiones organizativas se completan con las necesidades de definición de un modelo de negocio y la toma de decisión común, allí donde en el pasado una división informática tenía todo el poder sobre las elecciones técnicas.

En el plano funcional, los desafíos que se plantean son los siguientes:

* Definición de una hoja de ruta de funciones y socios nuevos si procede.
* Animación de la comunidad de expertos para captar las necesidades y priorizarlas.
* Definición de la elección de las funciones a desarrollar en común. Quizás, la elección del valor no siempre es la mejor solución.
* Definición de la política integración de actores nuevos y derechos de decisión si procede.
* Animación de la integración de actores nuevos.
* Realización del vínculo con la división informática y digital de la empresa.
* Realización del soporte funcional.

En el plano técnico, las siguientes tareas también son importantes:

* Definición de una arquitectura escalable, distribuida en el tiempo.
* Gestión de los derechos de acceso y del proceso de validación del dato.
* Seguimiento de aplicación y de la blockchain si procede.
* Integración en el directorio de empresas si existe y si procede.
* Gestión del aislamiento de los datos y de la confidencialidad objetivo.
* Aumento de la competencia de nuevos desarrolladores.
* Alimentación automática de datos.
* Desarrollo de las funcionalidades.
* Realización del soporte técnico.

Además de la etapa de MVP, un proyecto también debe enfrentarse a las actualizaciones de versión. En el marco de las blockchains públicas, se habla de forks. Estas últimas pueden tener un impacto muy fuerte en las aplicaciones colocadas encima. En el marco de las blockchains privadas, la actualización de versión todavía es muy laboriosa, manual y a menudo necesita reconstruir una blockchain de principio a fin. Por ejemplo, la actualización de versión de Hyperledger Fabric 1.1 a 1.4 puede necesitar diez días-persona. La compatibilidad con versiones anteriores no está garantizada de manera sistemática.

Los casos presentes hasta ahora contemplan un presupuesto y una elección anticipada de los casos de uso más prometedores. Este planteamiento puede ser sesgado. A veces, también es preferible lanzarse a un hackathon y sacar unas enseñanzas muy valiosas en un tiempo récord.

### c. Los hackathons

Un hackathon es un evento que reúne a un conjunto de desarrolladores durante un tiempo limitado, para resolver un conjunto de problemas generalmente predefinidos por los organizadores. A menudo conducen a recompensas que permiten a iniciativas darse a conocer o elegir un caso de uso en lugar de otro dentro de un planteamiento de proyecto o PoC.

Los hackathons más conocidos se celebran a principios del verano y raramente duran más de 48 horas. PayPal, el famoso servicio de pago en línea, es el resultado de un hackathon.

Las iniciativas de hackathon pueden ser a nivel gubernamental, de una empresa de software o incluso de una empresa que busca utilizarlo.

The Ideation Challenge

Healthit propone financiar proyectos de manera similar a los hackathons. Los participantes pudieron proponer sus proyectos desde principios de julio de 2016, por ejemplo, bajo la forma de documentación técnica (*white papers*) que no deben superar las diez páginas. No es necesario ningún prototipo. Al final de un período de evaluación, los ganadores se anunciaron a finales de agosto de 2016. Una parte de ellos tuvo el privilegio de poder presentar su proyecto a inversores a finales de septiembre de 2016 durante un workshop (Healthit, 2016) apoyado por National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología).

Se trata de una agencia gubernamental americana. Su objetivo es promover la economía basada en nuevas tecnologías, la metrología (estudio de las mediciones) y los estándares necesarios para la expansión de los sectores que los utilizan.

Los proyectos propuestos debían tratar al menos uno de los siguientes temas:

* Información firmada digitalmente.
* Smart contracts.
* Sistemas de gestión del IoT.
* Sistemas de almacenamiento distribuidos.
* Sistemas de confianza distribuidos.

Las recompensas oscilaban entre 1400 € y 4800 € para los ocho ganadores posibles.

El objetivo no era financiar una empresa nueva con estas recompensas, sino de proporcionar una visibilidad a los que habrían podido hacer una aportación a un sector en plena construcción.

Hackathons de Ethereum

En 2015, la fundación Ethereum buscó lanzar un hackathon. Si el prototipo funcionaba, los inversores interesados podían financiar el desarrollo completo y efectivo y de la idea.

El acontecimiento se había concentrado en tres días, y el tamaño medio de los equipos era de dos a tres desarrolladores. La duración parecía justificarse con la necesidad de tener soluciones más permanentes y utilizables. El importe del precio propuesto era consecuente y podía servir de incentivo para un planteamiento comercial real de una solución descentralizada.

Para su segunda edición en 2016, el evento se desarrolló a lo largo de cuatro semanas. La comunidad podía ver el desarrollo de las aplicaciones en curso y votar por su preferido. La fundación proponía seguir las propuestas en el sitio dedicado o mediante la aplicación descentralizada Slack-it (fuente: <https://slack.com/is>). Allí había ideas como por ejemplo un sistema de certificados médicos descentralizado o una herramienta de intercambio de activos ilíquidos (casa, terreno, etc.).

El evento suscitó un entusiasmo auténtico, y los organizadores observaron que los eventos más cortos eran más fructíferos. Así, por ejemplo, la sesión de 2019 pretendía centrarse en dos días, en marzo como de costumbre.

Hackathon IOTA

IOTA es una tecnología de registro distribuido muy activa en el mundo de los hackathons. Desde el 25 de febrero de 2019 al 6 de abril de 2019 (Ogwu, 2019), la empresa había lanzado un desafío sobre las smart cities que implicaba el uso de IOTA. El ganador recibiría 10 000 euros.

Se presentaron varios temas, entre ellos los siguientes:

* Smart charging for smart cars - transformar el vehículo en una cartera con ruedas, separada de la identidad de una persona.
* PayIOTA: Internet de los pagos de transportes públicos - pago de medios de transporte mediante la tecnología.
* Smart ride - identificación de los balances de pagos adeudados durante las compras pagadas mediante la tecnología.
* Smart transportation demo - monitorización en tiempo real de los convoyes que transportan materiales peligrosos, y del estado del objeto transportado.
* Open mobility market place - plataforma abierta de movilidad, desintermediación de todas las plataformas existentes.
* Uberisation of electric vehicle charging - geolocalización y pago del propietario del terminal mediante IOTA.
* Smart rider - uso de un token de identidad único para poner en contacto al conductor con el cliente.
* Where is my bus - gestión de flota, la geolocalización de la misma está a disposición del cliente.

Este hackathon es un ejemplo de ambición distinta a lo que propuso Ethereum. En lugar de un período relativamente restringido, la empresa había considerado que el tiempo de los experimentos había pasado y que era necesario dar más tiempo a los desarrolladores para llevar a cabo productos reales.

En la práctica, en la fecha fatídica se habían desarrollado pocos proyectos, donde una gran cantidad de ellos habían sido realizados por estudiantes. Para responder a la falta de participación y de realización, el hackathon se prolongó hasta el 3 de mayo.

Desgraciadamente, pasada esta fecha, el avance de los proyectos no era más concluyente. El hackathon es una forma muy precisa de evento. La naturaleza de su éxito reside precisamente en una duración corta. Extender un proyecto a lo largo de muchos meses implica una fase de formación o un auténtico proyecto inscrito en una lógica de costumbre. En caso contrario, la recompensa debe justificar el esfuerzo. En conclusión, parece que devolvieron los patrocinios porque en realidad ningún desarrollo pudo llegar a buen puerto.

Hackathon de empresa

Los hackathons de empresa pueden permitir identificar los casos de uso más prometedores, tanto si han sido identificados con antelación o no. En el contexto de una empresa, las condiciones en cambio son muy distintas, a causa de la legislación laboral. Hay muchas modalidades, con eventos que oscilan entre un día y una semana.

Por ejemplo, el grupo Renault inició un hackathon de empresa en torno a la recarga de vehículos eléctricos con ayuda de blockchain. El ganador demostró que era posible cargar un coche utilizando la tecnología Ethereum.

Varios grupos bancarios han hecho muchos intentos, especialmente Banco de Sabadell, que al final de su hackathon celebrado en febrero de 2017, en Palau de Mar (Barcelona), se presentaron proyectos con continuidad y aplicación a corto plazo en la vida diaria.

Se puede recurrir a organismos terceros que se han especializado en este tipo de evento, como Hackathon.com. La ventaja en este caso concreto es solicitar recursos que no están necesariamente dentro del grupo emisor del evento.

Recordando las metodologías de desarrollo, actualmente es apropiado plantearse la cuestión de la elección de la tecnología en función de las necesidades.

# La elección de la tecnología

Después de leer los apartados anteriores, podemos identificar los motivos por los que es apropiado elegir un proyecto blockchain, luego se han propuesto los métodos de desarrollo. Entonces, es legítimo que nos preguntemos por la elección de la tecnología.

## **1. Elección del tipo de blockchain: privada o pública**

Hay tres modelos de blockchain: pública, de consorcio y privada, como se ilustra en la figura que aparece aquí debajo.

Gráfico, Gráfico de burbujas

Descripción generada automáticamente

*Representación de los distintos tipos de blockchain*

Cada blockchain responde a una necesidad concreta.

### a. Blockchain pública

Históricamente, las blockchains públicas son las más antiguas, con la llegada de Bitcoin en 2008. Esta variante tecnológica es la más prolífica. Entre las más de dos mil tecnologías disponibles actualmente, lo fundamental de entre ellas parece centrarse en una lógica de pago en línea con una filosofía de eliminación de desintermediación bancaria.

Las tecnologías blockchains están especialmente justificadas para automatizar transacciones financieras sobre la base de realización de ciertas condiciones. Por ejemplo, cuando se recibe una factura un smart contract puede verificar las condiciones y activar el pago.

Algunos programas, como SAP, pueden hacer este tipo de operación, y actúan como bancos en sustitución de token virtuales. Sin embargo, SAP es una solución costosa, la blockchain pública puede paliar este problema y posicionarse en el segmento de las empresas de tamaño medio, pero ninguna tecnología pública paree haberlo hecho hasta ahora.

En este segmento de mercado se presentan muchos candidatos. En cabeza, podemos ver a Bitcoin, Ethereum, Ripple, etc. Como la competencia es difícil, tienden a especializarse mucho. Bitcoin es un actor histórico y tiene un rendimiento muy bueno por su comunidad de usuarios. Ripple, por ejemplo, se ha especializado en los intercambios transfronterizos con grandes bancos. Stellar se ha posicionado en los micropagos, pero va a atacar el terreno de Ripple. IOTA busca desarrollar su actividad de pago entre máquinas, por ejemplo, en el segmento de los Vehicule to X, o VtoX, en el sector de la automoción.

Un segundo caso de uso de las blockchains públicas consiste en compartir datos entre sistemas de información, con la certificación de que la transferencia se ha efectuado. En resumen, se trata de un sistema de información abierto donde todo el mundo puede leer y escribir, pero nadie puede modificar nada.

Ethereum parece un abuelo en este segmento. Hay un campo data disponible y se paga por los bytes de datos que se transmiten. Si hacemos un cálculo, en la plataforma Ethereum, transferir un gigabyte de datos cuesta cinco millones de euros. Por el contrario, las soluciones en la nube de Google, con reputación de ser muy agresivas, cuestan dos céntimos de euros por giga, con el mismo nivel de servicio.

La lógica de sistema de información abierto es muy amplia y no permite gestionar todos los casos de uso. Así, FileCoin e IPFS tienen el objetivo de permitir almacenar, consultar y destruir archivos en línea, sin pasar por una creación de cuenta en la nube con la gestión de las autorizaciones que se deriva. IOTA permite intercambiar informaciones entre pequeños sensores, originalmente dentro del universo del Internet of Things. Último ejemplo: Basic Attention es una plataforma de intercambio de publicidad para hacer más transparente la publicidad en línea. Otros, como Neurochain, proponen una solución en línea distribuida de aprendizaje automático, que aprende con una base de muestras mucho más extensa que una empresa única, por lo que propone predicciones mucho más fiables.

Para los profesionales de los datos, el modelo blockchain sigue el planteamiento «serverless» de las bases de datos. Esto significa que la base de datos no es un problema, y ni siquiera es un tema de preocupación. Se puede pasar de una base de datos X a Y en un instante y añadir componentes al vuelo, sin esperar la entrega de material, etc. La gestión y la supervisión de actuación ya no están en su ámbito de competencia. Los equipos que desarrollan el protocolo también se ocupan del proceso de optimización de las bases de datos.

Este argumento técnico diferenciador ha perdido su esplendor durante los últimos cuatro años, porque las plataformas en la nube se dirigen con fuerza hacia este modelo. En la práctica, las organizaciones parecen preferir el planteamiento en la nube por los siguientes motivos:

* las herramientas de base de datos en la nube son más eficaces, y su uso es más versátil;
* el aumento de la competencia en un paquete de software (p. ej.: herramientas Google Cloud platform) tiende a ser coherente y estar agrupada en un punto de acceso;
* la facturación les parece más controlada.

El último elemento diferenciador es la certificación disponible públicamente. Esta lógica es una necesidad real en algunos casos, pero no parece corresponder a la norma de los casos de uso de bases de datos. La mayor parte del tiempo, es suficiente con una base de datos en la nube asociada a una llamada por API (*Application Programming Interface*, Interfaz de programación de aplicaciones. Se trata de una herramienta que permite captar datos sin conocer el modelo de datos subyacente. Habitualmente, las informaciones devueltas corresponden a un estándar).

Entonces podría parecer que el segmento más pertinente de las blockchains públicas consiste en una hiperespecialización, un posicionamiento no esté orientado a clientes de grandes cuentas, y una capitalización en la lógica de certificación del dato. Otro intercambio puede basarse en una blockchain con un objetivo global (p. ej.: Ethereum), sobre la que se implanta una capa de especialización en la cima, para mejorar las características. Una pista evocada por la tecnología EOS.

Más allá de estos puntos técnicos, la fluctuación de la criptomoneda es un auténtico punto negro para gran cantidad de actores. Una solución consiste en invertir en monedas del tipo stablecoin. El token se apoya en un contravalor en divisas o en metales preciosos. Sin embargo, una vez más, no aludiremos ni a Ethereum ni a Bitcoin.

La elección de una blockchain pública corresponde a casos muy precisos y tiende a crear un sistema de información común cuando no existía. Todos los proveedores de tecnología apuestan por una implantación de una plataforma, a imagen de actores como Alibaba o Uber. Actualmente, la atención se centra en las blockchains de consorcio.

### b. Blockchain de consorcio

La lógica de blockchain de consorcio es más reciente, y forma parte de las tecnologías denominadas «permisionadas» (permissioned), por oposición a las blockchains públicas (permissionless).

Como recordatorio, los componentes básicos de una blockchain pública son:

* un protocolo de intercambio (p.ej.: entre pares);
* un registro que permite grabar los intercambios;
* un algoritmo de consenso para validar matemáticamente la legitimidad de una transacción;
* un lenguaje de programación que permite automatizar los intercambios de datos y de valores;
* una encriptación de los intercambios para protegerlos;
* opcionalmente, un token para permitir un intercambio de valores.

Estos elementos han aportado muchas innovaciones como las siguientes:

* una desintermediación en el proceso de pago mediante una arquitectura entre pares;
* derecho de acceso al dato, tanto de lectura como de escritura, así como una replicación virtual infinita que permite intercambios sin límite de información;
* reutilización de código existente, ya que está disponible y libre de derechos para los que lo necesiten.

En la práctica, este piadoso objetivo se enfrenta a numerosas ataduras. Muchas empresas no pueden utilizar la lógica de blockchains públicas porque:

* el rendimiento de las plataformas no corresponde al nivel de exigencia de sistemas de información esperado por las empresas;
* el acceso a los datos y los documentos de empresa debe hacerse de manera segregada y parametrizable. Los datos están sujetos a la propiedad intelectual;
* la propriedad intelectual tiene valor para justificar los desarrollos y su acceso y uso no pueden ser completamente libres;
* la desintermediación abre nuevas oportunidades de negocio que no se habían aprovechado hasta el momento, porque eran demasiado costosas para justificar mejorar los procesos entre empresas;
* las empresas ya tienen un sistema de información y no planean crear uno nuevo de sustitución.

En una cantidad muy pequeña de empresas ha vuelto a salir la necesidad para volver a desarrollar tecnologías que compitan con las blockchain públicas.

Las blockchains de consorcio forman parte de las blockchains denominadas «permisionadas». Permiten poner las empresas en red. Más concretamente, toman todo su sentido en el contexto de una necesidad de intercambio de datos automatizado entre varias empresas que evolucionan en un ecosistema. Los datos intercambiados necesitan tener una lógica de certificación. El ecosistema necesita intercambiar informaciones con algunos miembros, pero no con otros, en función de normas parametrizables. Al final, los datos intercambiados no sustituyen los sistemas de información existentes, sino que los completan o los crean cuando todavía no existen.

La blockchain también permite ser agnóstico respecto a los sistemas de datos de origen y los procesos internos. La figura que aparece aquí debajo representa este planteamiento.

Diagrama

Descripción generada automáticamente

*Blockchain de consorcio, comparte de datos útiles, pero no los procesos internos*

En la práctica, el paradigma de desarrollo es tan diferente de las blockchains públicas que es perjudicial clasificar estas tecnologías bajo el mismo nombre. El acceso a la blockchain está sujeto a una delegación de acceso por parte de terceros de confianza en las empresas y las soluciones disponibles son personalizables a voluntad en función de los proveedores de las tecnologías.

Esta hipermodularidad exige una especialización de los profesionales a menudo procedentes de las actividades del dato. Entonces, lanzar un proyecto de blockchain permisionada es potencialmente más largo, o demanda más esfuerzo con antelación. La reutilización de código no es tan evidente como podría serlo en una blockchain pública. Los datos siguen en la ubicación de los poseedores del mismo. Se pueden gestionar derechos de acceso a los datos o bien volver a copiar una parte del conjunto del dato para facilitar el trabajo del ecosistema. La lógica de blockchain de consorcio no sustituye a los sistemas de información existentes, sino que se implanta por encima. En el caso de que un socio no tenga sistema de información, es posible utilizar la tecnología para crear uno en común. En caso de que un socio desaparezca, es posible conservar los elementos requeridos en la blockchain para estudios futuros.

Como contrapartida de esta gran flexibilidad, se espera un gran rigor en la realización del ecosistema. No se trata de un *data lake*. Por lo tanto, los datos que entran en el canal de la blockchain deben corresponder a un grado de calidad elevado, con un esfuerzo de normalización con antelación. Resulta un dato utilizable con más facilidad a posteriori para poner en práctica un proceso de ecosistema. Este último está ausente en una gran cantidad de casos concretos. Usar una certificación del dato, en un proceso normalizado y parametrizable, hace desaparecer las zonas grises y tiene la finalidad de resolver las problemáticas de búsqueda repetitiva de información.

Por lo tanto, la gobernanza es una dimensión especialmente importante, presentada con más detalle en un apartado específico.

Actualmente, las tecnologías más avanzadas parecen ser Hyperledger Fabric, Corda y Quorum. En menor medida, se puede considerar MultiChain. Cada una de ellas tiene propiedades únicas. Observación importante: Hyperledger es una marca paraguas. Reagrupa productos muy distintos como IROHA, BURROW, SAWTOOTH, INDY, etc. Por ejemplo, IROHA es una blockchain que tiene la finalidad de proporcionar una solución para las aplicaciones móviles. Actualmente, está sujeta a una cierta cantidad de debilidades en la parte de seguridad informática.

Hyperledger Fabric es una solución que permite hacer intercambios entre varios actores. Originalmente, el intercambio de datos se hacía mediante el intermediario de *channels*. Estos últimos son similares a subredes blockchain, donde cada una lleva sus propios smart contracts y data models. Cuando una información transita por estas subredes, todos los actores tienen acceso al dato y una copia en propiedad. Por el contrario, esta aproximación al formato de difusión de información puede saturar la red con rapidez. También, según la experiencia, más de ocho o nueve canales en un ecosistema pueden hacer que la red blockchain se desplome. Esta observación, en cambio, es muy variable según las elecciones de arquitectura. Una multiplicidad demasiado fuerte de los canales añade problemas de rendimiento y costes de mantenimiento prohibitivos. Cuando un actor nuevo debe integrarse en este *channel*, hay que romper y volver a construir completamente la blockchain. Teniendo en cuenta estas limitaciones, los desarrolladores han creado un planteamiento denominado *SideB*. Entonces, la lógica de pool se transforma en intercambios entre pares, cada actor dispone de una copia del dato.

Los SideB se pueden utilizar para gestionar la confidencialidad en una misma subred, mientras que los canales permiten poner en red un conjunto de actores en torno a un caso de uso particular. Las herramientas de supervisión son escasas y demandarán desarrollos adicionales.

Corda, por el contrario, no dispone de esta lógica de pool. Todos los intercambios se realizan entre pares. Añadir un actor nuevo es un elemento sencillo de configuración. Las lógicas de intercambios jerárquicos a nivel pueden parametrizarse sin tener que realizar desarrollos nuevos. Así es posible aumentar la cantidad de actores con mucha rapidez. La transparencia mencionada en un planteamiento blockchain se sacrifica en beneficio de un aumento muy importante de la discreción. En una misma red, se pueden ocultar actores, lo que hace que la tecnología sea muy interesante para las actividades bancarias, por ejemplo. No se habla de blockchain, sino más bien de DLT (*Distributed Ledger Technology*, Tecnología de Libro Mayor Distribuido). En efecto, como todos los intercambios se hacen entre pares, no es necesario un algoritmo de consenso que valide la legitimidad de un dato. Finalmente, no hay histórico de los intercambios como se podía observar en Hyperledger Fabric. Solo se conserva el último dato. Esto tiene la ventaja de reducir las necesidades de construcción de registro y por lo tanto de almacenamiento, a cambio de una complejidad importante si hay que reconstituir un registro. Las herramientas de supervisión son inexistentes y demandarán desarrollos.

Quorum es un tercer candidato. De hecho, se trata de una versión privada y mejorada del protocolo Ethereum, revisitado por la banca JP Morgan. Se puede ocultar el contenido de una transacción. El algoritmo de este consenso se modifica en provecho de RAFT y BFT a elegir en el momento de la instalación. La etapa de entrada en producción es muy laboriosa. Actualmente no hay una solución empaquetada, lo que significa que un desarrollador debe hacer un trabajo de preparación importante. La actualización de versión y la verificación de las dependencias entre los componentes de Quorum son muy repetitivas. Hoy en día, las herramientas de supervisión para garantizar que la blockchain funciona también son muy escasas y el mantenimiento realmente fastidioso. Persisten bugs especialmente problemáticos, como por ejemplo un sello de tiempo incorrecto en una transacción. La banca planea muy seriamente gestionar esta actividad como una empresa tercera y la situación podría evolucionar mucho durante los próximos años.

En definitiva, el paradigma en la base de los desarrollos de esta tecnología es tan diferente que todo el desarrollo y el despliegue subyacente están en contradicción con la lógica de blockchain pública. Las blockchains denominadas privadas siguen la lógica de blockchain comprometida por las blockchains de consorcio.

### c. Blockchain privada

Las blockchains privadas también forman parte de la familia de las blockchains permisionadas. Su campo de aplicación es comparable al de las blockchains de consorcio. La diferencia reside en el perímetro de aplicación. En teoría, toda la tecnología blockchain es susceptible de crear una blockchain privada. Un informático, por ejemplo, puede utilizar el código del protocolo Ethereum, hacerlo funcionar en una máquina aislada de la red internet y hacer funcionar la blockchain.

Las blockchains privadas tienen un uso muy limitado. Su primer caso de uso es la formación de los profesionales, con la finalidad principal de probar su comprensión de los funcionamientos y de los pruebas de penetración con fines de seguridad.

Todas las proposiciones de valor que se aportarían en la creación de una blockchain privada en una organización única parecen ser sistemáticamente reemplazables por planteamientos tradicionales. Más complicado: la validez de las transacciones es el valor absoluto de la confianza que se tiene en la red. Si solo hay un solo actor, el proceso de creación de confianza se realiza a nivel de una pequeña cantidad de agentes validadores. La confianza se pierde con bastante rapidez por motivos simplemente técnicos, porque los mecanismos de acuerdo son posibles. La piedra angular no parece ser la transparencia o el compromiso, sino el acuerdo de las partes tomadoras en torno a un proceso común de ecosistema.

El hecho de que el conjunto de las herramientas estén empaquetadas en un conjunto coherente que responde a las necesidades de las empresas crea valor. Por eso el valor de las blockchains públicas del tipo navaja suiza no es probablemente el mejor planteamiento. Si el tamaño del ecosistema es muy importante, el proceso de convergencia en la creación de un proceso de ecosistema podría no ser suficientemente rápido para justificar la creación de valor.

En contraposición, el planteamiento blockchain de consorcio parece responder a la necesidad de coordinación de los esfuerzos entre agentes económicos distintos, y al principio tiene un impacto débil en los procesos internos. Al final, la tecnología puramente privada busca resolver problemas internos con una herramienta diseñada de momento para resolver problemas de interacciones externas. Por eso su uso tiene una legitimidad relativa.

La elección del tipo de tecnología, permisionada o no permisionada, da derecho a una cantidad limitada de protocolos de consenso.

## **2. Elección del consenso**

Las tecnologías del tipo Distributed Ledger Technologies (DLT) consisten en compartir un archivo entre varios actores. Idealmente, debería ser completamente equivalente a la red, y no corrompido. Eso implica que es necesario tener un mecanismo de consenso y de protección contra el fraude o la manipulación. Desde hace cincuenta años, los informáticos buscan crear una red protegida y resistente a la censura. El consenso se ocupa de este mecanismo de garantía de calidad, y la operación es sumamente costosa.

El objetivo de este apartado es presentar los algoritmos de consenso que se encuentran más habitualmente en la esfera blockchain. Algunos son relativamente accesibles, mientras que otros, más avanzados, utilizan literalmente conceptos de física cuántica aplicada.

Al principio, describimos los consensos principales e implantados hasta la fecha, y opcionalmente consensos más exóticos, pero que podrían llegar a ser más importantes en el futuro. Se han seleccionado unos cuantos de la treintena existente.

### a. Proof of Work o Prueba de trabajo

A menudo presentada bajo el acrónimo PoW (Proof of Work), la Prueba por el trabajo es la forma más conocida de los consensos, porque es la primera que existió con la llegada de Bitcoin.

El concepto de la prueba por el trabajo consiste en romper un puzle matemático. Se ha encriptado un mensaje, llamado el secreto, y hay que encontrar una clave para desencriptarlo, denominada clave de descifrado.

Esta clave es única y, una vez encontrada, no se puede reutilizar para otro puzle.

Problema: actualmente no hay ningún medio algorítmico que permita encontrar la clave de manera eficaz, gracias a la propiedad denominada asimétrica del puzle.

Por lo tanto, con ayuda del método de fuerza bruta, se van a aplicar combinaciones muy numerosas a una función de descifrado. En la práctica, eso significa que se va a elegir una cadena de caracteres aleatoria de X caracteres alfanuméricos una gran cantidad de veces para encontrar la solución. Una vez encontrada la solución, se descifra el mensaje y se detiene la prueba por el trabajo.

Aplicado al bitcoin, el protocolo que utiliza la prueba por el trabajo ofrece bitcoins *ex nihilo* (de la nada) en recompensa por haber encontrado el resultado. Esto crea así una motivación para pasar al siguiente problema. Los agentes que realizan estos cálculos se denominan mineros. Si no hay transacción, los mineros pierden dinero. Si no hay minero, no se validan las transacciones. Durante el pico de septiembre de 2018, la validación de una transacción podía durar cuatro días en lugar de los diez minutos habituales. Por lo tanto, este protocolo necesita dos agentes con intereses estrictamente divergentes. Los unos quieren un coste de transacción nulo, mientras que los otros quieren que sea lo más alto posible. Cuantas más transacciones hay, más interesante es encontrar estas soluciones. Esta actividad se llama el minado. Por el contrario, cuantos más mineros hay menos rentable es la actividad. Para protegerse de este efecto y aumentar la rentabilidad, se crean agrupaciones gigantescas de servidores especializados en el minado, que se denominan granjas de minado.

¿Qué prueba esto? Nada sobre la transacción en sí misma. Sin embargo, se ha empleado tanta energía para romper un código, que la información asociada al código forzosamente debe ser exacta.

Entonces, el problema está en el riesgo de manipulación de los mensajes validados. Si una persona dispone de más del 50 % de la potencia de cálculo, entonces es susceptible de trucar los mensajes validados, porque dispone de la mayoría de los órganos de validación.

Es el temor de todo actor que hace transacciones en esta red.

Para observar quién valida las transacciones, el sitio blockchain.com ofrece un análisis gráfico de los principales actores que miman, como se muestra en la figura siguiente.

Gráfico, Gráfico circular

Descripción generada automáticamente

*Reparto del porcentaje de hash por actor el 15 de mayo de 2019 en las últimas 24 horas. Fuente: (Luxembourg, 2019)*

La resolución de los puzles es aleatoria. Sin embargo, las proporciones son consistentes a lo largo de varios días, valor absoluto de una potencia de cálculo estable por granja. Nosotros hemos añadido la nacionalidad de las granjas más importantes. Entre las más importantes se encuentran BTC.com, F2Pool o incluso AntPool. Estas granjas parecen ser mayoritariamente chinas. Si añadimos los rendimientos de las granjas chinas seleccionadas, obtenemos un 62,4 % de índice de resolución de los puzles. Se puede percibir un riesgo geopolítico, porque la red Bitcoin representa 143 000 millones de dólares (127 000 millones de euros).

El riesgo geopolítico percibido por la comunidad de los usuarios de la red blockchain no parece estar más enturbiado por la situación. Como prueba, el sitio coinmaketcap.com indica que el volumen de transacciones durante las últimas 24 horas era de 32 480 millones de dólares (28 970 millones de euros).

Esto se contradice con lo que se había observado hasta mediados de 2017, donde se sobrepasó el 51 % durante ocho minutos, y las granjas chinas habían reducido bruscamente su potencia de cálculo.

En el caso contrario, temían que los usuarios de la red Bitcoin no la abandonaran, por falta de confianza.

Además de la barrera del 51 %, regularmente se señala el consumo eléctrico de la prueba por trabajo. El puzle más pequeño permite validar un bloque. Cuando hay pocos agentes de validación, los mineros deben resolver un problema en un tiempo limitado. Utilizado en el protocolo Bitcoin, son diez minutos. Si el problema tiene más de diez minutos, la dificultad del puzle se reduce de manera dinámica. En caso contrario, se aumenta, para asegurarse de que un agente que tiene una potencia de cálculo muy importante no se atribuya todas las validaciones de transacciones. Por eso, al principio, el coste energético era aceptable. Actualmente, a escala planetaria, la situación es muy distinta. En 2019, la validación de un bloque demanda una energía de 450 kWh (Digiconomist, 2019). En un año, eso representa el 13 % del consumo energético total de Francia, o el 90 % de la República Checa.

Última etapa, la transferencia de los bloques validados a través de la red. Una vez resuelto el puzle, se comunica al conjunto de los actores de manera metódica. Cuando la red está poco extendida, la transferencia se hace virtualmente en unos minutos. En el marco actual de globalización del minado, se necesitan ocho meses para que todos los actores de la red tengan una base común. Mientras esperan esta convergencia, se forman muchas ramas en la red. Entonces no hay una blockchain, sino una ramificación importante hasta la convergencia. Por lo tanto, si un lote de transacciones se valida correctamente en menos de diez minutos, en cambio, la comunidad entera no lo tiene hasta pasados muchos meses.

La prueba de capacidad (PoC) o prueba de espacio es una alternativa a la prueba de trabajo (PoW). Este mecanismo de consenso apareció en respuesta al problema de consumo de energía prohibitivo de la prueba de trabajo implementada en el Bitcoin.

Esta alternativa utiliza la capacidad de almacenamiento en lugar de la capacidad de minado del actor encargado de la validación de la transacción. En la práctica, en lugar de romper un puzle matemático que, junto con su trabajo, tiene por objetivo modificar frenéticamente una cadena de caracteres con una solución denominada *nonce*, la PoC almacena una lista de soluciones posibles en el disco duro del agente de validación antes incluso de que comience la actividad de minado.

Cuanto más importante es su capacidad de almacenamiento, más alta es la probabilidad de que encuentre una solución.

En resumen, la prueba por el trabajo valida una información mediante el intermediario de la resolución de un puzle matemático. Como requiere un gran esfuerzo, la información contenida forzosamente debe ser correcta. A pequeña escala, este proceso no plantea ningún problema. Durante el paso a una escala mayor, el coste del cálculo es cada vez más elevado para garantizar la convergencia de las informaciones intercambiadas de manera descentralizada y evitar la corrupción de los datos.

La finalidad no es criticar el protocolo Bitcoin. Sin embargo, cuando una blockchain alcanza un tamaño mundial, las limitaciones técnicas se vuelven muy fuertes. Por eso se han diseñado otros protocolos, como la prueba de participación, o *proof of stake* en inglés.

### b. Prueba de participación o Proof of Stake

El paradigma de la prueba de participación, o *proof of stake* (acrónimo PoS), es completamente distinto. En vez de minar, el protocolo le pide a un usuario de la red que demuestre la posesión de un objeto que servirá de métrica para validar una transacción, por ejemplo de criptomoneda.

El mecanismo de validación es notablemente más sencillo. En cuanto es necesario validar una transacción, el protocolo elige los actores que más méritos tienen, basándose en los tokens que tienen almacenados. Cuantos más tienen, más probabilidades hay de que sean seleccionados para validar las próximas transacciones. El valor de los tokens que tiene un validador se basa principalmente en la confianza de los usuarios de la red. Por eso, le interesa validar transacciones no fraudulentas. En caso contrario, la masa de criptomoneda que posee disminuirá. En último término, la riqueza que posee reside en la confianza que le otorgan los actores.

Así, cuando se ha realizado un volumen suficientemente importante de transacciones, el protocolo les pide a los propietarios de nudos de validación demostrar que tienen muchos tokens. Entre los que tienen más méritos, algunos actores elegidos aleatoriamente van a validar las transacciones en un período limitado.

Este planteamiento está muy cercano a la plutocracia, los actores más ricos se hacen todavía más ricos. Para retrasar este efecto, se han propuesto muchos planteamientos. El más ampliamente adoptado consiste en dar una duración limitada a la validez de un token. De esta manera, un token solo se tiene en cuenta cuando ha pasado un mes sin haberse desplazado o sin usarlo. PeerCoin ha implementado este algoritmo. Para evitar el hiperacaparamiento, se ha fijado un límite superior de tres meses. Otro planteamiento consiste en otorgar el poder de validación a los nudos que tienen el mayor valor capitalizado y el menor valor de hash. Dicho de otra manera, los nudos que han tenido muy pocas transacciones. BlackCoin utiliza este mecanismo. Un segundo planteamiento consiste en permitir que las transacciones sean validadas por nudos que tienen la mayor velocidad de hash. Implícitamente, es un planteamiento para favorecer la fluidez de la red eligiendo a los mejores. ReddCoin utiliza este planteamiento. Una última posibilidad consiste en invitar a una centena de actores que forman parte de los mejores acaparadores a votar por el nudo de su elección. No es forzosamente necesario que este nudo seleccionado forme parte de la centena de elegidos.

Todos estos planteamientos tienen la misión, al menos en teoría, de frenar la barrera de los 51 % que presenta la prueba por trabajo. Sería necesario disponer de una gran cantidad de tokens, en lugar de una cantidad muy grande de potencia de cálculo. Además, en lugar de esperar varios minutos y gastar centenares de kilovatios por hora, el proceso es casi instantáneo y consume poca energía. Además, contrariamente a la prueba de trabajo, no es necesario vender la criptomoneda para pagar los servidores en funcionamiento. Muy al contrario, cuanta más criptomoneda conserve, más rentable será para el actor conservarla en la red. El riesgo de conversión a papel moneda (p. ej.: euro o dólar) se reduce de manera simétrica. Al final, en contraposición al bitcoin, que es una moneda inflacionista (pierde valor en función del tiempo), los tokens en la base de este protocolo son deflacionistas. La masa monetaria se crea al inicio del proceso. Se recompensa a los mineros bajo la forma de gastos de transacción.

A pesar de estas ventajas importantes, el proceso tiene algunos inconvenientes. Se recrean centros de almacenamiento de tokens, y se destruye mecánicamente la lógica descentralizada. Además, el nivel de seguridad aportado por la prueba de participación no puede estructuralmente tener un nivel tan elevado como la prueba por trabajo. La explicación es técnica, aunque necesaria.

En el caso de la prueba por trabajo, el actor debe elegir entre dos cadenas de bloques, una sobre la que tiene más posibilidades de encontrar una solución. De manera predeterminada, se le invita a tomar la cadena más larga, porque se trata la que le ha demandado más esfuerzo. Si elige calcular las dos ramas, divide su potencia de cálculo entre dos. El voto para un bloque tiene un coste importante.

En el caso de la prueba de participación (Proof Of Stake), imaginemos una vez más que estamos frente a dos cadenas de bloques. Votar no cuesta nada. La estrategia óptima consiste en no elegir una rama, sino en votar por cada una de ellas, con una probabilidad de validar un bloque en al menos una de las cadenas. Desde luego, la finalidad es captar la recompensa asociada al proceso de validación. El problema viene del hecho que se puede validar transacciones de un lado y no validarlas del otro, porque se puede haber identificado un gasto doble en un segundo nudo, por ejemplo. Entonces, el proceso de consenso nunca puede tener éxito. Para protegerse, se han propuesto varios mecanismos. Uno de los más sencillos consiste en crear puntos de etapa, o checkpoints. Nudos validadores creados por el equipo de desarrollo decretan que una versión concreta es correcta y válida hasta una etapa determinada. Se trata de una proposición de la red PeerCoin. Luego, la red ha extendido suficientemente y se tiende a alcanzar la convergencia. Otras soluciones consisten en reorganizar la cadena de bloques en la red por frecuencia de bloques. Por ejemplo, la solución Nxt utiliza este planteamiento reorganizando los bloques de su blockchain cada 721 bloques. El último planteamiento, recomendado en la red Ethereum, se llama Casper. Se realiza un planteamiento prueba por trabajo en la cima de una serie de bloques procedente del proceso por prueba de participaciones. Así, en lugar de validar bloque por bloque, se valida conjunto de bloques por conjunto de bloques. La seguridad de la red se mantiene, pero el consumo energético se reduce, por el momento.

En este tipo de protocolo se conocen varios ataques. Es posible corromper el proceso de elección aleatorio en su favor. Este ataque se denomina *Grinding*. Igualmente es posible validar todas las transacciones que están sometidas al nudo. La cadena más larga no es necesariamente la más segura. En efecto, como no hay coste asociado al proceso de validación, al contrario que con el bitcoin, todas las transacciones pueden ser validadas. De hecho, se trata de una estrategia óptima para recibir el máximo de tokens como recompensa por el proceso de validación. Es el problema del ataque *Nothing-at-stake* o Nada en juego.

Al final, puede haber entendimiento entre socios, que hacen circular grandes cantidades de tokens por una determinada cantidad de nudos de validación y así optimizan su rendimiento colectivo. Es el ataque denominado circular, o *Circularity attack*.

Una variante de la prueba de participación (*Proof of Stake*) es la prueba de participación por delegación.

### c. Prueba de participación por delegación o Delegated Proof of Stake

La prueba de participación por delegación utiliza el acrónimo DPoS. Se trata de un refinamiento del modelo propuesto por la prueba de participación. Esta última invita inevitablemente a una concentración de los activos en la base de proceso de validación. Entonces la lógica de descentralización puede perder su valor. Por eso, en lugar de los actores que poseen muchos tokens, los actores elegidos van a validar las transacciones. Estos validadores se eligen en función de un número de votos obtenido. Este número de votos se calcula en función de los tokens en posesión del elector.

Imaginemos dos nudos A y B que proponen validar transacciones. A y B van a proponer una gama de servicios. Por ejemplo, una velocidad de hash especialmente elevada. Los nudos que poseen muchos nudos van a votar por A o B. Imaginemos que el nudo C dispone de 10 tokens, D de 100 tokens y E de 100 tokens. Si C vota por A y los dos otros votan por B, entonces B gana el proceso de voto por 110 contra 100. Además tendrá la posibilidad de validar transacciones durante un corto período, hasta las próximas elecciones. Este planteamiento permite que el protocolo abandone el estatuto de plutocracia y entre en la era de la democracia censitaria.

Mediante este planteamiento, los actores más potentes son menos susceptibles de ser atacados: no validan nada. Además, los nudos menos congestionados y los más eficaces tienden a ser validadores. El mecanismo de pago de los validadores puede ser inflacionista (se generan tokens al realizar la validación) o deflacionista (el autor de la transacción paga gastos, y todos los tokens se crean en el lanzamiento de la red). Entre estos dos extremos, se pueden generar muchas variantes.

En cuanto a rendimiento, se podría dudar de la eficacia del proceso de voto y de validación de las transacciones. El sitio blocktivity.info rastrea la cantidad de transacciones operadas en varias redes. La figura siguiente detalla la actividad en las diez redes de mayor rendimiento en materia de tratamiento de las transacciones.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

*Clasificación de blockchains por cantidad de transacciones realizadas el 20 de mayo de 2019*

La columna *Activity* rastrea la cantidad de transacciones durante las últimas 24 horas. La columna *Average* realiza una media por día durante los últimos siete días. La tercera columna, *Record*, presenta el pico de transacciones generadas. La columna *MarketCap* retoma la valoración del conjunto de tokens en circulación. La columna AVI (*activity valuation index*) es un índice que representa la relación entre la capitalización del bitcoin y la cantidad de transacciones del período en la red Bitcoin. Este índice está unido al valor de base 1.

En una segunda parte, este índice se compara con el rendimiento de otras blockchain, siempre sobre la base capitalización frente a cantidad de transacciones asumidas. Este índice crece para una blockchain dada cuando la cantidad de transacciones aumenta o el valor del token disminuye, o el efecto combinado. Cuando más elevado es, más se percibe una blockchain como rentable para un inversor o un usuario, porque se realiza una cantidad de operaciones mayor para una misma cantidad de dinero invertido. La columna CUI (*Capacity Utilization Index*) representa la diferencia entre la capacidad de la red y su uso.

A la derecha hemos añadido una nota indicando si se trata de un mecanismo DPoS o no. Se observa que, en las diez redes más eficaces, EOS, BTS, STEEM y WAX utilizan el mecanismo de prueba de participación delegada. EOS, por ejemplo, consigue una puntuación de 16 millones de transacciones validadas de media por día, muy por delante de la red Bitcoin y su millón de transacciones. Esto representa el manejo de más de 10 000 transacciones por minuto. En la práctica, la red EOS maneja más del 60 % de las transacciones realizadas en las redes utilizando la tecnología blockchain, pero solo representa un 4 % de la capitalización de las blockchains.

También se observa en la columna CUI que el bitcoin está a plena capacidad, allí donde las redes como Steem, EOS o BTS tienen una puntuación inferior al 20 %. La red blockchain de TRX utiliza un protocolo denominado TPoS (*Trustless Proof of Stake*), una variante de DPoS. Por lo tanto, el planteamiento de la prueba de participación por delegación está presente cuatro veces en las cinco primeras blockchains con una velocidad suficientemente importante como para autorizar aplicaciones verdaderas en funcionamiento en producción.

Por último, las mismas debilidades observadas en la prueba de participación vuelven a aparecer en la prueba de participación por delegación. Al querer optimizar el proceso de validación, el planteamiento ha permitido reducir la cantidad necesaria de actores para mantenerlo. A cambio, es mucho más fácil de atacar y para corromper la red se necesitan menos del 50 % de los tokens. Por lo tanto, no es necesario tener una gran cantidad de actores para hacer funcionar el mecanismo DPoS, se vuelve mucho más robusto con el crecimiento de la cantidad de actores de tipo validadores. Segundo problema importante: los actores que ya son ricos pueden serlo más.

Como poseen el derecho a voto, cuantos más recursos tienen más pueden influir en la blockchain. Último punto problemático, los validadores o los grandes propietarios pueden formar cárteles de influencia. Esto tiene el efecto de reducir el aspecto descentralizado del planteamiento concentrando el esfuerzo de validación en una cantidad limitada de validadores. Peor, usando el ataque circular, no solo se hacen más ricos, sino que pueden hacer validar transacciones ilegítimas.

Todos estos elementos ya se han observado muchas veces en ciencias sociales. Así hay que apostar fuerte por que estas situaciones pueden implantarse rápidamente en las esferas blockchain. La innovación sigue siendo necesaria para hacer que el proceso de validación sea más resistente y justo.

### d. BFT, PBFT y dBFT: los protocolos bizantinos tolerantes a fallos

Para explicar estos protocolos es necesario presentar el problema de los generales bizantinos. En teoría de la informática, se trata de una metáfora para tratar problemas de fiabilidad de la información y de la integridad de los interlocutores.

En la antigüedad, varias armadas diseminadas alrededor de una ciudad deben coordinarse para lanzar el ataque. Para ello, los generales deben utilizar mensajeros. El mensajero es un traidor en potencia (el autor del mensaje o el medio que transporta el mensaje). La cuestión es encontrar el algoritmo que permita a los generales leales ponerse de acuerdo sobre un plan de batalla.

En su forma más sencilla, consideramos nueve generales que deben decidir un ataque coordinado o una retirada. Una mayoría de los generales debe ponerse de acuerdo, porque un ataque con una fracción de las fuerzas causaría una derrota. El problema se complica si al menos uno de los generales no es sincero y envía un mensaje de retirada a un primer subgrupo de cuatro generales, y un mensaje de ataque a un segundo. Por último, la distancia entre los generales obliga a utilizar medios especiales para transmitir los mensajes que pueden no llegar nunca su destino o corromperse por el camino.

Aplicado al mundo de la informática, el general es un nudo, y el mensajero representa la comunicación electrónica entre los servidores. No se puede resolver el problema con una clave criptográfica, porque una debilidad técnica (p. eje.: red lenta o tensión baja durante del cifrado del mensaje) puede enviar un mensaje correcto a un nudo, pero un mensaje mal formado en el momento del envío a un segundo nudo. De lo que se deriva una imposibilidad de alcanzar un consenso entre los actores.

Vamos a llamar n a la cantidad de servidores defectuosos o malintencionados. Matemáticamente, se ha demostrado qué sería necesario que al menos un tercio de los mensajes estuvieran corrompidos para cuestionar el mensaje. Reformulado, esto significa que, para que una red sea fiable, es necesario que haya al menos (3n + 1) nudos operativos. Además, sea cual sea la solución técnica para responder al problema de los generales bizantinos, debe responder a esta imposición. Igualmente, para la prueba por trabajo, cuantos más nudos hay más resistente es la red, porque se hace muy difícil alcanzar la proporción de un tercio de los malintencionados.

El protocolo PBFT se realiza por turnos, también llamados vistas. Estos turnos se descomponen en cuatro partes.

* Un cliente envía una solicitud al nudo principal o líder para invocar un servicio.
* El nudo líder retransmite la solicitud a los nudos de back-up.
* Estos últimos ejecutan la solicitud y luego la reenvían al cliente.
* El cliente espera f+1 respuestas de los distintos nudos con la misma respuesta, donde f representa la cantidad de nudos potencial máxima renegados o defectuosos.

El nudo líder se puede cambiar en cada vista. También se puede sustituir durante una operación sí el envío de los datos a los nudos no tiene lugar durante una ventana de tiempo definida. También es posible que una supermayoría de nudos determinen si un nudo libre es defectuoso y lo sustituyan por el líder siguiente en la fila.

El consenso *Delegated Byzantine Fault Tolerance* (dBFT) es una variante que fusiona el planteamiento proof of stake con pBFT (*practical byzantine fault tolerance*, tolerancia práctica de fallos bizantinos). La idea general es la siguiente.

El conjunto de los usuarios elige nudos, denominados *bookkeepers*. Su función es añadir bloques nuevos al registro. Cada uno de estos nudos propone un bloque por turnos, y este se añade al registro cuando al menos el 66 % de los otros *bookkeepers* lo valida.

Las etapas que permiten encontrar un consenso mediante Delegated Byzantine Fault Tolerance pueden resumirse como se describe a continuación.

* Un cliente envía una solicitud a la red blockchain utilizando este protocolo bajo la forma de un mensaje. Todavía no es un bloque.
* El conjunto de los usuarios de la blockchain vota para designar nudos de manera individual, que tienen la función de añadir bloques nuevos al registro. Estos nudos delegados se denominan nudos de consenso o *bookkeepers*. Este grupo de nudos elegidos se actualiza periódicamente. El voto se pondera según la cantidad de criptomoneda poseída. Cuantas más criptomonedas posee el usuario, más peso tiene su voto. Un refinamiento podría consistir en una cuantificación única estandarizada que represente el rendimiento del servidor.
* Uno de los *bookkeepers* se selecciona aleatoriamente para enviar un bloque. Este nudo se llama *speaker*. Los *bookkeepers* se convierten en *speakers* por turnos al azar.
* El *speaker* recibe la solicitud enviada por el cliente en la primera etapa. Está operación está esperando a ser inscrita en el registro. El *speaker* verifica las firmas electrónicas que identifican al emisor de la transacción, su validez, luego las reúne en un bloque.
* El *speaker* envía su bloque a todos los *bookkeepers*.
* Los *bookkeepers* verifican el bloque para evitar que la transacción sea inválida, las firmas electrónicas incorrectas, etc., y por consiguiente la validan.
* El consenso se alcanza cuando al menos un 66 % de los *bookkeepers* votan por el bloque. Entonces se añade a la blockchain.
* Por último, periódicamente se designa un *speaker* nuevo de manera aleatoria y el proceso vuelve a empezar en la etapa 1.

El objetivo de estos mecanismos es hacer verificaciones cruzadas entre nudos de confianza. Este planteamiento también tiene la ventaja de que solo una comunidad restringida de actores soporta la carga de la validación.

Las blockchains Neo y Tezos usan este mecanismo.

Existen muchas otras variantes, como el *federated byzantine agreement* usado en Stellar. Sin embargo, se aplican los mismos mecanismos y tienen la misma finalidad: proteger la red, hacer converger las transacciones válidas y realizar estas operaciones con un nivel de servicio elevado.

En contrapartida, este planteamiento aúna los defectos de los dos enfoques anteriormente mencionados. Otro protocolo, denominado RAFT, es una variante aplicada para resolver el problema de los generales bizantinos.

### e. RAFT

RAFT es un algoritmo de consenso tolerante a los fallos (p. ej.: caídas) en un contexto distribuido. Se trata de una variante de los algoritmos de la familia PAXOS. Garantiza que en caso de fallo, el sistema siempre es capaz de gestionar las solicitudes que se le envía. Este algoritmo parte del principio de que las informaciones que circulan en la red son fiables y los interlocutores íntegros. Por lo tanto, no es posible aplicarlo en un contexto de blockchain pública, sino solo en las blockchains permisionadas (blockchains privadas).

Hyperledger Fabric o incluso Quorum, por ejemplo, utilizan este algoritmo. Parten del principio de que para acceder a la red, ya se han hecho una determinada cantidad de controles con una gestión estricta de la seguridad anticipada. Los certificados digitales se ocupan de la seguridad «funcional», mientras que RAFT se ocupa de la seguridad «técnica» como las caídas de sistemas, la pérdida de conexión a la red informática, los retrasos en el envío de información, etc.

En la práctica, este mecanismo de consenso es mucho más accesible que la prueba de participación o la prueba por trabajo. Al principio, los nudos de la red, llamados candidatos, van a elegir a un líder. El proceso de emisión de voto es parametrizable y puede consistir en la actuación de un nudo para tratar una información, por ejemplo. Una vez elegido el líder, todos los candidatos se convierten en seguidores, o *followers* en inglés. Cada vez que un usuario del sistema emite una solicitud en la red, se redirige de manera sistemática hacia el líder. Éste procede a la solicitud (p. ej.: escribir una compra de producto nueva en una base de datos) de forma transitoria.

Esto significa que valida y que se dispone a escribir cualquier cosa en la base de datos, y transmite esta información a todos los seguidores de la red.

Estos últimos reenvían una respuesta al líder para decir que han recibido el mensaje correctamente. Entonces y solo entonces se escribe la transacción en la base.

En el caso de Hyperledger Fabric, el proceso de voto se desarrolla en un componente conceptual denominado OSN (*Ordering Service Node*). Este componente tomará todas las transacciones y las pondrá en orden. Ordenar las transacciones es un problema técnico y no de la fecha o de la hora. Así, cada transacción emitida en la red tiene un lugar dedicado en el registro. Este planteamiento se denomina determinista y difiere de Bitcoin o de Ethereum, donde la posición de un bloque corresponde al ámbito de las probabilidades.

Este protocolo es muy distinto de los algoritmos anteriores de consenso que ya hemos mencionado. No valida realmente una transacción. En cambio, se asegura de que una información se ha comunicado correctamente a los distintos miembros de la red, y de que el emisor del mensaje se ha identificado correctamente mediante el intermediario de firmas criptográficas. En un contexto empresarial, con frecuencia es ampliamente suficiente. La red está fuertemente protegida con anterioridad y los actores son conocidos de antemano mediante otros procedimientos como el intercambio de certificados digitales.

Sin embargo, el protocolo es fundamental porque ofrece una resistencia que no ofrece una base de datos centralizada compartida entre actores. También es muy eficiente energéticamente. El minado no es necesario. El proceso de validación de las transacciones no es probabilista. Tercer punto de importancia, no es necesario garantizar la fiabilidad del emisor de la información. Denominamos n a la cantidad de nudos en la red. Los protocolos BFT (*Byzantine Fault Tolerant*), que se ocupan de este aspecto de la seguridad, habitualmente necesitan (3n + 1) nudos para garantizar que son fiables las informaciones que circulan por la red. RAFT solo pide (2n+1). Por lo tanto, los componentes técnicos necesarios para garantizar la fiabilidad de la red son notoriamente menos numerosos, menos costosos y consumen menos energía que cualquier otra solución.

En contrapartida de las ventajas mencionadas, este algoritmo padece una gran cantidad de debilidades. No se puede aplicar en un contexto de blockchain pública. Es fácil que la información que transmite por la red proceda de una fuente dudosa. Por ejemplo, para un actor de la red es suficiente con tener acceso al sistema de seguridad aguas arriba (p. ej.: el certificado digital) para otorgarse derechos sobre la red y pasar transacciones fraudulentas.

El proceso de voto también se puede alterar utilizando el mismo fallo.

En función de la implementación del protocolo, un actor puede aumentar su peso de manera artificial creando nudos ilegítimos en la red y validar transacciones que normalmente no deberían validarse.

Otro algoritmo: el DAG, o *Direct Acyclic Graph*, es una solución puesta en práctica en las tecnologías de registro distribuido.

### f. Directed acyclic graph, Tangle y Hashgraph

Algunas tecnologías están repartidas en la categoría de las blockchains, pero no comparten los fundamentos tecnológicos, siempre buscando resolver el mismo problema de validación y de certificación que una transacción en un contexto distribuido.

*Tangle* es una innovación tecnológica que forma parte de esta familia de registro distribuido. Su objetivo es hacer posible un intercambio de información seguro en el ámbito del IoT (Internet de las cosas) con gastos de transacción inexistentes. La segunda parte consiste en no hacer que un nudo en particular asegure el proceso de validación, sino que lo hagan todos los actores de la red. Esto impone una presión muy fuerte sobre la potencia de cálculo y de almacenamiento de los actores, porque el mundo del IoT no es comparable de ninguna manera a una granja de servidores.

En un principio, Tangle se basa en un gráfico acíclico dirigido. En matemáticas, hay un campo de estudio que se denomina la teoría de los gráficos. Se busca representar una red de manera abstracta. Un DAG es un gráfico particular que permite ir de un extremo a otro de una red sin poder volver atrás. La figura siguiente representa este tipo de gráfico. En a se observa que se puede navegar hacia b, c y e, pero nunca volver hacia atrás. Algunas etapas también son inaccesibles de manera directa.

Diagrama

Descripción generada automáticamente

*Representación de un gráfico acíclico dirigido*

En el ámbito del tangle, los elementos en cada nudo del gráfico son transacciones. Las flechas representan el sentido gráfico, así como el vínculo entre dos transacciones.

En el tangle, el proceso general es el siguiente:

* Un cliente envía una transacción. Este cliente puede ser un humano, una máquina o un objeto conectado, por ejemplo.
* La transacción se envía a la red. El protocolo del tangle se encarga de encontrar dos transacciones que todavía no han sido validadas, llamadas tips. Esta etapa se llama la selección del tip. Matemáticamente, la operación se realiza con ayuda del método MCMC que significa Método de Monte-Carlo por cadena de Markov.
* Se hace un paquete con la transacción en curso y las dos transacciones que todavía no han sido validadas. El paquete se llama un bundle. Las dos transacciones no validadas todavía se llaman padres.
* Se realiza un cálculo para validar las transacciones padres, pero no la transacción en curso. El cálculo es la prueba por trabajo. Esta etapa es necesaria para evitar los spams o los ataques Sybil (falsa identidad).
* Después, la transacción en curso es susceptible de ser validada como se describe en las etapas 3 y 4. Así, la transacción en curso será validada una vez que el protocolo la haya adosado como padre de una transacción nueva. Todavía no está completamente validada.

La figura que aparece aquí debajo muestra un esquema del recorrido de validación de una transacción. Vamos a fijarnos en el bloque con el número 5. Para poder ser candidato al proceso de validación, se debe crear un lote con las transacciones 2 y 3. Una vez realizado el cálculo de prueba por trabajo, se validan las transacciones 2 y 3. La transacción 6 podrá seleccionar la 5 en el siguiente proceso de validación.

Diagrama

Descripción generada automáticamente con confianza media

*Representación del proceso de validación y de ponderación en el tangle*

Cada transacción tiene un incremento. En la figura de arriba, empieza con un 0. Cuando hay una validación, se añaden los incrementos para formar un incremento nuevo. Así, en el bloque marcado con el número 5, se trata de la suma de los incrementos de los bloques 2 y 3. De hecho, cuanto más elevada es la cifra y más necesidad de trabajo tiene la rama, en el sentido prueba de trabajo, entonces se considera más segura que otra rama con una cifra menor.

La prueba por trabajo se ha reforzado con una lógica de firma mediante clave privada/clave pública más restrictiva que en la red Bitcoin, por ejemplo. Una clave privada solo puede firmar un único bundle. Por eso, el protocolo obliga a utilizar la firma de Winternitz, o el esquema *Winternitz one-time signature* (W-OTS) en inglés.

Sin embargo, hay una excepción en el uso de esta firma: los coordinadores. Hasta ahora, la red se autovalida. Entonces surge un problema importante. Si un actor en la red tiene suficiente potencia de cálculo, puede atacar la red sin grandes dificultades: los otros miembros de la red son IoTs. Por eso se necesita una potencia de cálculo más importante para proteger la red. Los coordinadores la protegen imponiendo hitos, denominados *milestones*. Verifican cada una de las firmas a intervalos regulares para evitar un posible efecto de doble gasto, y firman estos hitos.

Entonces son los únicos elementos de la red que pueden firmar varias transacciones. También tienen una segunda función de convergencia de las transacciones. Su mecanismo de funcionamiento es exactamente el mismo que en un mecanismo de prueba de participación por delegación.

Los milestones son fundamentales para garantizar la validez de las transacciones. Pero plantean algunos problemas. El primero reside en su propiedad. De hecho, son propiedad de la fundación IOTA, y su código fuente está oculto a la comunidad. La cantidad de transacciones que pueden validar los coordinadores está limitada por la definición estructural de las firmas digitales. Hay un proyecto en estudio para separarse de estas limitaciones técnicas. Además, sea cual sea la configuración de la red, con o sin coordinador, se puede atacar al igual que las redes por prueba de participación delegada. Así, por ejemplo, un tercio de la potencia de cálculo total es suficiente para poner la red en peligro.

No obstante, la red es muy prometedora, porque cada vez hay más actores y el proceso de validación es más rápido, en contraste con las tecnologías blockchains explicadas hasta este momento. Igualmente permite enviar transacciones sin gastos a través de una red. En efecto, no hay ninguna separación de funciones y tampoco de intereses en el proceso de validación. Desde luego consume energía, pero en otra proporción completamente distinta a la de las redes Ethereum o Bitcoin. El causante es la complejidad del puzle matemático enviado a los actores de validación.

Un protocolo similar utiliza los gráficos acíclicos dirigidos. Entre ellos, se puede encontrar el Hashgraph. Más allá del gráfico, el proceso de selección de las transacciones se sustituye por un protocolo denominado gossip-to-gossip, o de chismes en español. Un dato se intercambia entre muchos nudos. Cuanto más se intercambia, más probable es. El proceso de validación se realiza mediante nudos que calculan un algoritmo, que les da derecho a validar una transacción. El funcionamiento de este algoritmo es muy similar al del practical byzantine fault tolerance (pBFT). El protocolo, en cambio, no es de fuente abierta y no está previsto que llegue a serlo. Por su diseño, no puede ser abierto como las redes Bitcoin o Ethereum.

### g. Solo

Solo es el mecanismo más sencillo que se haya visto en un sistema distribuido. Podemos encontrarlo en el sistema Hyperledger Fabric y no está adaptado para una blockchain pública. Publica las transacciones a los nudos a los que está conectado. Este mecanismo no busca alcanzar un consenso. Tampoco resiste a los fallos de los sistemas cómo podría hacerlo RAFT. Localizado en el OSN (*Ordering Service Node*), envía datos, pero no realiza ningún control de la calidad de los nudos. No se puede mejorar. Como recordatorio, el OSN es el órgano de control que puede ordenar las transacciones de la red y garantizar la coherencia del registro.

Algunas PoC y experimentos empiezan con un consenso RAFT configurado por un solo nudo. Si el prototipo funciona y se quiere pasar al siguiente nivel, hay que cambiar la configuración sin tener que reinstalar el OSN. No se recomienda utilizar este algoritmo en condiciones de producción.

Desde finales de 2017 se han lanzado muchas otras tecnologías al mercado que exploran consensos y mecanismo muy distintos. Su aplicación, en cambio, se aleja de lo que convencionalmente se denomina una blockchain. Los protocolos de consenso utilizados tienden a ser muy creativos mientras aligeran algunos parámetros, como la seguridad, a cambio de más velocidad.

En el siguiente apartado, se presenta una serie de algoritmos de consenso. Su descripción es más breve, porque en este apartado ya hemos hablado de elementos controvertidos.

## **3. Coste del consenso**

Históricamente, el consenso es uno de los componentes más difíciles en una blockchain. Como se trata de una tecnología informática, teóricamente es posible intercambiarla por otra bajo petición. En la práctica, el proceso es fastidioso y es importante tener la experiencia necesaria. Por otro lado, cambiar o evolucionar el consenso puede tener repercusiones muy importantes en la validez de las transacciones.

Por eso, a menudo es preferible, como cliente, elegir una tecnología lista para usar, bajo la forma de una solución única. Habitualmente se presentan dos casos  entre una blockchain permisionada y una blockchain no permisionada o pública.

En el caso de las blockchains públicas, una gran cantidad de soluciones se inspiran significativamente en las plataformas Bitcoin y Ethereum, o las reutilizan completamente. Por ejemplo, la tecnología Arianee utiliza la EVM (*Ethereum Virtual Machine*), sobre la que aplica el consenso de prueba de autoridad. Entonces, el coste del consenso se calcula en función de la presión ejercida sobre los servidores en el mundo y del precio de la criptomoneda necesaria para realizar una operación. Veamos un ejemplo, validar una transacción en julio de 2019 consumía de 450 a 530 kWh para la red y aumenta con el tiempo. Considerando que un kWh cuesta entre 0,11 € y 0,17 €, el coste económico y energético de una transacción en la red es prohibitivo. Ethereum está en un tercio del orden de magnitud. Sin embargo, el porcentaje de energía renovable que utiliza el minado es del 28 % (M. Rauchs, 2018). Las nuevas tecnologías basadas en la prueba de participación delegada consumen notablemente menos. Además, si la factura energética es un factor de cálculo importante, entonces es preferible elegir recién llegados.

En el marco de las blockchains permisionadas, en cambio, se observan dos subconjuntos.

El primero consiste en utilizar tecnologías públicas (p. ej.: Ethereum), reformularlas y adaptarlas en un contexto permisionado. Quorum salió de este planteamiento. El consumo energético también monetario es muy variable. Como la mayor parte del tiempo se trata de instancias basadas en tecnologías en la nube (p. ej.: Infrastructure as a Service), la disposición del servidor tiene un coste que depende del proveedor. Los precios de alquiler en un entorno de producción oscilan entre 1000 € impuestos no incluidos por mes hasta el triple, en función de su uso. Un AntMiner S9, el material más habitual, anuncia una potencia de 1375 kWh por 13 Thash/s. En 2018, la red Bitcoin demandaba 45 millones de terahashs por segundo. En una red privada, incluso teniendo en cuenta el tamaño, las cifras serían desproporcionadas.

El segundo subconjunto consiste en crear tecnologías muy distintas desde el inicio. Es el caso típico de la iniciativa Hyperledger, que reagrupa más de una decena de implementaciones distintas. En esta familia numerosa que agrupa a los más conocidos como Fabric o Sawtooth, el cálculo se vuelve complicado enseguida. Concretamente, el cálculo se hace en dos etapas: un nudo por clientes o grupo de clientes por un lado, y el cálculo del servicio que se ocupa del consenso por otro lado. Hyperledger Fabric, por ejemplo, propone el consenso RAFT o utilizar una herramienta llamada Kfka para garantizar la seguridad de la red, transferir los mensajes y alcanzar un consenso. En una red de diez actores, considerando que un servidor de producción cuesta 1000 € impuestos no incluidos, esto nos da bases a 10 000 € impuestos no incluidos, a los que hay que añadir la duplicación, si se quiere una disponibilidad alta. Entonces, el precio total es de 120 000 a 240 000 € impuestos no incluidos. A este coste hay que añadir el ONS. Su cantidad se calcula como 2f+1, donde f es la probabilidad de fallo. Para simplificar, consideraremos que necesitamos tres nudos en la ONS para funcionar adecuadamente. Si se utiliza una sola máquina con una virtualización, se obtiene un coste anual de 252 000 € impuestos no incluidos. El consumo anual media de un servidor es de 1500 € kWh/año (G. Souffran, 2015). Las máquinas virtuales son muy variables, pero consumen una media de 75 kWh/año. Si queremos ser conservadores, podemos decidir que la ONS utiliza íntegramente los recursos del servidor. Entonces se obtiene un consumo eléctrico anual de entre 15,3 MWh y 16,5 MWh.

Sea cual sea la elección del consenso, es muy importante preguntarse por la viabilidad del mismo. Todos los meses se publican muchos algoritmos con una veracidad matemática no confirmada. Por ejemplo, se ha cuestionado el algoritmo utilizado por la tecnología IOTA, y su veracidad matemática se cuestionó en sus comienzos. Por otro lado, la implementación no siempre se alinea con la teoría.

Ahora que conocemos el coste de un consenso, podemos estudiar la lógica del token o criptomoneda.

## **4. Elección del token o criptomoneda**

La criptomoneda o token ha sufrido muchas modificaciones durante la última década. El token en sí mismo ha sido objeto de numerosas modificaciones y debates, frecuentemente en el plano legal. Hablaremos de este tema más adelante.

El caso de uso permite definir el token si se considera necesario.

El token, originalmente, es un elemento que permite hacer una transferencia de valor entre dos actores. Las plataformas de cambio se cargan después de hacer una conversión entre la criptomoneda y el contravalor en una divisa fiat (p. ej.: euro o dólar). Este fue el primer tipo de uso del que se sacó provecho y lo hizo sobre todo la tecnología Bitcoin (BTC). Con este protocolo el anonimato no es absoluto. Se puede asociar una dirección IP y luego una dirección física a un pseudónimo utilizado en la red tras un esfuerzo de investigación importante. Para protegerse un poco más, los propietarios de activos que quieren conservar su anonimato, han surgido otras divisas como Monedero (XMR). El protocolo hace que los mensajes de transferencia de activos reboten en muchos servidores, así dificultan más el proceso de búsqueda.

Siguiendo en el segmento de las transacciones, algunas criptomonedas se han especializado en la transferencia transfronteriza. Por ejemplo, el Ripple (XRP) se posiciona en las transacciones entre dos organismos financieros. Su caso de uso está especialmente adaptado a los tratamientos entre divisas poco líquidas o sometidas a prohibiciones de salida del territorio, como el baht tailandés. Sin embargo, esta solución tiene un factor de centralización nada despreciable incluso en la actualidad.

Otras criptomonedas se posicionan en los micropagos, como Stellar o IOTA. Muchísimas tecnologías intentan penetrar en este mercado por los nichos, amenazando así incluso la hegemonía de las divisas convencionales y una parte no despreciable de las actividades de los bancos minoristas o de inversión. IOTA, por ejemplo, se posiciona en los micropagos entre máquinas, ya que, por construcción, una transacción no tiene ningún coste.

Todas las iniciativas citadas experimentan un fenómeno: la fluctuación, a veces muy importante. De esta constatación nacieron las «Stable coins». Su definición así como su implementación pueden variar de un proyecto a otro. La idea es proponer sistemáticamente una divisa criptográfica ofreciendo un mecanismo de estabilización. Hay tres tipos:

* garantía fiat;
* garantizado;
* no garantizado.

La garantía fiat asegura que una divisa tiene un valor mínimo garantizado en divisa fiat (p. ej.: euro o dólar). La garantizada significa que hay un activo criptográfico o real que sostiene el valor del token en curso. Eso permite al comprador, en teoría, tener un valor residual garantizado en caso de caída del mercado. Sin embargo, sabiendo que las criptomonedas están muy estrechamente correlacionadas, a menudo esta característica tiene una utilidad discutible. El tercero es no garantizado. Un smart contract garantiza una estabilidad del precio introduciendo o retirando tokens del mercando en función de la oferta y de la demanda, para garantizar una estabilidad relativa del curso. Este mecanismo es bastante cercano al de un banco central.

Algunas iniciativas proponen ofrecer tokens a los que ya tienen. Es el caso por ejemplo de tezos. En el caso de esta blockchain, el protocolo de validación exige que los nudos validadores posean una gran cantidad de tokens, lo que implica un proceso de hiperacaparamiento. Haciendo esto, el mecanismo aporta intereses, igual que un activo financiero. Entonces se convierte en el tema de interés de las autoridades financieras (p. ej.: AMF y SEC) y exige potenciales declaraciones costosas que pueden tener un impacto desfavorable en el proyecto.

Siguiendo en el segmento del intercambio de valores, algunos valores proponen una parte fungible y una parte no fungible. Un activo fungible es un elemento que se puede intercambiar por otro de igual naturaleza y valor. Un billete de 10 euros es fungible y se puede sustituir por otro billete de 10 euros o 10 monedas de 1 euro, por ejemplo. Un activo no fungible sería, por ejemplo, un apartamento. En la red Ethereum, un activo desarrollado con el estándar abierto ERC-721 permite crear un activo digital único.

Así se puede dividir un inmueble en sublotes y venderlos por unidades, reduciendo significativamente los gastos administrativos y de cálculo de propiedad. En junio de 2019, en París, una empresa emergente puso en marcha una iniciativa similar con valor legal.

Algunas blockchains asocian a los tokens derechos de voto o incluso participaciones en los beneficios de la empresa. Otras, todavía más innovadoras, proponen utilizar estos tokens para disfrutar de servicios con un coste menor. Es principalmente el caso del Binance Coin (BNB), que propone gastos de transacciones muy reducidos si se compran o venden criptoactivos con esta criptodivisa. Mediante este mecanismo, la empresa china tiene el poder de posicionarse como divisa de primer nivel: la plataforma es una de las más importantes, con un intercambio mensual de 2000 millones de dólares. Algunos suponen que esta cifra está muy manipulada. Por ejemplo, cualquier introducción en la plataforma requiere que la empresa que desea aparecer en la misma haga transacciones con esta divisa.

Con la creación de tokens utilitarios tiende a emerger un uso relacionado. Estos tokens, por naturaleza, no producen ningún derecho de voto o de participación en los beneficios de la empresa. En compensación, permiten utilizar las capacidades de la red. Así, la apuesta de estas sociedades es utilizar estos tokens como un derecho de acceso. La red Neurochain propone utilizar estos tokens para alimentar robots independientes especializados en inteligencia artificial y aprendizaje automático. La distinción entre el token utilitario y la criptomoneda es fundamentalmente psicológica. El objetivo es alejarse de la dimensión especulativa, dar una utilidad a la criptomoneda y quizás también cambiar la situación fiscal de estas posesiones.

Para finalizar, el token no es fundamental en el funcionamiento de todas las blockchains. Por el contrario, es el medio que ha permitido un impulso de innovación sin precedentes que no puede resumirse con la especulación. La última década ha permitido ver emerger modelos de negocios muy innovadores cuestionando el *statu quo* sobre la transferencia de valor y de propiedad. La mayoría de las veces, la elección del token se resume en la elección de la criptomoneda más adaptada a la lógica de transferencia de valor, de coste de transacción, pero también de visibilidad de los intercambios.

## **5. Elección de visibilidad de los intercambios**

La elección de la visibilidad de los intercambios y del contenido de los datos intercambiados condiciona la elección de la tecnología. Una elección que durante mucho tiempo se ha limitado a la elección entre una blockchain permisionada o una no permisionada.

Los contextos de producción en la empresa tienden a exigir poder:

* permitir a determinadas entidades (p. ej.: empresa) encontrar la identidad física de una persona;
* permitir ocultar intercambios entre dos actores, pero revelárselos a otros.

Mientras que, las blockchains públicas tienden a no revelar la identidad de las personas y hacer pública la información fundamental de las operaciones.

Por eso, cuando hay datos confidenciales e intercambios que no son activos de valor (p. ej.: criptomoneda), las blockchains permisionadas se utilizan de manera casi sistemática. Las soluciones Hyperledger, Quorum, IOTA tienen una versión privada y Hashgraph también la tendrá próximamente.

Algunas excepciones vienen a mitigar esta situación. Los protocolos IPFS y FileCoin proponen compartir un archivo de manera descentralizada con una capa de protección de los archivos almacenados mediante un cifrado. Las capacidades técnicas son modestas, y todavía no parecen estar al nivel de una solución en la nube clásica en el plano del rendimiento. El coste, en cambio, es cinco veces menor, incluso gratuito. Más allá de la transferencia de archivos, IOTA propone un módulo experimental denominado MAM (*masked authenticated messaging*). La idea es permitir a un objeto conectado, de cualquier potencia, acceder a un flujo de datos encriptados. Los primeros experimentos funcionan.

En general, debido a su estructura, las blockchains públicas todavía no permiten intercambiar información de manera eficaz. Muchos intentos consisten en depositar documentos de manera descentralizada, y luego utilizar una solución en la nube para acceder a archivos por región o en todo el mundo.

Estas soluciones híbridas son objeto de numerosas patentes, la mayoría en los Estados Unidos.

En resumen, el intercambio de datos privados o confidenciales tiende a ser del dominio de las instancias permisionadas, aunque la frontera con las blockchains no permisionadas se reduce con los años. Este tipo de mutación profunda inicia la cuestión del alcance legal de la blockchain, los smart contracts y los documentos que pasan por ella.

# Los principales proveedores de tecnología Blockchain

Los proyectos de soluciones técnicas de empresas de software son muy numerosos. Algunos se han estructurado con prestaciones completas, desde la puesta a disposición de servidores hasta el consejo funcional. En el siguiente apartado, damos una visión de los principales proveedores con una distinción entre los grandes grupos y las empresas emergentes.

## **1. Las grandes empresas de software**

Actualmente, las grandes empresas de software como Microsoft e IBM proponen distintas opciones para acceder al entorno Blockchain. Una cosa está clara: estas empresas han invertido mucha energía y muchos medios para no perder el tren de blockchain.

Microsoft utiliza su plataforma Azure para proponer un entorno de desarrollo destinado la creación de aplicaciones basadas en la Blockchain Ethereum y en los smart contracts propuestos por resta última. Microsoft trabaja con socios para acelerar su posicionamiento y su visibilidad en el tema. Marley Gray, el director de la estrategia tecnológica de Microsoft explica: «Nosotros queremos, y francamente, nuestros clientes quieren poder acceder a cualquier Blockchain. Puede ser la de dos personas en un garaje que han hecho un fork de Bitcoin con una idea genial que la gente quiere probar. Nosotros no queremos levantar ninguna barrera. Estamos abiertos a todos. Incluso ayudamos a los más pequeños a subirse a bordo.»

IBM, por su parte, apuesta por su plataforma Bluemix, pero también por Docker. Con la tecnología Blockchain y su estructura para desplegar una red blockchain protegida, IBM busca favorecer la adopción de la tecnología a partir de los servicios ofrecidos en su PaaS Bluemix y para aplicaciones que también podrán desplegarse en su nube a partir de contenedores Docker. IBM anuncia nuevos productos con frecuencia. Hace hincapié en la facilidad de desarrollo mediante el Cloud IBM. El objetivo es llegar a proponer BaaS (*Blockchain as a Service*).

Siempre participando activamente en el proyecto Hyperledger, una iniciativa de código abierto con el objetivo de hacer evolucionar la tecnología Blockchain, Big Blue también va a proponer su propia versión de blockchain con un nivel de seguridad muy alto que permita responder a las elevadas expectativas del sector bancario.

Pero también se estudian otros terrenos de juego, como la gestión de stock o la sanidad. IBM trabaja en la evolución de blockchain, para reforzar su seguridad y aumentar las posibilidades de conexión, principalmente con los objetos conectados. La finalidad es conectar blockchain a nuevos tipos de captadores inteligentes (objetos conectados, vehículos, etc.). Blockchain tiene un interés claro en conectar estos captadores con los smart contracts.

Desde nuestro punto de vista, las grandes firmas estadounidenses no quieren perderse el giro de blockchain. Las inversiones son importantes para marcar una visibilidad elevada en el tema. Queda por ver qué saldrá de la convivencia entre el código abierto y el de pago, dos mundos opuestos, sabiendo que el ejercicio ya se ha llevado a cabo en las tecnologías Big Data. Las empresas estadounidenses se ciñen sin ninguna duda a la idea de utilizar blockchain para rentabilizar las inversiones importantes realizadas en las plataformas en la nube. Todo esto es un buen augurio para el futuro de blockchain. Si este tipo de empresas invierten tanto, seguramente es porque ellas también pronostican un futuro prometedor para esta tecnología.

### a. Tecnología y posicionamiento

Caso IBM

En 2015, IBM lanzó una iniciativa con muchos socios, unos 250. Se llamaba Hyperledger y se ha convertido en una marca paraguas que reagrupa muchos proyectos. La figura que aparece aquí debajo muestra de manera esquemática los distintos componentes.

Escala de tiempo

Descripción generada automáticamente

*Ecosistema en torno a Hyperledger. Fuente: Hyperledger*

La familia de productos ya está bien surtida y no para de crecer con rapidez. Las subsecciones siguientes describen las ventajas de la tecnología, sus inconvenientes, así como el ecosistema donde se encuentra Hyperledger.

Ventajas e inconvenientes de la tecnología

Hyperledger no es una tecnología, sino varias. Además, dar crédito a IBM sería deformar la realidad. En efecto, varios grandes actores trabajan activamente en este proyecto paraguas, como Intel, por ejemplo.

Primera ventaja, el proyecto se ubica bajo la fundación Linux con una licencia Apache 2. Esto significa que el código se puede utilizar de manera gratuita. También es posible hacerlo evolucionar y compartir estas evoluciones con la comunidad. Entonces no es necesario pagar una licencia.

Segundo punto fundamental, el proyecto se articula en frameworks, o marcos tecnológicos por un lado, y herramientas listas para usar por el otro. Son frameworks, no herramientas del tipo plug and play. Es necesario un trabajo acorde a estas características para colocar los componentes. A cambio de una hipermodularidad, lo fundamental de los componentes se debe construir y asociar a cada proyecto, además de afinarlo en función de las necesidades. Es posible hacer scripts de automatización de implementación, pero las actualizaciones de versión, por ejemplo, actualmente son muy laboriosas y se gestionan manualmente.

Por lo tanto, se necesita experiencia real para poder instalar, implementar y mantener en condiciones operativas una red en Hyperledger. Esto está claramente en oposición con tecnologías públicas como Ethereum. Hay contenedores listos para su uso, así como soluciones del tipo Blockchain as a Service o Platform as a Service. Se necesitará de manera sistemática un estudio, sobre la parte funcional y la capacidad de crecimiento de carga.

Una parte importante del valor de la tecnología reside en el smart contract, denominado chaincode en el ecosistema Hyperledger. Permite realizar una lógica aplicativa o actividad dentro de la parte back-end, antes de grabarse de manera efectiva en la base de datos. Este se desarrolla sistemáticamente en función de las necesidades y es del orden de la propiedad intelectual del ordenante.

Al contrario que con las tecnologías de blockchains públicas, como Ethereum, no se puede reutilizar código realizado por un tercero desconocido.

Además, a semejanza de otras tecnologías blockchain, poner mucha lógica de actividad en la blockchain tiene impactos importantes en la resiliencia y el rendimiento de la solución. Por lo tanto se recomienda hacer un análisis minucioso entre la automatización realizada en la blockchain y realizada por las capas de aplicaciones, habitualmente la interfaz gráfica y las capas de middleware.

En la actualidad hay seis soluciones principales en Hyperledger: Burrow, Fabric, Grid, Indy, Iroha y Sawtooth.

Burrow aspira a crear un vínculo final entre todas las blockchains. Así, una blockchain Hyperledger podría conectarse a Ethereum, IOTA, Tezos, etc. Para ello, utiliza especialmente una EVM (*Ethereum Virtual Machine*). En la práctica, el proyecto todavía está en desarrollo y su resiliencia es imperfecta.

Fabric es uno de los planteamientos más avanzados. Permite poner en red actores industriales para compartir un conjunto de informaciones privadas, y que no se desea ver intercambiar en una ubicación pública. El sistema es uno de los más avanzados y eficaces, con muchos miles de millones de transacciones por segundo (de dos a tres mil). El algoritmo de consenso se puede modificar. De manera predeterminada, se trata de un algoritmo del tipo practical byzantine fault tolerance (pBFT) llamado RAFT. La seguridad se tiene en cuenta de principio a fin con una gestión de los directorios de empresa. IBM ha invertido más de 200 millones de dólares en costes de desarrollo. Se trata de la solución Hyperledger más utilizada con muchos pasos a producción.

Grid no es una blockchain, sino una tecnología de registro distribuido. El objetivo es resolver una determinada cantidad de problemáticas en el ámbito de la cadena de suministro. Además, se trata más bien de un framework de buenas prácticas y de componentes que una solución que ha llegado a buen puerto. Se ofrecen programas informáticos estándar con modelos de datos apropiados a las necesidades. El proyecto todavía está en fase de incubación y todavía no se puede utilizar.

Indy es una solución de gestión descentralizada de la identidad digital. La herramienta es operativa y al final ofrece un planteamiento similar a googleAdsIDs. El proyecto está en migración y en curso de integración hacia una herramienta llamada Aries. Así, Indy fusionaría con la lógica de las herramientas de gestión más que como solución básica de gestión de la identidad.

Iroha es un proyecto prometedor que consiste en utilizar las capacidades de blockchain mediante los smartphones o aplicaciones de escritorio ligeras. El objetivo de este proyecto es aligerar en gran medida el esfuerzo de instalación de la solución blockchain y proporcionar conjuntos de datos predefinidos. A la larga, el diseñador tendría menos cosas que gestionar y entonces reduciría el plazo de entrega de los prototipos y de entrada en producción. La mayor parte de los recursos de IBM está actualmente en este proyecto. Aunque está disponible, todavía tiene fallos de seguridad y de inestabilidad al usarlo.

Sawtooth es una iniciativa lanzada por Intel. El proyecto es muy versátil y permite considerar muchas problemáticas, objetos conectados a las aplicaciones financieras (p. ej.: gestión documental). Ventaja interesante: se pueden programar smart contracts en la mayoría de los lenguajes principales. Por el contrario, Fabric solo acepta Go y Java para el chaincode. Otra característica diferenciadora: la lógica de actividad está disociada de la capa de consenso. El efecto teórico de esta característica es optimizar el uso de la red. Igualmente, el algoritmo de consenso predeterminado (Proof of Elapsed Time) se puede cambiar. Intel también propone desarrollar el ejercicio hasta el hardware con un encriptado del mensaje desde el nivel del procesador hasta el back-end seleccionado, sawtooth.

Además de estas soluciones, hay una serie de herramientas disponibles. En constante evolución, la mayoría están en su etapa preliminar.

Composer, por ejemplo, tenía el objetivo de permitir el lanzamiento de una blockchain Hyperledger Fabric con ayuda de una interfaz gráfica. El proyecto se abandonó porque el ritmo de desarrollo entre la solución y Explorer estaba demasiado descorrelacionado.

Explorer por el contrario, es una herramienta práctica de supervisión. Con un diseño todavía muy ligero, a cambio permite ver la cantidad de bloques creados en un nudo concreto. Se trata de una primera aproximación tímida a la consola de supervisión.

Es importante recordar que, sea cual sea la solución Hyperledger, ninguna se entrega con una solución de supervisión fácil de usar. La elección parece ser deliberada, porque cada empresa tiende a tener una base de supervisión con su propia política de gestión de registros de actividad y técnicos.

La herramienta Aries permite gestionar la identidad. No es obligatorio, pero promete algunas características muy interesantes como el ZKP (*Zero Knowledge Proof*). Esta propiedad permite garantizar la validez de una información sin revelarla. Así se puede garantizar la identidad de un individuo y su acción sobre un objeto de manera virtual.

Las otras herramientas aún están en una fase muy preliminar, y todavía no permiten una utilización pertinente y eficaz.

Ecosistema

Ante todo, Hyperledger es una fundación que reagrupa a muchos actores. De todas las soluciones, Fabric parece ser la primera versión verdaderamente operacional y aplicable desde las versiones 1.1 y 1.3. Estas versiones se publicaron a principios de 2018.

La fundación se divide en al menos tres categorías: los *premier members*, los *general members* y por último los *associate members & academia*. Hay 18 miembros *premiers*, lo que implica un gasto anual de 250 000 € para garantizar el buen funcionamiento de fundación, del desarrollo informático y el marketing. Incluyendo a todas las instituciones, la fundación cuenta con 272 socios, entre los que se encuentran IBM, Baidu (es decir, el Google chino) o incluso la universidad de Berkeley. Estos miembros se comprometen a utilizar la tecnología, experimentarla y mejorarla o al menos explorarla.

Durante al año 2018, muchos actores propusieron soluciones del tipo Blockchain as a Service (BaaS), Software as a Service (SaaS) o incluso Platform as a Service (PaaS). Oracle, por ejemplo, propone una solución integrada con nudos a menos de 1000 € impuestos no incluidos al mes y un planteamiento casi plug and play. En contrapartida, sustituyen todos los componentes de código abierto por componentes Oracle. SAP, una empresa de software alemana, al igual que Microsoft (Azure), Amazon e IBM, proponen soluciones del tipo BaaS. La tecnología es poco personalizable y el cliente tiene que desarrollar sus propios smart contracts.

Todas estas plataformas se basan fundamentalmente en el código proporcionado en el marco del proyecto Hyperledger Fabric.

La comunidad tiene unos 4000 desarrolladores activos en la esfera Hyperledger. El sitio web stackoverflow permite informar de las dificultades técnicas y registrar una petición de ayuda. Los desarrolladores de Hyperledger son relativamente dinámicos, con una media de plazos de respuesta inferiores a tres días.

Muchos actores ofrecen soluciones de formación a lo largo de varios días, evolucionando de la desmitificación a procesos más exhaustivos orientados al desarrollo. Las tarifas y la calidad del contenido dependen en gran medida de los actores. Por el momento, no parece haber procesos certificados por la fundación o por IBM. Esta situación podría evolucionar con rapidez, porque IBM suele proporcionar formaciones de certificación para las soluciones que propone.

La cantidad de proyectos lanzados en esta tecnología ha aumentado en gran medida entre 2018 y 2019. En París parece haberse superado la barrera de los cien proyectos de la fase PoC a la entrada en producción. En 2019 y sobre la participación en Francia, IBM comunica que hay 35 redes blockchain activas en producción y preproducción que utilizan Hyperledger Fabric. Podemos ver emerger proyectos tan diversificados como la trazabilidad alimentaria o el seguimiento de las formalidades en las secretarías de los tribunales. Parece que la solución técnica va encontrando poco a poco su público.

Este ecosistema dinámico vuelve a encaminar a los desarrolladores de la solución hacia problemáticas de producción y de estabilización técnica. Las próximas líneas de desarrollo que se esperan por cantidad de actores incluyen nociones de big data. En efecto, si la solución es lo suficientemente estable, algunos clientes parecen pedir poder transformar la solución en fuentes de datos comunes, lo que exige conectores hacia bases de datos masivas. Todavía no existen estos conectores.

Último movimiento principal de la empresa: un acercamiento con la tecnología Stellar. En efecto, Hyperledger no tiene token o criptomoneda nativa. Es posible crearla, pero parece relativamente raro. Stellar permite realizar micropagos, dispone de una estabilidad relativa de su cotización, e idealmente se integraría en los componentes de Hyperledger. En la práctica, actualmente no hay ninguna documentación sobre la interfaz.

Igualmente, las discusiones con los equipos comerciales al igual que con los desarrolladores no aportan más informaciones concluyentes.

Observemos ahora la posición de Microsoft en materia de blockchain.

Caso Microsoft

Microsoft es un actor emblemático de la informática desde los años ochenta. La empresa ha evolucionado mucho y se ha posicionado principalmente en la nube, donde ocupa un lugar preferente detrás del gigante Amazon. Microsoft fue uno de los precursores en proponer soluciones de blockchains contenerizadas mediante su solución denominada Azure. Vamos a ver las ventajas de esta solución y su ecosistema.

Ventajas e inconvenientes de la tecnología

Microsoft es un pionero de la implantación de soluciones blockchain en sus soluciones en la nube. Actualmente, la solución permite implantar con algunos clics una de las cuatro soluciones emblemáticas de blockchain:

* Ethereum (Enterprise edition);
* Quorum;
* Corda;
* Hyperledger.

En el plano comercial, la oferta blockchain con Azure parece ser competitiva. Por ejemplo, una oferta propone tener un nudo a partir de 196,50 € al mes con capacidades muy limitadas. Hablamos de un nudo de desarrollo más que de un nudo de producción. Por un nudo de producción, el coste mensual es de unos 650 € por mes y nudo. Si queremos añadir almacenamiento, la gestión de la seguridad y la consola de supervisión, los costes aumentan bastante rápido. Aunque la oferta de marketing ofrece almacenamiento a partir de 5 céntimos, la explotación de un auténtico back-end con una base de datos detrás de la blockchain anula muy rápido la ventaja comparativa.

Las soluciones propuestas bajo Azure tienen la forma de servicios *gestionados*. Esto significa que un desarrollador no se preocupa por la disponibilidad o la resiliencia del back-end de su aplicación. A cambio, no tiene la posibilidad de hacer una configuración con precisión de la aplicación, algo que puede ser problemático en ciertos casos. Más sutil todavía en el caso de Hyperledger, no puede crear "side DBs" con facilidad. Este punto es especialmente delicado, porque actualmente las soluciones más estables parecen utilizar precisamente las "side DBs" y emanciparse de la multiplicación de los canales comunicación dedicados llamados *channels*.

Azure ofrece una ventaja nada despreciable: una consola de supervisión lista para usar, el fruto de casi 18 meses de desarrollo. Lamentablemente, este componente no es nativo de Hyperledger.

Las otras herramientas disponibles no se quedan atrás. Hay herramientas específicas que permiten crear e implementar nudos Ethereum privados, Quorum, Hyperledger o Corda. Algunos permiten gestionar una serie de nudos privados en una misma plataforma. Hay herramientas como Mijin que permiten lanzar entornos de PoCs con unos cuantos clics. El cliente cuenta con el acompañamiento de profesionales para crear su propio token y desarrollar el modelo económico a base de criptomoneda que tendría asociado. La oferta comercial de Mijin también incluye una asistencia para crear seminarios y eventos públicos de comunicados de prensa. El precio es alrededor del doble de lo que vale un acceso sencillo a un servidor gestionado.

Krypcore, una herramienta disponible, es una plataforma que permite lanzar secciones completas de la blockchain Hyperledger Fabric sin escribir ni una línea de código. La herramienta incluye un generador de código que permite crear API sin esfuerzo. Así el desarrollador puede dedicarse sobre todo a la parte chaincode, más que a la parte DevOps. En la práctica, la solución permite ganar tiempo en la implantación de una PoC. Para realizar operaciones más complicadas, se requiere una experiencia real con una reactivación de código en su conjunto.

Finalmente, una última batería de pruebas permite trabajar sobre todo en entornos de pruebas. Así se puede hablar de Truffle: un entorno de desarrollo bajo Ethereum que permite crear canales de activos en un marco de método.

No podemos dejar de mencionar que, desde hace poco, Azure ofrece soluciones para otras blockchains como Syscoin o incluso Ripple. La oferta de la plataforma sigue limitada a lógicas de blockchain permisionadas o controladas, porque los entornos solo tienen una finalidad de formación y de exploración.

Última ventaja comparativa nada despreciable: el aspecto contractual. Muchas grandes empresas ya tienen un contrato comercial con Azure, lo que puede acelerar notablemente el proceso de implementación en una empresa. Todavía más, hacer salir el dato desde una solución en la nube hacia otra tiende a ser muy costoso. También, cuanto más comparten los actores de una red una solución en la nube única, más podría controlarse el impacto sobre los costes de explotación. Sin embargo, esta observación solo es válida si los actores están en el mismo grupo geográfico. En caso contrario se puede ocasionar un sobrecoste.

Ahora vamos a observar el ecosistema puesto a disposición en la esfera Microsoft.

Ecosistema

El ecosistema en torno a la solución de Microsoft es muy interesante. Durante la elección de la blockchain, los componentes off-chain nativos disponibles en Azure se pueden utilizar inmediatamente.

Las herramientas de desarrollo como Visual Studio se pueden poner a nivel importando las bibliotecas necesarias para el desarrollo de aplicaciones en blockchain. El proyecto Xamarin permite hacer desarrollos en Android e iOS. Los componentes técnicos clásicos para hacer canales de datos están disponibles (p. ej.: Azure IoT Hub, Service Bus o Azure event grid). Las capas de BI o de almacenamientos clásicos también se pueden utilizar (p. ej.: Microsoft Power BI, Azure SQL database). Finalmente, solo queda integrar los componentes de blockchain en proyecto para utilizarlos. En general, la gestión de la seguridad es muy clásica, con una configuración de un firewall al inicio del proyecto y el uso de una bóveda de seguridad con clave (p. ej.: Azure key vault). Sin embargo, hay que prestar especial atención a la factura, porque los precios de la solución pueden aumentar con rapidez en función de la elección de los componentes tecnológicos.

Con frecuencia, será necesario hacer operaciones híbridas entre componentes de código abierto y las herramientas puestas a disposición bajo Azure para contener el coste total. Este tipo de elección implica una pérdida del aspecto «llave en mano» y habrá que reservar especialista para gestionar la red y las herramientas que no dejarán de mostrar signos de debilidad durante la vida de la solución de software.

Hay que destacar que trabajar en Ethereum implica trabajar Solidity, o si no Java. En Corda, se potencia el lenguaje Kotlin y luego Java. Para Hyperledger, Go tiene el honor de ser el lenguaje principal, seguido por JavaScript. El proyecto Xamarin no parece abarcar lenguajes tan profundos. Entonces, es probable que un desarrollador deba formarse en lenguajes nuevos para lanzarse a un proyecto blockchain. Además, los desarrolladores, incluso los más experimentados, no siempre conocen las bibliotecas y los conceptos subyacentes. Esto emana de la naturaliza descentralizada de una blockchain. Tener una integración técnica no parece implicar un índice de éxito mayor para un proyecto.

Un cierto número de grandes actores han elegido utilizar los mecanismos de blockchain con Azure. En particular, Starbucks, Insurewave, Xbox o incluso el Nasdaq.

No es cuestión de comprometerse a utilizar una tecnología en particular, como en el caso de IBM, sino utilizar sistemas en producción. Starbucks, por ejemplo, utiliza blockchain para hacer un seguimiento de la procedencia del café en Colombia, Costa Rica y Ruanda. Insurewave utiliza la tecnología en el sector de los seguros de productos en el ámbito del transporte marítimo. Xbox utiliza un sistema de derechos de autor en la cima de la blockchain. Nasdaq utiliza la solución para gestionar la parte contractual de las infraestructuras puestas a disposición de los organismos financieros.

Por el momento, estos usuarios todavía no parecen organizarse entre ellos para realizar observaciones sobre la experiencia, porque los casos de uso aún son muy variados. En cambio, algo así podría hacerse realidad si la tecnología se amplía y se convierte en algo tan habitual como las tecnologías Big Data.

### b. Testimonios

Para proponer una visión completa de la tecnología, parece útil conocer las opiniones de los actores principales del sector. Teniendo en cuenta las limitaciones relacionadas con la redacción de este libro, solo han podido aportar su testimonio IBM y Microsoft.

Se han hecho cuatro preguntas para poder observar el nivel de progreso de sus proyectos, sus ambiciones y las dificultades con las que se encuentran.

Testimonio de IBM

**Ustedes tienen actividad en Blockchain desde hace algunos años: ¿cuáles son las grandes evoluciones que han constatado durante los últimos meses?**

El fuerte aumento de los precios de las principales criptomonedas a finales de 2017, encabezado por el bitcoin, aceleró enormemente la curiosidad público en general y de los responsables de la toma de decisiones de las empresas por blockchain. Esto abrió numerosos debates con empresas e instituciones, alimentados por dudas, comprensión parcial, incluso equivocada, porque es difícil comprender esta tecnología a primera vista, y muy a menudo se confunden los distintos protocolos blockchains, sus características y los casos de uso a los que van dirigidos.

Sobre los usos fuera de las criptomonedas, en las que estamos concentrados, esto ha permitido a los dirigentes percibir los elementos de valor que puede aportar esta tecnología, a corto y a medio plazo. Todavía más, han podido fundamentar fuertes convicciones en cuanto al potencial de Blockchain para su empresa.

Como consecuencia nosotros hemos podido concentrarnos en el acompañamiento de actores influyentes en su sector de actividad para el paso al nivel de redes blockchains, por ejemplo en las finanzas, la logística, la distribución o la energía.

Las familias de los casos de uso son extremadamente variadas: creación de servicios nuevos, optimización de procesos donde participan varias partes, transparencia y valoración de los productos, anticipación y gestión de los riesgos, trazabilidad de las acciones y responsabilidades, etc.

Muchos proyectos en el mercado no han tenido continuación, esto ilustra las aspiraciones y el entusiasmo por Blockchain. Ahora estamos llegando al final de la curva de la innovación de Gartner, lo que nos permite avanzar con serenidad en los proyectos con potencial comprobado. Blockchain todavía es un tema de innovación poco explotado, sin embargo las primeras redes de empresas e instituciones están implantadas desde hace varios meses y sirven de ejemplo para las otras. La diferencia respecto a las otras tecnologías es que Blockchain es una columna vertebral compartida entre varios actores. Colocar los primeros componentes da un impulso nada despreciable para posicionar la tecnología frente a sus prioridades tácticas, incluso estratégicas.

**¿Cómo calificaría su posicionamiento en Blockchain?**

Somos un punto de referencia reconocido en esta tecnología, por nuestra fuerte contribución al consorcio Hyperledger, especialmente en el desarrollo del protocolo Hyperledger Fabric (HLF), uno de los más utilizados en producción, pero igualmente se ha usado en muchos proyectos en el mundo, en Europa y en Francia. IBM también ofrece IBM Blockchain Platform, que corresponde a hacer disponible HLF en un modo PaaS, para acelerar y facilitar los desarrollos de proyectos blockchain.

Desde 2017, nuestra profunda convicción adquirida mediante nuestras observaciones y experiencias, es que el trabajo relacionado con el ecosistema es la piedra angular de todo proyecto blockchain. Porque está lejos de ser evidente que hay que acompañar la creación de una estrategia de equipo en paralelo con intereses individuales (por ejemplo, cuando empresas competidoras participan en el mismo proyecto).

Nosotros hemos desarrollado métodos y nuestros equipos para avanzar en este sentido, y seguimos haciéndolo todos los días para maximizar el índice de transformación de proyectos, de innovación en el cambio de nivel. Por supuesto, la función de socio tecnológico en el desarrollo de las soluciones con nuestros clientes sigue una parte esencial de todo proyecto y una parte fundamental de la actividad de IBM.

Nuestro leitmotiv también es muy claro: deseamos contribuir a identificar, construir, y sobre todo perpetuar los proyectos blockchain en el tiempo. Eso implica un elemento principal que hacemos con nuestros clientes: estar alerta sobre el buen y el mal uso que se hace de esta tecnología para no perder tiempo y dinero.

Testimonio de Microsoft

**¿Cuál es la estrategia de Microsoft respecto a esta tecnología y por qué?**

La estrategia de Microsoft sobre las tecnologías de registro distribuido, o Blockchain, es facilitar su adopción. En efecto, la tecnología Blockchain ha atraído la curiosidad colectiva del mundo comercial y tecnológico desde hace varios meses, incluso años. Sin embargo, esta innovación es distinta de otras. Es más bien un conjunto de tecnologías experimentadas y sabiamente aplicadas para crear los fundamentos del Bitcoin. Sin embargo, cuando esta misma tecnología se ha aplicado a otros casos de uso podría resolver problemas muy antiguos.

Blockchain, o más exactamente un registro distribuido, tiene más bien una función de catalizador para inspirar el cambio en la forma en que las organizaciones y los hombres intercambian bienes. Las transacciones de bienes entre seres humanos o sociedades tanto si son coherentes o a distancia generan costes enormes en el procedimiento y la reagrupación de los registros, «clearing y settlement». Todo esto podría resultar un ejercicio trivial utilizando la tecnología Blockchain.

En resumen, blockchain o las tecnologías antes mencionadas de registro distribuido podrían abastecer la próxima ola de innovación que simplificaría el funcionamiento del mundo de los negocios, de la misma manera que la Web, e iniciar una nueva economía colaborativa.

Para facilitar la adopción, Microsoft anunció la disponibilidad en Azure, su plataforma en la nube de soluciones «Blockchain as a Service», con la primera oferta de la plataforma Ethereum gracias a la experiencia de ConsenSys. Estos entornos han sido muy apreciados por los clientes y los socios porque cuando se deben probar configuraciones de registro distribuido con máquinas que «minan», las plataformas en la nube facilitan todas las problemáticas de disponibilidad de máquinas y reducen la administración.

Ofrecer una plataforma Blockchain en Azure es extremadamente útil para los clientes que desean innovar gracias a las tecnologías blockchain y beneficiarse de un ecosistema de prueba rápido y asequible.

Los clientes pueden evaluar distintas implementaciones y blockchains, probar sus características y construir prototipos de blockchains mucho más rápido.

Además, poner en marcha hackathons o talleres en torno a la blockchain es mucho más fácil y rápido. Por eso, se dedica menos tiempo a instalar infraestructuras y más tiempo a programar.

A nuestros socios también les parece que las infraestructuras en la nube permiten a sus clientes probar su tecnología, proporcionan una retroactividad rápida y permiten responder a las peticiones con más rapidez.

En el marketplace Azure hay muchos «templates» de servicios blockchains, como implementaciones de referencia C++ Ethereum, de Ethereum para Windows Server, configuraciones Ripple, etc.

Todo esto nos ha permitido aprender mucho sobre los principios esenciales de las plataformas distribuidas, sus características y sus capacidades que permitirán a las empresas adoptar la tecnología Blockchain.

Para contribuir a esta evolución tecnológica principal, Microsoft ha introducido el proyecto Bletchley.

El proyecto Bletchley es un planteamiento arquitectónico de Microsoft con el objetivo de facilitar el uso de estas tecnologías nuevas para el ecosistema de las empresas y de los consorcios blockchain. Para ser claros, no es una blockchain nueva. Es el planteamiento de Microsoft para contribuir al uso de plataformas de registro distribuido (blockchain) en las empresas para construir soluciones reales y responder a problemas comerciales reales, siempre conservando las plataformas abiertas.

El proyecto Bletchley aborda temas conocidos desde las primeras pruebas de blockchain, como la apertura de la plataforma, las funciones de identidad, de gestión de las claves, de confidencialidad, de seguridad, de gestión de las operaciones y de interoperabilidad.

En el proyecto Bletchley, Microsoft Azure proporcionó la plataforma Cloud donde se pueden construir y entregar las aplicaciones distribuidas. La disponibilidad de Microsoft Azure en 24 regiones del planeta, sus funciones de nube híbrida, su cartera de certificación, de conformidad ampliada y de seguridad son óptimas para permitir la adopción de la tecnología Blockchain, especialmente en sectores sumamente regulados, como los servicios financieros, la salud para los gobiernos.

Microsoft introdujo los Cryptlets mediante el proyecto Bletchley. Se trata de un bloque de construcción nuevo de la tecnología Blockchain, cuyo objetivo es permitir proteger la interoperabilidad y la comunicación entre Microsoft Azure, los ecosistemas middleware y las tecnologías de los clientes. Los Cryptlets entrarán en funcionamiento cuando sean necesarias informaciones suplementarias para ejecutar una operación o un contrato, por ejemplo: la fecha o la hora. Se convertirán en un elemento fundamental de los sistemas de blockchain, son sofisticados y permitirán a todas las tecnologías trabajar juntas de manera segura y evolutiva. Un poco como los «oráculos», pero diseñando la cadena de seguridad proporcionada en una blockchain.

Estos Cryplets permitirán a las empresas hacer que dos mundos se comuniquen entre sí, el mundo de los registros distribuidos y el mundo de las empresas con sus aplicaciones existentes y heredadas.

Hay muchas probabilidades de que, en el futuro, Microsoft proporcionará cada vez más utilidades para ofrecer un nivel de abstracción al mayor número posible de actores. El objetivo es que todos puedan aprovechar en sus aplicaciones las ventajas de las tecnologías de registro distribuido.

**¿Cuál es su estrategia de integración en la blockchain con los productos Microsoft?**

El ecosistema Blockchain está en constante evolución, al igual que la tecnología servidor, que ha evolucionado de una arquitectura de dos niveles hacia una de tres niveles con la creación de middlewares (J2EE, COM +).

A menudo, la blockchain Bitcoin se denomina Blockchain 1.0. Su arquitectura se presenta en la figura que aparece más abajo. Es una base de datos sencilla que graba las transacciones de manera secuencial como si fuera un proceso contable, y representa el estado de la red en todo momento. Básicamente, es una máquina de «estados» distribuida.

También puede compararse con las primeras bases de datos relacionales donde la integridad del sistema de referencia es su función principal mediante claves primarias y claves foráneas. Entonces estamos de acuerdo en que las plataformas Bitcoin, Hyperledger, Bitcoin Forks o UTXO entran dentro de la Blockchain 1.0.

Diagrama

Descripción generada automáticamente

*Esquema de una Blockchain 1.0*

En el pasado, los sistemas de gestión de bases de datos evolucionaron para incluir una lógica bajo la forma de procedimientos almacenados para ayudar a las operaciones de datos más complejos. De manera similar, muchas soluciones de registros distribuidos han añadido una capa de lógica bajo la forma de smart contracts. Este código existe junto con los datos en la base de datos. Esto puede considerarse como la Blockchain 2.0. Ethereum, Eris y otras forman parte de esta tecnología.

Diagrama

Descripción generada automáticamente

*Esquema de una Blockchain 2.0*

Estos smart contracts son muy prometedores, una de sus posibilidades es crear sistemas inteligentes a base de contratos autónomos para permitir a los procesos operativos funcionar de manera autónoma.

En lo que se ha denominado Blockchain 1.0 y 2.0, si deben interactuar datos externos o eventos basados en condiciones de mercado o de tiempo con una blockchain, necesitamos un oráculo. No hay ningún método estándar para proporcionar datos de oráculo con una seguridad completa, lo que puede convertirse rápidamente en un problema cuando se trata de la gestión de los smart contracts entre varias partes. En general, la llamada del código o de los datos fuera de un smart contract rompe el muro de confianza. Por eso, esto amenaza la autenticidad de las operaciones que dependen de ella. La finalidad de los Cryplets es proporcionar esta funcionalidad.

Los Cryptlets son componentes de código, fuera de las blockchains, que están redactados en todos los lenguajes y se ejecutan dentro de un contenedor protegido y fiable. Este contenedor está comunicado mediante canales protegidos.

Como complemento, los Cryptlets y sus CryptletContainers podrían estar firmados o incluir firmas electrónicas. Imaginemos que un usuario quiere crear un Cryptlet. Le asocia una firma. Cuando se llama a este Cryplet, podemos saber inmediatamente que una serie de acciones se ha efectuado siguiendo órdenes del usuario y en su nombre. El Cryplet garantiza que la ejecución del contrato sigue la voluntad del usuario.

También permite identificar al autor del contenido del Cryplet.

Añadir este tipo de middleware puede considerarse como la «Blockchain 3.0».

Diagrama

Descripción generada automáticamente

*Comparación de las tres versiones de Blockchain*

Este middleware Blockchain proporcionará servicios básicos en la nube, como la gestión de identidades y de operaciones, además de servicios de *business intelligence* y de analítica o de aprendizaje automático.

Estas tecnologías garantizarán que la blockchain proporciona un funcionamiento seguro e inmutable, pero al mismo tiempo ofrecerán una posibilidad de tener en cuenta las normativas existentes.

Recientemente desarrollado, este middleware trabajará a dúo con los servicios *Azure* existentes, como Active Directory, KeyVault y otras tecnologías Blockchain del ecosistema, para ofrecer una plataforma global.

Teniendo en cuenta la importancia del registro, cuando mayor sea la cantidad de participantes más distribuido y más protegido estará. Entonces se hace evidente que los consorcios van a dominar el panorama. Esta circunstancia hace que aparezcan necesidades de interoperabilidad, de administración, de identidad, de gestión de las claves y de un modelo de ejecución mejorado.

Este middleware proporcionaría los siguientes tipos de servicios.

* Identity and Certificate Services: funcionalidades de Active Directory con Azure y KeyVault para ofrecer servicios de PaaS (*Platform as a Service*), para la autentificación, la autorización, la emisión de claves, el almacenamiento, la gestión de los accesos y el ciclo de vida.
* Encryption Services: encriptado parcial, o cifrado a nivel de campos para las transacciones blockchain con distintos esquemas de cifrado (homomórficos, etc.).
* Cryptlet Services: servicios como la ubicación, la validación del fiduciario, los contenedores aislados protegidos, los CryptoDelegates, etc.
* Blockchain Gateway Services: servicios que garantizan la integridad transaccional entre escrituras como la transferencia de instrumentos financieros en una cadena de suministro que se extiende por varias Blockchains-Interledgers.
* Data Services: servicios de datos clave como los sistemas de archivos distribuidos, la auditoría, los análisis avanzados, el Machine Learning y los cuadros de mando.
* Management and Operations: herramientas para el despliegue, la gestión y la explotación de registros distribuidos para consorcios de empresas, aportando a las empresas la madurez que le falta al mercado actual.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

*Esquema del ecosistema Azure con la tecnología Blockchain*

Aunque son comparables a los oráculos, los Cryptlets proporcionarán más seguridad y confianza en un ecosistema evolutivo.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

*Comparación entre Cryplet y Oráculo*

Estos Cryptlets son la respuesta de Microsoft para integrar el mundo de las blockchains y el mundo existente de manera protegida. Evidentemente, la integración con las herramientas existentes de Microsoft forma parte del perímetro de desarrollo.

**Para Microsoft, ¿la plataforma Azure tendrá una función de plataforma de desarrollo o alojará proyectos en producción?**

Los Cryptlets proporcionarán la infraestructura necesaria para desplegar un conjunto de funcionalidades de Blockchain en el middleware como bibliotecas de servicios, entre ellas:

* Blockchain Gateway Services;
* Identity & Key Management;
* Privacy & Encryption;
* Servicios vinculados a los datos (Machine Learning, Analytics and BI Dashboards).

Enseguida comprendemos que las ventajas de las blockchains y de la nube se complementan muy bien.

Sin embargo, parece evidente que, en la lógica de aplicación de soluciones de registros distribuidos, es conveniente que las máquinas estén distribuidas y no concentradas en una nube pública. La nube va a proporcionar ventajas no despreciables para los entornos de desarrollo, la puesta a disposición de entornos y la combinación de la administración. Pero lo hemos entendido bien: las blockchains van a tener que interactuar con el mundo exterior o entre ellas. Por eso, las soluciones en la nube como los Cryplets van a permitir imaginar soluciones robustas que interactúan unas con otras. Entonces es completamente factible utilizar la plataforma Azure para soluciones basadas en blockchains en producción.

**En su opinión, ¿cuáles son los casos de uso más prometedores?**

La promesa de que las blockchains van a revolucionar la manera en que las empresas y los particulares intercambian bienes o comercian en Internet es asombrosa.

Los usos inmediatos de la tecnología Blockchain son muchos. Muchas instituciones bancarias la utilizan para construir soluciones que facilitan las interacciones financieras entre varias partes; ya sea para dar un servicio nuevo que históricamente era demasiado costoso, para implementar nuevos modelos de negocio que originalmente eran demasiado complejo ponerlos en marcha, como los minibonds.

Muchos ven en esta tecnología una fuente de economía de costes combinando los entornos necesarios que cada uno construiría por su lado. Por ejemplo, podemos citar los KYC o la gestión de las relaciones con los proveedores.

Una de las ventajas únicas de las blockchains reside en el hecho que una vez cargados los datos en el registro, no se pueden modificar. Los casos de uso no se limitan de ninguna manera a las finanzas.

Todo el sector de la cadena de suministro también recibirá el impacto. Gracias a los smart contracts, es posible pedir un producto y pagarlo solo a la entrega de una parte, y por otra comprobar que el producto en cuestión corresponde al pedido o está en buen estado.

Este tipo de mejora va a tener un impacto enorme en las tesorerías de todas las empresas.

Las blockchains también van a facilitar el despliegue del Internet de las cosas, como lo demuestran en la actualidad muchas pruebas en torno a las smart grids. Entonces los objetos podrán hacer intercambios entre ellos con total seguridad. Podemos observar un intercambio de kilovatios por euros, por ejemplo. Un coche autónomo podrá recargarse o pagar una plaza de parking mediante una sencilla transacción inmutable que todos podrán auditar, ya sea el fabricante, el propietario o solo el usuario.

Rápidamente nos damos cuenta de que el sector público también puede beneficiarse de este tipo de tecnología. ¿Por qué no imaginar que se hará un historial de la gestión de los presupuestos del Estado en Blockchains? También pensamos en las soluciones de voto electrónico, de validación de presupuesto, de catastro, etc.

Pero lo que puede ser muy útil en algunos casos, también puede crear problemas graves en otros.

¿Qué pasa con el derecho al olvido que se ha garantizado a los europeos (reglamento general de protección de datos) y ampliado para los menores en la ley digital? ¿Qué pasa con la confidencialidad?

Como lo explicaba recientemente Vitalik Buterin, cofundador de Ethereum: «private Blockchains are not a solution to privacy.» (Las blockchains privadas no son una solución al mantenimiento de la vida privada).

Las últimas declaraciones, durante la segunda DevCon en Shanghai en 2016, giraban principalmente en torno a la rapidez de construcción de bloques, de la proof-of-stake y la capacidad de evolución («Because mauve has the most RAM»).

Sin embargo, las reflexiones sobre la confidencialidad de los datos almacenados avanzan. Hay varias líneas de estudio, como la ofuscación indistinguible (*indistinguishability obfuscation* en inglés), la prueba de conocimiento cero (o el *zero-knowledge proof* en inglés) así como los últimos desarrollos entorno a *succinct non-interactive argument of knowlegde* (SNARK).

La finalidad sería permitir a un usuario demostrar su conocimiento de un secreto sin, de hecho, revelar qué es el secreto en cuestión.

Cada vez comprendemos mejor las ventajas de las blockchains para muchos usos públicos o financieros, pero cuando se menciona el almacenamiento de datos de carácter personal, es necesario hacer progresos y estudiar el tema. Sin embargo, soñamos con que las blockchains puedan permitir confiar al 100 % en una aplicación, un programa, incluso confiar más en esta aplicación que en un ser humano, que podría sesgar un sistema para su beneficio personal.

Las aplicaciones existentes, su ecosistema y el potencial de su impacto en los sectores están evidentemente limitados a la inspiración de los innovadores de hoy y de mañana. Si es evidente que la invención del bitcoin era una primera iteración, el advenimiento de los smart contracts parece ser una segunda iteración de la tecnología del registro descentralizado. Sin embargo, hay otra iteración por venir: la de las organizaciones autónomas descentralizadas.

## **2. Las empresas emergentes**

La lógica de blockchain no procede de las grandes empresas, sino de las empresas emergentes. En esta familia se encuentra un impulso prodigioso de innovaciones, en las antípodas de los modelos clásicos de negocio. Hay más de dos mil tecnologías blockchain públicas. En la región de París, ya se han lanzado a la aventura más de doscientas empresas con muchas orientaciones (p. ej.: desarrollo de nuevas tecnologías o integración de soluciones existentes). Otras regiones no se quedan atrás con sectores muy dinámicos en Madrid, Barcelona, Valencia y en el parque tecnológico Walqa (Huesca).

En este apartado hablaremos de las ventajas e inconvenientes, así como de los ecosistemas asociados a iniciativas de blockchain.

### a. Ethereum, Enterprise Ethereum Alliance y Quorum

Ethereum es un proyecto lanzado en 2014 con una primera entrada en producción durante 2015. Luego, el proyecto evolucionó mucho y una parte importante de su código fue reutilizada por empresas emergentes y otros proyectos, que aparte de eso se inspiraron en él en mayor o menor cuantía. La fundación con sede en Suiza se ha enfrentado a ataques muy numerosos, pero hasta ahora han sido derrotados a nivel global. El protocolo no se ha cuestionado, sin embargo, algunas implementaciones han hecho temblar a muchos inversores, especialmente un ataque en 2016 que permitió a los hackers desviar casi 150 millones de dólares.

El proyecto vio la creación dos versiones: una nueva rama Ethereum y una antigua llamada Ethereum classic. La rama nueva ha sido explotada posteriormente en tres categorías:

* Ethereum: forma pública de la blockchain;
* Enterprise Ethereum Alliance: forma permisionada de la blockchain con muchas mejoras específicas para las empresas;
* Quorum: forma permisionada empaquetada por un banco (JPMorgan) de la versión original de Ethereum.

En el siguiente apartado se abordan los tres proyectos relativamente conectados por las ventajas que presenta cada uno de ellos, así como los ecosistemas en los que se encuentran.

Ventajas e inconvenientes de la tecnología

Ethereum es ante todo un protocolo, una criptomoneda y una infraestructura. Este protocolo es una innovación principal que permite crear todo tipo de objetos de manera descentralizada. La tecnología tiene algunas ventajas: le ofrece al desarrollador la posibilidad de programar una lógica de aplicaciones en modo *serverless*. Eso significa que no se pregunta dónde se encuentran los servidores y mucho menos la redundancia. Sin embargo, esta ventaja se ha cuestionado mucho con los últimos planteamientos de la nube. La criptomoneda se utiliza para pagar por el uso, en lugar de un abono como se podía ver en el lanzamiento del proyecto. Pero este planteamiento muy interesante ha mostrado sus límites.

Como desarrollador, no siempre es fácil conocer la cantidad de tokens necesarios para lanzar un cálculo. Una vez más, las soluciones de la nube han tenido en cuenta esta petición, y es posible hacer una estimación del coste antes de lanzar la petición, y sin pasar por una criptomoneda. El riesgo de volatilidad es virtualmente más débil para una nación que utiliza una divisa estable.

Además, el sistema incluye un modelo de implementación y de uso del código desarrollado bajo la forma más sencilla que se pueda imaginar. Por ejemplo, después de la descarga del módulo Parity con unos pocos clics, se añade un wallet, y se puede empezar a programar, para luego desarrollar el código en la blockchain pública. No es necesaria ninguna cadena de build y de scripts más o menos fastidiosa. Sin embargo, es costoso desarrollar código en la blockchain. Para funcionar correctamente, el código desarrollado debe ser de una simplicidad infantil, y los bucles deben usarse con mucha precaución. Retroceder es imposible por naturaleza, pero se puede activar un *kill switch*, que simplemente evita el uso del código. Aunque atención: descargar Parity cuesta poco, pero hacerlo funcionar exige descargar toda la blockchain de Ethereum. Hablamos de muchos gigabytes. Sabiendo que hay que descargar el conjunto de la blockchain Ethereum y que al mismo tiempo esta crece permanentemente, actualmente, se hace muy complicado crear un nudo Ethereum actualizado sin utilizar material de última generación (discos SSD y línea de internet con una velocidad muy buena).

En resumen, el proyecto Ethereum es una maravilla de simplicidad de uso, en teoría. Es tan fácil que la plataforma se ha convertido en el punto estándar de acceso para recaudar fondos mediante una ICO (*Initial Coin Offering*) y luego crear su propia tecnología de blockchain. Igualmente es el punto de entrada de todos los desarrolladores deseosos de sumergirse en la tecnología. Sin embargo, los proyectos se detienen muy rápido y el interés cambia para dirigirse hacia soluciones más robustas.

En efecto, la gestión de la seguridad está en las antípodas de las prácticas empresariales. Una contraseña perdida puede recuperarse con ayuda de una serie de palabras aleatorias cuidadosamente conservadas. Una contraseña comprometida no puede anularse.

El rendimiento de la plataforma no está asegurado. No es factible ningún cambio de escala. Tiene problemas para mantener la carga, tanto que un intercambio de tokens virtuales puso a la plataforma de rodillas durante varios días. No es posible hacer programas complejos. El bucle más pequeño (p. ej.: mirar los elementos de una lista) consume mucho GAS (unidad de consumo que permite evaluar el coste de un cálculo pagado con criptomonedas). Así, la mayoría de los programas se limitan a series de condiciones con objetos muy simples.

La gestión de los aspectos privados es inexistente. El envío de datos más pequeño es prohibitivo. Para proyectarse, hay un campo llamado data, donde se pueden escribir datos para el almacenamiento en la blockchain. Según la cotización del ether (divisa de la plataforma), un gigabyte de datos cuesta cinco millones de euros. A título comparativo, el almacenamiento en una solución de la nube para el mismo volumen de datos oscila entre dos y cinco céntimos de euro.

El canal de código que permite visualizar las versiones de un código es escueto o inexistente. Con frecuencia, un desarrollador necesitará crear un canal de código y para ello tendrá que piratear los módulos, como Parity, estos últimos son víctimas de muchos bugs críticos incapacitantes. Entonces tendrá que probar en una plataforma local con soluciones en la nube antes de enviar el código a la blockchain de manera efectiva. Último punto incapacitante: un desarrollador abandone la propiedad del código. En efecto, Ethereum está bajo licencia GPL. Lo que significa que se puede reutilizar el código de otro de manera gratuita, pero también que se ceden todos los derechos de autor. En cambio, la utilización del código da derechos de uso, bajo la forma de criptomonedas. Un código no utilizado no genera nada.

Último punto letal: el algoritmo de consenso, Ethereum utiliza la prueba de trabajo (Proof Of Work). Desde luego, este algoritmo consume tres veces menos que en la red Bitcoin, porque los recursos disponibles son menos importantes. Sin embargo, en una red comparable, el consumo energético sigue siendo colosal.

En visto de estas problemáticas bien conocidas, y enfrentándose a una disminución crónica de las reservas para financiar el desarrollo de la solución Ethereum, la fundación ha lanzado una nueva iniciativa, llamada Enterprise Ethereum Alliance (EEA). Se trata de una solución de software que ofrece una blockchain en un contexto empresarial.

La gestión de la seguridad es más avanzada, con una integración en el directorio de empresa. El algoritmo de consenso se puede modificar con una facilidad muy relativa. Por ejemplo, se puede utilizar la prueba de autoridad en lugar de la prueba de trabajo. También es posible intercambiar datos privados entre terceros, con una gestión de la confidencialidad que no existe en la versión pública de la blockchain. Sin embargo, el código utilizable es de una gran sencillez. Según el caso, es posible incluir o excluir la lógica de los tokens. En ausencia de tokens, todos los cálculos se hacen con *GAS* igual a cero.

La solución se empaqueta en contenedores, lo que hace el despliegue mucho más rápido que si hubiera que volver a empaquetar todo. Un desarrollador experto que ha practicado en EEA sabe lo fastidioso que es el esfuerzo de hacer su propio lote en Ethereum. Se añaden nuevas capacidades con regularidad, las últimas datan de mayo de 2019. En los hechos destacados de las API (capas que facilitan el acceso al dato) que permiten desplazar las operaciones de cálculo fuera de la blockchain y así aliviar la red. La gestión de la identidad está un poco más estandarizada y se centra más en las lógicas empresariales. Se hace posible comunicarse más fácilmente con otras blockchains. Por último, se ha integrado una capa de gestión de la confidencialidad para responder a una fuerte demanda de los usuarios potenciales.

Al navegar por el git (base de código) del proyecto EEA, se observa una cierta cantidad de bugs redhibitorios como problemas en el sello de tiempo de los bloques enviados a la red o incluso con la firma de los bloques. No obstante, la comunidad es muy activa y solo se puede esperar que la solución se estabilice y se corrija con el tiempo.

Quorum es una solución basada en Ethereum a caballo entre la solución pública y EEA. La iniciativa fue lanzada por los especialistas en blockchain de JP Morgan Chase, un banco de inversión estadounidense. Ofrecen una solución de empresa con componentes técnicos desarrollados internamente. Por ejemplo, la entidad que gestiona Quorum ofrece módulos que permiten ocultar al emisor de una transacción y los importes intercambiados (Allison, 2019). Esta tecnología se presenta como agnóstica de los sectores donde podría aplicarse.

El uso del código es gratuito y está disponible en Internet a cambio de un trabajo de preparación importante (p. ej.: descarga, compilación, containerización).

Hay un entusiasmo que parece gravitar alrededor del proyecto con muchos usos a una escala mínima de la PoC. Hay conversaciones en curso para hacer salir el proyecto de la banca y convertirlo en un derivado del grupo bancario. Las líneas de desarrollo están genuinamente orientadas a las finanzas y al intercambio de valor.

Ecosistema

El ecosistema alrededor de Ethereum parece ser inmenso. Parece que es necesario recordar qué es una comunidad y un ecosistema. Ethereum apareció en 2014 y tiene el primer *mainnet* (red en producción) desde 2015. La cantidad de smart contracts aumenta con mucha rapidez. A mediados de septiembre de 2016 se contabilizaban más de 20 000. A finales de 2018, se habían desarrollado casi 1,7 millones, de los que un poco menos de la tercera parte siguen activos.

Hasta ahora, la tecnología ha permitido validar más de 100 millones de transacciones, y no piensa parar. La comunidad de los desarrolladores es muy activa y constantemente está buscando mejorar los rendimientos y los componentes tecnológicos. Desde hace varios meses, está previsto que el algoritmo de consenso evolucione hacia una prueba de participación y abandone, al menos en parte, la prueba de trabajo.

El ecosistema tiene 250 000 desarrolladores en el mundo. Igualmente se contabilizan 120 000 descargas de la herramienta de desarrollo llamada Truffle, y 80 000 descargas de Ganache, la herramienta de simulación de blockchain (Chriqui, 2019). Todos los años se organizan decenas de reuniones, con no menos de 24 programaciones en Madrid durante 2019. Por último, la fundación lanza hackathons todos los años en muchas ciudades del mundo, entre ellas Londres o Buenos Aires, para explotar la tecnología.

Muchas empresas como Arianne, asentada en Francia, reutilizan los componentes técnicos de Ethereum. Modifican algunos parámetros (p. ej.: el algoritmo de consenso), añaden código desarrollado por ellas y así crean una variante tecnológica con modelos de gobernanza distintos.

Finalmente, una parte importante de las recogidas de fondos se hace mediante el intermediario de programas especiales: ERC20. Estos smart contracts están en la blockchain Ethereum. Entonces, la tecnología se convierte en un pilar de la economía descentralizada, hasta el punto de tener un status especial hasta en la legislación sobre el tema en los Estados Unidos.

Sin embargo, estas cifras ocultan una realidad muy distinta. El sitio de internet StateOfTheDApps inventaría las aplicaciones en la plataforma. Los usos más frecuentes son contratos de tipo ERC20. Recordemos que estos contratos permiten hacer intercambios entre la criptomoneda de Ethereum y otras criptomonedas. Entre las cinco aplicaciones más utilizadas se encuentras los juegos de dados y una ruleta que permiten apostar criptomonedas. En cuanto a la comunidad de sus actores, difícilmente sobrepasa los 3000 usuarios diarios.

Así, hablar de cientos de miles de desarrolladores es una cosa. Verlos contribuir con soluciones que desembocan en producción con un uso masivo es más difícil.

En lo que concierne a la solución Enterprise Ethereum Alliance, es muy difícil evaluar la cantidad de proyectos en curso tanto en la etapa PoC como en producción. Su sitio web informa de una cantidad de miembros importante, con 225 participantes.

No es una sorpresa que allí se encuentren el proyecto Hyperledger y JP Morgan Chase. La participación cruzada tiene el objetivo de hacer converger puntos importantes como la gestión de la identidad, o incluso la posibilidad hacer que las dos tecnologías se comuniquen. Allí también se encuentran algunos nombres importantes como Accenture, el grupo bancario Citi o incluso la universidad de Cambridge. Los otros miembros son menos conocidos que en la esfera Hyperledger.

Los proyectos que utilizan EEA parecen comunicarse poco, aparte de eso todavía son poco comunes. Emergen *playbooks* eventuales para incitar a los desarrolladores a utilizar la tecnología en su contexto, por ejemplo, en la gestión de activos inmobiliarios.

Quorum es un proyecto con una comunidad que también es muy compleja de evaluar. La tecnología no está claramente orientada a las aplicaciones financieras. Los casos de uso encontrados son tan variados como el seguimiento de las vacunaciones, la gestión de los datos de conductores de automóvil o la trazabilidad del café.

Los proyectos Quorum, como EEA, están disponibles en la plataforma en la nube de Azure. Amazon planea proponer soluciones basadas en Ethereum en los próximos meses, pero todavía no es posible saber qué versión se ofrecerá. Es probable que se ofrezcan las dos alternativas de empresa.

Para concluir, Quorum es ligeramente más mayor que EEA, y hasta hace poco demostraba más madurez, especialmente en lo relacionado con la gestión de la identidad y de la confidencialidad. A cambio, la implementación es más laboriosa. Las herramientas de gestión existen, pero siguen siendo escasas. Quorum es una edición aumentada de Ethereum por un buen motivo. Así, todo el código implementado en Quorum es completamente transportable a Ethereum public y viceversa. Es la única versión que tiene esta propiedad. Por el momento, esta ventaja es muy relativa, porque las empresas tienen tendencia a ser reticentes a enviar datos dentro de un entorno abierto.

Otra tecnología, muy distinta, es susceptible de interesar a los desarrolladores en las tecnologías del tipo blockchain: IOTA.

### b. IOTA

IOTA no es una blockchain. De hecho, se trata de un grafo acíclico dirigido. Una transacción se envía a una red para ser validada. El autor de esta transacción primero debe validar dos transacciones antes de ver la suya validada. Dicho de otra manera, el dispositivo que emite una transacción primero debe validar otras dos antes. A priori no hay ningún registro único que permita consultar las transacciones pasadas. Para corregir este problema técnico, la función en el origen del proyecto utiliza un nudo coordinador, que próximamente será sustituido por *permanodos*. Estos últimos tendrían la función principal de grabar el historial de las transacciones.

Una vez efectuado este recordatorio tecnológico, podemos volcarnos en sus ventajas y su ecosistema.

Ventajas e inconvenientes de la tecnología

IOTA está diseñado para permitir un paso de nivel de manera genuina. Cuantos más terminales susceptibles de validar una transacción hay, más rápidamente se valida la citada transacción. Por lo tanto, está en las antípodas de una tecnología blockchain, donde cuantas más transacciones hay para validar, más se atasca el proceso, especialmente en la etapa de creación de un bloque.

Segunda ventaja: la tecnología se puede utilizar sin necesidad de tener recursos desmesurados. En efecto, la necesidad nació de garantizar que un objeto conectado realice bien una operación y posiblemente recoja una contribución bajo la forma de criptomonedas. La tecnología ha podido observarse en la práctica en muchos sectores, especialmente en una fábrica aeronáutica. Una instancia privada del protocolo ha permitido una trazabilidad de las operaciones hasta el tipo de taladradora o destornillador utilizados.

Por último, es eficaz en un contexto de producción. Hay disponible una versión pública con la compra de token. También hay entornos de prueba y la fundación los ha puesto a disposición de los desarrolladores de manera gratuita.

A cambio, se trata a la vez de una tecnología pública y privada. No hay ninguna diferencia entre las dos instancias. El código se puede descargar en Internet, compilarlo y utilizarlos en función de las necesidades. Una cierta cantidad de elementos son parametrizables, especialmente el algoritmo de consenso, que en parte emplea la prueba por trabajo. Sin embargo, el diseño de la herramienta exige un consumo muy bajo.

Las implementaciones privadas son tan frágiles como la seguridad en los comienzos de la versión pública de IOTA, al menos en el lanzamiento de la red. Sin embargo, se trata de una alternativa sólida de protección y de seguimiento de las operaciones en un universo IoT (Internet de las cosas).

Mejorar la capacidad de esta tecnología a menudo causa volver a aprender todo desde el principio. En efecto, la gestión del dato, los protocolos, la lógica de identidad y las bibliotecas son completamente distintas. IOTA no funciona en una máquina virtual Ethereum (EVM). Se trata de un proyecto completamente reescrito, con su propia lógica interna.

Por lo tanto, al igual que con Ethereum o Hyperledger, por ejemplo, hacen falta seis meses para (volver a) formar un desarrollador en la tecnología.

No parece que exista una solución IOTA lista para usar, como podríamos encontrar un Hyperledger Fabric o un Quorum en un entorno en la nube. La documentación es tan abundante como para las plataformas blockchain emblemáticas. Así que es posible lanzarse en un PoC con bastante rapidez.

No parece que existan todavía herramientas de gestión y de supervisión. Probablemente habrá que crearlas.

Por último, la continuidad de la solución no parece estar en peligro. En efecto, la fundación dispone de capitales importantes asociados a su recogida de fondos y a la valoración de la cotización de la criptomoneda.

Ecosistema

El ecosistema es muy activo, pero está a la altura de la reputación del proyecto. En efecto, se estima que la comunidad tiene entre 2500 y 3000 desarrolladores activos, de los que un poco más de 80 se dedican exclusivamente a la mejora de la solución técnica. Las redes sociales como Discord y Reddit tienen 27 000 y más de 100 000 miembros respectivamente. La gran mayoría de esta comunidad de interesados no son desarrolladores.

Existen muchos tutoriales y tratan numerosos campos, especialmente en el sector de las smart cities y de las transacciones entre máquinas. Se calcula que un poco más de 200 proyectos habrían visto la luz, pero no se sabe en qué etapa están (IOTA, 2019). Estas cifras, al igual que pasa con Hyperledger o incluso Corda, probablemente son inexactas, porque utilizar la solución no exige una declaración en una entidad central.

La comunidad también parece muy activa, con muchos eventos en todo el mundo, principalmente en las capitales. Estos se concretan en forma de reuniones o incluso de hackathons.

La fundación financia un brazo armado que está listo para ayudar al desarrollo de la tecnología por familia de caso de uso. Se ha podido ver, por ejemplo, una colaboración muy fuerte entre los desarrolladores de IOTA y los de Land Rover durante la primera mitad de 2019. Se han firmado muchos acuerdos para crear zonas de experimentación a tamaño real.

Los más recientes incluyen, por ejemplo, la ciudad de Austin en Texas para un caso de alquiler de coches, el telepeaje en Noruega o la detección de carretera deteriorada en el Reino Unido.

Además, la fundación ofrece una ayuda específica en la orientación y el aumento de competencia de los desarrolladores deseosos de implementar la tecnología.

Por último, IOTA ha puesto a disposición un mercado donde se pueden intercambiar datos a cambio de un pago en IOTA. Sin embargo, el sitio web es poco frecuentado. También, durante los hackathons, a menudo el índice de respuesta está por debajo de la media para este tipo de evento. En efecto, la tecnología no se conoce bien y es única en su modelo de aplicación.

Como IOTA es una solución pública, los desarrolladores y los responsables de toma de decisiones pueden temer la volatilidad de la cotización de la criptomoneda que sustenta sus aplicaciones. Un IOTA tiene un valor muy débil, la menor información pública puede hacer que un especulador se haga muy rico con ganancias importantes, pero debilitar el uso de la solución en un contexto de producción.

Otra empresa emergente propone un modelo comparable de animación de comunidad: Corda.

### c. Corda

Corda no es una blockchain. Se trata de un sistema que propone registros compartidos entre pares con una lógica de firma electrónica para garantizar la seguridad de las transacciones. La tecnología cae en la categoría de registros distribuidos de uso exclusivamente permisionado. No tiene variante pública. No hay una criptomoneda predeterminada, sin embargo, a mediados de 2019 salió un kit de desarrollo (SDK) para paliar esta carencia. Inicialmente prevista en un contexto exclusivamente bancario, la solución encontró su camino en sectores muy variados. La solución es suficientemente versátil para que los grandes responsables de la toma de decisiones en Accenture la coloquen como un estándar en el universo blockchain.

Ventajas e inconvenientes de la tecnología

La principal ventaja de la tecnología es una atención a la confidencialidad que por el momento ninguna otra tecnología de registros distribuidos parece haber igualado. Se pueden crear redes a partir de dos actores. Cuando se quieren intercambiar datos entre varios actores, no es necesario pasar por *canales* como Hyperledger. Un archivo de configuración, al que no es fácil acceder ni comprender para un principiante, es suficiente para enriquecer la comunicación. También, a 1800 transacciones por segundo, estamos muy lejos de los estándares de las soluciones de banca de inversión, y casi un 30 % más lentas que una solución Hyperledger. Sin embargo, la solución responde a problemas reales documentales laboriosos que consumen mucho tiempo e implican muchas compensaciones.

Otro punto muy interesante, añadir un actor nuevo a la red no exige romper y reconstruir la blockchain cada vez. En efecto, en Hyperledger, añadir un actor exige volver a hacer el bloque origen, llamado *seed*, porque contiene las firmas de los nuevos participantes.

Siempre con la preocupación de la discreción, es posible actuar en una red siendo completamente desconocido para ciertos actores. En el contexto bancario, esta propiedad es especialmente apreciada.

La introducción de un nudo es relativamente accesible. El código subyacente es Kotlin o Java. Sin embargo, el nivel es alto y adecuado para un desarrollador de Java experimentado, porque se deben hacer adquirido y comprendido una cierta cantidad de conceptos relacionados con la informática distribuida. Una vez lanzados los primeros nudos, la gestión de actores nuevos entrantes o salientes se hace casi completamente mediante la configuración.

Las herramientas de gestión y de supervisión no parecen existir todavía. Entonces probablemente habrá que crearlas, salvo si el desarrollador utiliza soluciones en la nube integrantes de este componente técnico.

Corda es una empresa emergente apoyada por un consorcio de origen bancario. El código es de libre utilización. Sin embargo, hay conversaciones en curso para hacer pagar por el uso. La solución está disponible en la plataforma Azure, pero actualmente en ningún otro servicio de la nube. El sitio web de la empresa ofrece versiones en contenedores.

También es posible solicitar asistencia local. Sin embargo, tienen más demanda de la que pueden asumir y la capacidad de reacción depende los recursos disponibles.

Es posible convertirse en miembro premium a cambio de un abono anual con un importe anual comparable a los miembros *premiers* en Hyperledger. Esta opción permite dirigir los desarrollos futuros y acceder a una cantidad de horas de formación y de asistencia en el desarrollo y la implementación de aplicaciones que utilizan Corda. El pago permite que la empresa sobreviva y los desarrollos futuros, de manera similar a Hyperledger.

Ecosistema

El ecosistema de Corda evoluciona constantemente. Originalmente, estaba formado por grandes bancos miembros del consorcio R3CEV. Por eso, los desarrollos están muy dirigidos a responder a las necesidades del sector bancario. Este último parece estar listo para sacrificar un poco de eficiencia a cambio de una seguridad y confidencialidad muy importantes. Entonces es potencialmente arriesgado implementar esta solución en otro sector.

La comunidad de desarrolladores en Corda es difícil de evaluar. La empresa cuenta con algo más de 350 empleados. Por lo tanto, es probable que hay un centenar de empleados dedicados al desarrollo de la solución técnica. Por tradición, los bancos son poco comunicativos. Una búsqueda en la red social LinkedIn© devuelve más de 13 000 resultados. Considerando la hipótesis de que un 50 % son resultados no adecuados (p. ej.: coincide el apellido o son comerciales), eso nos da una comunidad con más de 7000 desarrolladores potenciales.

La comunidad es muy activa, especialmente a través de reuniones y hackathons. Es posible seguir una formación de manera gratuita, pero en Europa el sitio solo está situado en Londres, en Nueva York para los Estados Unidos y Tokio en Asia. Esta formación está certificada. El sitio web stackoverflow no se vacía, con preguntas respondidas en menos de tres días sin dificultad. También hay disponible un soporte activo de la comunidad. Así, un principiante puede pedir asistencia, buscar un trabajo o compartir su experiencia. Este modelo es completamente comparable con IOTA.

La naturaleza de código abierto del proyecto hace que el seguimiento de los proyectos sea muy delicado. Según la empresa Corda, durante 2018 se lanzaron más de 80 proyectos, de los que al menos siete están en fase de producción.

La solución Corda está disponible, lista para usar como servicio gestionado en Azure. La integración de los componentes tecnológicos externos no es nativa. En la práctica, el uso de las API para acceder a la capa de registro distribuido permite una integración con las herramientas existentes en el contexto de Microsoft y sobre todo en el de las soluciones de terceros.

Corda también ha implantado un mercado. Hasta ahora parece recibir pocas visitas. El tiempo demostrará la idoneidad de esta herramienta.

En el conjunto, la solución demuestra su importancia en el sector bancario. La tecnología es estable y continúa su progreso técnico. Es poco probable que su rendimiento progrese de manera significativa, pero hay muchos desarrollos en curso para aportar propiedades adicionales a los smart contracts.

## **3. Conclusión**

En conclusión, las soluciones técnicas de blockchain son muy numerosas. Los grandes grupos internacionales y las empresas emergentes se han lanzado a un proceso técnico muy distinto. IBM ha optado por la creación de un consorcio para crear una tecnología completamente nueva, mientras que Microsoft ha hecho un esfuerzo de integración de las herramientas en su solución en la nube. Las empresas emergentes han seguido métodos muy distintos. Así, la fundación Ethereum ha propuesto dos versiones tecnológicas similares, aunque con implementaciones distintas, que son incompatibles entre ellas. Quorum es una alternativa permisionada que surge principalmente de un planteamiento empresarial y perfectamente compatible con la versión pública. IOTA es un enfoque completamente distinto, que se aleja de la lógica blockchain en beneficio de una tecnología muy distinta, porque parte del caso de uso del Internet de las cosas (IoT). La implementación es equivalente en una lógica pública y en una permisionada. Corda es una alternativa que surgió de una importante necesidad profesional con imposiciones de confidencialidad importantes. Por el momento no tiene ninguna tendencia a orientarse hacia una lógica pública.

Ya hemos visto las soluciones tecnológicas más frecuentes conocidas, ahora ya podemos presentar los casos de uso.

# Aplicaciones existentes

Hace muchos años que se conocen los casos de uso de blockchain, pero a las soluciones técnicas les faltaba rendimiento frente a las ambiciones expresadas. El progreso tecnológico es constante, con un auge de las inversiones en el tema. El año 2018 vio explotar los modelos de financiación por ICO (*Initial Coin Offerings*), que permiten recoger fondos en divisas fiduciarias a cambio de criptomonedas. De esta manera se han recogido miles de millones. Por ejemplo, Telegram, una aplicación de mensajería rusa, ha recogido más 980 millones de euros en unas horas procedentes de menos de una decena de oligarcas. EOS, tezos, NEO han recogido más de mil millones acumulados en unos días.

El sector del capital riesgo no se queda atrás. Durante los últimos cinco años, los importes invertidos han sido muy importantes, y se han multiplicado por 40 entre 2017 y 2018, como podemos ver en la figura que aparece aquí debajo.

Gráfico, Gráfico de líneas

Descripción generada automáticamente

*Capital riesgo invertido en el mundo en Blockchain y las empresas emergentes vinculadas a blockchain. Fuente: Crunchbase*

En el año 2019 se produjo una disminución del importe total invertido. Además, se hicieron menos transacciones, pero con importes más elevados que los observados a finales de 2018, en continuo aumento. La zona geográfica que más se expandió parece ser la región asiática.

Se han desarrollado muchas aplicaciones. La consultora McKinsey ofrece un análisis sectorial del uso de blockchain en dos direcciones: el impacto y la debilidad (B. Carson, 2018).

Gráfico, Gráfico de dispersión

Descripción generada automáticamente

*Las oportunidades blockchain por sectores industriales. Fuente: McKinsey*

No es una sorpresa que el sector público sea uno de los que reciben un impacto mayor, con un factor de viabilidad neutro. El sector financiero también recibe un fuerte impacto, con un grado viabilidad mucho más razonable que muchos otros sectores. Por el contrario, el sector automovilístico y el industrial parecen ser los menos propicios a la viabilidad y despiertan menos interés. El sector agrícola también parece tener un grado de viabilidad muy bajo, con un impacto mucho más fuerte.

Siempre según el análisis, el aporte de valor de la blockchain se hará en dos etapas. A corto plazo, residirá en una reducción de los costes y una optimización del ecosistema. Más tarde, la tecnología favorecerá la creación de nuevos modelos de empresas. Los sectores que quieran lanzarse a la aventura de blockchain tendrán que trabajar en un entorno de "coopetición" para converger hacia estándares locales que, mediante iteraciones, favorecerán nuevas maneras de trabajar. Sin esta etapa, es poco probable conseguir un crecimiento, sea cual sea la tecnología.

El desafío en las empresas será estructurar una estrategia de blockchain coherente con las estrategias previamente existentes. Para ello, habría que proceder de la siguiente manera:

* Estimar el valor utilizando criterios factuales, de forma pragmática, buscando la resolución de problemas concretos y definiendo los casos de uso específicos en la empresa.
* Captar el valor poniendo en práctica la capacidad de agrupar el ecosistema, de establecer normas y de tratar las problemáticas normativas correspondientes.
* El valor aportado a la blockchain evolucionará sobre la marcha hacia la creación de nuevas oportunidades (creación de datos nuevos) que permiten la introducción de nuevos modelos de negocio y por lo tanto de nuevas generaciones de ingresos. Este análisis permitirá ajustar con agilidad las estrategias existentes.

Los elementos que aparecen más abajo retoman, por sector, casos de uso más o menos apropiados. Cada caso presenta la problemática encontrada, la tecnología utilizada cuando se tiene esta información, y los resultados. Algunos casos de uso parecen contradecir al estudio antes citado, porque la tecnología aporta un valor auténtico en su contexto. En el extremo opuesto de la representación, algunos casos no se han examinado desde el punto de vista de una auténtica estrategia.

Naturalmente, el primer caso empieza por la administración.

## **1. Administraciones oficiales/instituciones públicas**

El sector de la administración es uno de los más prometedores en el uso de la tecnología blockchain. Se han lanzado numerosas iniciativas en todo el mundo. Dos en particular se han seleccionado para mostrar lo que puede hacer la tecnología. Los últimos avances, especialmente en tecnologías permisionadas, responden a una necesidad auténtica.

### a. Las secretarías de los tribunales de París

La administración francesa está instalada sobre varias décadas de mutaciones, cambios y mejoras incrementales que tenían el objetico de garantizar los principios fundamentales de nuestra democracia, el disfrute de las libertades y las obligaciones que generan. Por ejemplo, todas las empresas deben pasar por el registro mercantil (RCS en Francia) para poder ejercer su actividad legalmente. Esta etapa fundamental para el estado permite crear identificadores únicos, números de IVA y otras formalidades necesarias para el buen funcionamiento de la economía del país.

Las secretarías han visto un aumento progresivo de su ámbito de competencia junto con un incremento de su carga de trabajo. Los secretarios judiciales reciben, controlan y certifican toda la información jurídica y económica relacionada con las empresas. Sin embargo, no se ha hecho ninguna gran inversión para modernizar la actividad. Los documentos exigidos y los procedimientos correspondientes en cada región no siempre están normalizados. Los intercambios se hacen fundamentalmente en papel, luego por correo y eventualmente mediante el intermediario de una caja fuerte digital. Abrir o cerrar una empresa puede costar fácilmente seis meses, dependiendo de la secretaría de la que dependa la empresa. Los documentos se pierden, el proceso se amontona o las cartas con acuse de recibo nunca se reciben. El empresario que no conoce los procesos internos de la secretaría en cuestión debe tener mucho cuidado, porque el menor fallo interno recae irremediablemente sobre sus hombros.

Algunas modificaciones del estatuto de una empresa exigen una colaboración entre las 134 secretarías de Francia. Por lo tanto, se necesita un trabajo meticuloso y coordenado para permitir una convergencia de las informaciones y de los documentos requeridos (Dussutour, 2019).

Para responder a una necesidad de modernización y de mejora del servicio público, el Consejo nacional de los secretarios de los tribunales de comercio (CNGTC) ha lanzado una iniciativa autónoma con IBM mediante una asociación utilizando la tecnología blockchain. EL RDC es en sí mismo un registro. La tecnología blockchain también es un registro, que se conecta a los sistemas informáticos existentes. El impacto sobre los sistemas existentes ha demostrado ser muy pequeño.

El objetivo de la solución es hacer un seguimiento y poner un sello de tiempo en todas las operaciones realizadas en cada secretaría. Además, los documentos se intercambian de manera digital con el objetivo de tener una visión única de las formalidades en curso en todo el territorio. Hay un proceso de ecosistema en fase de definición. Se realiza mediante iteración con los distintos participantes. Sea cual sea la operación, debe realizarse en 72 horas. La pretensión es interesante, porque actualmente, entre el envío del correo y la recepción, habitualmente suelen pasar dos semanas, sin garantía de realización de la prestación.

Se utiliza la tecnología Hyperledger Fabric. No se conoce el tamaño del equipo. El proyecto todavía está en fase de PoC, pero los resultados son alentadores. La tecnología utilizada va a permitir, de manera progresiva, hacer los controles y la certificación de manera automática, aliviando la carga de trabajo de los secretarios mientras ofrece los usuarios un servicio de mejor calidad. El CNGTC consideró la posibilidad de un aumento de las capacidades de la tecnología en temas relacionados.

### b. Venezuela y criptomoneda

La gestión de un país es de una gran complejidad y solo algunos elegidos se arriesgan a enfrentarse a ella. Venezuela es un país de una gran riqueza minera, con reservas de petróleo muy importantes. Sin embargo, durante las dos últimas décadas, el país se ha enfrentado a problema sociales, de corrupción y repetidas crisis económicas. La divisa, el bolívar, está sometida a una hiperinflación, lo que hace caer la cotización a niveles que recuerdan en la memoria colectiva a las fluctuaciones del marco alemán tras la Segunda Guerra mundial.

Por otro lado, en los años 20, una corriente de pensamiento económico proponía garantizar el valor de una divisa con contravalor en materias primas. Así, una divisa como el dólar podía apoyarse en una promesa de extracción de barriles de petróleo en el futuro. Una oposición fuerte de los propietarios de oro y de otras facciones impidieron esta posibilidad a las economías emergentes durante los acuerdos de Bretton Woods en 1944.

El gobierno venezolano buscaba contener la devaluación y propuso implantar una criptomoneda basada en el petróleo todavía no extraído, para utilizar los mecanismos económicos mencionados casi un siglo antes. Al principio del proceso, el gobierno emitió títulos que daban derechos sobre barriles a extraer en el futuro. Estos títulos se vendieron durante períodos de fuerte demanda económica, y así llenaron la tesorería del estado. Durante las etapas de crisis, cuando la cotización de las materias primas se hunde, vuelve a comprar esos títulos. En lugar de títulos se utiliza una criptomoneda llamada petro. Así podemos contemplar la primera criptomoneda emitida por un país y apoyada por un contravalor real.

La solución, específicamente desarrollada para la ocasión, es una blockchain privada. Las características asociadas a esta tecnología han evolucionado con regularidad entre el anuncio de una emisión de criptomoneda en octubre de 2018, la aparición de la documentación técnica que describía el proyecto en diciembre de 2018 y finalmente su abandono en marzo de 2019 (Brown, 2019).

El aspecto privado desconcertó a los inversores, habituados a prácticas ligeras del gobierno en varios temas relevantes del estado. Este último, plenipotenciario en la blockchain, conserva el derecho de anular algunas transacciones o de añadirlas en su favor. Por otro lado, los procesos de gestión de una divisa son difíciles de programar y, cuando lo son, ofrecen las mismas influencias de poder que han llevado al bolívar a un estado de inestabilidad. El contravalor sobre el que se apoya el petro evoluciona con regularidad. El petróleo es de mala calidad y su extracción claramente más costosa que en Oriente medio. Esta característica hace que el ajuste entre el petro y el barril a extraer sea todavía más delicado. Otra cuestión igualmente delicada es que la promesa de una extracción no es en ningún caso su realización. Teniendo en cuenta las dificultades que atraviesa el país, la promesa puede carecer de sentido.

Detrás de este fracaso preliminar, observamos una semilla plantada. La idea, en sí misma, no es mala. Seguramente los economistas mantendrán un debate agitado en los próximos años sobre las propiedades de las criptomonedas y su interés a nivel de una nación o de una región. Muchos estados pequeños, como Noruega, consideran seriamente la alternativa criptomoneda a su nivel. En efecto, mantener una divisa fiduciaria es muy costoso, y la visa de un billete de cinco euros no supera los seis meses. Además, la creación de moneda falsa sería muy difícil para los falsificadores. El tiempo y la evolución tecnológica deben contribuir con sus efectos.

## **2. Arte**

Actualmente hay muchos proyectos para facilitar el ascenso de algunos artistas y certificar la autenticidad de algunas obras. Dos proyectos asociados a la tecnología Blockchain que parecen adecuados.

### a. Ampliative Art o arte descentralizado

Ampliative Art es un proyecto de aplicación descentralizada en construcción que tiene el objetivo de permitir a los artistas o contribuyentes con el mundo del arte compartir libremente sus creaciones y ser remunerados en consecuencia.

Habitualmente, el mundo del arte se enfrenta a unas cuantas dificultades. En primer lugar, los artistas deben pagar para presentar sus trabajos. Luego, es frecuente que sus creaciones adquieran valor una vez fallecido el artista. Por último, algunas obras de arte (por ejemplo, las creaciones digitales o el street art) no son reconocidas como tales. El sitio flaticons, por ejemplo, propone a algunos artistas que publiquen sus creaciones y ofrece la posibilidad de dejar a voluntad del usuario la remuneración de los creadores de contenido. A eso se suma una restricción de red. Para poder vivir de su arte, hay que conocer a ciertas personas.

El objetivo de Ampliative Art es atacar en estos tres frentes y añadir una dimensión ética y social a su proceso.

En la práctica, un artista coloca sus obras en una galería dedicada a él en una plataforma web. Él elige la licencia asociada a la obra. Por ejemplo, el artista puede elegir limitar el acceso o al contrario, renunciar a sus derechos sobre la creación.

En la segunda etapa, los observadores comentarán la obra, la compartirán y propondrán mejoras, por ejemplo. También pueden remunerar al artista bajo la forma de donaciones con cantidades relativamente modestas, como propinas. Estas donaciones pueden hacerse mediante medios de pago convencionales (por ejemplo: tarjeta bancaria, PayPal) o mediante sistemas alternativos (como Bitcoin, Flattr). Un segundo tipo de recompensa está relacionado con las valoraciones en forma de estrellas, de una a diez, como en los sitios de viajes o de calificación de restaurantes.

Flattr es un servicio social de microdonaciones fundado en 2010. Permite que los creadores sean remunerados en función de un presupuesto mensual fijado por el acreedor de la cuenta Flattr. Este último elige a quién donar este importe, es decir, a los artistas que quiere apoyar.

En una tercera etapa, el sitio propone aumentar la reputación del actor, ya sea artista o comentarista. Esta reputación crece en función de los siguientes elementos:

* contribuciones hechas a la organización;
* evaluaciones hechas y recibidas;
* recompensas hechas y recibidas;
* trabajos y obras presentados.

Por el momento, el proyecto todavía no describe la parte de estos elementos en el aumento de la reputación.

A continuación, los ingresos generados por la organización se distribuyen en función de la reputación de sus miembros. Así, cuanto más ha contribuido un actor al sitio, ya sea artista o no, más ingresos obtendrá en función de los recursos disponibles.

El sitio no tiene documentación técnica explicativa. Tampoco explica cómo financia su actividad. Sin embargo, es muy posible que retenga una comisión de funcionamiento entre el pago de las donaciones y la etapa de redistribución.

Tampoco dice ni una palabra sobre el problema de distribución inmediata de recursos al creador, habitualmente mediante Flattr, que no es el modo general de remuneración de los actores. Por último, no se informa de las medidas de protección de los derechos de autor.

La aplicación también tendrá que enfrentarse a las dificultades de los moderadores. Por el momento no se ha pensado ningún sistema de filtrado. El objetivo anunciado es permitir a la comunidad expresarse sin límites, la función de moderador está garantizada por sus propios miembros. Es peligroso basarse exclusivamente en la reputación.

Hay una alternativa más sólida que añade una particularidad interesante: la certificación de una obra.

### b. Monegraph o cómo proteger un contenido artístico

En el extremo opuesto del tablero, Monegraph ofrece una solución estable de verificación de la propriedad intelectual. La actividad principal de la aplicación descentralizada es proteger las creaciones de arte digital.

En la práctica, un creador de contenido se registra con una dirección de correo electrónico y una contraseña. Deposita su obra en el sitio mediante un sencillo arrastrar y soltar. A continuación, elige los acuerdos de licencia. Define si quiere vender, transferir o registrar su obra. Igualmente define los derechos de acceso y el precio de venta. Este sistema está pensado para personas que no tienen un gran conocimiento de la tecnología, es rápido y eficaz. Existe la posibilidad de describir la obra y darle un título, luego tiene que validar.

A continuación, la obra se almacena en la blockchain Namecoin. Desde un punto de vista técnico, se trata de la aplicación de un smart contract. Mientras espera la validación, se genera un bloque para pasarlo a la cadena. Desde sus comienzos, la parte técnica ha mejorado mucho y se ha simplificado para ofrecer la tecnología a la mayor cantidad de personas posible. Hace dos años, el proceso era laborioso y exigía colocar una serie alfanumérica en la cadena Namecoin, en el sitio dedicado (Cawrey, 2014).

El interés para el artista es inmediato, porque puede proteger su obra y el uso que se hace de ella. Del mismo modo, puede autorizar o denegar su modificación, algo que raramente está garantizado con las condiciones actuales. Teniendo en cuenta los costes generados por un procedimiento judicial, en caso de litigio, a menudo es preferible para el artista dejar que el usuario haga lo que prefiera con la creación.

Para los compradores de contenido, se trata de una plataforma accesible, ordenada y específica en función de las necesidades. No necesitan asegurarse de los derechos de autor y tienen inmediatamente un mercado con un precio fijo conocido y prefijado. Igualmente, y sobre todo, disponen del original y están seguros de las condiciones de uso de la obra.

Las dificultades de esta aplicación varían en función de la legislación de los distintos países. Habitualmente, cuando un comprador de contenido, como una escuela de comercio, quiere cambiar su logotipo, sistemáticamente debe solicitar un permiso al autor del logo para modificarlo, incluso si solo quiere cambiar el color. Esta aplicación descentralizada también parece ser una buena idea.

El problema de este proceso es que solo funciona si lo utilizan todas las partes: los creadores y los compradores. En efecto, si el original está «marcado», sigue siendo posible reproducirlo, copiarlo o duplicarlo hasta el infinito. Sin embargo, solo el original pasará la prueba de autentificación.

Dicho de otro modo, la tecnología permite controlar algunos elementos que antes no era posible. Limitadora por naturaleza para proteger al creador, podría ser útil que evolucionara y promoviera la democratización de este uso de la blockchain. La ambición de *Monegraph* es mucha, porque planean tocar todas las dimensiones de una obra de arte, haciendo de la redirección de pagos una gestión granular de los derechos de uso y el envío focalizado de mensajes de los patrocinadores.

Esta ambición podría verse frenada por alternativas más focalizadas. Por ejemplo, plataformas, como *Peertracks*, proponen poner directamente en contacto a los creadores de contenido musical con los clientes. Así las compañías y los sellos discográficos ya no serían necesarios como intermediarios.

## **3. Asociación y beneficencia**

El sector de la beneficencia tiene mucho que ganar al utilizar la tecnología blockchain. Cada año, se invierten millones en ayuda humanitaria, las asociaciones y las ayudas caritativas. Cada uno de estos sectores tiene sus características propias y una gran disparidad de gestión y de uso en función de su finalidad y su posición geográfica.

La corrupción y la malversación privan a las poblaciones en situaciones a menudo muy delicadas de los recursos que necesitan. En el otro lado de la mesa, los actores que se presentan como defensores del interés de las comunidades frágiles malversan el dinero en su interés.

El reto es muy importante en la selección de los socios, la trazabilidad y el seguimiento de los actores es el que más se exige, si no es el más urgente, y el pago de los capitales o el desbloqueo de los recursos y del material necesario.

La empresa emergente AidChain se fundó con la perspectiva de responder a la necesidad de transparencia y de confianza en el sector de la beneficencia. Al principio, los desarrolladores se centraron en la recogida y redistribución de donativos, con una trazabilidad del fin que recibía los fondos. La parte que concierna a su uso todavía no se ha considerado.

Para eso, utilizan la plataforma Ethereum, en su cima desarrollan smart contracts. Se ha creado una divisa denominada AidCoin y la empresa emergente ofrece una aplicación de smartphone para hacer donaciones (AidCoin, 2019). El equipo al completo no supera una decena de personas.

Aún falta evaluar el éxito. Mediante esta plataforma, la asociación de defensa de los animales WWF pudo recoger 20 dólares. La organización ya tiene una estructura adecuada para encontrar fondos. Por el contrario, en julio de 2018, unas fuertes lluvias arrastraron casas y personas. Se donaron alrededor de 100 000 dólares en apoyo a las víctimas. Cabe señalar que el 99 % de los fondos fueron donados por un solo participante *AidPool* (Aidchain, 2019). El incendio de la catedral de Notre-Dame en París pudo recoger la suma de 5000 dólares.

El planteamiento es en sí mismo una de las muy numerosas innovaciones en el sector de la beneficencia. La empresa emergente solo se ha ocupado de la problemática de la donación. Esta parte se ha considerado bajo el punto de vista técnico. Sin embargo, la mayoría de las donaciones pueden hacerse fácilmente mediante una llamada telefónica o una transferencia bancaria. Quizás este no es el mejor planteamiento. Además, este se limita a transferencias de fondos. Si, en efecto, la tecnología garantiza la trazabilidad de los fondos, el donante no tiene la garantía de que la dirección técnica a sonde se envían los fondos corresponda a una entidad específica, legítima y de pleno derecho.

Las actividades de beneficencia son complejas, laboriosas y muy sensibles. Probablemente, sería interesante volver a centrar rápidamente la iniciativa sobre un soporte transversal a las estructuras existentes. En caso contrario, la empresa emprendedora se arriesga a perder su público y a no responder a las problemáticas del sector.

## **4. Seguros**

El sector de los seguros es extremadamente competitivo. Los profesionales están bajo presión y la necesidad de renovación de las plataformas informáticas es un pilar de la competitividad del sector. Hay muchas iniciativas en marcha para volver a dinamizarlo, encontrar nuevos mercados o reducir la carga operacional.

### a. Fizzy: reembolso en caso de retraso en los transportes

Los seguros de los vuelos y el reembolso en caso de retraso son un tema espinoso para muchas aseguradoras. En las plataformas de reserva en línea, si se rechaza un seguro en beneficio de otro, porque ya está asegurado, es muy probable que el cliente tenga que pasar por una carrera de obstáculos en caso de siniestro o de incumplimiento contractual por parte del proveedor.

La idea de Fizzy es ofrecer en unos pocos clics un seguro de retraso y anulación cuando el vuelo tiene más de dos horas de retraso o no va a despegar nunca. No se requiere ninguna formalidad administrativa y la verificación de que el cliente ha comprado un billete es sencilla.

El sistema implantado por Aza se conecta a los registros oficiales de salidas y llegadas en el mundo y reembolsa en consecuencia al cliente perjudicado desde el instante en que se cumplen las condiciones.

Están cubiertos un 80 % de los vuelos internacionales y el proceso de integración sigue adelante.

Esta innovación es posible desde la aplicación de una directiva europea que le exige al transportista un reembolso del billete, sin importar el motivo. Así, incluso un tren de la red ferroviaria es susceptible de ser reembolsado sin ninguna forma administrativa específica bajo reserva de poder presentar un justificante de transporte. Igualmente, el proceso es posible gracias a estandarizaciones muy relativas y la accesibilidad de los datos recogidos.

La tecnología empleada es la plataforma Ethereum, una aplicación móvil y un sitio web. En principio, el equipo técnico no está compuesto por más de cinco personas. Es muy probable que se refuerce más tarde.

En la práctica, el planteamiento funciona, pero no se ha comunicado ninguna cifra para conocer el éxito comercial. Además, utilizar la plataforma Ethereum tiene restricciones de carga que hacen muy difícil el uso de soluciones de gran volumen. Sin embargo, la iniciativa es muy interesante y muy probablemente evolucionará en el futuro si encuentra su público. Es indudable que se necesita un trabajo importante para hacer que la aplicación sea masiva. Por otro lado, la proporción de vuelos con retraso quizás no justifica el precio del seguro. Por último, ya existen muchas soluciones y, en su estado actual, se trataría de un sobreseguro por encima de las plataformas existentes.

### b. B3i: el seguro descentralizado

El sector de los seguros es el objetivo de una cierta cantidad de modificaciones legales que a veces rebajan sus obligaciones reglamentarias, a menudo influyen en sus márgenes de maniobra y margen operativo. Muchas actividades administrativas que pueden compartirse a nivel del ecosistema de seguros son repetitivas, manuales y consisten fundamentalmente en los controles realizados a varios niveles.

Hay un tema en particular que ha recibido el impacto de la transformación de la legislación: los seguros crediticios. En el marco del crédito inmobiliario, el seguro suscrito generaba un rendimiento del 100 %. Dicho de otra manera, un asegurador facturaba un servicio por 10 €, y solo se necesitaban 5 € para cubrir el riesgo y los gastos de gestión anexos.

La ley ha evolucionado, dándole derecho a un cliente a cambiar el seguro en cualquier momento o casi al terminar la firma del crédito. Posteriormente, la competencia tiene tendencia a reducir este margen operativo. La transferencia de seguros entre dos organismos es muy costosa, porque los procesos y los elementos que hay que verificar entre dos organismos no se recuperan necesariamente. Fundamentalmente, el trabajo consiste en un envío de correo en papel, correos electrónicos y otras tareas burocráticas.

Entonces, la idea es normalizar el proceso de transferencia del contrato de seguros para una selección de actores. En efecto, captar un cliente aporta valor. Realizar los controles y el proceso administrativo se percibe como un centro de costes.

B3i es un consorcio que se ha lanzado a esta aventura de normalización en casos muy precisos. Utilizan la tecnología Hyperledger Fabric para intercambiar información de manera estandarizada y automatizar el proceso todo lo posible. El chaincode (smart contract) realiza una serie de controles, y el resultado se integra en los sistemas de información existentes. Los equipos técnicos dedicados al esfuerzo inicial oscilarían entre diez y veinte. Utilizan un planteamiento en la nube.

La iniciativa ha tenido mucho éxito, tanto que ha recogido 16 millones de euros (Coronel, 2019), elevando así su capital social a casi 22 millones de euros. Cuenta con muchos accionistas importantes, como Aegon, Allianz, Tokio Marine o XL Catlin.

Las ambiciones del consorcio son muy importantes y tienden a luchar contra los procesos de los muy numerosos actores que pretenden hacer la trazabilidad del comercio marítimo y el seguro asociado. El proceso ha sido posible gracias a una segmentación importante de los datos y de su uso en la tecnología empleada. Los desafíos técnicos serán muy importantes para el paso a otro nivel.

En efecto, si hay redes Hyperledger con una decena de actores y por lo tanto de nudos, podría observarse un límite técnico con el aumento de los volúmenes de datos y de los actores.

## **5. Automoción**

El sector de la automoción es el principal objetivo de las empresas que se dedican a blockchain. Los campos de aplicación incluyen las etapas anteriores (p. ej.: cadena de suministro), las etapas posteriores (posventa), pero también nuevos mercados con la llegada de las *smart cities* y la evolución de los usos del coche. Toyota, por ejemplo, utiliza la tecnología para hacer un seguimiento mejor del pago a los publicistas, mientras que el grupo Volkswagen busca hacer la trazabilidad de materiales peligrosos desde la mina hasta la descarga. Este sector es uno de los más innovadores y seguramente los próximos años verán emerger nuevas maneras de hacer negocios.

### a. Vehicle passport o libro de mantenimiento

En 2015, la empresa Renault a lanzó un prototipo de libro de mantenimiento del vehículo, cuyo objetivo es seguir el ciclo de vida de las reparaciones y controles realizados.

Un coche pasa por la inspección técnica con una cierta regularidad. Estos controles son accesibles en línea. Por el contrario, las operaciones de mantenimiento, los accidentes y los problemas encontrados en el vehículo durante su vida no se registran y tienen un impacto importante en el valor residual en el momento de la reventa. Sin embargo, aproximadamente, un coche de cada dos termina en el mercado de ocasión. Esta tarifa aumenta con nuevas formas de uso como los alquileres de larga duración. El concesionario o el comprador apuestan sobre la fiabilidad de un coche en la recompra con una prima de seguridad para cubrir el riesgo.

La idea es utilizar la blockchain para almacenar la información de mantenimiento, así como las facturas relacionadas. En el mejor de los casos, serviría como canal de comunicación para que el fabricante pudiera seguir en contacto con el propietario del vehículo con fines comerciales. En una segunda fase, sería un vínculo entre el constructor y el propietario en caso de retirada. De hecho, en todo el mundo, uno de cada dos vehículos se retira del mercado durante su vía útil. Por último, el sistema permitiría garantizar que un vehículo ha sido desguazado, una información que no siempre se recibe.

La ventaja para el propietario es garantizar la fiabilidad del vehículo con un historial de operaciones de mantenimiento. Si el vehículo está en buen estado y el libro de mantenimiento así lo indica, el valor residual es más elevado. El comprador no necesita reservase una prima para correr el riesgo. El objetivo es entrar en un ciclo honesto de confianza.

El planteamiento no tiene en cuenta los vehículos que han sufrido una cierta cantidad de reparaciones asociadas a un propietario poco escrupuloso. Nada le obliga a inscribirse en las operaciones de mantenimiento y no hay un sistema que garantice que se inscriben todas las operaciones. El segundo problema principal es la elección de la tecnología. Durante los experimentos en 2015, la plataforma utilizada era Ethereum. El almacenamiento de los archivos como las facturas tenía un coste prohibitivo. Hablamos de unos 5 millones de euros por gigabyte. Mientras que los gigabytes oscilan entre 2 y 10 céntimos de euro en las soluciones en la nube durante el mismo período.

Desde entonces, la mayor parte de los constructores europeos han lanzado su iniciativa de libro de mantenimiento en blockchain. A priori, ninguna ha despegado hasta hora, porque la falta de estandarización de la información inscrita y de animación del ecosistema ha reducido su impacto. Casi siempre, estos prototipos se quedan en las divisiones de innovación de las empresas.

Soluciones de almacenamiento como Filecoin o IPFS pueden sustituir a Ethereum si se quiere almacenar archivos con un coste menor en una blockchain pública. Soluciones de blockchain permisionadas como Hyperledger, Corda o incluso Multichain también pueden dar respuesta a esta necesidad si los constructores o los actores de la reparación quieren animar su comunidad.

### b. RWE y Slock.it: cargar su coche eléctrico al céntimo

En contraposición, hay proyectos simples y funcionales que son resistentes. La empresa RWE y Slock.it se aliaron para hacer pagos de recarga de coches eléctricos en terminales específicos gracias a la tecnología Blockchain (Higgins, 2016). RWE es una empresa alemana de generación de electricidad similar a Endesa. Dispone de una base de más de 20 millones de consumidores en el mundo. Su volumen de negocio es de 42 000 millones de euros. El enfoque era realizar una gestión automática de la facturación mediante smart contracts en la cadena Ethereum.

De hecho, el proyecto está financiado por el proceso de recarga de vehículos. El cliente no necesita conocer los detalles técnicos de una divisa virtual intercambiada por una divisa real. En la práctica, el cliente deposita el dinero en una cuenta mediante la aplicación móvil. El sistema captura este dinero de manera efectiva después de realizar la recarga. El proceso es más eficaz que los terminales de recarga actuales donde se le factura al cliente el tiempo que ha pasado en el terminal de recarga, y no el consumo efectivo de electricidad.

La próxima etapa consiste en que la asociación analice el entorno jurídico que podría bloquear la entrada en producción del prototipo más allá del sencillo Proof of Concept. La siguiente fase, realizada en 2017, consistió en que la asociación analizara el entorno jurídico que podía bloquear la entrada en producción del prototipo más allá del sencillo Proof of Concept. En la práctica, el humano debía comunicarse directamente con la máquina, sin necesidad de una empresa de factorización o de un contable para pronunciarse sobre la transacción. Parecía que las ganancias económicas iban a ser inmediatamente visibles. Sin embargo, desde 2017, no se ha filtrado ninguna comunicación sobre el proyecto.

A mediados de 2019, Blockchain compró la empresa, especialmente para aumento su campo de competencia entre blockchain y el mundo real. Desde las primeras iniciativas de 2016, los productos han mejorado tanto en el aspecto de la seguridad como en el técnico.

Por lo tanto, se trata de un ejemplo inmediatamente aplicable de la tecnología Blockchain. No es necesario centrarnos en la parte económica con la creación de divisas virtuales propensas a la especulación para obtener beneficios de esta herramienta nueva. Es tan fácil de utilizar como de aplicar, por ejemplo, en un alquiler de películas o en una suscripción clásica.

### c. Car e-wallet

El uso de los coches evoluciona, y lo hace muy rápido. Las jóvenes generaciones de Europa occidental tienden cada vez menos a obtener el carnet de conducir. Las grandes aglomeraciones están saturadas desde hace muchos años y la tendencia no mejora. La tendencia de pérdida de propiedad del vehículo en beneficio de un pago por uso o mediante alquileres también parece ser una tendencia del mercado. Así el cliente se protege de nuevas normativas ambientales que le prohíban una utilización plena de su vehículo durante un período largo.

Estas modificaciones profundas tienen un impacto importante para la industria que debe producir los coches del mañana. Eso implica que debe hacer un coche más robusto, porque se utilizará más. En un contexto de vehículo conectado, y quizás autónomo, se debe facilitar la gestión todo lo posible. Este punto es especialmente importante en usos nuevos del alquiler de corta duración como el free floating.

Una tecnología única no resolverá todos los desafíos del sector. Sin embargo, el e-wallet es uno de los casos de uso que tiene más posibilidades de llegar al día a día de los clientes a corto plazo. Es uno de los temas más dinámicos con primeros prototipos que se remontan a 2014. Muchas empresas se han lanzado sobre el tema usando su propia tecnología, como el fabricante de equipos ZF en Hyperledger, el constructor Jaguar en IOTA o independientes como BTU.

El termino se utiliza en muchas situaciones que no son necesariamente coincidentes. Land Rover, mediante su filial Jaguar, ha lanzado una PoC utilizando la tecnología IOTA. El prototipo tiene muchas finalidades que incluyen la localización de un vehículo circulando libremente. Es prometedor y su ambición es informar a la red caso de zonas de obras, un punto especialmente delicado en el contexto de los vehículos autónomos. En efecto, los modelos actuales funcionan cada vez mejor en carreteras despejadas con una señalización clara. Por el contrario, no tienen información de puesta en práctica (p. ej.: zona de accidente), por el momento tienden a reaccionar de manera inapropiada.

El prototipo está en proceso y solo afecta a un único modelo de vehículo en un trayecto bien definido. Sin embargo, la información que se busca recoger (p. ej.: gasolina restante en el depósito) se ha recuperado como se esperaba. El equipo original apenas supera la decena de personas y recibe un gran apoyo de la comunidad. Parece que la empresa quiere utilizar la tecnología como una navaja suiza de transferencia de información a través de un canal seguro.

La empresa emergente BTU propone una visión más modesta, que consiste exclusivamente en reservar un coche y utilizarlo durante un período determinado. La ganancia de valor se hace en la desintermediación de una plataforma, como la compañía Uber. Se ha comprobado el impacto en el precio (Raymond, 2018), con una reducción de 10 € en una factura de 19 €.

En efecto, una plataforma cobra un coste fijo, como mínimo, y luego una tarifa proporcional a la carrera. Por lo tanto, la tecnología es una alternativa interesante para los trayectos muy cortos. Segunda ventaja de la solución: una reconexión entre el proveedor y el cliente y libre fijación de precios. La empresa recogió un poco menos de cinco millones de euros en 2018, tuvo que encontrar medios de subsistencia con mucha rapidez para continuar con los desarrollos.

La compañía ZF creó una filial llamada Car e-wallet, establecida en Alemania. Su método es crear un mercado de intercambio de datos para facilitar la vida diaria de los actores de un ecosistema en torno a un automóvil. Sin embargo, la solución no consiste de ninguna manera en una cartera integrada en un coche. En cambio, proponen transmitir información desde un coche hacia los actores del ecosistema. Para una estación de servicio, por ejemplo, la solución facilita la gestión de las tarjetas de fidelidad y de la información de cliente vinculada a las tarjetas. La solución técnica todavía está en sus comienzos y solo se aplica a vehículos conectados. Sin embargo, en una lógica de ecosistema donde desarrollar su propio estándar aporta poco valor, la solución merece un aplauso. Pero se plantea la pregunta de si es interesante para un fabricante de automóviles externalizar una posible fuente de ingresos a través de una plataforma de mercado por construir. Técnicamente, la solución se basa en Hyperledger Fabric. No hay ninguna información sobre el tamaño del equipo. El proyecto se habría lanzado en 2018.

De esta manera, hay proyectos muy serios que ven la luz en el sector de la automoción y en los próximos años deberían aparecer cambios reales, además de las obligaciones ambientales y jurídicas.

## **6. Energía**

Paradójicamente, el sector de la energía es uno de los más prometedores de la tecnología Blockchain. Algunos críticos alzan su voz contra la tecnología del registro descentralizado porque consumiría una cantidad muy importante de energía eléctrica para validar un cálculo matemático sin una finalidad intrínseca.

Progresivamente, se montan muchos proyectos piloto y empresas para resolver problemas técnicos y tecnológicos de verdad.

### a. TransActive Grid o la etapa inicial de smart-grid

Desde el 11 de abril de 2016, en el barrio de Brooklyn, en Nueva York, es posible intercambiar y comprar electricidad entre particulares y empresas (Deluzarche, 2016). Actualmente, en el estado de Nueva York, como en España, el proveedor central de electricidad compra toda la energía producida por el particular. Este planteamiento puede representar una pequeña revolución a nivel de un país.

En efecto, las capacidades de producción a nivel del particular son muy modestas frente a una central nuclear. Para garantizar la transición energética, se han establecido créditos «energía renovable», con resultados moderados en función de los países, del régimen fiscal, de los niveles de subvención, etc.

El sistema descansa sobre tres pilares. El primero es un sistema llamado de microgrid. Se trata de subconjuntos de generación y de reparto de consumo de energía. Permiten producir y consumir energía eléctrica localmente de manera simultánea. En caso de sobretensión, un problema bien conocido por los productores de electricidad, esta solo puede alcanzar que una cantidad restringida de hogares.

El segundo pilar afecta al sistema de medida y seguimiento de producción y consumo de energía renovable producida. El sistema, denominado *smart meter*, permite seguir esta información casi en tiempo real con una granularidad suficiente para la facturación. Este sistema se basa en un smart contract de la plataforma Ethereum que monetizará el exceso de energía producido por un hogar. Este exceso da lugar a la generación de una moneda interior en la red.

Estos créditos energéticos se pueden intercambiar y comercializar en un mercado energético asociado a microgrid. Este intercambio siempre se hace mediante smart contracts.

Teóricamente, es posible que los microgrids adyacentes compitan entre sí energéticamente para garantizar un nivel de precios aceptable. Igualmente se ha desarrollado una aplicación para poder seguir el consumo del hogar en un período elegido. Esto es posible gracias al sistema smart meter (Lilic, 2015).

El consumidor tiene la posibilidad de elegir qué parte de su electricidad consumida procede de un microgrid TransActive, y qué parte procede de un productor regional de energía renovable. Por contrato, también es posible establecer gastos de mantenimiento de las infraestructuras. De la misma manera, el sistema tiene la ventaja de funcionar sobre infraestructuras existentes. En efecto, las capacidades de producción están suficientemente contenidas para limitar los riesgos de sobretensión, que podrían dañar gravemente la red. La facturación mensual se gestiona automáticamente.

El atractivo de esta experiencia también recibe en su génesis. TransActive Grid salió de una asociación entre Lo3 Energy, un proveedor de energía solar, y ConsenSys, una compañía especializada en la tecnología Blockchain. Por lo tanto, no es necesario tener todas las tecnologías internamente para permitir que emerja el mundo del mañana.

Hay que señalar que este sistema todavía es experimental. Sin embargo, parece ser el primer paso hacia el mítico smart grid, un sistema de generación de electricidad más cercano a los lugares de consumo para reducir los costes de producción y las pérdidas durante el transporte. Por ejemplo, en la red eléctrica española se pierde alrededor de un 10 % de la electricidad en fugas que tienen lugar durante el transporte.

El segundo punto débil de este proyecto consiste en su coste. Para un particular no es nada rentable comprar energía producida por el vecino. En España, por ejemplo, el precio de reventa de la energía solar de un particular a Endesa se eleva a 0,050 €/kWh. En 2020, cuando el particular le compra 1 kWh a Endesa, el precio de venta está fijado entre 15,18 y 15,47 céntimos (precios tomados de la página web de Endesa y utilizados únicamente para ilustrar este ejemplo).

La tercera dificultad reside en la conexión de esta red a multitud de redes. Hoy en día es muy difícil hacer migrar los actuales sistemas de producción masiva hacia modelos más restringidos, con un nivel de servicio comparable. En estos momentos no existe un sistema que pueda satisfacer el control de gestión de las tensiones en una infinidad de microgrids. Además, no hay medios para almacenar la energía eléctrica. También, si una zona de la red está averiada, en sobretensión o sufre otro problema, no puede recurrir a una forma de almacenamiento de energía viable o de reparación rápida.

La cuarta dificultad surge de las restricciones ambientales. TransActive Grid se basa en energías renovables. En la cesta de la compra, el proyecto no se plantea aumentar más del 20 % la parte de las energías renovables en el consumo medio de un hogar del barrio donde se está experimentando. Además, Nueva York dispone de una posición geográfica privilegiada en cuanto a luz solar, al contrario que Francia. El estado se encuentra en el mismo paralelo que Marruecos. La figura que aparece más abajo muestra la luz solar media de Europa en kWh/m2 (Soalrgis, 2019).

Mapa

Descripción generada automáticamente

*Irradiación solar anual en Europa. Fuente: Solargis*

La luz solar de Nueva York es comparable a la de Madrid o Rabat. El valor medio observado es de 1700 kWh/m2. En París, en el mismo período, la irradiación horizontal no sobrepasa los 1100 kWh/m2, es decir, un 36 % menos de luz solar. Por lo tanto, el potencial energético es menor.

Actualmente, los mejores paneles solares consiguen transformar entre un 18 y un 20 % de esta energía en electricidad, es decir, ligeramente inferior a 3,8 KWh/m2 a la altura de Bilbao frente a más de 5 kWh/m2 en Santa Cruz de Tenerife (Universidad de Jaén). Este nivel de energía es variable en función de la contaminación, de las nubes, de las estaciones, de las condiciones geográficas, etc. Hay que comparar esta cifra con los 9922 kWh consumidos al año por una familia española (OCU).

### b. SolarCoin: el Bitcoin de la energía renovable

SolarChange es una empresa que busca dinamizar el sector de la producción de energía renovable con particulares y empresas.

El proyecto se basa en un documento de trabajo de 2011 (Gogerty, 2011). El objetivo era darle los medios a un banco central para utilizar la energía como moneda con la finalidad de gestionar una economía. La idea original parece salir directamente de una novela de ciencia ficción postapocalíptica. Sin embargo, aunque el resultado fue decepcionante porque exigía la participación activa de un banco central, el proyecto dio lugar a otra idea.

El coautor de la documentación técnica y fundador de SolarChange apostó por una generación de energía solar con un horizonte de 40 años. Concretamente, el sistema se basa en una remuneración mediante un token llamado SolarCoin, similar al bitcoin. Se distribuye un SolarCoin por cada megavatio/hora producido mediante un panel fotovoltaico.

El límite de SolarCoins disponible se eleva a 98 100 millones. El propietario de estos tokens se llama Open Currency Association y se encarga de distribuirlos a los productores de energía. Sin embargo, para evitar la carrera hacia la potencia de cálculo y transformar el proyecto en pozos de energía, el sistema de validación de las transacciones se apoya en un algoritmo de prueba de trabajo aligerado. La validación de la generación de electricidad la hace principalmente mediante una prueba física de trabajo, es decir, lo que declara el contador a la salida de la producción.

Al principio, se minaron unos 105 millones de SolarCoins. Se minaron 500 millones de SolarCoins adicionales para atraer voluntarios, consejeros y a los grupos medioambientales. Siempre es Open Currency Association la que se ocupa del proceso de distribución de estos SolarCoins. Las modalidades, en cambio, no se conocen.

El instigador del SolarCoin, lanzado en 2014, contaba con una cotización del token de entre 20 y 30 euros en tres años (Bradbury, 2014). También esperaba utilizar la red entre pares para poder justificar la generación de energía fotovoltaica ante las autoridades locales, y así ofrecer a las partes tomadoras un medio práctico para obtener el certificado SREC (*Solar Renewable Energy Certificate*).

Se trata de un documento emitido por las administraciones públicas que ofrece ventajas fiscales. Su finalidad es estimular al sector de las energías renovables. Estos certificados se intercambian en mercados especializados, como una acción o una obligación.

Desde una perspectiva temporal, la empresa parecía tener la estrategia correcta. Por un lado, los políticos del otro lado del atlántico debatían ferozmente sobre medios rentables y duraderos para apoyar la expansión del sector de las energías renovables. Por otro lado, los pronósticos de crecimiento de Deutsche Bank sobre la creación de unidades de producción fotovoltaica eran prometedores. Apostaban por un crecimiento de 100 GW en 2015 y 2016. Además, con la desaparición de Solar Investment Tax Credit, la instalación de los paneles solares ya no estaba subvencionada a partir de 2016. Entonces, los instaladores de paneles propusieron alquilar el material anualmente, en lugar de tener que desembolsar una gran cantidad de dinero de una sola vez.

El concepto también era interesante para los productores de energía. Los SolarCoins representan un medio eficaz de recoger fondos para un sector que tiene dificultades para convencer.

En la práctica, estos estímulos no parecen haber sido suficientes. A mediados de 2019 se constató una cotización que difícilmente oscilaba por encima de los dos céntimos de euro (Solarcoin, 2019), es decir, un 50 % menos que tres años antes. Los proyectos que utilizan los SolarCoins de manera efectiva son raros y el sitio oficial de la criptomoneda no da información sobre ellos.

Aunque los mercados alemán e inglés parecían estar en expansión, tuvieron que enfrentarse a una reducción substancial de las subvenciones en vista de las dificultades económicos que atravesaron ambos países.

Parece que el único apoyo del modelo de SolarCoin es una moneda virtual, sin una integración auténtica en un tejido económico. Según las propias palabras de su creador, el uso de la red entre pares solo se ha diseñado para dar una existencia a un concepto que puede conducirse de muchas otras maneras distintas. Además, SolarCoin representa un riesgo que corren muchos proyectos asociados a la tecnología del registro descentralizado: el fracaso. Debe aportar un auténtico valor añadido para permitir que el proyecto eclosione completamente, y que sobre todo no se resuma en una criptomoneda vagamente apoyada por fondos casi inexistentes.

## **7. Videojuegos**

Los juegos representan muchos miles de millones de euros. Era inevitable que la tecnología blockchain alcanzara este sector, pero con puntos de vista muy distintos. Hay muchos intentos, algunos más convincentes que otros. Por ejemplo, el proyecto Etheria aspiraba a realizar un juego parecido a Minecraft utilizando la tecnología blockchain. El proyecto se abandonó casi inmediatamente después de su lanzamiento.

### a. UBISOFT: compra de goodies

Ubisoft es una de las grandes empresas de software de videojuegos que han marcado a muchos jugadores. De todos los sectores, el de los videojuegos es uno de los más agitados, con la necesidad de reinventarse contantemente. Hace mucho tiempo que los juegos que se compraban en la tienda en un soporte físico han pasado a ser historia. Muchas empresas de software se han lanzado a la aventura de las plataformas en línea, con una guerra encarnizada por captar la atención en menos de un minuto mediante el smartphone. En el polo opuesto, el paso a la nube es inminente, con licencias que necesitan inversiones cada vez más importantes.

Se ha descubierto e imitado un filón permitiendo intercambiar objetos virtuales por dinero real, creando, o completando, los ingresos necesarios para la continuación de los desarrollos y el mantenimiento de las plataformas de juego.

Así, League of Legends o Diablo III son ejemplos de juegos que han sabido sacar beneficio de este aspecto. El juego Fortnite supo generar él solo 2000 millones de ingresos en 2018 vendiendo objetos digitales, mientras mantenía el juego gratuito. Los juegos en el teléfono móvil no se quedan atrás, porque a menudo comprar un juego y luego desinstalarlo hace perder todos los objetos que había comprado.

El enfoque del trabajo de Ubisoft es ofrecer comprar objetos virtuales, si es posible no fungibles, pero intercambiables en la plataforma para permitir que los jugadores los intercambien entre ellos. Todavía no se sabe a qué juegos se aplicaría la tecnología, pero se daría prioridad a licencias nuevas para evitar empañar la imagen de los éxitos (Bloch, 2019).

El proyecto en curso consiste en utilizar la tecnología Ethereum, y especialmente en usar las propiedades no fungibles ofrecidas con los smart contracts ERC721. No se conoce el tamaño del equipo que trabaja en el tema. Sin embargo, los primeros trabajos habrían empezado a finales de 2018.

La empresa prosigue con su estudio y solicita empresas emergentes con experiencia en la tecnología (Ubisoft, 2019). A mediados de 2018, la empresa ya había organizado un hackathon llamado *Blockchain Heroes*. Entonces el Strategic Innovation Lab de Ubisoft había creado un prototipo de juego en blockchain.

El futuro promete ofrecer una serie de tentativas que aportarán muchas enseñanzas.

### b. XBOX: gestión de los derechos de autor

El sector de los videojuegos se ha alejado de la dimensión: una consola seguida de algunas empresas de software. Las plataformas de Sony o incluso de XBOX ofrecen una amplia gama de videojuegos que corresponden a casi todas las necesidades. Cuando un cliente descarga un juego en la plataforma, esta última debe pagar derechos de autor a la empresa de software.

El procedimiento de remuneración se ha complicado mucho durante la última década, tanto en el plano legal como en el contractual.

Las empresas de software han aumentado mucho la cantidad de controles y auditorías para garantizar los ingresos correspondientes a la descarga de los jugadores. En algunos casos, los ajustes terminan ante los tribunales con una multa y honorarios nada despreciables.

Para actualizar la gestión comercial del pago de los derechos de autor, XBOX, en asociación con la consultora Ernst and Young, lanzó un prototipo en la plataforma Azure utilizando la tecnología Quorum. El equipo evitó elegir Hyperledger de manera deliberada, porque se considera que su implantación es muy compleja. El ecosistema se ha limitado deliberadamente a dos empresas de software, con el objetivo de pasar a veinte en muy poco tiempo (Ducellier, 2018).

Las observaciones de la experiencia son positivas y proporcionan transparencia a los actores de la red blockchain. El proceso ha pasado de 45 días para la tramitación de contratos y el pago de derechos a unos minutos. El recurso a las auditorías tiende a disminuir en gran medida, porque la tecnología utilizada garantiza el esfuerzo.

En el futuro se plantearán muchas preguntas, como el paso a otro nivel y la aceptación de las empresas de software de utilizar esta tecnología para garantizar la gestión de los derechos de autor.

## **8. Finanzas**

Según el estudio de McKinsey mencionado al principio de este apartado, el sector financiero es uno de los que más está creciendo. Algunas tecnologías parecen sacar ventaja a otras. En 2015 las instituciones financieras empezaron a trabajar con la tecnología Ethereum. Desde entonces, las soluciones se han diversificado y especializado. Han aparecido planteamientos nuevos. Las iniciativas con tan numerosas que necesitarían un libro entero. Hemos elegido algunos proyectos que tienen el poder de influir en el sector.

### a. R3CEV: un ejemplo de consorcio bancario en torno a blockchain

Los bancos intercambian datos confidenciales con regularidad, mediante modalidades muy distintas en función del tipo de institución. Los bancos de mercados de capitales y financiación intercambian grandes volúmenes de dinero y de datos fuera de los mercados. Un banco medio recibe alrededor de 50 terabytes de datos al día, y el flujo aumenta cada año. Desde hace muchas décadas, estas instituciones recurren a la automatización de manera masiva, pero los problemas de correspondencia entre flujos siguen siendo muy importantes. Por ejemplo, un operador financiero en sala de mercados organiza transacciones.

Un contable en el back-office escruta, valida y firma las transacciones. Sin embargo, un operador financiero funciona por cartera, es decir, por agrupación de varios tipos de productos financieros. El contable trabaja por familia de productos. La división genera variaciones tanto positivas como negativas entre lo que el operador financiero ha organizado y los que el contable recibe en sus sistemas. Un departamento, por ejemplo, de comercio con volatilidad, puede constatar cada mes diferencias del orden de 3000 millones en valor absoluto.

Para este fin, han surgido trabajos nuevos: middle-office, que en parte tiene la función de hacer la reconciliación informática. Las instituciones bancarias tienden a externalizar la parte back-office y buscan reducir los efectivos de middle-office, percibidos como centro de costes. Además de esta complejidad, el intercambio de datos entre dos organismos implica sistemas de referencia distintos, y la convergencia contable entre los dos no siempre es trivial y genera retrasos. En concreto, entre el momento en que se concluye la transacción y su pago, el retraso máximo legal es de dos a tres días en general en Europa. Eso también genera una gestión de la tesorería no ajustada a la gestión del valor.

Este planteamiento pragmático a corto plazo oculta ambiciones a medio plazo mucho más elevadas. En efecto, los especialistas financieros piensan encontrar en él un gran interés gracias a las prometidas reducciones de costes de transacciones transfronterizas. Estas economías podrían beneficiar sensiblemente al mercado de divisas y de ventas. Más allá de estas consideraciones de costes, Thomson, por ejemplo, estima que una gran cantidad de fondos durmientes utilizados como garantía podría volver a ponerse en circulación en el mercado.

Parece existir una relación entre el valor monetario de una divisa, los swaps y los futuros, tres familias de productos utilizadas en el sector financiero. Comprender mejor esta relación puesta de manifiesto por la tecnología causaría el efecto de reducir las necesidades de depósitos de garantía entre las partes tomadoras durante los intercambios internacionales. Esta liberación de recursos podría dinamizar las economías de todo el mundo. Para hacernos una idea, en junio de 2019 pasaron unos 360 000 millones de euros por las plataformas de intercambios del grupo Thomson Reuters. La liberación de un 1 % podría tener consecuencias nada despreciables.

Los futuros productos cuyo precio deriva de un subyacente (p. ej.: acciones bursátiles, barril de petróleo, etc.). A menudo se utilizan para protegerse del riesgo de pérdida de dinero en una transacción. Los swaps son productos derivados que permiten a los dos participantes del contrato intercambiar el rendimiento de un activo en su posesión.

En lo que respecta a la financiación internacional, las ganancias potenciales son sustanciales, al igual que pueden parecer inciertas. Este sector implica números actores: importadores, exportadores, transportistas, agencias gubernamentales (por ejemplo: aduanas y ayudas al crédito para exportación), aseguradoras, y muchos otros. En cada etapa, se copia una cantidad importante de documentación en varias ocasiones, a veces con errores, con mucha frecuencia a mano, con estándares casi inexistentes, sino muy distintas de un país a otro. De todo ello resulta un empleo de recursos que muchos empresarios preferirían no tener que soportar.

En este contexto de una gran complejidad con muchos intervinientes, los bancos se han agrupado en un consorcio para definir estándares nuevos y crear una tecnología inspirada en blockchain. Esta última tiene la misión de responder a problemáticas de trazabilidad de los activos y de intercambio protegido de los documentos. La confidencialidad es el parámetro más importante a tener en cuenta.

La ambición es grande, teniendo en cuenta que ya existe un cierto número de tecnologías en el lanzamiento del consorcio.

R3CEV es la base de una fintech estadounidense, es decir una empresa emergente especializada en la elaboración de nuevos productos financieros con ayuda de tecnologías de vanguardia. Aunque Digital Assets, su competidor directo, es un actor de peso, no parece tener los mismos apoyos y socios. Fundada en 2015, en un tiempo récord ha conseguido reunir más de un centenar de actores importantes. Su estrategia es empezar por la creación de una tecnología, llamada Corda, y luego formular arquitecturas. En una segunda fase, su ambición es crear prototipos utilizables que puedan establecer una comunicación entre las distintas entidades financieras. Por último, en una tercera fase, el consorcio planea poder incluir a sus socios comerciales y utilizar lo mejor posible las oportunidades de la tecnología.

Corda es una solución estable, robusta y se mejora constantemente. Esta tecnología de registro distribuido no es una blockchain. Sin embargo, hay muchos proyectos en desarrollo, y algunos en producción. Por ejemplo, la institución financiera llamada CBA (*Commonwealth Bank of Australia*) ha llevado a cabo tres proyectos piloto, uno de ellos consiste en medir en tiempo real el índice de humedad dentro de un contenedor que transporta algodón. A continuación, los datos se envían por GPS a los actores relacionados (aseguradoras y compradores). En este caso la tecnología Blockchain sirve para confirmar la veracidad de la información y para proporcionar una red global (Eyers, 2016). La solución ha resultado ser concluyente hasta el punto de empujar a la empresa a crear un centro de excelencia y lanzar muchas iniciativas 2018 sobre el transporte de materias primas (CBA, 2019). Durante 2019, se ha dedicado a la trazabilidad de los metales, de los que Australia es un exportador importante.

La empresa en el origen de esta tecnología está al nivel de una empresa emergente, pero ya tiene casi 200 empleados en el mundo. El proyecto de crear «contratos maestros» como si fueran un calco es un éxito, pero no parece utilizarse. Las próximas evoluciones están relacionadas con un aumento del rendimiento, así como la adición de una propiedad particular para añadir a los smart contracts: la propiedad ricardiana. Se trata de un método para grabar un documento bajo la forma de un contrato a los ojos de la ley con emisión de valor, para luego vincularlo de manera protegida a otros sistemas (p. ej.: contables). Por último, el objetivo anunciado es el de proteger al máximo estos contratos contra cualquier forma de ciberataque.

### b. Qiwi: del pago por criptomoneda a la banca especializada

Qiwi es una fintech rusa especializada en pagos electrónicos y líder en su mercado. La compañía tiene unos 1400 empleados, y su volumen de negocios era de 435 millones de euros en diciembre de 2018 (Qiwi, 2019). En ella también participa Accenture, una consultora internacional. Los otros miembros son B&N Bank, MDM Bank, Bank of Khanty-Mansiysk y Tinkoff Bank.

Actualmente, la empresa Qiwi permite realizar pagos de manera intuitiva utilizando la tecnología blockchain. El proceso es sencillo: solo hay que registrar un número de teléfono y asociarle una tarjeta Visa. Luego, la aplicación se ocupa de los pagos en línea si pedir ninguna contraseña, e igualmente permite las transferencias inmediatas una vez introducidos datos bancarios de la otra parte. Sin embargo, esta última condición no es obligatoria.

El argumento publicitario reside en la posibilidad de efectuar una transferencia de dinero sin conocer los datos bancarios del contacto, siempre y cuando se conozca su número de teléfono y esta persona esté afiliada a Qiwi.

El coste del servicio también es comedido. El servicio retiene un 1,6 % de comisión por transacción, con un mínimo de 100 rublos (alrededor de 1,42 euros). Por el contrario, en un banco francés los gastos son una media de 3,30 euros de gastos fijos para un giro ordinario, es decir, más lento. A este importe puede añadirse una parte variable en función de los organismos bancarios. También es posible hacer la transferencia por Internet de manera gratuita, pero hay que esperar dos semanas de media para que el conjunto administrativo esté operativo.

La tecnología utilizada no se ha revelado abiertamente y el proyecto parece haber fracasado. Más allá de la comunicación, ningún rastro real parece vincular los pagos en línea con una criptomoneda.

A pesar de todo, Quiwi ha intentado crear su propia criptomoneda, llamada *BitRubble*. El contexto legal es especialmente hostil para las criptomonedas, que hacen que el estado pierda poder económico. El estado es el único que tiene derecho a emitir moneda, induciendo así un efecto de inflación incontrolado. El esfuerzo ha sido en vano con las presiones legales, pero la documentación técnica está disponible en línea.

En 2016, Qiwi parecía ser mucho más ambicioso que R3CEV, la opción estadounidense. Por ejemplo, la Fintech apostaba por la capacidad de realizar liquidaciones en cinco años con ayuda de la tecnología Blockchain (P.Rizzo, 2016).

En 2019, R3CEV se lanzó a un desarrollo de esta naturaleza (contratos con la propiedad ricardiana), pero ninguna de las dos parece haber alcanzado esta finalidad.

Este proceso puede parecer sorprendente. A nivel de un organismo financiero, las liquidaciones corresponden a asegurarse de entregar valores o depositar fondos siguiendo las limitaciones técnicas, legales y administrativas. Para comparar, implantar un sistema de gestión contable conocido, controlado y poco específico en una institución puede costar tres años. En comparación con lo que se puede encontrar con el consorcio anglosajón, las soluciones desarrolladas por Quiwi están en producción, es decir, operativas y utilizadas, y siguen siendo relativamente accesibles desde un punto de vista técnico.

Finalmente, en junio de 2018, la alta dirección de Quiwi se lanzó a una nueva aventura: un banco de inversión especializado en criptomonedas. Esta institución, llamada HASH, tiene la misión de ofrecer servicios de ayuda a las recaudaciones de fondos de tipo ICO, consejo a las instituciones deseosas de aplicar la tecnología a su empresa y ayuda técnica (Baydakova, 2018).

Este ejemplo muestra un entusiasmo y un intento de los actores de hacer que blockchain penetre, especialmente como mecanismo de pago. El proceso siempre parece ser mal percibido en la mayoría de los países del mundo, que ven en él una amenaza a la hegemonía de la distribución de las divisas. Hay que destacar que el motivo no es necesariamente imperialista. Las divisas se apoyan en mecanismos de estabilización económica. Las criptomonedas no se apoyan globalmente en ningún contravalor real y por lo tanto son presa de numerosos abusos por parte de sus inversores y usuarios.

### c. Emisión de deuda

El mercado de la deuda representa muchos cientos de miles de millones de euros a nivel mundial. Las empresas y los estados ofrecen valores financieros que pagan una suma de dinero periódica llamada cupón, a cambio de una inversión inicial. El proceso implica totales muy importantes (varias decenas de millones de euros), y la venta de los valores obligatoria necesita recurrir a muchas instituciones.

La gestión administrativa es muy laboriosa, implica una gran cantidad de actores y las restricciones legales asociadas son importantes. En el lado opuesto, la entidad que emite la deuda se enfrenta a auditorias habituales para garantizar la solvencia de la empresa y su capacidad de restituir los fondos cuando termine el período de la obligación.

Este contexto es un terreno fértil para la implementación de la tecnología blockchain. Por eso el Banco mundial ha emitido por primera vez los Bond-I (*Blockchain Operated New Debt Instrument*, Nuevo instrumento de deuda operado por Blockchain), que son una versión de una obligación que utiliza blockchain.

Técnicamente, la solución está alojada en la nube Azure y se utiliza una versión privada de Ethereum. En el comunicado no se precisa si se trata de Quorum o de una instancia privada de Ethereum (EEA). Los equipos de la CBA (*Commonwealth Bank of Australia*) han dirigido e implantado la solución a través de su área de experiencia (Leclerc, 2018).

La recogida de fondos ha sido un éxito, porque ha habido más demandantes que ofertas disponibles. La suma representaba 69 millones de euros. En efecto, este importe es una gota de agua para la institución, que recoge cada año entre 50 000 y 60 000 millones de euros mediante la emisión de obligaciones, pero facilita el camino hacia una automatización mayor del proceso. No hay información de las ganancias estimadas. Sin embargo, las líneas directrices incluyen una mejora de la trazabilidad de los fondos, más facilidad para la distribución de los capitales y una reducción de la carga administrativa. Seguramente la etapa de conocimiento de la identidad de los inversores físicos ha sido una parte importante del esfuerzo para permitir la venta de los Bonds-I.

En paralelo, la ciudad de Berkeley planea muy seriamente hacer una emisión de deuda municipal, sin precisar el plazo. La ciudad alberga especialmente un laboratorio especializado en blockchain, asociado a las iniciativas Corda, Ethereum e Hyperledger.

### d. WeTrade: facilitación de la financiación internacional

El sector del comercio financiero es uno de los que más recibe la influencia de la tecnología. Los desafíos humanos y técnicos provocados por la globalización son innumerables. Por ejemplo, la transferencia de divisas transfronterizas puede exigir primas de un 30 %. Algunas divisas no pueden abandonar el país, transformando el ejercicio de importar/exportar en una auténtica acrobacia. Al atravesar fronteras hay más de pesadillas que formalidades. Por ejemplo, hacer salir un producto manufacturado de la India y luego reenviarlo a la India por defecto de conformidad, obliga al exportador a pagar la tasa dos veces. El país no está equipado para reconocer los productos que vienen de su interior. Los legajos no concuerdan entre países, a veces tienen una adición, a veces una eliminación de información y muy a menudo problemas de estandarización. La búsqueda de financiación internacional está en la encrucijada de estas dificultades y las empresas de tamaño medio son las grandes perdedoras. A menudo, estas últimas no pueden pagar los servicios de un departamento de virtuosos encargados de un desarrollo correcto y del pago de las mercancías.

Es precisamente en este preciso segmento donde se ha formado un consorcio rebautizado WeTrade. Al inicio, este último agrupaba a Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Société Générale y UniCredit. Después, el grupo pasó a tener catorce miembros. Con la ayuda de IBM como consejera y prestataria del servicio, creó una plataforma con el objetivo de gestionar, hacer un seguimiento y proteger las transacciones y los intercambios entre las pequeñas y medianas empresas. Así, mediante una suma razonable, un cliente puede hacer un pedido, gestionar las condiciones contractuales, asegurar los bienes a intercambiar y garantizar el pago cuando las condiciones lo requieren, sin recurrir a un tercero de confianza. La plataforma está disponible 24 horas al día y 7 días a la semana (Manders, 2017).

Solo pueden utilizar el servicio los clientes de estos bancos. Los bancos tienen ciertas obligaciones normativas, especialmente garantizar la solvencia de las empresas, y garantizar, por ejemplo, que los fondos vinculados a la transacción no han sido obtenidos ilegalmente. Este procedimiento, llamado KYC (*Know Your Customer*) está en curso de digitalización con un uso compartido parcial de información entre los bancos.

La solución está instalada en múltiples nubes con Hyperledger Fabric, todos los bancos disponen de una copia del registro. El trabajo de preparación ha sido importante, con una modificación de los métodos de trabajo y de las maneras de pensar de los socios.

La creación de un consorcio y de la plataforma ha revelado los desafíos clásicos del trabajo colaborativo entre las distintas empresas. Las restricciones parecen haberse aplicado primero al aspecto humanos antes que al técnico. Además, para facilitar el proceso de gestión, se ha creado una empresa conjunta que percibe periódicamente los fondos de las distintas empresas fundadoras para garantizar el buen funcionamiento de la plataforma y su evolución. Un comité de gobernanza decide las evoluciones.

Se lanzó en pruebas en febrero de 2018, la plataforma funciona, pero no se ha informado de ninguna cifra en cuanto a su éxito. Los desafíos son colosales, porque las pymes representan una parte creciente del comercio internacional. La demanda es importante y las soluciones técnicas que facilitan el acceso a los mercados extranjeros darán inevitablemente una ventaja económica a las empresas que utilizan la plataforma.

La plataforma es joven, pero el paso al siguiente nivel parece desarrollarse con normalidad. El futuro de la plataforma está garantizado si y solo si encuentra su público. El planteamiento concertado que responde a una necesidad del cliente y lo coloca en el centro de las preocupaciones, parece ser una garantía de éxito.

### e. Banco privado

Desde hace mucho tiempo, la industria financiera ha sido una de las pioneras en la innovación, especialmente en cuestiones digitales. La actividad está estrechamente vinculada a verificaciones de conformidad y a un trabajo meticuloso, ambos realizados por numerosos especialistas. En paralelo, la actividad se centra fundamentalmente en la creación de un mercado. El objetivo de un banco privado es ofrecer soluciones de inversión más rentables e igualmente más arriesgadas que las soluciones clásicas que se pueden encontrar en las bolsas europeas. Una gran cantidad de empresas prefieren quedarse en el segmento de la banca privada para recaudar fondos en lugar de cotizar en bolsa. En efecto, no siempre se obtiene el entusiasmo de los inversores, las obligaciones legales son importantes y los gastos elevados.

El mercado de los bancos privados se ha transformado durante las dos últimas décadas. Los competidores ya no están en París, sino en Hong Kong. El abanico de competencias también ha aumentado sensiblemente, con una necesidad de comprender en detalle los mercados y las necesidades de los clientes. Del mismo modo, los clientes acaudalados tienden a estar ya asignados, o bien se agotan con el desarrollo de las empresas. Es necesario encontrar relevos de crecimiento o buscar mercados nuevos.

En este contexto, blockchain utilizada de manera juiciosa permite crear oportunidades. La empresa emergente Smart Valor, por ejemplo, ofrece un servicio de tokenización de activos reales, que reduce en gran medida los costes administrativos. Los inversores que disponen de menos de un millón de euros, ticket de entrada generalmente admitido, pueden invertir en empresas deseosas de aumentar su actividad. Los formularios de adhesión están completamente automatizados, los controles se hacen mediante smart contract y la gestión de la propiedad está respaldada por un token criptográfico no fungible.

Este tipo de oferta aumenta en el mercado parisino, especialmente desde la llegada de la ley Pacte, que define un marco legal dentro de la gestión de activos criptográficos. Las soluciones técnicas son muy variadas. Las más prometedoras, especialmente aceptadas por grandes grupos como BNP Paribas, parecen centrarse en la tecnología Corda.

En la práctica, no hay grandes cambios, porque se trata de un punto de vista legal de una titulización, innovación financiera de principios de siglo. La innovación trata sobre todo de una reducción de los costes y una apertura a clientes nuevos. La adopción por los mencionados clientes todavía es una cuestión en suspenso.

## **9. Gestión de la identidad**

El sector de la verificación de la identidad es un mercado con un peso de muchos miles de millones de euros anuales. Por su naturaleza, algunas empresas se han especializado en la lógica de gestión de la identidad y facilitan el trayecto de un usuario. En algunos casos, la gestión de la identidad es nativa. El caso de las blockchains permisionadas exige poder utilizar los directorios de empresa y establecer una interfaz entre las dimensiones criptográficas de la solución de registro distribuido y los sistemas de gestión de identidad existentes.

### a. Ledger: el wallet físico

Desde 2008 y la llegada del bitcoin, han aparecido muchas criptomonedas. En 2019 se contabilizaron más de dos mil. Para un usuario de la red Bitcoin, el proceso de creación de una cartera electrónica, llamada Wallet, puede ser laborioso. Hay que introducir en un documento una serie de palabras aleatorias que permiten recuperar la clave de seguridad de solo 256 caracteres aleatorios. La realización de este tipo de operación es especialmente fastidiosa cuando se repite en varias plataformas o con la aparición de una criptomoneda nueva en la que desea invertir.

Es posible conseguir la asistencia de una plataforma de intercambio en línea que ofrece conservar las claves, a cambio de identificadores de conexión, cuidadosamente guardados en el sitio. Este planteamiento es un objetivo principal de los hackers, que periódicamente sustraen de las mencionadas plataformas grandes cantidades de claves de cuenta y vacían su contenido. Los importes son sistemáticamente de varias decenas de millones de euros.

Para responder a este problema, la empresa emergente Ledger ofrece un módulo físico externo que conserva el conjunto de las claves. Este módulo, que se presenta bajo la forma de una llave de memoria USB, está protegido por una contraseña que el usuario debe configurar una sola y única vez. Luego, el ledger exige la descarga de un módulo complementario en el navegador que elija el usuario para facilitar el acceso a las cuentas del cliente y realizar transacciones son solo unos clics.

La sociedad, fundada en 2015, ha realizado muchas recogidas de fondos, entre ellas una de 70 millones de euros a principios de 2018 (Maignan, 2018) y cuenta con unos 100 empleados. Su módulo cuesta unos 100 € y tuvo éxito durante 2018. Sin embargo, cuando el frenesí de las ICO se atenuó ese mismo año, ,también lo hizo el interés por el Ledger. La solución evoluciona se atenúa poco a poco, siempre haciendo que el acceso a las distintas criptomonedas sea más fácil. Sin embargo, su integración en el ecosistema de las plataformas existentes todavía es limitada. Las grandes plataformas cómo Bitcoin o Huobu tienen su propio sistema de identificación y ofrecen de manera complementaria interfaces gráficas con funciones dignas de mercados.

### b. ICOMPLY: KYC y la conformidad de las ICO

En 2018 triunfó un nuevo mecanismo de recogida de fondos, ICO (*Initial Coin Offerings*). El modelo consiste en proponer tokens de una criptomoneda nueva a cambio de ether, su correspondiente en la red Ethereum. Sin embargo, recoger fondos exige seguir un proceso de identificación física de las personas riguroso y, si es posible, un análisis del origen de los fondos. Este proceso se llama KYC (*Know Your Customer*).

Segunda complejidad: Las plataformas de cambio especializadas en criptomoneda. Todas las principales plataformas exigen tener acceso al KYC asociado a la recogida de fondos, bajo pena de no aparecer nunca en la lista. Por último, los recientes ajustes en el plano legal han hecho evolucionar el proceso de gestión de los tokens emitidos. El seguimiento de la conformidad y de los propietarios de ciertos tipos de tokens exige un equivalente a las campañas de auditoría.

ICOMPLY es una solución del tipo Software as a Service (SaaS) que facilita este trabajo con los empresarios deseosos de hacer una ICO. Ofrecen un análisis off-chain, y luego lo sustituyen por un análisis que realiza la EVM (*Ethereum Virtual Machine*), que permite investigar las transferencias de fondos cuenta por cuenta. En la práctica, eso significa que el inversor debe pasar por una plataforma y enviar su identificación, que será controlada manualmente por un empleado. Hay muchas empresas que ofrecen este servicio, como la compañía Thesaurio. La ventaja del servicio también consiste en aprovechar la hipotética experiencia legal de la que presume la compañía, y por lo tanto del respeto a la legalidad en vigor en las distintas naciones de influencia.

Como complemento, la solución ofrece la creación de contratos ERC20, que permiten hacer la conversión entre las criptomonedas de origen y destino. Esta última etapa está sujeta a una proposición de modularidad: un token por una unidad de divisa (por ejemplo: euro), o una parte de la empresa por una unidad de divisa. Esta etapa es crucial y exige experiencia en la redacción del código. Un ejemplo es el escándalo de TheDAO, estaba relacionado con un fallo en el código que permitió al pirata informático desviar los fondos asociados a la ICO.

## **10. Gran distribución y trazabilidad alimentaria**

La trazabilidad alimentaria es un tema especialmente importante en la vida diaria de miles de millones de individuos. Se destina una cantidad importante de recursos para garantizar el origen de los productos alimentarios que llegan a nuestros platos. A los agricultores cada vez se les pide más en el plano administrativo, mientras que las grandes superficies ven cómo disminuyen sus márgenes poco a poco. De igual manera, los hábitos de los clientes están en constante evolución, con un aumento de la importancia de la calidad de los alimentos más que de la cantidad y la búsqueda desmesurada de promociones. Las normativas son cada vez más severas tras cada nuevo escándalo sanitario y hay que encontrar un delicado compromiso entre las expectativas y los recursos disponibles.

Se han lanzado muchas iniciativas en el mundo, tanto en Asia, como en los Estados Unidos o en Europa. Wallmart se posiciona como uno de los pioneros de la trazabilidad alimentaria. Aunque los hechos contradicen parcialmente esta verdad, la información destinada a restaurar la confianza de los consumidores le dio a la aplicación de blockchain otra dimensión completamente distinta.

### a. Provenance: una solución de trazabilidad de los productos alimentarios

Una de las empresas más avanzadas en este tema se llama Provenance. Ofrece soluciones de trazabilidad en el sector alimentario para garantizar la procedencia y las etapas de fabricación de un producto dado.

En la práctica, el sistema es muy sencillo. Primero hay que ir a la página web de Provenance, en la dirección <https://www.provenance.org/>. Luego se trata de crear un perfil de empresa en unos minutos.

En la página web es posible introducir información sobre la empresa, las certificaciones y distintas recompensas, si existen. Después, hay que introducir la información relacionada con los productos a los que queremos hacer un seguimiento.

Es posible conectar los productos con vínculos que redirigen a sitios web comerciales. Se ponen a disposición de la empresa pegatinas con la forma de códigos de barras QR. De aquí en adelante, se puede escanear este código de barras en cada etapa de la cadena, desde la transformación de la materia prima, por ejemplo, hasta la llegada al cliente final.

El empresario tiene libertad para elegir él mismo las etapas del seguimiento. El sistema tiene la ventaja de retomar los mismos fundamentos que los sistemas de gestión convencionales. Segunda calidad: la información transmitida es infalsificables gracias a la tecnología del registro descentralizado. La carne, declarada como producida en Argentina, por ejemplo, no se puede asociar a ningún otro sitio de producción: la información se graba en el registro. Gracias a las tecnologías de la IoT, es posible llegar hasta la geolocalización de cada etapa de transformación. Finalmente, es posible obtener la trazabilidad de las temperaturas durante el transporte de carne o el índice de humedad durante un transporte de algodón, con un coste menor.

Provenance también permite comunicarse con los consumidores gracias a una aplicación móvil. Es posible mostrar las etapas de fabricación, a elección del empresario o del artesano, y así permitir que el consumidor descubra otra faceta del producto. Este aspecto es doblemente importante. Por un lado, los estudios de marketing actuales destacan que el consumidor desea comprar mejor, y no comprar más. Está observación va desde el traje de sastre a la taza de café.

Por otro lado, este aspecto responde a las expectativas de los consumidores que buscan adoptar una visión responsable durante sus compras.

Por ejemplo, todos queremos tener la posibilidad de elegir si queremos consumir productos de proximidad como una manera de proteger al medio ambiente. Gracias a esta tecnología, es posible mostrar hasta la granja donde se crió el animal o se cultivó el cereal.

Aunque el proceso de trazabilidad parece enormemente sencillo, sin embargo, requiere una gran cantidad de trabajo por adelantado. Para ser viables, todas las etapas deben estar introducidas en el sistema.

La tecnología utiliza códigos de barras QR. Aunque tienen la ventaja de poder contener mucha más información que un código de barras clásico, no son infalibles. Su fiabilidad está alrededor del 99 % cuando se imprimen correctamente, y forman uno de los pilares del sistema de seguimiento. Así, si un producto no se ha escaneado o se ha escaneado mal, la tecnología actual todavía no permite corregir el error.

El inventario de las etapas se realiza por duplicado, porque todas las etapas no son forzosamente útiles para el consumidor final. Aunque casi un 40 % de los consumidores de supermercado comparan el precio de sus productos en los Estados Unidos (Schottmuller, 2011), saben que al escanear un paquete de cereales, es posible acceder a una parte de esta información mediante un smartphone.

Por último, técnicamente, el modelo parece funcionar en cadenas privadas. Ningún tercero valida la transacción. Entonces, es potencialmente menos fiable que si se utilizara en combinación con cadenas públicas. Algunas soluciones utilizan la doble verificación, y solo envían una parte limitada de la información. Esta etapa refuerza la seguridad, sin ser necesariamente obligatoria.

Teniendo en cuenta la tarea, actualmente solo hay muy pocas soluciones que han desembocado en una aplicación concreta. Aunque tendría la enorme ventaja de reducir drásticamente las necesidades de intermediarios y de unidades terceras de verificación. Una vez más, el próximo obstáculo no es tecnológico, sino administrativo y legal.

### b. Carrefour aplica la tecnología a la trazabilidad

Carrefour, a imagen de los grandes distribuidores, utiliza a un millón de proveedores. Eso implica una cantidad muy grande de actores y de tipologías distintas. Aunque algunos están informatizados, esta situación es una excepción. Por otro lado, la gestión contractual ha sido especialmente señalada durante los dos últimos años, el gobierno exige más transparencia y justicia en el tratamiento de los proveedores.

En lugar de lanzarse a un planteamiento más transparente de la facturación, al igual que XBOX intentó hacer en el pago de derechos de autor, Carrefour se lanzó a la trazabilidad de los alimentos. En efecto, más allá de la primera línea de proveedores, para una gran superficie es muy complicado conocer la procedencia exacta de la materia prima o de los productos envasados. Por ejemplo, una bolsa de cuatro lonchas de jamón procede de cuatro a seis animales, originarios de distintas explotaciones.

Al principio, el equipo de cinco personas utilizó la tecnología Ethereum para hacer un seguimiento del pollo de Auvergne, una región francesa, criado al aire libre. Aplicó un protocolo de trazabilidad integral a una materia prima escasamente transformada, relativamente fácil de localizar durante su PoC. Los resultados superaron sus expectativas: en lugar de esperar varios días o semanas para conocer el origen del ave, el plazo se había reducido a unos minutos.

Como la plataforma Ethereum no podía dar respuesta a los volúmenes de rastreo, el equipo cambió a Hyperledger Fabric con una solución en la nube. El prototipo se transformó en un auténtico proyecto, con la trazabilidad al día de numerosos productos, en general frescos.

Para llegar más lejos, el equipo puso a disposición de los clientes una aplicación para smartphone, que favorecía la transparencia con el cliente. Respecto a los productores, el esfuerzo no es desinteresado y mediante blockchain han encontrado un canal para comunicar sus habilidades y la calidad de su tierra. El tiempo de lectura de los productos por los consumidores supera los cuarenta segundos, algo que, respecto a la aplicación, es especialmente largo. Por último, el equipo original del proyecto solicitó la experiencia de IBM para poder estabilizar más su plataforma y mejorar el paso a un nivel superior.

En el plano económico, los consumidores también estarían listos para pagar más por los productos con una trazabilidad garantizada y accesible. Salvo rectificación, el planteamiento permite reforzar en el cliente el sentimiento de confianza en la marca. Por el momento no parece haber tenido lugar una retirada a raíz de una alerta por producto dudoso. En caso contrario, el ahorro de tiempo es especialmente grande.

## **11. Geolocalización**

A primera vista, la geolocalización asociada a blockchain puede parecer curiosa. Sin embargo, los usos son reales y las soluciones existentes no parecen satisfacer las necesidades.

### a. La geolocalización: ir más lejos que Google Maps©

Vevue Project ofrece algo completamente revolucionario, extrapolable hasta el infinito o casi. El objetivo es ofrecerle al usuario una vista de su elección mediante un vídeo de 30 segundos. La vista puede estar relacionada con un restaurante, un hotel, un evento, una visita de casa o incluso un altercado.

La aplicación necesita dos partes. La primera publicación pregunta sobre la aplicación, por ejemplo, para conocer la ocupación de un restaurante a una hora dada. Coloca la solicitud en un mapa asociado con la aplicación, escribe el mensaje de petición y vincula una suma en bitcoins para motivar a una tercera parte. La segunda parte ve la solicitud en su smartphone. Si quiere, la acepta y va a grabar el vídeo, luego lo publica en la aplicación. La persona que ha grabado el vídeo recibe bitcoins o la criptomoneda específica de la aplicación.

La aplicación funciona y se orienta hacia una lógica de red social que remunera a los actores. La aplicación está disponible en Google Play Store, así como mediante la extensión que se ofrece en Google Chrome. Las vistas están disponibles cuando el navegador de internet utiliza Google Maps para encontrar tiendas o restaurantes.

Ahora imagine la aplicación de esta tecnología combinada con los últimos avances de los laboratorios de Google bajo la dirección de John Flynn. Gracias a los algoritmos y a partir de una cantidad limitada de fotos (al menos dos), desde ahora es posible recrear un lugar en 3D con la realidad virtual (Flynn, 2015).

Desde un punto de vista técnico, la dificultad se resume en el almacenamiento de los minivídeos y en la manera de encontrarlos. Hay muchas probabilidades de que la aplicación utilice el componente Swarm de la plataforma Ethereum.

Para la transferencia de las criptomonedas, actualmente las carteras y el sistema de transferencia se han probado desde hace varios años.

Los posibles defectos de esta aplicación, en Francia o en Alemania, por ejemplo, afectan con mucha precisión a algo de lo que se arrepienten en Google Maps: una vida privada seriamente amenazada. Por el momento, la aplicación no parece difuminar los rostros, las matrículas u otras informaciones consideradas sensibles. Tratándose de una DAO, se supone que el trabajo de moderador deben hacerlo las funciones de la aplicación y no una persona. Se corre el riesgo de que las administraciones y legislaciones estatales exijan un trabajo importante de Machine Learning.

### b. Naviaddress: la blockchain para mejorar el sistema de las direcciones postales

El sistema de direcciones postales puede ser muy distinto de un país a otro. En Japón, por ejemplo, el acceso al sistema no es fácil a primera vista. Por otro lado, entre los 7000 millones de personas, cuatro no tienen ninguna dirección física. Por último, entre las direcciones disponibles, alrededor de un 20 % no están verificadas.

Para un distribuidor de mercancías, la situación puede plantearle serios problemas de logística. Las direcciones no proceden del sistema de coordenadas GPS (latitud y longitud) que, sin embargo, es necesario para optimizar el tránsito en un contexto de ciudades congestionadas, y donde la entrega tiende a predominar sobre el desplazamiento del cliente a la tienda.

Naviadress es una empresa emergente fundada en 2015, ubicada en Rusia, que ofrece geolocalizar cualquier sitio. Utiliza el sistema de coordenadas que hemos mencionado antes y le añade un código de dirección. En la práctica, un cliente de la aplicación inscribe su dirección, describe el camino para llegar allí, y luego lo envía a quien corresponda.

El principal interés para un transportista es tener la seguridad de que una dirección existe sin sombra de duda. El del cliente es más moderado si se encuentra en un entorno bien definido (p. ej.: en una ciudad grande). La situación cambia en el caso de un cliente más desfavorecido. Por eso, las compañías Uber y DPD, especializadas en el transporte de personas y de mercancías respectivamente, han lanzado prototipos para evaluar el interés de la tecnología.

Sin embargo, quedan muchas preguntas por responder. Las empresas ya ofrecen un identificador único, aunque no siempre vinculado a una geolocalización. Así podemos citar la solución del código DUNS. Las empresas de un cierto tamaño ya tienen una referencia interna. No se ha mencionado la integración en sus sistemas existentes, pero a menudo es un trabajo importante. A menudo, la caracterización de los sitios es al menos tan importante como su geolocalización. Por ejemplo, en un contexto industrial, una fábrica se caracteriza de manera notoria por más de un único punto de entrada.

El equipo creó la tecnología que se ha utilizado, se hizo una recogida de fondos mediante una ICO. Su ambición es crear una plataforma mundial nueva para la gestión de las direcciones. De algo tan sencillo como el direccionamiento, se derivan auténticos modelos de negocio y los proveedores de soluciones GPS pagan sumas enormes para obtener esa información. Es posible que la empresa emergente suministre un estándar a menor coste en los próximos años.

## **12. Inmobiliaria**

Hay muchos intentos en el sector inmobiliario, pero se perfilan tres tendencias:

* la desintermediación en la lógica de alquiler de un bien;
* la venta de productos inmobiliarios;
* la gestión de soluciones inmobiliarias.

El primer caso tiene éxitos moderados, especialmente con Slock.it. Se trata de la misma compañía que permitió pagar la recarga de vehículos eléctricos anteriormente citada. La gestión de soluciones inmobiliarias parece estar en un estado  embrionario. La idea es hacer dos funciones por turnos: gestionar los contratos de servicio, muy numerosos en la gestión de las residencias, o si no certificar que ha tenido lugar un evento.

Durante las dos últimas décadas, el sector de la venta inmobiliaria se ha enfrentado a innovaciones periódicas, hasta el punto de que la actividad clásica de agente inmobiliario está en serias dificultades. Los desafíos económicos son muy importantes y la mínima venta le garantiza al agente comercial una comisión sustanciosa.

Los compradores, al igual que los vendedores, tienen a buscar la emancipación del coste asociado al intermediario. Las plataformas en línea ofrecen actividades análogas en respuesta a estas expectativas. La profesión se moviliza y alguna plataforma creada para operar entre particulares ha sido perseguida en los tribunales por ejercicio ilegal de la profesión, por ejemplo.

Muchos países han experimentado la venta de bienes reales, especialmente de apartamentos, con un éxito moderado y anulaciones, porque el país no siempre estaba dispuesto a participar en el ejercicio, por diversos motivos. Sin embargo, podemos citar dos casos de éxito: la venta de un hotel de la estación de esquí en Aspen (Colorado) y la venta de apartamentos en Manhattan en 2018. Las sumas involucradas eran de 14 millones de euros y 27 millones de euros respectivamente

En España, en octubre de 2020, se ha aprobado el Proyecto de Ley de Medidas de Prevención y Lucha contra el Fraude Fiscal que implica la obligación de declarar y suministrar información sobre la adquisición, transmisión, permuta, transferencia, cobros y pagos de criptomonedas (ASEPYME)

En la práctica, se ha utilizado la tecnología Ethereum. Para realizar la operación se ha usado la lógica de los tokens no fungibles. Así, una parte es única y distinta de la otra.

Se han emitido diez tokens, cada uno fraccionable en 100 000 subunidades y fácilmente intercambiable en el mercado secundario por un valor unitario de 6,5 €. La principal ventaja mencionada es la liquidez. En efecto, un hotel es en sí mismo un activo inmobiliario con una liquidez muy débil. El proceso de titulización permite llegar a un público mucho más amplio que los circuitos tradicionales. Así, pequeños usuarios pueden invertir en ladrillo, mientras que normalmente hacía falta un mínimo de 500 €. Sin embargo, por el momento el objetivo no es reducir los costes administrativos asociados a la venta de un activo inmovilizado.

## **13. Logística y cadena de suministro**

De todos los casos de uso posibles, es innegablemente el sector más mencionado cuándo se habla de campos de aplicación de blockchain. En la encrucijada de muchos caminos y dando lugar a mucho trabajo manual, la tecnología encuentra su lugar sin limitaciones. Una parte importante del trabajo de un logista consiste en confirmar información, manejar con destreza los distintos estándares y garantizar que todos los actores tienen la información correcta. La gestión de las facturas también es un desafío muy importante, porque si un transportista emite la factura, relacionarla con una entrega puede ser muy difícil. El uso de la tecnología puede reducir los riesgos vinculados a la facturación, aumentar la transparencia y responder a las obligaciones legales cada vez más importantes en nuestra sociedad que se judicializa.

### a. TradeLens: la cadena de suministro aumentada

La logística a nivel internacional es un quebradero de cabeza diario. Los documentos varían, las exigencias evolucionan en función del sitio, los socios a los que hay que mantener al corriente son muy numerosos. Los volúmenes son vertiginosos, con más de 15 trillones de euros de mercancía entregada entre fronteras. Sin embargo, la información y las organizaciones siguen estructuradas en vertical, los procesos de recepción y de envío son manuales y muy a menudo en formato de papel. La verificación en las fronteras es igualmente larga y fastidiosa, siempre dejando poco margen de maniobra a los aduaneros para evitar los fraudes. Por último, las repetidas dificultades, los imprevistos y la incapacidad de poder planificar eficazmente la recepción de los bienes jalonan el día a día de los profesionales de la cadena de suministro.

En este contexto, el grupo de transporte marítimo Maersk, asociado con IBM, empezó a construir un prototipo a finales de 2017 para responder a las limitaciones bien conocidas de los operativos. En primer lugar, el valor de solución se traduce dentro de su ecosistema. Los transportistas marítimos, los puertos, los operadores intermodales (p. ej.: camión o tren) y las autoridades (p. ej.: aduanas) se reunieron en torno a una solución técnica común. Segundo punto fuerte: normalización de las etapas desde el sitio de carga hasta el sitio de la entrega. Se contabilizan 120 tipos de eventos disponibles. La estandarización también tiene lugar a nivel de las interfaces técnicas y de las informaciones proporcionadas.

El acceso a la información se hace mediante el intermediario de funciones. La información está compartimentada y la documentación describe la implementación de un nudo de la red para cada actor. Esta arquitectura técnica facilita la segregación de los datos entre los distintos actores. A mediados de 2019, la solución contaba con más de un centenar de empresas participantes, que representaban a casi la mitad de los contenedores que transitan por mares y océanos. En materia de valor, una parte importante está automatizada, reduciendo por igual el coste administrativo. Por ejemplo, para obtener un conocimiento (documento de embarque), el coste acumulado es de 90 €, contra 12 € con esta solución.

La solución técnica se basa en la tecnología Hyperledger Fabric, alojada en la solución en la nube de IBM llamada Bluemix. Las inversiones necesarias han debido ser gigantescas, pero el resultado está ahí. En cuanto a rendimiento, la plataforma está en condiciones de soportar 10 millones de eventos por semana, así como 100 000 documentos en el mismo intervalo.

En el mundo se lanzan numerosas iniciativas para bloquear la progresión de TradeLens. La solución no es una copropiedad, si no propiedad exclusiva de sus instigadores. Para utilizar el sistema, es necesario formar parte del consorcio, o ser cliente de uno de sus miembros. El uso de la tecnología no solo ha creado nuevos negocios o reducido los costes, ha permitido crear un semimonopolio para su propietario y una ventaja económica real frente a la competencia.

### b. Volkswagen y la trazabilidad del cobalto

En un contexto de calentamiento climático y mejora de las condiciones de vida de los ciudadanos, las materias primas son el objetivo de cada vez más limitaciones.

Algunas son especialmente tóxicas y tratamos de separarnos de ellas progresivamente. En otros casos, las zonas de extracción son especialmente sensibles y se busca garantizar que se han respetado las condiciones contractuales. En un último caso, el argumento es puramente comercial, especialmente en el caso del comercio justo.

Algunos minerales estratégicos son absolutamente necesario para el buen funcionamiento de nuestras industrias y de nuestros modos de vida. Con la descarbonificación de nuestra sociedad para 2050, es urgente reducir el uso de ciertas tecnologías, como el motor de combustión, en beneficio de tecnologías consideradas más neutras, como las baterías de iones de litio. Uno de los problemas principales consiste en hacer un aprovisionamiento responsable, y el cobalto es uno de estos minerales estratégicos fundamentales para la fabricación de las baterías de iones de litio. El problema es, según Amnistía Internacional, que estas baterías de iones de litio parecen estar vinculadas a violaciones de derechos humanos, especialmente al trabajo infantil en la República democrática del Congo.

La sociedad Volkswagen se ha unido a una iniciativa abierta en el sector de la automoción durante la primera mitad de 2019 (Coronel, 2019). El objetivo es seguir al cobalto, y realizar una trazabilidad desde la mina hasta el final de su vida. Las baterías de iones de litio son muy contaminantes si se dejan en la naturaleza.

El proyecto todavía está en una fase embrionaria, pero usará la tecnología Hyperledger Fabric. Desde principios de 2019, en la industria pesada emergen con regularidad proyectos de este tipo con problemáticas reales de trazabilidad intercontinental entre múltiples partes. Serán auténticos desafíos de normalización.

## **14. Lujo**

Actualmente, vivimos en un mundo que nos permite comprar cada vez más productos en línea. Pero todo esto no hace sino aumentar el riesgo de comprar objetos falsificados. La introducción de la tecnología Blockchain en el sector de fabricación está destinada a la lucha contra las falsificaciones, que se ha convertido en un problema principal dentro del sector de los productos de lujo.

Algunos objetos de lujo ya tienen un número de serie. Eso les convierte en candidatos ideales para una herramienta vinculada al registro descentralizado. Así se podría almacenar la fecha de fabricación, el nombre de la persona que ha ensamblado el objeto y todo el historial. Durante toda la vida del objeto, también podría almacenarse el nombre de los distintos propietarios.

Eso permitiría conocer el historial de un vehículo o saber si un objeto, comprado porque perteneció a una celebridad, realmente perteneció a esta persona.

Igualmente es posible integrar un historial de reparaciones para poder hacer una compra con total transparencia. Eso haría que los certificados físicos en papel fueran inútiles. Podríamos tener algo así como un súper certificado, donde apareciera todo el historial del objeto. El propietario de este súper certificado no podría perderlo nunca y tampoco podría ser falsificado por un posible falsificador. Esto podría proponerse bajó la forma de un servicio ofrecido por una marca de lujo para que sus productos no pierdan valor al imitar las falsificaciones. La trazabilidad garantizaría la autenticidad.

Las compañías utilizan blockchain para garantizar la seguridad digital de las obras de arte. Estos certificados electrónicos almacenados en blockchain pueden verificarse instantáneamente. Los artistas y coleccionistas podrán utilizar la tecnología del registro distribuido para documentar, verificar y certificarlas obras. Al almacenar en la blockchain un valor de hash único para cada obra, eso permitirá distinguir con total seguridad y transparencia las obras reales de las copias.

Una empresa emergente llamada Chronicled ha terminado un tipo nuevo de prueba de propiedad y de autenticidad para los bienes materiales. En este ejemplo, la empresa cliente está en el sector del calzado de lujo. El principio es sencillo: sustituir la clásica prueba de autenticidad imprimida en papel por un chip.

Con ayuda de una aplicación, la firma electrónica presente en el chip se vincula a usted de forma permanente en la blockchain Ethereum. No es solo que el chip no se pueda copiar, sino que la carpeta de la propiedad no se puede modificar. En el caso de la implantación de la trazabilidad en el sector de lujo, la idea es sacar provecho de las cualidades de centralización y de inviolabilidad de la blockchain para realizar este tipo de proyectos.

Por otra parte, el grupo LVMH ha lanzado un producto nuevo, llamado AURA. El objetivo es ofrecer una solución de trazabilidad y de certificación de autenticidad basada en la blockchain de los productos realizados por sus marcas Luis Vuitton y Christian Dior. La plataforma, lanzada en junio de 2019, todavía está en fase de MVP, y las observaciones de la experiencia todavía deberán esperar algunos meses.

Han manifestado su deseo de ampliar rápidamente la iniciativa al conjunto de las marcas del grupo y así poder luchar contra la falsificación.

La solución se basa en la blockchain Quorum y está alojada en la solución en la nube de Azure (Rencurrel, 2019). La sociedad Consensys ha sido seleccionada para prestar asistencia al grupo de lujo. La trazabilidad unitaria de los productos se hace mediante el intermediario de activos no fungibles: técnicamente, se trata de los contratos ERC-721. LVMH no está en su primer ensayo, porque hace varios años que explora la tecnología. La cuestión, en cambio, ya no es hacer prototipos y explorar, sino más bien se trata de realizar software robusto que entre en producción.

Además del sector del lujo, otro sector está haciendo experimentos con blockchain: la mensajería.

## **15. Mensajería**

El sector de la mensajería es uno de los menos conocidos y, sin embargo, de los más críticos en la vida de los ciudadanos. La dimensión estratégica de una mensajería es igualmente de importancia capital. Hay que mencionar que Facebook compró WhatsApp, una empresa especializada en la mensajería, por 19 000 millones de dólares, unos 14.000.000 euros.

Para comprender estas cifras, hay que comprender los pormenores. Al usar las aplicaciones de mensajería, el usuario abandona una cantidad importante de derechos que hacen temblar a la CNIL.

Luego, los datos de mensajería se tratan para ser revendidos a los anunciantes, por ejemplo. Ellos se encargan de utilizarlos para ofrecer productos a los consumidores que corresponden a los sectores para los que trabajan.

Ofrecer una mensajería y herramientas de lectura adaptadas, es poder entrar en la intimidad de los usuarios para estudiar mejor el comportamiento y los hábitos de compra.

### a. Whisper

Hay una norma y estándares para intercambiar correos electrónicos. Pero no la hay para las mensajerías instantáneas. Whisper es una primera tentativa de comunicación descentralizada similar a Messenger, Skype, Snapchat o WhatsApp. Es un componente del protocolo par a par que permite intercambiar en la misma red que se utiliza para la blockchain Ethereum (Mohan, 2016).

La versión actual es un prototipo de trabajo en versión alfa, más que una solución fiable de intercambio entre partes. Teniendo en cuenta la evolución de este componente, no está activado de manera predeterminada. Por otro lado, como el protocolo está separado de la blockchain, los smart contracts no tienen acceso al mismo. Además, incluso si un desarrollador desea utilizar Whisper para permitir que un smart contract se comunique con este medio, es muy probable que no se transmita la información. A continuación, se plantea una segunda dificultad todavía más difícil de superar

De manera predeterminada, los nudos de la red no transmitirán el mensaje canalizado por Whisper. Utilizar Whisper sin modificarlo es muy difícil.

Diagrama

Descripción generada automáticamente

*Esquema que describe la interconexión entre Swarm, Whisper y Ethereum. Fuente: Ethereum Stack Exchange (Tron, 2016)*

En un principio, estaba diseñado para utilizarse conjuntamente con un smart contract y Swarm, mientras el sistema de transferencia de archivos funcionaba en la plataforma Ethereum. Los smart contracts hacían aquello para lo que habían sido escritos, Swarm transmitía los archivos y Whisper servía de microinterfaz de intercambio, más parecido a una nota adhesiva que a un correo electrónico. La misión del protocolo es permitir a las máquinas comunicarse entre ellas, pero invertir mucha energía en Whisper no pareció ser una prioridad para la fundación. Sin embargo, su uso concierne a muchas posibilidades.

Es posible que ciertas aplicaciones descentralizadas necesiten publicar una pequeña cantidad de información entre ellas. Puede ser necesario que esta información sea pública un tiempo determinado, como si se tratara de un anuncio pequeño o de una publicación de ratio de intercambio entre divisas. Entonces, se utiliza la mensajería para publicar la información durante un tiempo arbitrario que puede ir desde unos minutos a varios días. Luego el mensaje no tiene ninguna fuerza contractual, a lo sumo, tiene una vocación informativa.

La segunda posibilidad que ofrece Whisper afecta a la coordinación de los esfuerzos durante una transacción. Por ejemplo, una aplicación descentralizada que tiene la finalidad de intercambiar distintas divisas puede utilizar la mensajería para coordinar la transacción y permitir a una primera parte intercambiar euros por dólares. El contrato solo se instancia cuando se han reunido las partes. Eso permite reducir las latencias de uso.

El tercer caso agrupa los usos de comunicación general sin necesitar forzosamente un intercambio de datos en tiempo real, como un foro.

El cuarto caso de uso atañe a la posibilidad de establecer un nexo entre dos personas que no se conocen. El objetivo es ocultar al otro la identidad; convencionalmente, este tipo de intercambio de productos se puede encontrar en un sitio comercial o durante una transferencia de información sensible entre un informador y un periodista.

En general, Whisper está diseñado para permitir una transacción entre dos o varias partes, sin recurrir al archivado de las conversaciones. Twister, por el contrario, permite almacenar los mensajes de Twitter, un sitio de microblogging, en una blockchain Ethereum. Existen otras soluciones en el mercado, como UDP, 0MQ, TeleHash y Tox.

Sin embargo, todas ellas son susceptibles de ser objeto de ataques habituales y no están protegidas en una blockchain.

La solución también experimenta latencias graves. Si el mensaje está encriptado, el protocolo utiliza un sistema de relevos para disimular quién es el auténtico emisor y el destinatario. El modelo utilizado tiene un rendimiento bajo y es lento, a pesar de implementación cerca de la máquina. De lo que se deriva que no es viable un uso masivo.

Hay un sitio claramente vacío. Sin embargo, el modelo para desarrollar una mensajería de este tipo sigue sin definir. Como los mensajes no se pueden interceptar, en teoría, salvo por el emisor y el destinatario, capturar información para restituirla a continuación parece fuera del alcance. Actualmente, utilizar una mensajería es gratuito y de muy fácil acceso. Parece que el camino será largo y arriesgado, aunque las iniciativas gubernamentales inviten a la realización de un proyecto de este tipo.

### b. DARPA: una convocatoria de proyectos

En abril de 2016, la agencia estadounidense DARPA (*Defense Advanced Research Agency*) publicó una convocatoria de proyectos para crear una mensajería cifrada descentralizada mediante la tecnología del registro descentralizado (DARPA, 2016). DARPA es la división de investigación y desarrollo del ejército estadounidense. Desde hace varios años desempeña un papel preponderante en el desarrollo y la aplicación de nuevas tecnologías, sin limitarse forzosamente a las aplicaciones militares.

A priori, el cuaderno de carga es fácil de explicar, pero mucho menos de realizar. En primer lugar, necesita un mecanismo de cifrado sofisticado, a imagen de Signal o WhatsApp. Signal y WhatsApp son aplicaciones de mensajería que permiten intercambiar mensajes escritos, como SMS, o mensajes de audio, mediante una interfaz móvil. Su ventaja reside en el encriptado de las informaciones transmitidas entre individuos.

El proyecto debe utilizar necesariamente una blockchain, como la del bitcoin, pero no está restringido a esa. Los mensajes deben estar encriptados y ser visibles para todos. Sin embargo, solo deben ser legibles por los destinatarios que tienen la clave de cifrado. Entonces atacar se vuelve muy difícil, porque la fase de escritura está completamente desconectada de la fase de lectura.

No es factible recurrir a un servidor que centralice los intercambios, que generalmente es el objetivo principal de los ataques clásicos del tipo man-in-the-middle. Este ataque consiste en hacer creer al emisor que el destinatario ha recibido el mensaje correctamente mientras que es el atacante el que lo recibe, lo lee y luego lo transmite.

Sin embargo, la DARPA espera mucho del aspecto aumento de carga. Hay muchas limitaciones. Una aplicación de intercambio entre dos personas solo es realizable después de unas cuantas horas de desarrollo. En cambio, hacer que esté disponible para millones de personas no es tan fácil.

Uno de los primeros obstáculos consiste en hacer pasar un mensaje dado por toda la red en tiempo casi real. De aquí se deriva el segundo problema. La mayoría de los mensajes se utilizan en terminales móviles con una potencia de almacenamiento y de cálculo limitada. El ancho de banda también es un problema de tamaño. No es factible pedirle a un teléfono que calcule permanentemente o incluso que se conecte a una red inaccesible.

Desde un punto de vista operativo, la necesidad militar es real. En cada implementación, los ingenieros y técnicos deben montar todas las piezas de una red de comunicación interna, sin tener necesariamente acceso a Internet. La información sensible en la zona de operaciones o la imposibilidad de conectarse a una red clásica son motivos suficientes para justificar este proyecto, sin contar la necesidad de reducir el éxito de los intentos de pirateo.

Ya hay soluciones de intercambio en una plataforma descentralizada. Los mensajes también están encriptados, como en BitMessage o Vuvuzela. Lo que hace que el proyecto sea original, es precisamente su integración en una blockchain. Entones el problema de trazabilidad de los mensajes se vería potencialmente reducido. Por lo tanto, es muy posible que la agencia espere poder utilizarlo con fines de investigación.

## **16. Farmacéutica/Sanidad**

El sector sanitario se enfrenta a muchos desafíos. Blockchain se ha experimentado en muchos casos de uso, entre los que figuran la lucha contra las falsificaciones, la lucha contra los errores médicos, la trazabilidad de las muestras de prueba, la conservación de las pruebas clínicas, la gestión del consentimiento, la transferencia protegida de datos de pacientes entre instituciones, el pago de tratamiento reales o incluso la mejora de la adherencia farmacológica.

### a. FarmaTrust: lucha contra las falsificaciones de medicamentos

El sector farmacéutico es un objetivo principal de blockchain. En 2015, la organización IACC (International AntiCounterfeiting Coalition, Coalición Internacional Antifalsificaciones) estimó en 1770 miles de millones de dólares las pérdidas vinculadas a las falsificaciones en el mundo, teniendo en cuenta todos los sectores (Hulseapple, 2015). Fundado en 1979, el objetivo del organismo es luchar contra la piratería y la falsificación de productos. Está formado por más de 250 miembros en todo el mundo. Además, el número de víctimas vinculadas a la toma de medicamentos fraudulentos contra la malaria y la tuberculosis en 2012 se estima en 700 000.

La empresa británica Farmatrust ofrece utilizar una tecnología propia para realizar una trazabilidad de los productos que entran en la cadena de aprovisionamiento del medicamento.

En la práctica, los problemas de falsificación no se producen al principio o al final de la cadena, sino en eslabones intermedios de renombre menos controlados.

La empresa farmacéutica que desea utilizar el mecanismo de trazabilidad de *FarmaTrust* debe comprar tokens en un mercado: los FarmaTrust Tokens (FTT), y luego guardarlos. Cuando la empresa dispone de 100 FTT, eso le genera *Compliance Tracking Tokens*. Estos últimos no son criptomoneda sino una referencia al producto escaneado.

Al inicio del proceso, se genera un código de barras de dos dimensiones (código QR). Se le hace una fotografía con un simple smartphone y una aplicación móvil ya desarrollada. La foto permite capturar el código único asociado al producto y vincularle los *Compliance Tracking Tokens* (CTT). La referencia única se almacena en un registro independiente. Los CTT, en cambio, se intercambian de mano en mano en el registro distribuido durante la vida del producto.

Al final de la cadena de suministro, si los productos se han vendido o destruido, se destruyen los CTT (Liquid, 2018).

La solución tiene la ventaja de colocarse por encima de los sistemas existentes y romper los silos de empresa con sus propios sistemas de referencia. Sin embargo, la asociación entre las referencias de medicamentos y los tokens sigue siendo poco clara. Si un producto todavía tiene CTT, eso significa que no se ha vendido todavía y se facilita mucho el análisis logístico. Es posible saber dónde se encuentra en la cadena de suministro y también si caducará pronto, sin tener que implementar un sistema informático pesado. Los desarrollos futuros incluyen otros tipos de captadores o de sensores, como el IoT o chips.

Durante 2018 se lanzó un experimento con el gobierno de Mongolia. Actualmente todavía no hay información sobre las observaciones de la experiencia. Sin embargo, si hubieran tenido éxito, es muy probable que se hubiera divulgado más información.

La solución en sí misma se ha liberado de una gran cantidad de limitaciones y la legislación debe evolucionar para permitir una aceptación a gran escala. Sin embargo, ha intentado pasar los acuerdos ISO requeridos (ISO 9000). El paso por una blockchain pública puede parecer curioso. En efecto, una blockchain de consorcio habría podido ser suficiente en el sector de la cadena de suministro, sin correr el riesgo asociado a la volatilidad de los tokens. El uso de propiedades no fungibles como las que se pueden obtener con Ethereum y los smart contracts ERC721 sería probablemente más agradable. Por último, el doble uso token público - token privado es un movimiento sorprendente que fundamentalmente permite liberarse de la lógica de mercado si la especulación se vuelve demasiado fuerte. Para un inversor, eso se llama un riesgo de devaluación arbitraria.

### b. MedRec: tarjeta de salud descentralizada del paciente

El uso de la tecnología de registro descentralizado es una ventaja de peso en la lógica para compartir información de los pacientes entre instituciones del sector médico. Hay dos planteamientos posibles: la misión pública por un lado y el interés comercial por otro.

En Francia, el intermediario de la tarjeta sanitaria se ocupa en parte de la misión de servicio. Luego se transmiten una serie de informaciones a los distintos especialistas. Las equivocaciones técnicas son muy numerosas, y habitualmente se requiere el envío por correo hacia las mutuas. Cuando un paciente se desplaza entre distintas ubicaciones médicas, es muy frecuente que se le invite a desplazarse con una copia en papel de su carpeta cuando se le entrega.

En un mismo centro hospitalario, la copia y la reintroducción de datos son más la norma que la excepción, y un servicio informático averiado es una invitación a actos de valor para el personal médico.

En el plano comercial, el envío de datos entre un organismo hospitalario y una aseguradora también es la fuente de una gran cantidad de dificultades, los impagados están en primera línea. Hay numerosos motivos, el primero es probablemente la falta de documentos justificativos, los datos introducidos erróneos o incompletos. Por ejemplo, el fraude con los números de la seguridad social costaría 14 000 millones de euros al año, considerando que son unos dos millones de números (Deharo, 2018).

Francia se lanzó a un proyecto muy ambicioso: el expediente médico compartido (DMP, *Dossier Médical Partagé*). Este último tenía la ambición de mejorar un servicio público y resolver una parte de los dos lados mencionados.

Philippe Douste-Blazy lo lanzó en 2004 sin éxito, en cada presidencia se ha vuelto a poner sobre la mesa, con un coste estimado entre 500 y 1000 millones de euros. Solo su mantenimiento en condiciones costaría 35 millones de euros al año, por un servicio que todavía no se ha probado (Robert, 2019).

La sociedad *MedRec* ofrece una solución basada en blockchain para responder a los deseos expresados por la constitución del DMP. MedRec no conserva los datos de los pacientes. En cambio, utiliza los metadatos de los documentos intercambiados para calcular un hash. Este hash se graba en blockchain. Los metadatos describen al propietario del dato, el permiso y la integridad del dato requerido.

El envío del dato a blockchain se hace únicamente con el consentimiento del paciente.

Cuando se hace una solicitud de acceso a un dato, se envía a un *Gatekeeper* (guardián) de la base de datos. Esta parte se hace off-chain. El Gatekeeper implementa una interfaz de acceso a la base de datos local del nudo del paciente, nudo gobernado por los permisos grabados en blockchain. Los smart contracts y las claves criptográficas permiten garantizar la identidad del emisor y se le vinculan autorizaciones. Si la dirección de emisión es válida, se calcula la solicitud (p. ej.: envío de carpeta cliente) y el resultado se envía al emisor. Esta lógica aplicativa implica que los actores ya han desarrollado las API de acceso a los datos con un nivel elevado de seguridad informática. Así, blockchain permite gestionar de manera programática el acceso a los datos entre actores autorizados.

La compañía utiliza la tecnología Ethereum que ha retocado, especialmente sustituyendo el consenso por la prueba de autoridad (PoA). La Prueba de autoridad implica que solo pueden validar las transacciones una pequeña cantidad de nudos, su simple firma da fe de ello. Entonces el minado es mucho menos atractivo en el plano energético. Los propietarios de nudos validadores ya son actores de confianza que conservan los datos de los pacientes. La blockchain es una instancia permisionada restringida al ecosistema. Los smart contracts y el código difieren sustancialmente de los últimos desarrollos realizados para Ethereum en su versión pública y ya no son compatibles.

El proceso de hash no lo realizan los nudos validadores, sino que sigue siendo un proceso que consume muchos recursos. Esta previsto que sea realizado por actores del ecosistema a cambio de un acceso a los datos agregados y anonimizados que les permitan proseguir con sus investigaciones médicas.

El proyecto está en su versión 2.0. Nunca se realizó un análisis de seguridad en su versión 1.0, pero está previsto próximamente. El paso al siguiente nivel es un tema muy importante. Teniendo en cuenta los pocos datos enviados mediante blockchain, la limitación será más en el uso de la red y el envío de documentos. El proyecto habría podido programarse con una blockchain permisionada. Los datos de IRM, por ejemplo, son notoriamente más voluminosos que un PDF. Un hospital, por ejemplo, no siempre tiene el ancho de banda necesario para continuar con su actividad. La cuestión es especialmente importante en las zonas con una cobertura de red débil.

Los problemas con los que se ha encontrado el DMP apenas han surgido con este planteamiento. Sin embargo, la arquitectura distribuida y el acceso a los datos, y luego su envío, probablemente tienen mucho más sentido que una centralización a ultranza con envíos de datos y una replicación en masa como en la solución actual. La mutualización de dos planteamientos puede ser un camino interesante en el futuro.

Para terminar, como los desafíos en el sector médico son muy importantes. La tecnología es un medio interesante que puede permitir dar respuesta al tema de la fuga de datos médicos. De manera similar a lo que sucedió en el sector bancario casi cinco años antes, los intentos todavía no han madurado y los proyectos futuros podrían mejorar sustancialmente el protocolo de atención médica de los pacientes en el mundo.

## **17. Publicidad**

El sector de la publicidad tiene un peso de miles de millones de euros y sobre todo es la base de los modelos de negocio de Google o Facebook. Solo ellos, poseen un 75 % del mercado mundial de la publicidad en línea. Se han lanzado muchos proyectos con ayuda de blockchain, pero pocos han llegado a alcanzar una supervivencia comercial o una resiliencia técnica.

### a. Basic Attention

Desde siempre, el sector de la publicidad sufre el sesgo bien conocido de los anunciantes como de los consumidores potenciales. Los usuarios no reciben la publicidad que podría interesarles. Peor aún, cuando se hace una búsqueda de un objeto en un sitio web en concreto, se envían numerosas proposiciones de compras relacionadas en sitios web que no tiene nada que ver con el sitio inicial, dando lugar a una impresión de acoso y de espionaje.

El proceso contractual de difusión publicitaria es muy opaco. Una empresa que desea hablar de su producto pasar por una cadena de intermediarios de valor añadido no siempre demostrado. Los fraudes son habituales y a menudo los anunciantes tienen que pagar sumas a cambio de eslóganes cuya validez es difícilmente probable o incluso rastreable. Para retomar el ejemplo de Facebook, un algoritmo favorece su vídeo en lugar de los vídeos publicados en otra red social (p. ej.: YouTube).

Se considera que un sitio ha sido visto cuando se ha visionado durante al menos tres segundos. La lectura automática cuando se navega por la página web adultera estas cifras aumentando artificialmente la cantidad de visionados. Los mensajes utilizados no están interesados en retener a la audiencia más allá de unos segundos.

Pon último, a los creadores de contenido les expolian regularmente los ingresos asociados a su creación. Un individuo puede copiar el contenido desde un primer sitio web, luego pegarlo en una red social y ver que se le adjudican numerosas consultas. Recoge el dinero asociado a la cantidad de visionados, mientras el creador original no recibe nada. Así, solo se benefician las redes sociales y los ladrones. YouTube ha implantado contramedidas, pero no Facebook, porque son contrarias a sus intereses.

La finalidad del Basic Attention Token (BAT) es intentar remediar estos problemas. Al principio, el mecanismo planea eliminar los intermediarios que perciben una comisión. Se pagará a los usuarios según la manera en que vean la publicidad. Los creadores de contenidos recogen la mayoría de los ingresos. Los anunciantes obtienen un mejor retorno de la inversión en relación con su inversión publicitaria.

Para funcionar, un usuario debe descargar un navegador llamado Brave, que aspira a proteger la vida privada de su usuario todo lo posible. Por otra parte, un anunciante comprar tokens (BAT) y luego los utiliza para ejecutar los smart contracts en la blockchain Ethereum. Con cada visionado de publicidad por un cliente potencial, una parte de los tokens se distribuye entre los usuarios que han visto la publicidad. El navegador Brave percibe una parte. Por último, la persona que ha creado el contenido también recibe un porcentaje.

Se esperan múltiples ventajas:

* Un cliente potencial solo ver la publicidad que le interesa.
* Un creador de contenido aspira a ganar más dinero, Brave se convierte en el único intermediario, posiblemente percibe menos que los otros dos grandes del sector.
* Un anunciante recibe un informe más preciso de los clientes potenciales que tienen más probabilidades de comprar sus productos.

Es importante mencionar que Brave y BAT han sido desarrollados por el mismo equipo. La recogida de fondos de 30 millones de euros que tuvo lugar el 31 de mayo de 2007 finalizó en menos de treinta segundos. Participaron 130 personas, donde solo 20 de ellas disponen de dos tercios de los BAT emitidos para la recogida de fondos. Con esta suma, los desarrolladores van a crear su propia tecnología basada en el navegador. Sin embargo, otros navegadores podrían verse afectados en los próximos meses.

En la práctica, los desarrolladores podrían decepcionarse. Es técnicamente posible crear un robot informático que simule el comportamiento de una persona, haga clic en una publicidad y reciba una remuneración por haberlo hecho. Así se engaña al anunciante. Mientras que, para el usuario, ver una publicidad no implica que haga clic en ella. Por otro lado, algunas empresas como *Platincoin* ofrecen una red social que funciona de la misma manera.

Utilizar la red genera tokens, invitar a amigos genera todavía más tokens y la remuneración se hace mediante la compra de emoticonos o por los anunciantes.

### b. Lucidity y Toyota

La industria de la automoción gasta miles de millones todos los años en publicidad. En 2018, el sector gastó unos 15 000 millones de euros solo en los Estados Unidos. El caso de uso es exactamente el mismo que para Basic Attention: la cadena de suministro de las compras de publicidad.

Al principio, se emplearon técnicas conocidas de optimización para identificar las actividades dudosas generadas por el tráfico de bots o el spoofing de dominios. En el primer caso, se trata de identificar los programas informáticos que hacen clic en los anuncios publicitarios y restarlos del cómputo, porque no están adosados a clientes potenciales reales. En el segundo caso, se identifican los sitios web falsos de prestigio donde se pretende haber vendido el espacio publicitario (por ejemplo: puesta a disposición en el sitio Le Monde cuando se ha colocado en el sitio le Mo**m**de), y se les descuenta de la factura.

En una segunda etapa, la compañía Lucidity creó una ruta auditable de cadena de suministro vinculada a la blockchain Ethereum. Una serie de smart contracts garantiza la trazabilidad entre actores y el posicionamiento de la publicidad. La empresa ha afinado su solución en torno al componente Casper de Ethereum.

La finalidad de esta capa de nivel 2 es responder a los problemas de paso al siguiente nivel. Se espera que este componente esté en producción a finales de 2019 y principios de 2020. Actualmente, la solución está en pruebas mediante pilotos en el laboratorio técnico del *Internet Advertising Bureau*.

Los resultados son prometedores, porque con un rendimiento técnico relativamente débil y en ausencia del componente Casper, la eficiencia de la publicidad de Toyota en el PoC ha superado el 21 %. Esta puntuación, recordemos, se ha obtenido con los mecanismos de optimización de audiencia y de limpiado de datos. Segundo argumento de valor, y nada despreciable: un conjunto de datos propio en la parte programada de la cadena de suministro.

Sin embargo, los desafíos futuros son muy importantes. En efecto, la tecnología que puede dar soporte a la publicidad en línea debe ser tan rápida como la red VISA y poder entregar contenido al nivel de Facebook. Aunque por el momento la problemática del real-time biding solo es un sueño, esta experiencia así como los progresos subsiguientes en las blockchain publicas serán determinantes. Igualmente, es importante mencionar que Lucidity trabaja de manera activa con la blockchain Rchain.

Rchain tiene dos ventajas enormes: la ejecución concurrente y la prueba formal. La primera permite realizar varias tareas de manera simultánea, acelerando sustancialmente las operaciones en la blockchain, mientras que la otra aumenta la seguridad del smart contract que hace aquello para lo que ha sido creado.

## **18. Almacenamiento**

El almacenamiento de los datos es muy lucrativo. Tanto el profesional como el particular tienen la impresión de poder almacenan los datos de manera continua, sin tener que preocuparse por la renovación del material. Además, la velocidad de acceso a estos datos y la resiliencia a los fallos dan lugar a unas tarifas a veces astronómicas. Por ejemplo, un terabyte de almacenamiento puede alquilarse hasta por 110 000 euros al año para los servicios premium. Un abono anual para un particular cuesta como mínimo alrededor de 80 euros al mes, es decir, casi 1000 euros al año.

### a. Swarm

Swarm es una plataforma descentralizada de almacenamiento de intercambio de contenidos. Es nativa de las capas fundamentales de los componentes ofrecidos por Ethereum. El objetivo inicial de Swarm es proporcionar un depósito suficientemente descentralizado y redundante para permitir la ejecución de las aplicaciones descentralizadas y de las blockchains de manera utilizable.

Tiene muchas ventajas, porque este sistema promete un almacenamiento entre pares, como las redes BitTorrent y similares. La infraestructura es resistente a los ataques por denegación de servicio, a los fallos de servidores, a la censura y a los errores de archivos (por ejemplo, un archivo dañado en un nudo, pero utilizable en otro).

Un ataque por denegación de servicio (o DDos) consiste en bombardear un servidor con millones de peticiones de acceso en un intervalo de tiempo muy corto. Como el servidor no puede soportar la carga, deniega el acceso a todos. Ya no puede transitar ninguna información a través de él.

El sistema Swarm ha sido diseñado para poder dar soporte a una red de varios protocolos. También permite utilizar la potencia de la blockchain Ethereum identificando los nombres de dominios, y así identificar las partes tomadoras de una transacción gracias a su dirección mediante el DNS. Igualmente lo utilizan los servicios de pago y garantiza la disponibilidad de contenido.

Para comprender Swarm, hay que comprender su posición en la visión de la fundación Ethereum. Allí donde los smart contracts implementan una lógica descentralizada, Swarm implementa el almacenamiento descentralizado. Más concretamente, Swarm está diseñado como un protocolo contable que se beneficia de la ejecución de los smart contracts en la máquina virtual Ethereum. Una ventaja enorme: no está vinculado a ningún mecanismo de almacenamiento particular por el hecho de la virtualización del almacenamiento. En otras palabras, su naturaleza lo hace intrínsecamente libre de todo el dispositivo de almacenamiento material específico.

Detrás de todas estas promesas, la solución propuesta todavía está en la fase de prototipo. Sin embargo, el avance es prometedor. Swarm permite realizar un intercambio de información entre pares de manera efectiva en una red descentralizada (Swarm, 2019).

Segunda ventaja: permite almacenar archivos HTML, CSS y JavaScript de las aplicaciones ejecutadas en los sistemas de centralizados. También se pueden almacenar archivos estáticos durante un tiempo indeterminado. Las últimas auditorias parecen garantizar la integridad de los archivos, incluso de los que no se consultan con frecuencia.

A menudo, el sistema ha sido criticado por los especialistas porque la fundación parece querer reinventar la rueda con esta tecnología de almacenamiento. Más específicamente, otras alternativas viables como IPFS o BitTorrent, o una tecnología futura pueden sustituir a Swarm en la arquitectura actual de Ethereum sin problemas. Si es absolutamente necesario utilizar un sistema nativo, Filecoin puede hacer esta función perfectamente.

Uno de los competidores más fiables es IPFS. Este sistema dispone de todas las cualidades de Swarm. Segmenta los archivos voluminosos automáticamente antes de transferirlos, algo que no hace Swarm. Por lo tanto, es posible almacenar todo tipo de archivos de tamaño arbitrariamente grande o pequeño en una red descentralizada.

Sin embargo, las pruebas en el entorno de producción parecen ser ligeramente favorables para la situación Swarm respecto a las transferencias pequeñas de información, por ejemplo: un importe de criptomoneda a una dirección dada.

Segunda ventaja no despreciable: la estructura de almacenamiento utilizada es un árbol de Merkel DAG descentralizado. Detrás de este término criptográfico se oculta un concepto simple y potente. Es posible crear versiones de un mismo objeto. Así, no es necesario almacenar n veces una versión de un archivo y por lo tanto, captar n veces el espacio del disco. La estructura de almacenamiento está diseñada para analizar las diferencias entre la primera y las siguientes versiones del archivo, reduciendo en gran medida las necesidades de almacenamiento. En la red solo se registran las diferencias. Entonces la transferencia es igualmente mucho más rápida.

Además de estas soluciones de almacenamiento, la primera nativa y en estado de prototipo, la segunda en producción, hay proyectos comerciales que ven progresivamente la luz, como Storj.

### b. Storj: o cómo alquilar su disco duro

Storj es una solución fundada en 2014 gracias a un proyecto en el sitio de crowdfunding KickStarter, con una recogida de fondos de unos 300 000 euros. El proyecto consiste en permitir una entidad, un individuo o una empresa alquilar la capacidad de almacenamiento que tiene disponible a cambio de una remuneración. Los datos se almacenan en la red Storj en la nube y están encriptados.

El argumento comercial de la empresa reside en el coste considerado muy elevado entre el precio de venta del servicio y el coste real. La diferencia entre los dos oscilaría entre un factor 10 y un factor 100.

En la práctica, el proceso todavía es laborioso. Primero, hay que crear una cuenta como en todos los sitios de transacciones. Luego, se invita al cliente a crear una carpeta, donde va a poder almacenar los datos. Hay que asegurarse de tener determinadas herramientas de programación instaladas, como Node.js y npm, y lanzar una serie de comandos.

Todas las cargas de documentos se hacen mediante el intermediario de líneas de comando, como en GitHub. La consulta sigue el mismo esquema. Es posible utilizar una API, como las ofrecidas por Google o Facebook. Es absolutamente necesario pasar por una fase de aprendizaje y la solución no tiene un acceso fácil. En cambio, desde el punto de vista de un desarrollador es un juego de niños si tiene formación en JavaScript.

Para evitar estas dificultades, es posible descargar DriveShare y MetaDisk. Se trata de aplicaciones que permiten respectivamente poner en alquiler y alquilar el espacio de almacenamiento. Actualmente, DriveShare se puede instalar y MetaDisk no es funcional. La primera se parecerá a las soluciones de almacenamiento clásicas, lo que debería facilitar la captación de clientes nuevos. Sin embargo, la solución no está lista, y todavía queda al menos un año de trabajo para permitir que la gran mayoría disfrute de ella.

Desde un punto de vista técnico, Storj utiliza la blockchain Bitcoin. Las transacciones se hacen con ayuda de un token específico de la aplicación, el Storjcoin X (SJCX). Esta criptomoneda utiliza el protocolo CounterParty, considerado como uno de los más fiables en el lanzamiento de la aplicación. El smart contract utilizado es rudimentario. Solo hay que incluir la dirección de almacenamiento, la disponibilidad en bytes y la dirección de entrega de los tokens.

La inteligencia parece estar principalmente en la disponibilidad del espacio de almacenamiento y en la seguridad intrínseca. La tecnología Blockchain se utiliza de la forma más rudimentaria posible: un registro de los pagos y de las disponibilidades de almacenamiento.

Aunque el argumento comercial es interesante, quizás lo es menos para los arrendadores. A priori, serían remunerados con una parte de lo que un industrial está dispuesto a facturar. En los foros, los creadores no parecen estar en posición de estimar el precio de coste del alquiler.

Además, alquilar un espacio de almacenamiento no es algo trivial. Un tercero tiene un acceso contractual a una unidad central privada, lo que puede dejar perplejos a los consumidores y proveedores de este servicio. Estas críticas son bien conocidas y se han oído hasta en el mundo del alquiler de domicilios privados. AirBnB es una multinacional que floreció sobre esta paradoja conceptual.

El paralelismo parece justificado porque, desde enero de 2016, se observa un entusiasmo real por la criptomoneda. La valoración de los Storjcoins ha dado un gran salto hacia adelante. En efecto, el 1 de enero el capital total era de 711 618 dólares frente a 6 009 194 el 1 de septiembre del mismo año. Antes de este período, la cotización estaba relativamente plana, con la solución en desarrollo.

El entusiasmo por este token no parece poder explicarse exclusivamente como un simple fenómeno de especulación. Parece que existe un auténtico modelo de negocio subyacente. Es evidente que la solución no se ha enfocado comercialmente, parece basarse en sólidos fundamentos técnicos. Sin embargo, el almacenamiento no es el único sector incipiente que se puede beneficiar de la tecnología del registro descentralizado.

## **19. Conclusión**

Al principio de la ola iniciada por el intermediario Ethereum, se consideraron muchísimos casos de uso. Casi todos los sectores recibieron la influencia de la tecnología. Su influencia es más o menos pronunciado con las instancias administrativas más prometedoras (p. ej.: instancias gubernamentales, actividades bancarias, etc.).

Desde principios de 2018, con la llegada de las soluciones permisionadas de blockchain y la estabilización de las soluciones públicas, emergieron los primeros casos de uso industriales donde ciertos sistemas entraron en producción. Uno de los mayores éxitos es probablemente TradeLens. Para todos los casos de uso, la tecnología utilizada con astucia técnica pero, sobre todo, con una visión estratégica tiene un impacto importante en la productividad de la empresa. Sin embargo, el auténtico potencial que ofrece la tecnología se encuentra en el sector en su conjunto. Se trata de una oportunidad fantástica para crear procesos de ecosistemas que no siempre están definidos. Curiosamente, su auténtica promesa no está en la excelencia tecnológica, sino en la transformación de los métodos de trabajo que induce.