INCOM CHILE

Blockchain para periodistas y medios de comunicación

RAYMOND COLLE

Título: Blockchain para periodistas y medios de comunicación

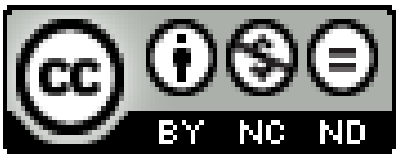
Autor: Raymond Colle

Edición: INCOM-Chile (Asociación Chilena de Investigadores en Comunicación), Santiago de Chile, 2017.

Portada del autor

R.Colle, académico pensionado, es doctor en Ciencia de la Información y analista de sistemas. Ha sido por más de veinte años profesor e investigador de la Facultad de Comunicación de la Pontificia Universidad Católica de Chile. Es socio honorario de la Asociación Chilena de Investigadores en Comunicación ("INCOM-Chile") y vocal de la Sociedad Latina de Comunicación Social (España).

Las imágenes incluidas en el texto provenientes de fuentes diversas se insertaron bajo el principio de *"fair use"*, dado que la presente obra es de tipo académico y no tiene fines comerciales.



Tabla

Introducción

En noviembre de 2014, Sony Pictures fue el objeto de una intrusión que paralizó los sistemas informáticos de la compañía y derivó en grandes filtraciones de datos, incluidas revelaciones inéditas acerca de la industria hollywoodense. A la fecha, fue el mayor ataque sufrido por una empresa de Estados Unidos según la Wikipedia. A principios de agosto de 2017, los cibercriminales hackearon HBO y robaron 1.5 TB de información, desvelando guiones y episodios no emitidos de las series más populares de la compañía, incluyendo guiones inéditos de Juego de Tronos. Y los ataques siguen. Según Gartner, se gastarán 86.400 millones de dólares en productos y servicios de seguridad de la información en 2017. (TICbeat, 16/8/2017)

Los casos de Sony, HBO y otros muestran cuán difícil puede ser para las compañías asegurar la protección de sus datos. Y la red se ha hecho eco de un anhelo cada vez mayor por sistemas de información donde la seguridad sea muy superior y, ojalá, inquebrantable. Es lo que ofrece la "*blockchain*" o sistema de cadena de bloques, cuya ventaja no es solamente esta, como lo mostraremos aquí.

El año 2017 habrá sido marcado por un auge importante en la cantidad de noticias del área de las tecnologías digitales referidas al *blockchain*, más allá de las limitadas a las monedas virtuales o criptomonedas (como el ya famoso BitCoin). Se considera cada vez más que esta nueva tecnología podría ser una solución para los crecientes problemas que afectan a internet. Como dicen Sally Adee y Carl Miller , *"el protocolo TCP/IP estaba bien en la década de 1970, cuando se podía mapear toda la Internet en una sola hoja de papel. En estos días, es un desastre, siendo difícil averiguar quién es realmente la gente en Internet e impedirles hacer cosas malas."* (New Scientist, 10/8/2017). A medida que más información se pone en línea, crece la necesidad de mayor protección tanto para los datos personales como para los documentos. Aún con el mismo protocolo TCP/IP ha sido posible, desde sus inicios, transferir documentos encriptados, pero no se desarrolló un estándar para ello y depende de cada uno elegir el sistema que prefiera. Tal sistema tampoco es dinámico, permitiendo que, por ejemplo, un documento encriptado pueda pasar de una persona a otra, cada uno aportando algún detalle sin poder, eventualmente, modificar nada del contenido anterior. Es lo que permite la cadena de bloques.

La tecnología de las cadenas de bloques podría llegar a reemplazar todas las formas de contrato, pagos incluidos, con una seguridad que, por ahora, parece irrompible. Pablo Herreros[1] ve ahí, incluso, "*una tecnología que va a cambiar el mundo más de lo que lo hizo internet"* y *"el mayor avance socio-tecnológico que vivirá la humanidad desde la revolución industrial"*. Robin Marvin también dice que la cadena de bloques es la respuesta a una pregunta que hemos estado haciendo desde el inicio de la era de Internet: *"¿Cómo podemos confiar colectivamente en lo que pasa en línea?"* y *"El cambio que trae la cadena de bloques representa para nuestro mundo digital es tectónico."* (PC Magazine, 2/8/2017). El *blockchain* introduce una internet centrada en los usuarios, dando a estos el control sobre los datos, los activos digitales y la reputación en línea asociados con ellos.

1Periodista español, autor de "El Poder Es De Las Personas". Ver su artículo sobre blockchain en la bibliografía.

Ilustración 1: Adaptado de PC Magazine, 2/8/2017

El potencial de las cadenas de bloques es enorme: *"Cuando se trata de activos y transacciones digitales, puede poner absolutamente cualquier cosa en una cadena de bloques. En el próximo puñado de años, grandes franjas de su vida digital pueden empezar a correr sobre una base de cadenas de bloques, y es posible que ni siquiera se de cuenta de ello."* (PC Magazine, 2/8/2017). En una charla TED de 2016, Don Tapscott dijo que *"el blockchain nos trae de la internet de la información a la internet del valor"* (Ted.com).

En enero de 2017 tuvo lugar en Madrid el I Encuentro Internacional sobre Blockchain y Periodismo, señal del interés que está surgiendo en este campo. A fines de mayo de 2017 tuvo lugar en Berlín, Alemania, la Convención IoT Tech, Blockchain y AI, indicadora de un interés más general y de cierta relación entre estas tres tecnologías. Como veremos adelante, las iniciativas prácticas en el campo que nos ocupa son aún limitadas, pero no cabe duda que el interés está creciendo. En la tienda Amazon, no se encuentra aún (agosto 2017) ningún libro que aborde la aplicación de la cadena de bloques en el periodismo. En español, Google solo mostraba -a la fecha- artículos señalando dicho interés pero no descripciones de experiencias concretas ni de cómo operar.

Lo que pretendemos hacer aquí, después de explicar de modo general que es el sistema de cadena de bloques y cómo funciona, es esencialmente llenar el vacío que hemos encontrado en torno a cómo puede aplicarse en el campo de los medios de comunicación.

Por cierto, cuando hemos hablado del tema, las primeras veces, las reacciones fueron *"¡Esto es complicado!"*. Es cierto, es complicado, y hay que leer bastante y revisar ejemplos (pocas veces sencillos) para entender. Pero esta complicación es la clave de la seguridad y la confiabilidad que son los dos valores más apreciados de este sistema y los más requeridos en la internet de hoy. Esperamos haber simplificado aquí lo suficientemente el tema para que los comunicadores – periodistas, audiovisualistas, editores, gerentes de medios, etc. - logren tener una clara visión de lo que es posible hacer y de lo que, probablemente, se irá imponiendo rápidamente en los próximos años.

> NOTA: La tecnología digital está en permanente desarrollo y más aún la de las cadenas de bloques, aún bastante "fresca" fuera del ámbito de las criptomonedas. Es inevitable, de este modo, que lo aquí expuesto pueda contener propuestas que lleguen a ser rápidamente superadas o algunas imprecisiones debidas al esfuerzo de simplificación realizado.

1. Visión general

La historia del *blockchain* empieza con el protocolo desarrollado por Satoshi Nakamoto, el misterioso creador del Bitcoin, la criptomoneda que "dio la partida" a esta tecnología en 2008. Varios años después se adoptó para crear otras criptomonedas y, más recientemente, se empezó a estudiar su aplicación en otros campos con un creciente interés, como ya sugerido en la introducción. Con el paso de los años y a la vista de la experiencia, los bancos se han ido convenciendo de las bondades del sistema al punto que se unieron hace poco en una alianza internacional para establecer una plataforma y una moneda virtual común:

> "Barclays, Credit Suisse, Banco Imperial Canadiense de Comercio (CIBC), HSBC, Banco MUFG y State Street Bank, seis de las mayores entidades financieras del mundo, unen fuerzas para crear una moneda digital basada en tecnología blockchain. Finales de 2018 sería la fecha señalada en la que las entidades podrían efectuar transferencias interbancarias de hasta 100 millones a bancos extranjeros de forma prácticamente instantánea gracias a esta divisa digital. Los dos grupos de entidades que participan en el desarrollo de la criptomoneda tienen ahora que continuar dialogando con autoridades reguladores y entidades bancarias para asentar las políticas de protección de datos y seguridad cibernética." (TICbeat, 1/9/2017)

1.1. ¿Qué es?

"*Blockchain*" es una palabra que vemos cada vez más en las páginas de tecnología pero raras veces encontramos una explicación sencilla de lo que es y menos aún de su importancia para el futuro. El *blockchain* o cadena de bloques puede ser entendida como un libro mayor contable (*"ledger"*) o como una base de datos en la que se apuntan múltiples transacciones. Es distribuida, es decir que se encuentra repartida en numerosas máquinas, donde la información se encuentra replicada de forma idéntica. Contiene la información de cada nueva operación que se realice, en un nuevo bloque que se reproduce en todos los computadores que la contienen ("nodos") y en tiempo real. Y cada vez que se pone un bloque nuevo, ese bloque lleva toda la información de todo lo anterior, que no se puede modificar ni borrar (ni duplicar, ya que sería una nueva operación: ¡nada de *spam*!).

> "Piense en *blockchain* como un tejido histórico que graba todo lo que sucede exactamente como ocurre. Luego, la cadena cose esos datos en bloques cifrados que nunca pueden ser modificados, y dispersa las piezas a través de una red mundial de computadoras distribuidas o `nodos´." (PCmag, 2/8/2017)

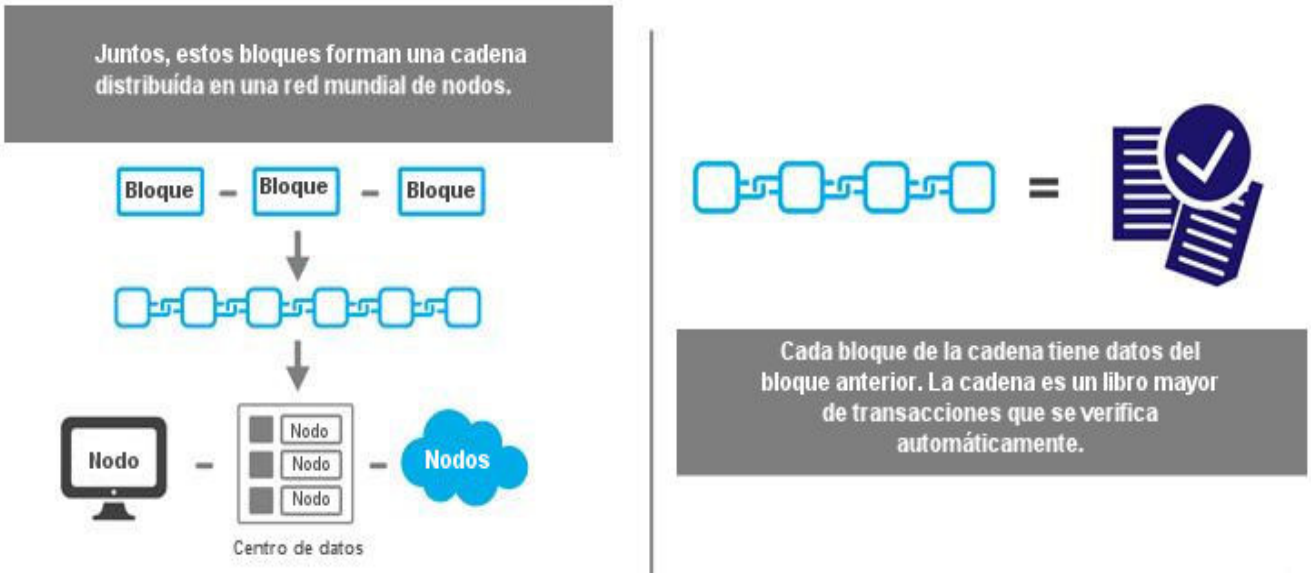


Ilustración 2: Adaptado de PC Magazine

Cada bloque contiene un número de bloque, un número arbitrario llamado "nonce" y un campo de datos que contiene los datos de la operación ("transacción") y además la fecha y hora (*"timestamp"*), la versión anterior completa de la cadena (*"previous hash"*) y la firma criptográfica del bloque. El *hash* es la "traducción" criptográfica de la cadena al terminar la transacción, que es lo que le da su seguridad. Para crear un bloque se requiere una aplicación específica (*software*) y un procesador adecuado (Vea n° 1.4.). Quienes, además, participan en la tarea de verificación se denominan "mineros".

Ilustración 3: Adaptado de PC Magazine

1.2. Cómo funciona

1.2.1. Una explicación sencilla

E. Camerinelli publicó una explicación que destinó a su abuela, que no entiende de tecnología. Traduzco aquí la parte central de la misma:

> "Suponga que todo lo que tiene es una cantidad de $ 100 para comprar bienes en un centro comercial. En la caja usted dice que enviará un email prometiendo pagar $ 100, con el email representando una promesa de pagar esta cantidad. El comerciante felizmente acepta el email y va al banco. El banco también acepta el email y agrega $ 100 a la cuenta del comerciante. ¿Suena raro? Ciertamente, por una razón: asumiendo sólo por un segundo que todo sucede como se describe, ¿qué hay de su monto de $ 100? Todavía está en su cartera. ¿Así que eso significa que usted puede comprar mercancías para más de lo que tiene, simplemente enviando emails? Demasiado bueno para ser verdad. Sin embargo, créalo o no, la transacción puede suceder (y de hecho lo hace en el mundo real).
>
> Para entender cómo esto podría ser posible vamos a agregar un grupo de clientes en el centro comercial. Ahora, cuando usted dice que enviará el email de pago, esta gente le pedirá recibir el mismo email. Hay algunos clientes «especiales» en la multitud que competirán para ser los primeros en validar el email (por ejemplo, el remitente, el receptor, la cantidad intercambiada, la posesión real de la cantidad reclamada). Una vez que lo validan, el contenido se vuelve «verdadero» para todos. Pero espere un minuto: Ya que todos los clientes «especiales» en el centro comercial querrán que su validación se convierta en «la» versión de la verdad, ¿cuál debería seguirse?
>
> Todos los participantes especiales siguen una regla (es decir, un «protocolo»): el primero en resolver un rompecabezas electrónico, digamos un Sudoku, gana la carrera. Como todos sabemos, un Sudoku es bastante difícil de resolver, pero la solución es fácil de comprobar. El ganador es compensado por el duro trabajo de resolver el Sudoku. Hay un incentivo para que los contendientes ganen la próxima vez. Después de comprobar que el rompecabezas está debidamente resuelto, los contendientes rechazan su versión [la que habían recibido antes] y aceptan el email validado del ganador como la «versión de la verdad». El email se envía a todas las personas en el centro comercial, que ahora tienen la misma copia, reconocida como válida e inmutable. Con la versión de la verdad aceptada públicamente, todos en el centro comercial sabrán que debe $ 100 a la tienda.
>
> Ahora puede pasar a la próxima tienda en el centro comercial y tratar de comprar otras mercancías por un valor de $ 100. Hace de nuevo la promesa de pagar por email. Esta vez su oferta será rechazada. ¿Por qué? Bueno, ¿dije que también el comerciante recibió el email? Esto significa que él sabe perfectamente que no le queda dinero. Antes de que me olvide de nuevo, tanto su banco como el banco del comerciante también están en el bucle. Por lo tanto, el sistema es autocontrolado y no hay necesidad de que ningún intermediario (por ejemplo, una cámara de compensación o el Banco Central) informe a las partes cuánto posee cada uno y si la transacción es aceptable." (en Finextra.com, 2016[2])

2 Referencia completa en la bibliografía.

En el siguiente gráfico, podemos ver la diferencia que hay entre un registro (libro) contable tradicional y uno en cadena de bloques: mientras en el sistema habitual puede haber cuatro copias -en realidad independientes- (de las que no es fácil asegurar que son idénticas), con la cadena de bloques se asegura que todos tienen exactamente la misma copia.

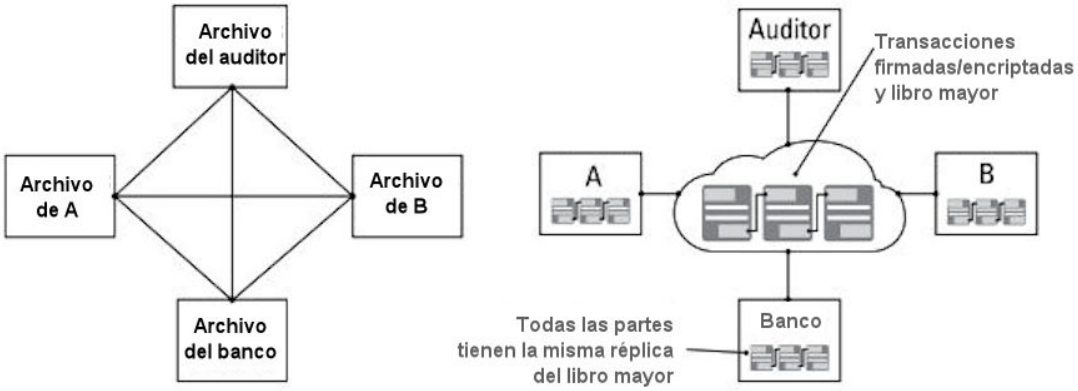


Ilustración 4: Traducido de Gupta, p.7

1.2.2. Ahora, algo más técnico

La cadena de bloques funciona sobre una red P2P (*peer-to-peer*, de «igual-a-igual») sin intermediarios. Lo primero es encriptar todos los datos, creando el *hash*.

> "Todo comienza con una versión simplificada y una función matemática importante: la función *hash*. Las matemáticas de las funciones *hash* se conocen desde 1953 más o menos y se popularizaron con la criptografía moderna. Se definen como una función que «resume» una cadena de datos de cierta longitud (normalmente larga) en una cadena más corta de longitud fija. Es algo parecido a una «suma de control» o «firma única», con ciertas virtudes peculiares: la misma información de entrada proporciona siempre la misma información de salida, dos entradas distintas no pueden producir el mismo *hash* (o es astronómicamente difícil que eso suceda) y todos los *hashes* tienen la misma probabilidad, entre otras cosas. Adicionalmente suelen ser de «un solo sentido»: con el *hash* de unos datos no se puede recrear cuáles eran los datos originales.
> Como cada operación se puede rastrear hacia atrás, cuando A paga a B una cantidad como 25 fichas se puede volver al bloque anterior en el que se comprueba que A tenía efectivamente 25 fichas para gastar." (Microsiervos, 18/12/2016)

Cada transacción (operación) da lugar a un nuevo *hash* y a un nuevo bloque. Como ya señalado, los bloques deben ser validados y solo pasan a formar parte de la cadena cuando lo son. Las cadenas de bloques se conservan en múltiples nodos, que se encuentran en los computadores de quienes se ofrecen voluntariamente para ello y disponen de la capacidad requerida. Si los nodos son importantes, más lo son los "mineros", un subgrupo de nodos, que son los que realizan las operaciones y vigilan el funcionamiento

del sistema. Los mineros son los que resuelven los retos matemáticos asociados a las operaciones y las validan (ver numeral siguiente).

Las cadenas de bloques pueden ser privadas ("sujetas a permiso"), públicas, es decir de acceso abierto (*"permissionless"*) o híbridas. Si una cadena es privada, cada usuario autorizado tendrá una identificación única que le dará acceso a la información detallada, lo que eleva aún más el nivel de protección de datos. El sistema también permite que se creen accesos diferenciados, permitiendo a algunos ver parte de la información que otros no podrán ver: Si A transfiere algo a B, ambos pueden ver todos los detalles, pero C podría tener permiso para ver que hubo una transacción - y eventualmente la certificación por una agencia supervisora - pero no para ver los otros detalles (monto e identidades, por ejemplo).

Nótese que se trata siempre del registro de transacciones. Veremos más adelante si puede aplicarse a otro tipo de informaciones.

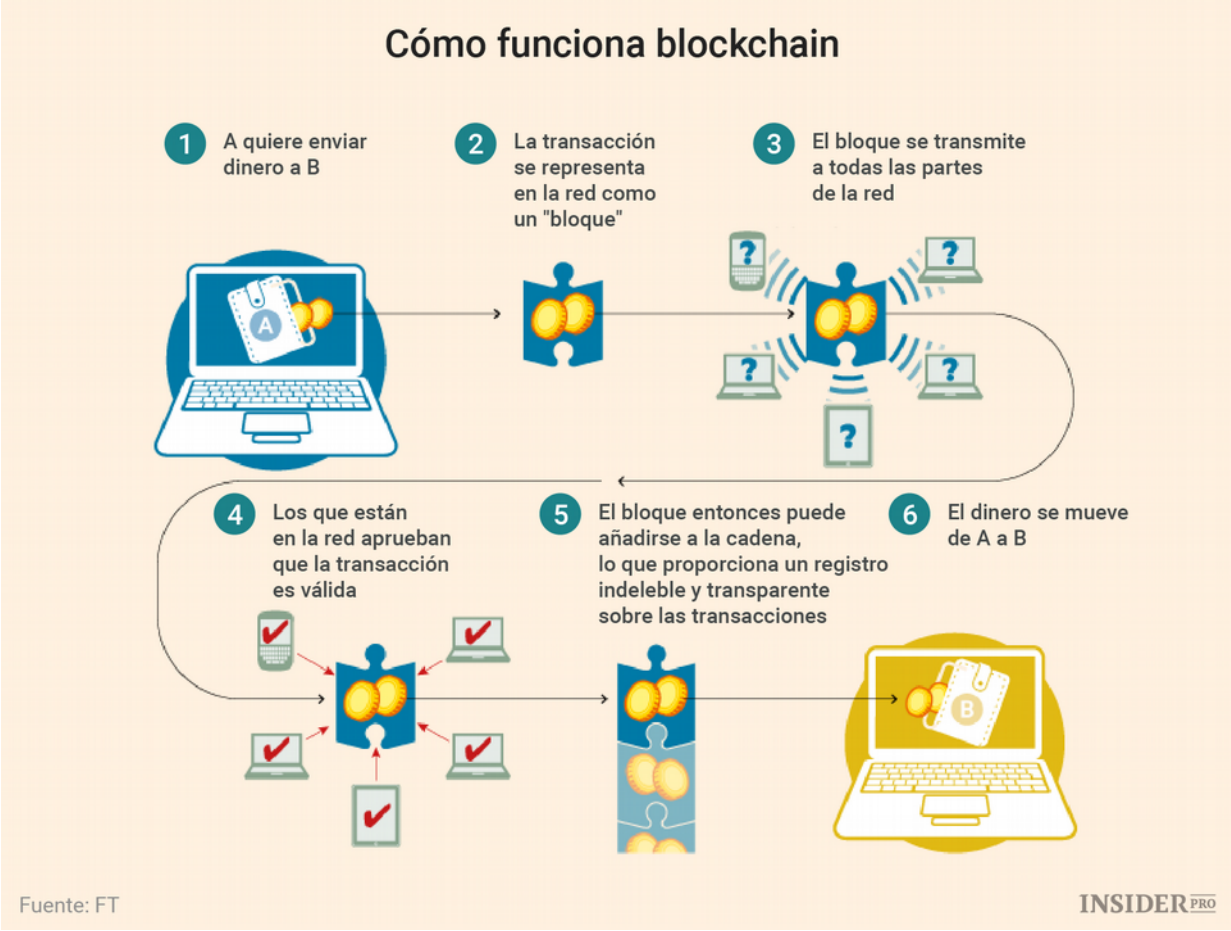


Ilustración 5: De Insider.pro

1.3. Su seguridad

La seguridad del sistema y de las operaciones dependen del encriptado de todos los datos pero también de la repetición del "*hash*" en todos los computadores de quienes utilizan esta base de datos (los nodos del sistema). Para el encriptado se usa generalmente el algoritmo SHA-256 que produce una salida de 256 bits (32 bytes, en hexadecimal). Además, en una cadena pública, cada operación es acompañada de un reto

matemático (acertijo) que los nodos deben resolver y la obtención del mismo resultado por la mayoría es la garantía final y condición de aceptación del nuevo bloque. (Este control, que ocupa mucho poder de procesamiento, no es necesario en una cadena privada porque se conocen de antemano todos los actores.)

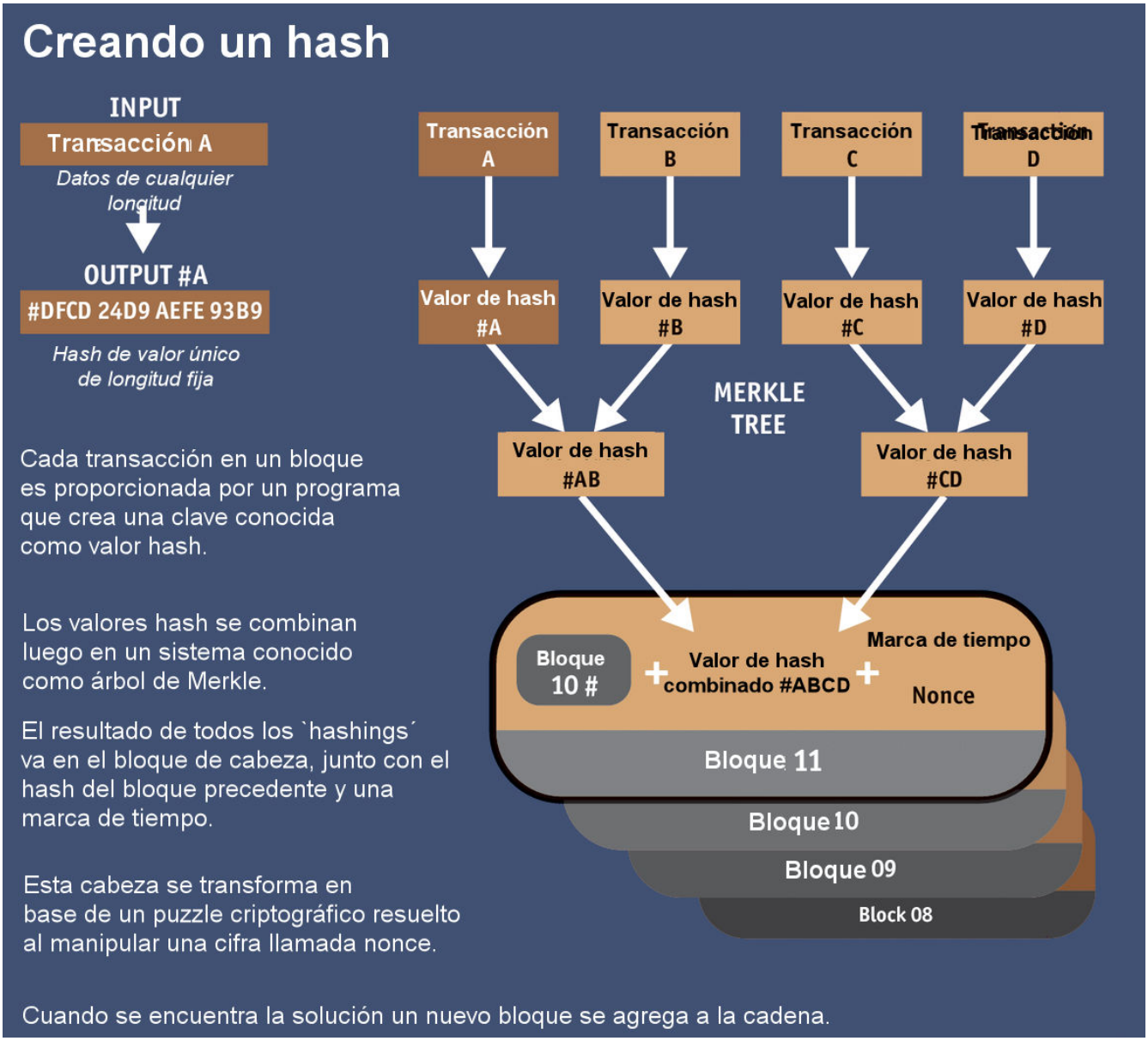


Ilustración 6: Traducido de The Economist, 31/10/2015

"Un bloque válido firmado es aquel cuyo *hash* comience por 0000. Entonces se puede ir probando a cambiar el valor del nonce hasta que el *hash* cumpla esa condición. Esto es lo que hace el botón «minar»: dedicar un tiempo a ir comprobando número tras número hasta que el *hash* cumple esa condición. Lo interesante es que si el nonce es correcto pero cambian los datos, adiós validez del bloque; habría que volver a empezar y encontrar otro nonce." (Microsiervos, 18/12/2016)

Aspecto de bloques válidos de Bitcoin

Ilustración 7: Bloque verificado
Aspecto después de un ingreso de dato y validación (no se ve aquí el *hash* completo)

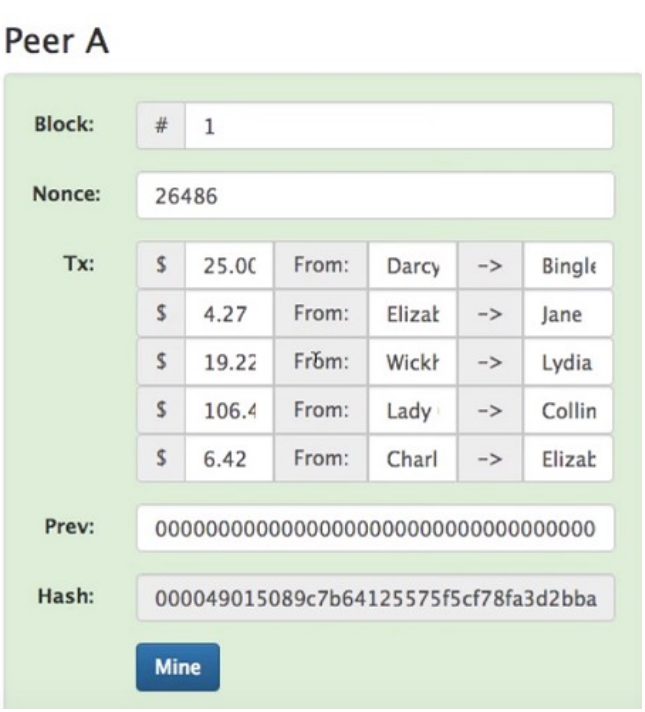


Ilustración 8: Contenido de bloque
El contenido del bloque n°1 para el actor A. Se pueden observar las transferencias realizadas en transacciones anteriores.

El emisor -o quien haga la operación- usará la clave pública del destinatario para cifrar un mensaje, pero solo este podrá descifrarlo con su clave privada (En sistemas híbridos, es posible que se consideren claves "privadas" compartidas.). Todo lo demás es automático y nadie más puede intervenir (salvo ver el contenido si se dispone de una copia de la clave privada). Si se cambia cualquier dato en cualquier bloque queda invalidada la firma de ese bloque y también la de todos los siguientes, porque a partir de ahí los *hashes* dejan de coincidir. ¡Adiós a los fraudes! Y se puede usar para todo tipo de intercambio de datos, contrato, acuerdo o pago, de ahí que se hable de "contratos inteligentes" (y la Cámara de Comercio Digital de Estados Unidos creó ya la *"Smart Contracts Alliance"*), siendo también una interesante solución para el problema de la seguridad en la internet de las cosas y el enlazamiento de objetos cercanos sin necesidad de recurrir a un servidor central. También facilitaría el voto digital seguro en elecciones.

Sin embargo, si bien la seguridad es altísima, se han descubierto ya algunas posibles amenazas (reseñadas en el libro de Preukschat), como el llamado "ataque del 51%" (si la mayoría de los nodos se ponen de acuerdo para actuar en forma deshonesta; pero esto dejaría de ser rentable por el abandono de los participantes) o el "ataque de equilibrio" (que permitiría ralentizar la distribución de las transacciones, aumentando el gasto). Pero estas vulnerabilidades son de los sistemas que procesan la cadena de bloques, no propios de la cadena de bloques misma. También son siempre posibles errores de código, como en todo *software*, pero también existen mecanismos de verificación.

La criptografía, las matemáticas, la teoría de juegos e internet son los cimientos de esta nueva tecnología y han resuelto los problemas asociados a su descentralización. La innovación más importante que ofrece esta tecnología es que nos dota de un mecanismo que nos permite alcanzar un consenso entre partes que no se conocen, usando una red pública, incluso si puede estar comprometida.

Ilustración 9: Adaptado de PC Magazine, 4/8/2017

1.4. Requisitos computacionales

En teoría, cualquiera con un buen computador y bastante memoria podría ser un nodo, pero para "minar" se requiere una capacidad que pocos poseen:

> "Antes se minaba hasta con tarjetas gráficas de videojuegos; ahora hay un *hardware* específico para el minado de criptomonedas. Se han desarrollado *pools* de mineros, y China, con enormes granjas de minado, está copando el mercado, en el que el precio de la energía es un condicionante decisivo. En España no es precisamente barato." (López y López, en El País.com, 28/7/2017)

Esta capacidad podría no ser necesaria para otro tipo de proyecto, pero hará falta precisarla para cada tipo de uso, especialmente si se pretende generalizarlo. ¿Serán capaces los PC más comunes e incluso los *smartphones*? Minar criptomoneda en estos parece por ahora imposible. En el caso del Bitcoin, ya se ha producido una suerte de "guerra civil" entre desarrolladores del *software* y un grupo de inversores y empresarios que ven como perjudicial la falta de avances para poder aumentar el número de transacciones que Bitcoin puede manejar, actualmente de 7 operaciones por minuto, lo cual -en un caso como el sistema de pagos con esa moneda- llega a ser insuficiente para ser masivamente útil.

> "La tasa de transacciones de Bitcoin es ínfima frente a los sistemas de pago convencionales como Visa, por ejemplo, que procesa un promedio de 2.000 transacciones por segundo y es capaz de soportar hasta 56.000 transacciones por segundo. Las medidas para solucionarlo han generado una enorme y preocupante división entre sus usuarios." (MIT Technology Review, 3/8/2017).

Otro problema es que la cadena autorizada en Bitcoin tiene una longitud de 1MB, lo cual también limita las operaciones posibles. Los partidarios de aumentarla crearon Bitcoin Cash, con una cadena de hasta 8MB (PC Magazine, 8/8/2017). Esto podría ser crucial en el caso de una generalización del sistema de cadena de

bloques para todo tipo de interacción (hasta en los *smartphones*). ¿Deberemos tener todos una cuenta "en la nube", donde un tercero se encargará de conservar las cadenas? Podría llegar a ser necesario en algunos casos pero, por cierto, en muchos casos la cadena no será muy larga por tres razones:

- Los datos son extremadamente compactos (las cadenas ocupan mucho menos espacio que una planilla Excel, al menos en los usos dados hasta ahora al sistema).
- Muchas operaciones son contratos entre dos personas o una persona y una institución y, por lo tanto, hay pocas operaciones (pocos bloques, con pocos datos) en la cadena.
- La cadena NO contiene el tipo de información que pueden ofrecer, por ejemplo, los medios de comunicación. (Veremos más adelante cómo se resuelve esta limitación.)

No se visualiza aún la necesidad de recurrir a la nube, pero quizás se llegue en algún momento a crear ahí "monederos virtuales". En todo caso, Microsoft e IBM ofrecen ya en su nube el *"blockchain-as-a-service (BaaS)"*, lo cual soluciona tanto el problema del espacio como de la capacidad del procesador.

Una cosa es segura: el *software* debe mejorar para permitir operaciones más masivas (como en el caso de las compañías de tarjetas de crédito), pero el actual es suficiente en la mayoría de los casos.

> "Decenas de *startups* están utilizando la tecnología para todo, desde pagos globales a compartir música, desde el seguimiento de las ventas de diamantes a la industria legal de la marihuana. Es por eso que el potencial del *blockchain* es tan grande: cuando se trata de activos y transacciones digitales, puede ponerse absolutamente de todo en una cadena de bloques." (PC Magazine, 2/8/2017)

Algunos pasos se están dando en esta dirección, abordando los problemas antes mencionados:

> "Microsoft está trabajando con socios como Intel, JP Morgan y Ethereum, para construir un nuevo marco de cadena de bloques abierto que tiene como objetivo aumentar la velocidad (1.600 operaciones por segundo) y reducir la complejidad. Es el marco «Coco» (abreviatura de Consorcio Confidencial). Podrá operar en la nube o localmente; será compatible con cualquier protocolo del libro mayor y funcionará con cualquier sistema operativo y cualquier supervisor que apoye un entorno de ejecución confiable y compatible (TEE).
> Las extensiones de protección de *software* de Intel (SGX) son uno de esos TEE, que ayudan al marco a entregar velocidad, escala y confidencialidad mejoradas a las empresas. Intel SGX es una solución basada en *hardware* que aísla partes clave de un programa *blockchain* para crear un área privada en la CPU y en la memoria, que puede proteger el código y los datos durante la ejecución.
> Microsoft ya empezó la integración de Ethereum y R3 Corda. Intel, Hyperledger, Sawtooth y J.P Morgan Quorum también comprometieron su integración." (V3.co.uk, 14/8/2017)

1.5. Aplicaciones

El uso de la cadena de bloques se inició con las criptodivisas, principalmente el Bitcoin, pero existen ya más de mil criptodivisas en circulación y Bitcoin sigue dominando el 48,5% del total de la capitalización (Microsiervos, 5/8/2017). Ethereum es la segunda criptodivisa por volumen, después de Bitcoin[3].

Ilustración 10: De CoinMarketCap

Pero ya se empezó a utilizar en otros campos.

> "Es un mundo complejo que empieza a estar muy poblado: en el mapa del ecosistema aparecen los bancos de bitcoin, las empresas de «minería» (creación de moneda) y grupos de trabajo. Todo tiene un curioso aspecto de ciudad SimCity organizada por barrios: Soluciones Blockchain, Medios, Servicios Financieros, Tecnología, Desarrollo, Tiendas, *Hardware*, Carteras virtuales, Inversionistas…
> Entre las entidades conocidas que quizá te suenen están el BBVA, Santander Serfin, Bankinter y otros bancos y bolsas como el Nasdaq o el NYSE (la bolsa de Nueva York). También están Microsoft, Dell, Wordpress, Expedia y decenas y decenas de empresas nacidas al albor de esta –de momento– pequeña revolución." (Microsiervos, 8/06/2016)

3 Ethereum es más que una criptomoneda: es una plataforma descentralizada sobre la cual se pueden ejecutar diversos tipos de contratos inteligentes, pero administra su propia moneda digital, llamada ether. Más de 150 organizaciones empresariales se han unido a la Enterprise Ethereum Alliance desde su lanzamiento en febrero 2017, abarcando corporaciones tecnológicas, bancos e instituciones financieras, *startups* de cadenas de bloques y criptomonedas, industrias como de la salud y de energía e incluso algunos gobiernos. (PC Magazine, 29/8/2017)

El ecosistema actual de las cadenas de bloques

Ilustración 11: De Visualcapitalist.com

Para Lara Olmo,

> "La publicidad será una de las primeras industrias que se transformará por la irrupción del *blockchain*. Esta tecnología promete menos intermediarios, más transparencia en las campañas y menos anuncios intrusivos para los usuarios. [...] Es lo que ofrecen empresas como AdShares, un mercado descentralizado P2P que permite a anunciantes y editores la capacidad de negociar directamente por los espacios, o NYIAX (*New York Interactive Advertising Exchange*), para fijar contratos publicitarios garantizados." (TICbeat, 1/8/25017)

Para los destinatarios de esta publicidad también hay ventajas: se terminarían las intrusiones indeseadas y se garantiza el contenido.

Para la distribución de música existe, por ejemplo, Mycelia (http://myceliaformusic.org/), un *"colectivo de creativos, profesionales y amantes de la música"* fundado por el músico Imogen Heap (PC Magazine, 2/8/2017). Spotify anunció que había adquirido la *startup* Mediachain Labs para utilizar el sistema (Copyrightandtechnology.com, 27/4/2017). Binded.com ofrece un servicio de registro (*copyright*) de fotografías y ya tenía 332.914 registros en agosto 2017.

También existe un nuevo tipo de navegador que bloquea automáticamente los anuncios y los rastreadores y, en su lugar, ayuda a impulsar los ingresos de los editores a través de micropagos basados en bloques: es Brave, fundado por Brendan Eich, cofundador de Mozilla (PC Magazine, 2/8/2017). A su vez, China estudia el uso de *blockchain* para cobrar los impuestos (MIT Technology Review, 7/8/2017). Sony ha anunciado el 9 de agosto 2017 que pondrá en práctica una plataforma de registros de educación estudiantil desarrollada a través de una cadena de bloques. Permitirá gestionar los datos de varias instituciones educativas, además de guardar el historial de aprendizaje y transcripciones académicas. (Hipertextual, 10/8/2017)

> "Un fotógrafo o un músico pueden ya monetizar sus imágenes y canciones con plataformas como Monegraph, que permite con *blockchain* garantizar que el autor es quien vende los derechos y hacerle llegar el dinero que genere su uso al precio que él ponga. Se evita averiguar quién tiene los derechos y se paga y se cobra automáticamente, entre máquinas y sin intermediarios." (Herreros)

Sitios web como Blockai, Pixsy, TinEye, Ascribe, Mediachain y Proof of Existence ofrecen el uso de la tecnología para registrar el *copyright* y proteger de las infracciones. (Bitcoin Magazine, 9/8/2016). Blockai ofrece un registro de propiedad intelectual para fotógrafos/dibujantes y Ujo para que los músicos puedan cobrar directamente de sus fans y resolver a la vez el tema de las licencias mediante contratos inteligentes.

1.6. Ventajas

La seguridad va más allá de la confiabilidad del contrato (o contenido, cualquiera sea). Un ejemplo que da Herrero:

> "Compras un billete de avión por 100 euros para ir a París y le añades un seguro de 10 euros que dice que si el vuelo sale con más de 2 horas de retraso, te devuelven el importe íntegro. Cuando estás esperando a que salga tu vuelo y pasan dos horas sin que despegue, ves en el iPad que te acaba de llegar a tu banco una transferencia de 110€. Nadie dio la orden: la base de datos oficial vinculada al *smart contract* fue la condición cumplida para que el sistema te indemnice, sin que ningún humano mueva un papel. ¡Ojo al ahorro de trámites a la compañía y al ahorro de papeleos, tiempo y cabreo para el cliente!" (p.2)

También obtenemos una trazabilidad inigualable *"desde los ingredientes de un producto fabricado al origen real de un alimento o al destino exacto de cada céntimo de una donación a una ONG"* (Herrero, p.3)

En el periodismo la cadena de bloques puede ser un efectivo modo de combatir las noticias falsas: *"Si se puede verificar algo con la cadena de datos, con seguimiento de autor y fuente, ya no hay opción a la falsedad"*, dice Jacobo Toll-Messia (Retina, El País, 6/8/2017). Ofrece también una nueva manera de administrar los muros de pago:

> "La eficiencia de *blockchain* permitirá micropagos de un céntimo por leer un artículo, y podrá ser el propio periodista quien lo cobre sin que intervenga un medio. Podrá haber un gran quiosco donde cada medio o cada autor cobren la cantidad exacta en función del tiempo que un lector pase leyéndolos. Habrá mejor periodismo: se terminará el fraude del #*clickbait* (noticias-cebo) porque los medios no buscarán el clic sino que pasemos tiempo en su página (cobrarán de anunciantes o lectores por tiempo de visualización y no por número de clics)." (*ibidem*)

Una plataforma como Steemit ya ofrece este tipo de servicio a los periodistas *free lance,* y no es la única. Si se generaliza esta forma de operar podría acabarse el negocio gigantesco -y el control- de las plataformas como Facebook y Google.

A continuación nos concentraremos en estos posibles usos en el campo del periodismo y de los MCM y como podrían operar.

2. Las bases del modelo

2.1. Estado de reflexión y de desarrollo

El tema ya ha sido abordado en algunos artículos en español[4], especialmente como resultado del I Encuentro Internacional sobre Blockchain y Periodismo de enero 2017, organizado por «OléChain»[5], un grupo de debate sobre esta nueva tecnología, o de la publicación del libro *"Blockchain: la revolución industrial de Internet"* [6] coordinado por Alex Preukschat (Trecebits, 31/5/2017). En agosto 2017, pude encontrar ya algunas organizaciones que presentaban proyectos de plataformas periodísticas operativas en *blockchain* como Civil, DNN, Steemit y Decent. Excepto DNN, se trata de empresas que no son medios de comunicación sino que ofrecen una plataforma para periodistas, un modelo sin duda nuevo que puede parecer amenazador para la prensa tradicional. Como dice Covadonga Fernández *"en este nuevo modelo, las empresas tradicionales de medios deberán aprender a convivir con las jóvenes compañías tecnológicas que están irrumpiendo en su modelo de negocio"*, como ocurre en varias otras industrias (Retina, El Pais, 14/6/2017).

> "Es en la desintermediación donde el potencial de la tecnología *blockchain* de Bitcoin podría cambiar el futuro de los medios mediante transacciones inmediatas y sin intermediarios, abriendo una puerta de esperanza a la industria de los medios y también a los profesionales de la información al permitir a los usuarios comprar, por fracciones de euros o bitcoins, artículos, reproducciones de vídeos, noticias, fotos, dibujos, suscripciones al medio por páginas o secciones concretas, minutos de lectura, horas o días. Yendo un poco más allá, cada periodista podría programar sus propios *Smart Contracts* poniendo las condiciones concretas en las que se consumiría su producto. Es decir, cada periodista podría definir su propio modelo de negocio para editores o consumidores finales." (C.Fernández, en Preukschat, p.42)

La *startup* Civil se propone desarrollar una plataforma para el periodismo en cadenas de bloques (con la criptomoneda de Ethereum) *"que puede ser utilizada para crear «salas de prensa» y «estaciones» - mercados basados en cadenas de bloques donde los ciudadanos y periodistas forman comunidades alrededor de un propósito compartido y un conjunto de estándares, apoyan financieramente el reportaje factual y el trabajo de investigación y limitan sustancialmente la desinformación mediante métodos efectivos de edición colaborativa"* (Niemanlab, 21/6/2017). Este sistema de sala de redacción debería permitir que los usuarios combinen sus fondos para pagar por la cobertura de temas que les interesan, facilitando *"la cobertura de nichos y tópicos locales mientras se amplían para servir temas nacionales y globales populares"*. (*ibidem)*

4 Ver El País, 24/1/2017, ABC.es 19/1/2017, BBVA, 27/1/2017, El Economista, 21/3/2017, La Razón, 29/4/2017, La Vanguardia 23/1/2017

5 www.olechain.com

6 Ver bibliografía.

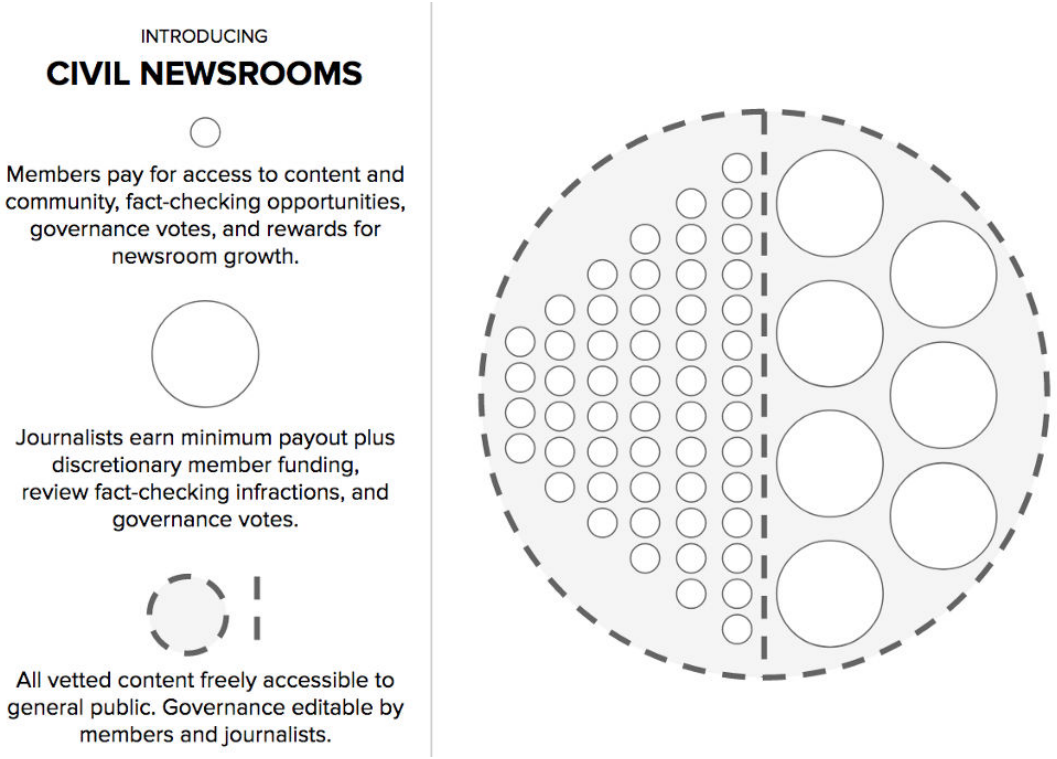


Ilustración 12: De Civil

> "La intención de Civil es crear una red de malla de mercados de noticias autónomos en los que se premia económicamente la creación de noticias, la comprobación de hechos y la sostenibilidad de la plataforma. El resultado es un ecosistema de noticias totalmente desagregado y descentralizado donde simultáneamente cualquier persona puede crear, contribuir y apoyar sólo lo que quiere, y donde el *trolling*, las cámaras de eco y la desinformación son económicamente inviables." (*ibidem*)

Por su parte, Samit Singh y Dondrey Taylor crearon la Decentralized News Network (DNN) que pretende reunir noticias *"por el pueblo y para el pueblo"*, remuneradas con la criptomoneda ether de Ethereum (Cryotocoinsnews.com. 2/5/2017). Así es como operan:

> "Un escritor escribe una noticia y la envía a DNN para que revise la exactitud y el equilibrio; luego es vista por un panel de siete revisores anónimos seleccionados al azar. Evalúan los artículos de acuerdo con las directrices editoriales de DNN y sugieren cambios al escritor. Si el artículo pasa la revisión, el escritor es recompensado con fichas DNN. Así, también, lo son los revisores que aprueban una historia con la mayoría de los otros críticos." (Cryotocoinsnews.com. 2/5/2017)

En Noruega, el ingeniero español Jacobo Toll-Messía junto a seis personas repartidas entre Noruega, Brasil, Tailandia y Alemania, creó la plataforma Hubii para la compra y venta de contenido, del creador al distribuidor sin intermediarios (Retina,El País, 6/8/2017). También ha surgido CoinDesk, una *startup* que está tratando de implementar un sistema de micropagos multiplataforma para contenidos noticiosos, para lo cual se asoció con el navegador Brave que opera con Bitcoin (C.Faife).

Y, en lo que parece ser la primera universidad que se propone desarrollar el periodismo en *blockchain*, la Universidad Técnica de Istambul está proponiendo construir una *"aplicación descentralizada donde la gente puede compartir libremente noticias, artículos u opiniones sobre los acontecimientos actuales"* (www.atositchallenge.net/).

Covadonga Fernández dice en La Razón:

> "Esta nueva manera de conectar a periodistas con usuarios nos pone frente al abismo de un periodismo sin medios, al menos sin medios tal y como los conocemos ahora. Hay que tener en cuenta que, hasta ahora, la lógica del funcionamiento de los medios de comunicación ha sido justamente la contraria. El medio centralizaba el flujo de información, que surgía en los diferentes lugares y lo centralizaba bajo su marca, dando una especie de certificado de «existencia»." (14/4/2017)

2.2. Modelo operativo

2.2.1. Identificación de actores

- Usuario: Cualquier participante que puede realizar transacciones u observarlas.
- Regulador: Alguien a quien se permite supervisar las transacciones.
- Desarrollador: programador que crea una aplicación de cadena de bloques y contratos inteligentes.
- Operador de red de cadena: Alguien con autoridad especial para definir, crear y administrar cadenas de bloques en una organización.
- Plataforma de proceso: Sistema computacional utilizado.
- Fuente de datos tradicional: Que puede ser utilizada para crear contratos inteligentes o ayudar a definir cómo pueden ocurrir las comunicaciones y las transferencias de datos.
- Autoridad certificadora: Encargado de emitir los certificados necesarios para operar con una cadena de acceso reservado.

2.2.2. Componentes conceptuales[7]

- Contrato inteligente (*"smart contract"*): Es un código informático (*software*) que reúne diversas reglas, con la capacidad de autoejecutarse en forma automática para aplicar y validar las condiciones preestablecidas. Estas condiciones pueden ser solo tecnológicas o también legales[8]. Puede ser escrito por un programador, generado por otra aplicación (como SmartContract, ver más adelante) o adoptado de una plataforma existente.

- Activos (*"Assets"*): Las definiciones de activos permiten el intercambio de casi cualquier cosa con valor a través de la red y, por lo tanto, de todo tipo de producto medial. Los activos se representan generalmente como una colección de pares clave-valor, con cambios de estado registrados como transacciones en el libro mayor.
- Código de cadena (*"Chaincode"*): El *chaincode* es el *software* que define un activo o activos y las instrucciones de transacción para modificarlos. Su ejecución se divide en particiones ordenadas de transacciones, limitando los niveles requeridos de confianza y verificación a través de los tipos de nodos y optimizando la escalabilidad y el rendimiento de la red.

7 De acuerdo a la documentación de Hyperledger Fabric y algunas otras fuentes.

8 "El uso de *smart contracts* para la contratación comercial se mueve en la incertidumbre jurídica" dicen X.Foz & col. (en Preukschat, p.178)

- El libro mayor (*"ledger"*): Libro de registro (base de datos) compartido e inmutable que codifica todo el historial de transacciones de cada canal e incluye una capacidad de consulta similar al SQL[9] para una eventual auditoría y resolución de conflictos. Este libro constituye el contenido de la cadena de bloques y solo puede haber un libro/cadena de bloques por canal. El libro contiene un bloque de configuración que define políticas, listas de control de acceso y otra información pertinente.
- Transacción: Cada transacción da como resultado un conjunto de pares de valores-clave de activos que se registran en el libro mayor cuando se crea, actualiza o elimina. Cada transacción en la red se ejecuta en un canal, donde cada parte debe ser autenticada y autorizada para realizar transacciones. La transacción puede ser de "solo lectura" o también de escritura y agrega la firma de quien la realiza más los datos-valores que correspondan, generando un nuevo bloque, que pasará por los controles previstos (validación).

- *Token* (ficha): *"Un token representa a menudo un valor financiero o un activo digital, de forma similar a como las fichas de un casino simbolizan o representan dinero fiduciario solo para poder usarlas en las distintas máquinas y juegos de azar."* (Criptonoticias.com, 8/6/2017) Aunque los *tokens* pueden representar cualquier cosa, si un valor financiero está involucrado, el *token* se referirá a este. La forma de un *token* es una cadena alfanumérica de caracteres. Es importante trabajar con *tokens* estandarizados: *"Si los desarrolladores saben de antemano cómo funcionará un token, pueden integrarlo fácilmente en sus proyectos con menos temor a cometer errores."* (E. Vollstädt)

- Canal: Un canal es una subred de comunicación entre dos o más miembros específicos de una red, con el propósito de realizar transacciones privadas y confidenciales. Un canal está definido por los miembros (de organizaciones), los pares de anclaje por miembro, el libro mayor compartido, las aplicaciones de los códigos de cadena y los nodos del servicio. Cada usuario que se une a un canal tiene su propia identidad dada por un proveedor de servicios de membresía que lo autentica. Cada canal puede tener participantes diferentes (aparte de la organización que lo establece). Una empresa puede definir varios canales, cada uno con una cadena de bloques diferentes, por ejemplo para diferentes productos.

- Privacidad a través de canales: Los canales permiten transacciones multilaterales con el alto grado de privacidad y confidencialidad como puede ser requerido por empresas competidoras e industrias reguladas que intercambian activos en una red común.

- Servicios de seguridad y membresía: La membresía permitida proporciona una cadena de bloques de confianza, donde los participantes saben que todas las transacciones pueden ser detectadas y localizadas por los reguladores y auditores autorizados. Se utiliza una infraestructura de clave pública para generar certificados criptográficos vinculados a organizaciones, componentes de red y usuarios finales.

9 *Sequential Query Lenguage*: el modelo estándar para hacer consultas en bases de datos.

- Consenso: Se establece un enfoque único para el consenso, que permite la flexibilidad y la escalabilidad necesarias para la empresa. Se logra cuando el orden y los resultados de las transacciones de un bloque han cumplido los criterios de verificación pre-establecidos. Este control tiene lugar durante el ciclo de vida de la transacción. El código de cadena es el que asegurará que hay suficientes respaldos, que se derivaron de las entidades que correspondan y que la transacción no es duplicada.

2.2.3. Bases computacionales

Hemos de considerar aquí dos componentes: la plataforma de servicio y la aplicación que maneja la cadena de bloques.

Plataforma

Evidentemente se debe seleccionar primero la plataforma de *hardware* en la cual se operará y decidir si se utilizará un proveedor externo o si se creará un sistema propio. En el n°2.1. se nombraron varios proveedores que ofrecen sus plataformas. Los hay tanto genéricos (que permiten diferentes usos) como especializados (p.ej. que solo ofrecen registrar y eventualmente comercializar fotografías). IBM es una de las empresas que ofrecen a los desarrolladores su "nube" para el desarrollo de sus proyectos si no tienen la infraestructura necesaria, pero es posible descargar todo el *software* requerido del depósito Docker Hub[10], que tiene aplicaciones de libre uso.

Pero si se cuenta con un buen departamento de ingeniería y computadores con procesadores potentes y rápidos y con amplia memoria, se puede instalar una plataforma propia gracias a la existencia de *software* de código abierto (*"Open Source"*) como *"Hyperledger Fabric"*, ofrecido por la Fundación Linux. Vale la pena explorarlo dado que, como proyecto *Open Source*, es de libre utilización y soporta múltiples formas de aplicación, con una estructura modular, que respecta todas las exigencias de confidencialidad, seguridad y escalabilidad. Permite programar las reglas de los contratos, operar – si se desea – sin acudir a las criptomonedas existentes (sin "minería") y establecer diversos tipos de usuarios (con o sin permisos de acceso a ciertos datos). Es uno de los más importantes jugadores en los avances para lograr sistemas estandarizados interoperables según PC Magazine (29/8/2017).

Aplicación

El *software* que maneja la cadena de bloques es una aplicación descentralizada o DApp (*"decentralized application"*). Esto quiere decir que funciona en una red compartida y, en este caso, hay múltiples usuarios de la misma aplicación.

Para ser considerada DApp, una aplicación debe cumplir con los criterios siguientes:

- La aplicación debe ser totalmente de código abierto, debe operar autónomamente, y sin entidad controlando sus fichas (*tokens*).
- La aplicación puede adaptar su protocolo en respuesta a mejoras presupuestas y *feedback* del mercado, pero todos los cambios deben ser decididos por consenso de sus usuarios.

10 https://hub.docker.com

- Los datos y anotaciones de operaciones de la aplicación deben ser almacenados criptográficamente en una cadena de bloques pública y descentralizada.
- La aplicación tiene que usar una ficha criptográfica (criptomoneda existente o una ficha propia de su sistema), necesaria para acceder a la aplicación, y cada contribución de valor de mineros debería ser recompensada con esas fichas.
- La aplicación debe generar fichas según un algoritmo criptográfico estándar, sirviendo como prueba de valor, con la contribución de los nodos (Bitcoin usa el *Proof of Work Algorithm*). (E.Vollstädt[11])

Una DApp puede crear su propia cadena de bloques o utilizar el protocolo de una plataforma ya existente (como Ethereum). Las hay de código abierto y existen aplicaciones que ayudan a crearlas.

Un proveedor externo podrá tener su propia oferta de DApps. En una instalación propia es posible no solo hacer múltiples ajustes a una existente sino crear una propia y específica a partir de un generador de DApp. Los hay que no requieren saber programar, y explicamos brevemente cómo se hace en el capítulo siguiente. También existen aplicaciones complementarias, para capas que se agregan a la DApp para realizar funciones complementarias.

No es nuestro objetivo aquí entrar en todos los detalles técnicos. Los ingenieros podrán encontrar una guía útil en la documentación de Hyperledger Fabric[12]. También pueden encontrar un curso gratuito de introducción en el sitio de IBM[13]. Reuter utiliza esta plataforma desde el año 2016 para vender "información inteligente". Agregaremos sin embargo información acerca de las etapas de trabajo y muestras de algunas interfaces gráficas que puedan ilustrar estas (ver Capítulo 3).

Soporte comunicacional

Es el momento de aclarar cómo se realizan las comunicaciones cuando se usan cadenas de bloques. Excepto si se trata de una cadena privada, por ejemplo de exclusivo uso interno de una empresa, se utilizará internet pero no necesariamente la web, aunque – al parecer – lo más común es utilizar los servidores de nombres (DNS) como lo hace la web para las direcciones de contacto. Los navegadores más comunes como Chrome, Safari y Firefox son generalmente capaces de exhibir las interfaces requeridas.

2.2.4. Manejo financiero

Hay tres maneras principales para adquirir criptomonedas:

1. Comprando bitcoins u otras criptomonedas en una casa de cambio especializada (Bitstamp.net, Kraken.com, Coinbase.com o Xapo.com; en Chile y Latinoamérica: SurBTC). Es lo mismo que abrir una cuenta bancaria. Se puede comprar generalmente con dólares o euros.
2. Recibiendo un salario o pago por servicios en criptomonedas o bitcoins.
3. "Minando" criptomonedas (prestando servicio de nodo validador de transacciones). (El Economista América, 19/12/2016)

Como señalado en el n°1.5, existe ya un millar de criptomonedas y se siguen creando nuevas. Esto se hace mediante una oferta llamada *Initial Coin Offering* (ICO), que funciona en forma parecida al *crowdfunding*. Pero,

11 Erik Vollstädt, ¿What are DApps?, https://blog.bitnation.co/what-are-dapps/
12 http://hyperledger-fabric.readthedocs.io/en/latest/
13 https://developer.ibm.com/courses/all/blockchain-essentials/

como ha señalado el comité chino encargado de vigilar el mercado financiero, algunas de estas ICOs no son más que fraudes financieros y estafas piramidales, algo que también ha provocado la preocupación el Banco Central de Singapur y de algunos otros países (Xataka, 4/9/2017).

"Este año, docenas de empresas han recaudado unos 1.250 millones de euros a través de este nuevo mecanismo de recaudación de fondos" según la MIT Technological Review (14/9/2017). Pero aquí, generalmente, no se trata propiamente de crear una nueva moneda sino de obtener fondos que serán cambiados por acciones, formar un capital riesgo descentralizado o bien ser un fondo de prepago para ciertos servicios, como el uso de espacio de almacenamiento en la nube (*ibidem*). Por ello, la Comisión de Bolsa y Valores de Estados Unidos (SEC) dijo en julio que considerará este tipo de fichas como títulos y no como moneda, y que *"cualquier token que funcione como un valor será regulado como tal"* (Technologyreview.es, 14/9/2017).

También se pueden crear criptomonedas para propósitos específicos, como lo hizo Burger King en Rusia: los clientes reciben un *"Whoppercoin"* en un monedero virtual por cada rublo gastado en su tienda y por 1.700 *Whoppercoins* reciben un burger gratis. También los pueden intercambiar con otros clientes, como otras criptomonedas (Adweek.com, 14/9/2017). Un medio de comunicación podría emitir su propio sistema de criptovalor como lo hizo Burger King.

En el futuro, se podrá probablemente cargar los pagos a las tarjetas de débito y de crédito: Mastercard ya entró en el sistema en Finlandia donde el Servicio de Inmigración la da a los solicitantes de asilo, junto con su identificación nacional (MIT Technology Review, 5/9/2017). Los bancos se han ido convenciendo de las bondades del sistema al punto que se unieron hace poco en una alianza internacional para establecer una plataforma y una moneda virtual común. La suiza UBS, Santander, BNY Mellon y Deutsche Bank formaron ya el año pasado la *Utility Settlement Coin* (USC). BBVA, Santander, Sabadell y Bankia, junto con Iberdrola, Gas Natural, Cepsa y Correos de España han formado la red Lyra, un consorcio español multisectorial de *blockchain* (Retina, El País, 13/9/2017). Barclays, Credit Suisse, Banco Imperial Canadiense de Comercio (CIBC), HSBC, Banco MUFG y State Street Bank también se unieron para crear una moneda digital basada en tecnología *blockchain*, que entraría a operar a finales de 2018 si logran el acuerdo de las autoridades reguladoras (TICbeat, 1/9/2017).

También se están interesando las bolsas como el Nasdaq o el NYSE (la bolsa de Nueva York), y grandes empresas como Microsoft, Dell, Wordpress y decenas de otras empresas del área tecnológica. (Microsiervos, 8/6/2016).

3. Operatividad

Recordemos que la cadena de bloques es un sistema distribuido que consiste en muchos nodos que se comunican entre sí. La cadena de bloques ejecuta los programas llamados *chaincode*, mantiene el estado y los datos del libro mayor y ejecuta las transacciones. El *chaincode* es el elemento central ya que las transacciones son operaciones invocadas en este *chaincode*. Las transacciones tienen que ser "endosadas" (verificadas) y solo las transacciones endosadas pueden ser realizadas y tener un efecto en el estado de la cadena. Puede existir uno o más códigos de cadena especiales para funciones y parámetros de gestión, denominados "códigos de cadena de sistema".

3.1. El contrato inteligente

Es evidente que la cadena de bloques puede aportar al periodista una forma de trabajar segura y también una alternativa financiera. Pero también proporciona una nueva modalidad de operación a los medios de prensa.

El trabajo debe basarse en el concepto y la mecánica del contrato inteligente (*"smart contract"*). Los expertos consideran que la cadena de bloques no es de ninguna utilidad si no hay algún tipo de contrato de por medio. Y, obviamente, solo se instalará si se consideran importantes sus características y beneficios y que estos compensarán el costo de instalación y operación. A nuestro juicio asegurar la confiabilidad de la autoría y la integridad de los contenidos nos parece lo más importante.

> "Un contrato inteligente es un acuerdo o conjunto de reglas que rigen una transacción comercial. Se almacena en la cadena de bloques y se ejecuta automáticamente como parte de una transacción. Los contratos inteligentes pueden tener muchas cláusulas contractuales que podrían auto-ejecutarse o auto-aplicarse total o parcialmente". (Gupta, p.17)

Así, un periodista podría tener un contrato con un editor en que se especifique que, si su texto (u otra producción) es visto por alguien, se le pagará una determinada cantidad. Y esto podría ocurrir en forma automática. Precisemos inmediatamente que el contrato ya es un tipo de contenido, que formará parte de la cadena de bloques, mientras la obra (el mensaje) es otro tipo de contenido, que no formará parte de la cadena pero le quedará estrechamente ligado y podría estar encriptado de modo que solo un usuario-miembro lo pueda abrir.

3.1.1. Definir objetivos y reglas

Así, después de estudiar el sistema (esperamos que este texto le ayude un poco), le conviene empezar definiendo sus objetivos. Pregúntese qué problema actual (o que visualiza a futuro) podría solucionar con esta tecnología; qué procesos podría supervisar mejor, qué resultados positivos podría obtener. ¿Su producto ganará en calidad a los ojos de sus destinatarios? ¿Reemplazará con ventaja su muro de pago si lo tiene o piensa implantarlo?

Los objetivos podrían ser, por ejemplo:

- asegurar el acceso a un mensaje con autenticidad e integridad verificados
- recoger un micropago por ello
- pagar al autor según el número de accesos (y eventualmente el tiempo de lectura)
- (en caso de acceso abierto) pagar al autor si su obra aparece en la primera página del buscador de Google[14].

Luego debe definirse el tipo de acceso adecuado para sus usuarios: privado o público. Podría tener un sistema de acceso privado para uso interno pero es evidente que, para un medio de comunicación, el acceso público es el indicado, aunque se podrán definir datos de libre acceso y otros de acceso limitado (sistema híbrido). Es importante también tener claro qué funciones pueden ser automatizadas y cuáles no.

Ahora se deberá definir los tipos de usuarios y el nivel de acceso para cada tipo. El nivel más alto, evidentemente, será para el administrador del sistema (nivel ingenieril), luego el administrador de

14 Requiere un contrato complementario llamado "Service Level Agreement".

contenidos (como el editor general) y el administrador comercial, los usuarios-proveedores de contenidos (p.ej. los periodistas) y, finalmente los destinatarios. Otros niveles y otros actores por cierto son posibles y deben ser definidos, con las correspondientes reglas de acceso y transacciones autorizadas.

Las reglas de acceso a la cadena, a los mensajes y eventualmente de pago, deben ser explicitadas primero en un texto (*"whitepaper"*) y luego traducidas en algoritmos y lenguaje de programación, para pasar a formar parte de la cadena de bloques (Detalles más adelante).

Hay que tomar en cuenta que *"a mayor complejidad de las condiciones, menor es la capacidad del contrato para realizarlas"* ya que exige más a los computadores que operan la cadena (Preukschat, p.141).

3.1.2. Programar el contrato

No hace falta saber programar para crear los contratos inteligentes porque existen sitios en la web que facilitan hacerlo mediante una interfaz WYSIWYG (*"What You See Is What You Get"*). Pero si uno sabe programar sus propios contratos, el nivel de control podrá ser mayor.

Debemos considerar dos partes: la Plataforma de *Smart Contracts* (SCP) y el Sistema de Gestión de *Smart Contracts* (SCMS). La plataforma puede ser el sistema Ethereum, HyperLedger o alguno similar. El SCMS es una superestructura que se sitúa encima del SCP, que permite usar el contrato como si fuera un servicio más. Permitiría, por ejemplo, ofrecer una forma gráfica de fácil uso para acceder a la lista de los contactos que han suscrito el contrato o de las obras disponibles, ver un calendario de publicación, conocer el autor o el editor y comprobar su registro de actividad.

La programación de una DApp se lleva a cabo en tres etapas:

1. redacción y publicación del libro blanco (*whitepaper*);
2. distribución inicial de la ficha (bloque génesis), con las reglas programadas;
3. distribución extendida de las fichas (bloques sucesivos) entre los participantes.

El libro blanco debe apuntar a formular las reglas a modo de «si esto, entonces aquello», que pueden ser pasadas fácilmente a algoritmos y a la programación informática.

Para todo propósito, se puede desarrollar un *frontend* ("fachada") para una DApp en HTML, exactamente como para desarrollar un sitio web, pero dado que el contrato está encriptado publicarlo no implica que pueda ser leído por terceros. Un medio de comunicación, por ejemplo, revelará en forma legible la parte que deben conocer sus suscriptores. El contrato mismo, encriptado, formará parte de la cadena de bloques.

La empresa norteamericana SmartContract[15] ofrece la posibilidad de crear diferentes tipos de contratos inteligentes sobre las *blockchains* de Bitcoin y Ethereum sin necesidad de saber programar.

15 Tiene una plataforma de pruebas en https://testnet.smartcontract.com/#/signup (Requiere registrarse con email y password).

Para la SCP, se suele utilizar Git, el sistema más popular de gestión y seguimiento de contenidos, de código abierto, desarrollado por Linus Torvalds, el creador del sistema operativo Linux. Si se han de cumplir condiciones externas (como aparecer en la primera página de Google Search para generar una remuneración), se redactan estas en el formato de Javascript JSON (que es un formato de texto). Ahí también se colocan los enlaces a las obras que se podrán consultar. El ejemplo adjunto de combinación de ambos es de Blockchainhealth, una plataforma de administración de datos médicos.

Ilustración 13: Git y Json, de Blockchainhealth

En el servicio SmartContract de creación del contrato, veríamos la interfaz siguiente (Ilustración 14) para ayudarnos a crear el contrato sin necesidad de programar, definiendo una a una las cláusulas. En Ethereum es mucho más complejo, como se puede ver en la Ilustración 15.

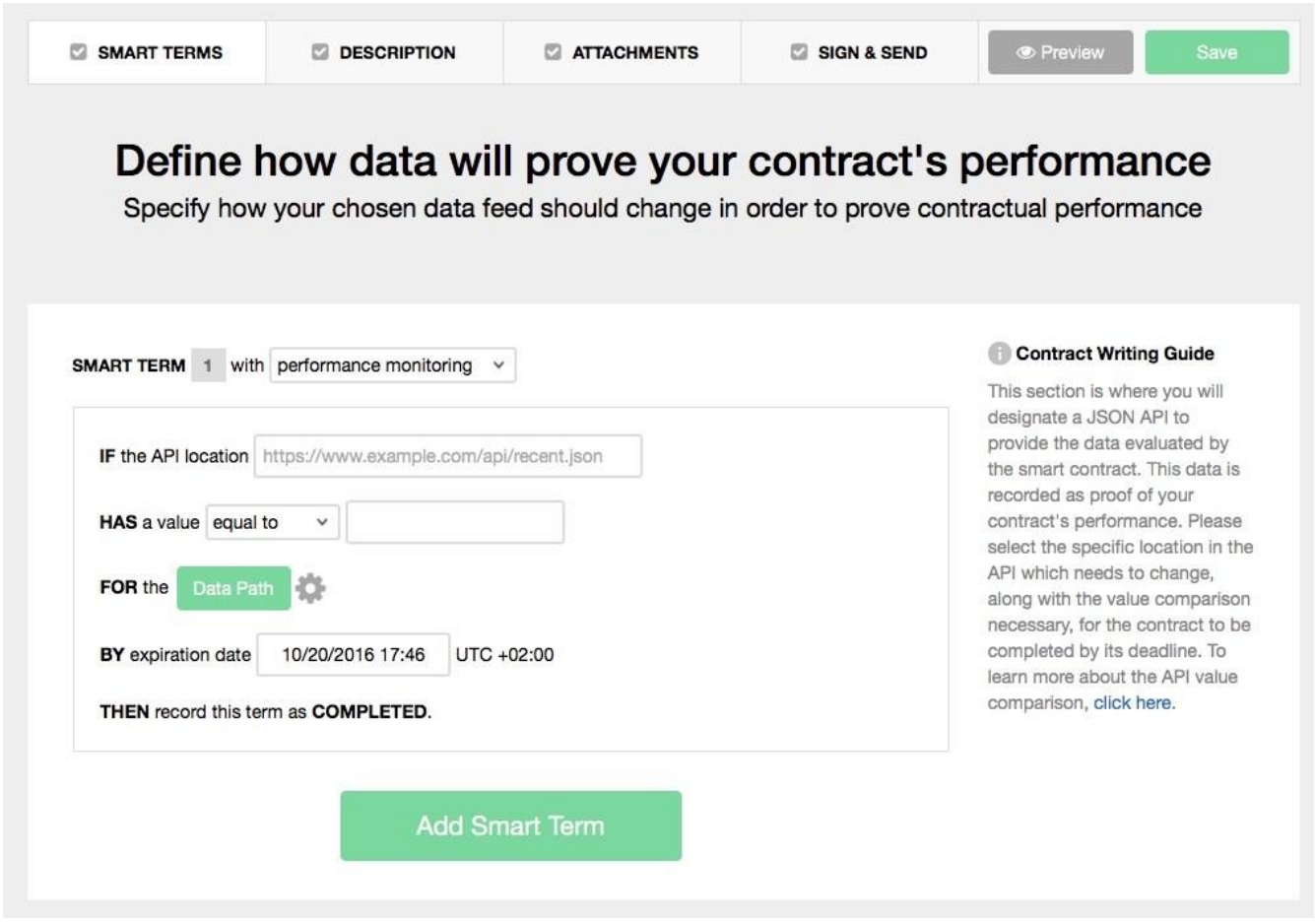


Ilustración 14: Interfaz de creación de contrato en SmartContract (de J.Morell)

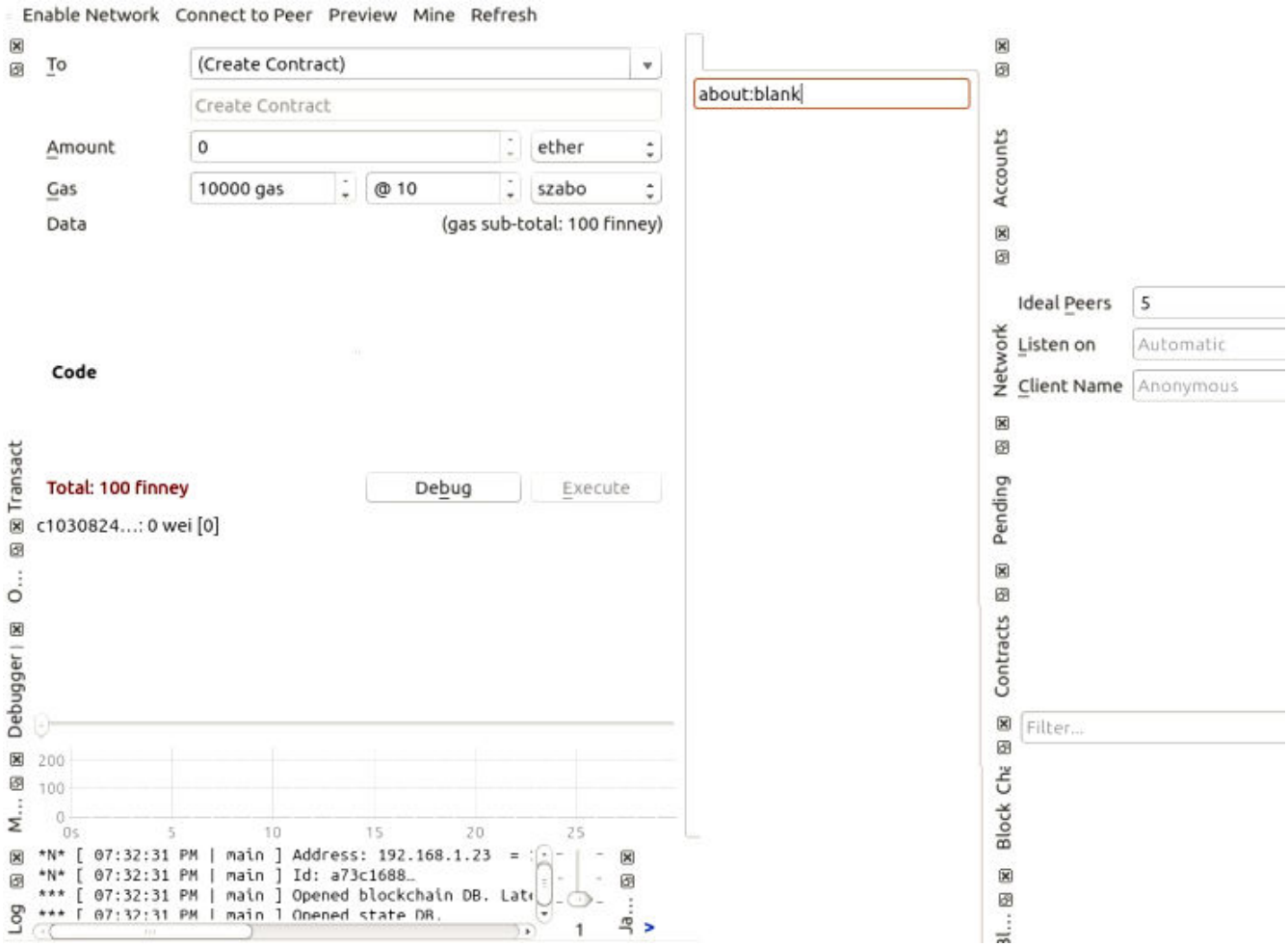


Ilustración 15: Interfaz de creación de contrato Ethereum (de S.Tual)

3.2. Contenidos de la cadena

Antes de construir el primer bloque ("bloque génesis"), hemos de asegurarnos de identificar correctamente el autor (o equipo productor) del mensaje y dar a este mensaje una clave única de identificación. Luego combinaremos esto con el contrato inteligente.

3.2.1. Identificar el autor

El primer elemento a considerar en el bloque es la identificación segura del profesional. Recurrir al número del documento nacional de identidad (DNI) es posiblemente la forma más adecuada actualmente si no se desea mantener el anonimato (en cuyo caso se creará una clave especial) y algunos países agregan ya también un código de identificación digital. Pronto, sin embargo, la identidad digital será certificada en *blockchain* por los mismos estados. Así, por ejemplo, el estado de Illinois (EE.UU.) acaba de anunciar un proyecto piloto de identificación de sus ciudadanos, con acceso a certificados de nacimiento, basado en cadena de bloques (Newscientist, 27/9/2017). El Reino Unido y Brasil también lo estarían estudiando. Finlandia ya lo hace para los inmigrantes. Y las mismas Naciones Unidas están explorando el uso de esta

tecnología para ofrecer identificación legal a más de mil millones de personas que no tienen documentos oficiales (MIT Technology Review, 5/9/2017).

Otros datos más detallados podrán ir en un documento anexo consultable (por ejemplo un *curriculum vitae*) y autenticado. Cómo señalado, esto no quita la posibilidad de utilizar el anonimato, reemplazando el DNI por otro código único, asociándolo a un anexo que solo dé algunos antecedentes que respalden la idoneidad. En un caso como en el otro, la seguridad exige que utilicemos la criptografía para que los datos sean autenticados y se pueda verificar su integridad.

> "Desde el punto de vista de la identidad, puedo imaginar una cadena de bloques que gestione la verificación de la identidad de un ciudadano. Un contrato inteligente podría asegurar algo como mi hija que va saliendo por su 21 cumpleaños y el portero [adonde va] sólo puede ver su edad, no su dirección. La cadena de bloques puede establecer un sistema centralizado de verificación de identidad que podría hacer el mundo más seguro para los papás como yo", dice Jerry Cuomo, vicepresidente de Blockchain Technologies en IBM. (PC Magazine, 29/8/2017)

Existen tres tipos de procesos criptográficos que permiten realizar y utilizar esta función y uno de ellos es el *"hashing"*, que es el que se utiliza en las cadenas de bloques. El hash es una especie de huella digital propia de un documento. Esto es un típico proceso criptográfico, que transforma algo "legible" en una cadena de caracteres única, sin ningún significado inteligible. *"Siempre que apliquemos la misma función al mismo contenido, obtendremos el mismo hash."* (Nuñez, en Preukschat, p.205). Cualquier alteración cambiaría el hash.

Mensaje	Resultado hash (hexadecimal)
«Perro»	5CDC4F3FEB31CEB78
«El perro de San Roque»	96C32852CB4C69E71
«El perro de San Roque.»	20B003E7747353A6F

Ilustración 16: Ejemplo de hash, de Preukschat, p.204
(Nótese el cambio debido al punto agregado en la tercera frase.)

El hash en una cadena de bloques se realiza recurriendo al protocolo SHA256 (*Safe Hashing Algorithm*)[16]. Como es largo y, por lo tanto, difícil de reproducir, se le aplica generalmente un programa que lo acorta (como los que acortan las direcciones web). Es casi imposible prever de antemano el hash que resultará de la función de cálculo y lo es también de que dos mensajes produzcan el mismo hash. Tampoco es posible, a partir de un hash, reconstruir el mensaje que lo originó. Así, se garantiza totalmente la integridad de un documento aunque, por sí mismo, no da acceso al contenido original. Para ello, hay que utilizar otro sistema.

> "Una de las ventajas que proporcionan los protocolos *blockchain* es que gracias a la criptografía asociada, la información puede separarse de la identidad. Por ejemplo, yo podría subir un artículo con mi sello criptográfico y que la red social pueda ver que soy un autor válido e identificado para generar esa noticia." (Carlos Kuchkovsky, CTO de nuevos negocios digitales BBVA, Criptonoticias, 21/01/2017)

16 El algoritmo SHA ha sido diseñado por la Agencia Nacional de Seguridad (NSA) de los Estados Unidos y aceptado como estándar por el Instituto Nacional de Estándares y Tecnología (NIST) de dicho país.

Blockstack, por ejemplo, utiliza una cadena de bloques para rastrear nombres de usuarios y claves de cifrado, la base de este nuevo tipo de sistema de identidad que no estaría vinculado a ninguna red social u otro sitio web. En Blockstack, el autor de un documento puede incluir como valor cualquier información de identificación relevante (como su sitio web o perfil) y luego (asumiendo que su clave privada no está comprometida) realizar cambios asociados con ese nombre sin que nadie más pueda hacer modificaciones. Se puede usar como una capa agregada sobre los bloques de Bitcoin. (Ver Barabas & alt. pp.51-59).

Aunque podemos utilizar un seudónimo o un mero código, el anonimato no es absoluto:

> "Los expertos en seguridad lo llaman privacidad seudónima, como escribir libros bajo un alias. Usted puede preservar su privacidad, siempre y cuando no esté vinculado al seudónimo. Pero en cuanto se crea un vínculo con uno de sus libros, la artimaña se revela. Todo su historial de escritura bajo su seudónimo se convierte en público. Del mismo modo, tan pronto como sus datos personales se vinculan a su dirección de Bitcoin, su historial de compra también se descubre." (MIT Technology Review, 29/8/2017)

3.2.2. Identificar el mensaje

Para poder definir los contenidos de la cadena de bloques, conviene definir luego el activo, en este caso lo que llamamos habitualmente "el mensaje", es decir el producto (sonoro, escrito o audiovisual) que se desea transmitir, y definir de qué manera se asegurará su identidad única e inmodificable.

Existen varias alternativas para la identificación única del contenido: desde los clásicos DOI para artículos académicos, ISBN para libros, y los registros nacionales de propiedad intelectual -para todo tipo de obra- hasta los nuevos registros digitales con protocolos descentralizados, como Mediachain.io, o plataformas que ofrecen tanto la identificación como, además, almacenar y distribuir las obras. Pero registros como el DOI y el ISBN sólo aseguran la relación entre un título y un autor (o varios). No garantizan que una copia sea auténtica e íntegra. Para ello es indispensable recurrir a un sistema matemático que calcula una "suma de control" (*"checksum"*), como lo hace el algoritmo SHA (Existen ya varios sistemas que aseguran de este modo la autenticidad de un mensaje, como SPF y DKIM, además de la antigua firma PGP). Cualquier modificación que se haga a la obra original desembocaría en una *checksum* diferente, lo cual asegura la integridad y autenticidad, indispensable para la confiabilidad de la investigación científica pero también la del periodismo. Irving y Holden[17] han mostrado como el protocolo de las cadenas de bloques puede mejorar la confiabilidad de la ciencia médica y lo mismo vale para cualquier otro tipo de contenido.

> "Las organizaciones pueden aplicar cadenas de bloques mediante la emisión de certificados de nacimiento[18] digitalmente autenticados que son inolvidables, con hora marcada y accesible a cualquier persona en el mundo." (Gupta, p.28)

Cómo funciona un servicio de registro de una obra (Seguimos aquí el ejemplo de Binded.com, servicio de registro de fotografías[19]):

1. "Subir" la obra. Puede ser desde la computadora personal o incluso, eventualmente, (depende de la plataforma) del teléfono o una red social (como Instagram para las fotos).

17 Ver Bibliografía
18 De un documento.
19 Binded también realiza la detección de quienes infrinjan eventualmente el copyright.

2. Registrar los derechos de autor (*copyright* o equivalente). El servicio creará una huella digital única guardada permanentemente en la cadena de bits.
3. Obtener el certificado. El servicio genera un certificado de *copyright* como prueba que puede ayudar a protegerse contra la infracción de derechos de autor.

Obviamente, un medio de comunicación puede hacerlo sin recurrir a este tipo de servicio y lo puede hacer utilizando en mismo protocolo SHA.

Como el plagio nunca ha sido tan fácil y se hace extremadamente difícil "seguir la pista" de las reproducciones incluso legítimas o de los enlaces y citas en redes sociales, la cadena de bloques le aporta una solución: cada vez que se comparte un contenido, hace posible avisar de ello a su autor, dando origen a un sistema universal de rastreo y notificación. Y también, si se desea, guiar hacia otras obras, por ejemplo ofreciendo acceder a una bibliografía complementaria (Preukschat, p.113).

3.2.3. Fijar el valor

Mientras internet ha dado a todos sus usuarios la posibilidad de acceder a innumerables contenidos, el mayor problema, para muchos autores y para los editores, es que la difusión de sus obras en los canales digitales es muy difícil de retribuir. El mecanismo de la cadena de bloques trae la posibilidad de condicionar la recepción al cobro de cantidades hasta ínfimas (hay plataformas que consideran desde 0,01 euro), lo cual es una excelente alternativa para los "muros de pago" y ya está siendo utilizado por algunos importantes medios noticiosos. Cada emisor puede definir sus propias reglas: acceso gratuito, cobro por acceso o incluso por tiempo de visionado. Es lo que permite el *smart contract*.

> "La *startup* de origen holandés Blendle, que cuenta con el respaldo del diario The New York Times y Axel Springer, ha conseguido en dos años que alrededor de 200.000 usuarios paguen por leer contenidos sin necesidad de suscribirse al medio ni consumir publicidad no deseada." (Preukschat, p.86)

Ilustración 17: De Bendle

Para el cobro, los receptores deberán obviamente disponer de un monedero virtual en la criptomoneda que se haya elegido o creado. Mientras los bancos locales no adopten un sistema de criptodivisa, el medio de comunicación podría operar con la forma tradicional de cobro de suscripción (tarjeta de débito o crédito o transferencia digital) dando al usuario una suerte de criptotarjeta de prepago que lo habilitará para adquirir tiempo de lectura o acceso a contenidos específicos, según lo establecido en el contrato inteligente. Del mismo modo podrá pagar a sus periodistas y otros creadores de contenidos según el contrato.

3.2.4. Anexar el contenido (mensaje)

Como hemos visto, la esencia de la cadena de bloques es el registro de transacciones. Los contratos inteligentes implican identificar las partes del contrato, las condiciones del mismo y las reglas de aplicación. Si todos los usuarios mantienen una copia de la cadena de bloques, es evidente que no se les puede recargar con copias de todos los contenidos que pueden publicar un medio de comunicación. ¿Cómo pueden ser integrados o asociados entonces al contrato los contenidos periodísticos o multimediales? Un servicio puede construir una red separada que puede almacenar más información y luego usar criptografía para codificar esa información como una cadena de números y letras -identificadora- lo suficientemente pequeña como para ser escrita en la cadena de bloques (MIT Technology Review, 8/5/2015). El típico mensaje publicado en un medio de comunicación se considerará como un "anexo", ligado a este a través de la identificación de la obra (etiquetado), la cual es también un elemento clave del contrato. Se le puede agregar la identificación del autor o editor, que puede a su vez remitir a un anexo relativo a este. Esta relación puede establecerse de varias maneras. Visualizamos las siguientes posibles opciones (no excluyentes):

Opción 1: Una primera posibilidad sería adjuntar al documento público (p.ej. una página web con titulares) un enlace en el que se pueda libremente "pinchar" para acceder a datos incluidos en la cadena de bloques. Esta puede contener datos visibles para todos, como el nombre del autor, y datos reservados para cierto tipo de usuarios, como el editor y el autor, y el pago del primero al segundo. Se podría además efectuar una *"checksum"* de la obra e integrar esta al contrato. El contenido disponible "en abierto" podría estar acompañado de un micro-programa que calcule y muestre su propia *"checksum",* un enlace a la cadena de bloques permitiendo realizar la comparación. De este modo, se aseguraría su integridad y se impediría cualquier alteración.

Opción 2: Integrar en el contrato la URL del contenido al cual los receptores podrán acceder siempre que acepten el contrato en la parte que les corresponde. Se podría también publicar abiertamente en la web el título de la obra y su autor, con un enlace a la cadena de bloques.

Opción 3: Presentar en forma abierta y legible exclusivamente las condiciones del contrato, solicitando al destinatario interesado identificarse, creando una cadena o un documento anexo con sus datos, e ingresando luego la referencia a la cadena de bloques de la obra o colección. Aquí es posible tanto inscribir suscriptores como lectores ocasionales, cobrando montos diferenciados por cada acceso.

En la ilustración que sigue, que corresponde al servicio de Mycelia para músicos, se pueden ver los múltiples anexos que dicho servicio contempla.

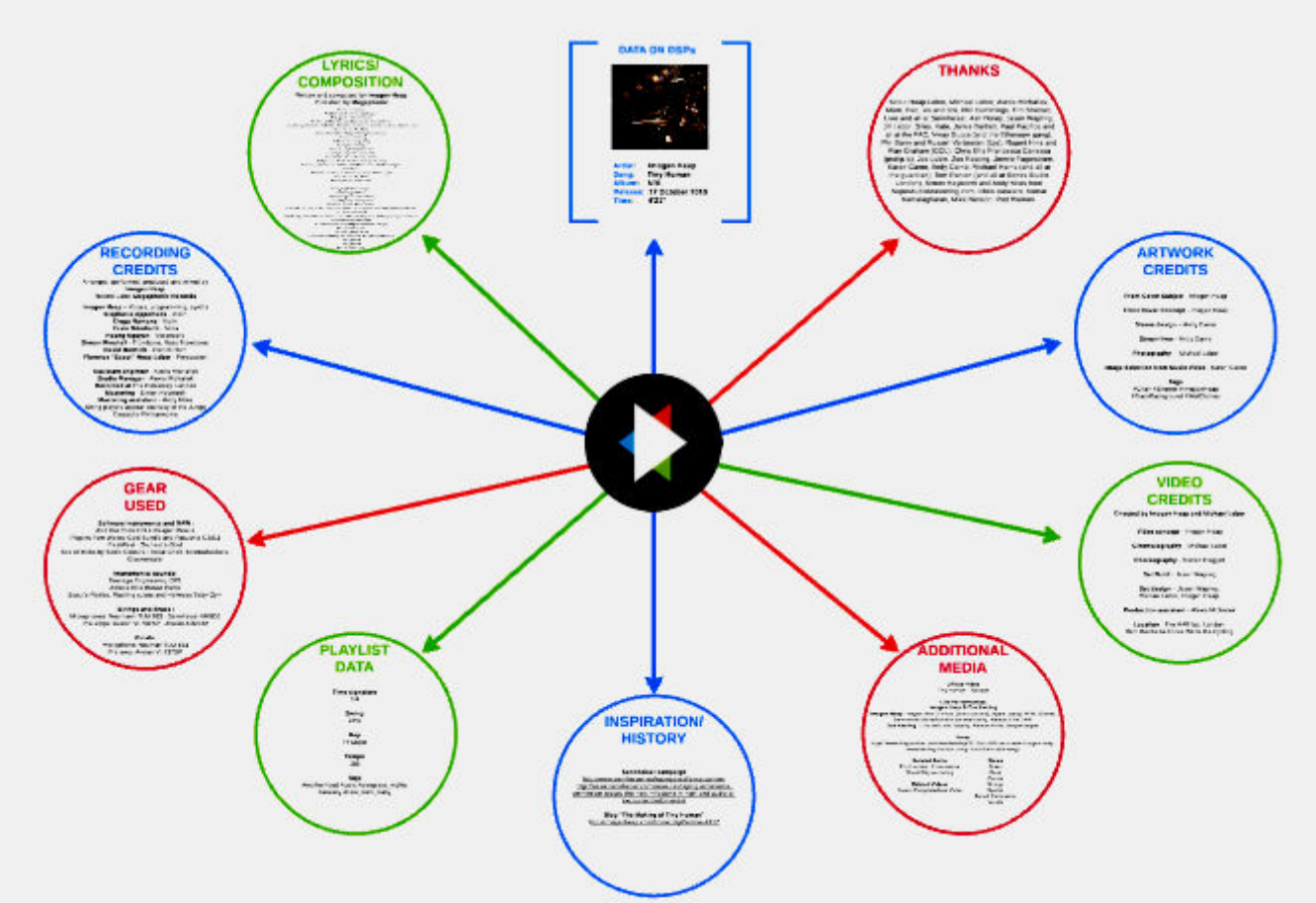


Ilustración 18: Los anexos de Mycelia

3.3. El bloque de datos

3.3.1. Contenido

Es el momento de definir los datos que deberán contener la cadena de bloques. El bloque inicial es conocido como "bloque génesis" y tiene el número 0.
Los contenidos de un bloque (aquí los típicos de bloques de criptomonedas) son:

1. Número arbitrario, definido por el creador del protocolo ("mágico" en la ilustración adjunta)
2. Tamaño del bloque
3. Cabecera, que contiene la versión del bloque, el hash del bloque anterior, el hash de la raíz del árbol de transacciones, la marca de tiempo (fecha y hora), el valor asociado a la dificultad requerida para generar el bloque y el nonce (bloque de 32 bits cuyo valor se establece de modo que el hash del bloque se inicie con una ristra de ceros, lo que confirma la validez del bloque).
4. Cantidad de transacciones ya efectuadas
5. Lista de las transacciones y datos.

Ilustración 19: Modelo de bloque (según Mediumcom/ all-things-ledger)

En los datos se podrá poner el código de certificación/identificación del documento (mensaje medial), incluyendo necesariamente su fecha y eventualmente con que *hardware* y *software* ha sido producido (como los datos que se registran al tomar una foto). Como ya señalado, se puede utilizar el mismo protocolo SHA256 del *blockchain* para obtener una clave única -una *checksum*- que represente la integridad del documento y luego ingresarla en el bloque. Cualquier cambio realizado en el documento original genera una clave SHA256 diferente que indicará que el documento ha sido alterado: es lo que permite, por ejemplo, seguir su evolución si varias personas trabajan en un mismo documento, cada cambio pudiendo ser considerado una transacción y ser agregado a la cadena de bloques.

Preukschat nos recuerda lo difícil que puede ser identificar y remunerar todos los intervinientes en una obra musical. Con la cadena de bloques, cada uno puede quedar registrado al mismo tiempo que la remuneración proporcional que le corresponde y esta le puede ser remitida en forma automática, simplificando enormemente el proceso y superando la "anticuada contabilidad" del sector de la música (p.115). (Ver ilustración siguiente).

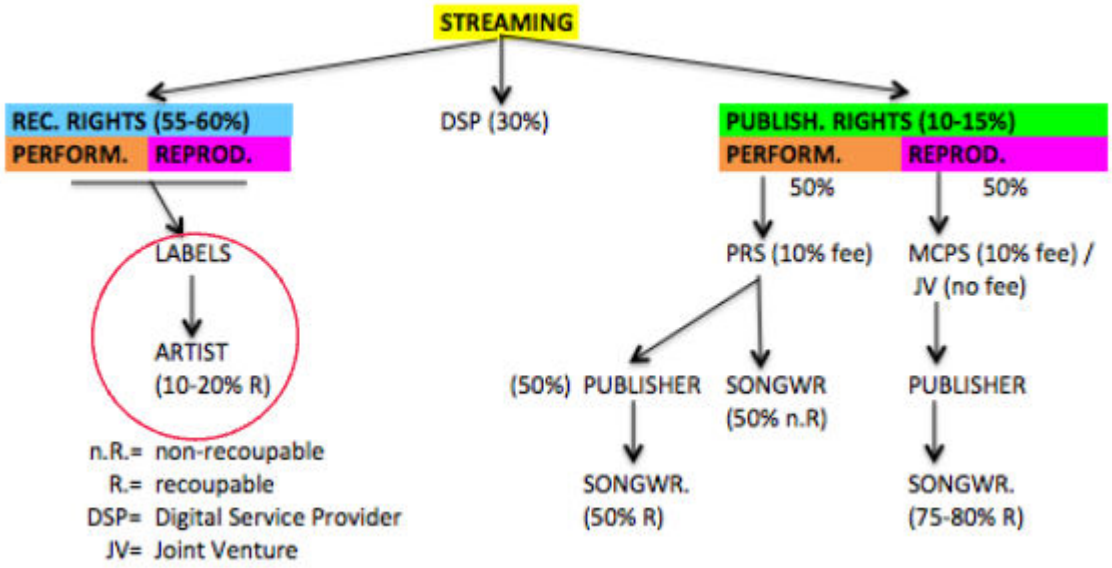


Ilustración 20: Financiación en caso de streaming, en Mycelia

También se puede pensar en incluir un algoritmo de valoración (como las estrellas de Amazon) o que registre la adición de un comentario (en un anexo), e incluso hacer que este sea remunerado, por ejemplo con un acceso gratuito a ciertos contenidos o un descuento futuro. *"El uso de las identidades digitales descentralizadas permite además a todos los usuarios votar de forma transparente y comprobable."* (C.Kuchkowsky, en Preukschat, p.270).

Es importante tomar en cuenta que cada bloque contiene un número de transacciones que va creciendo con el tiempo y en cada transacción se almacenan una serie de datos como el remitente, el destinatario, el monto y la eventual tarifa. Cuando un bloque tiene muchas transacciones, es necesario establecer un registro antes de pasar al siguiente bloque y su validación tomará más tiempo (más trabajo de computador y más gasto de energía). Todo depende por lo tanto de la cantidad de información contenida en cada bloque. La capacidad operativa de la red de usuarios se mejora aumentando la capacidad máxima (fija) de los

bloques, como lo propone la alternativa de escalabilidad SegWit (*Segregated Witness*), que la duplica. (Coincrispy, 22/8/2017).

Cuando la cadena se va alargando y los datos de los bloques aumentan, esto puede ser un problema para la validación consensuada (que exige un buen procesador y consume tiempo y energía) si se pretende que participen en ella todos los clientes, lo cual no es ni indispensable ni exigible en un medio masivo. Como ya señalado, es posible definir varios tipos de usuarios - con acceso a diferentes procesos y tipos de datos - y dejar que la validación de un nuevo bloque quede en manos de un grupo reducido (los "mineros"), por ejemplo miembros de la misma empresas con PC más poderosos o clientes empresariales (que podrían así ganar fichas intercambiables por derechos de lectura).

3.3.2. Tecnología

Lo anterior nos permite visualizar tres grupos de datos, que Preukschat llama "capas":

> "La primera de ellas es la capa *blockchain* (una *blockchain* como Bitcoin o Ethereum, o las que sean relevantes en el futuro), que sería la encargada de gestionar el procesamiento de los contenidos digitales. La segunda estaría especializada en el etiquetado (un protocolo como Coala IP o Mediachain, por ejemplo) y sería la que gestionará los metadatos de los contenidos de forma descentralizada. La tercera y última capa es la de almacenamiento, que podría ser un servicio como IPFS (*InterPlanetary File System*) en combinación con IPDB (*InterPlanetary Database*)." (Preukschat, p.116).

Blockchainhealth muestra del siguiente modo (Ilustración 21) cómo son sus tres capas, pero en columnas: la primera columna contiene los datos de identificación de cada activo (paciente en su caso) y datos de transacción, la segunda la identificación y descripción de un documento anexo y los permisos de acceso, y la tercera los archivos asociados. También podemos visualizar las capas una sobre otra como en la Ilustración 22, pensando en el tipo de aplicaciones involucradas.

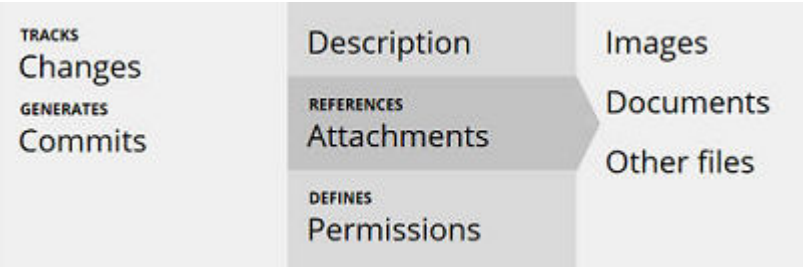


Ilustración 21: Grupos de datos (capas), de Blockchainhealth

Finalmente podemos considerar otras aplicaciones, como las interfaces de programación de aplicaciones (API) que proveen un estándar de código abierto para su alojamiento en páginas web, normalización y compartición de datos.

En la ilustración 23 se puede observar como opera una plataforma para recibir e insertar en la cadena de bloques un nuevo documento. En el recuadro señalado en verde, se puede ver -de abajo hacia arriba-, las etapas de "carga del documento" (*"Content Submit"*), el comprobante (*"Proof of Custody"*), la generación de clave (*"Deliver Keys"*) y finalmente la comprobación de la publicación (*"Published"*). Las otras líneas (fuera del rectángulo marcado en verde) corresponden a otras operaciones registradas en el bloque.

Ilustración 22, inspirada de Preukschat, p.263

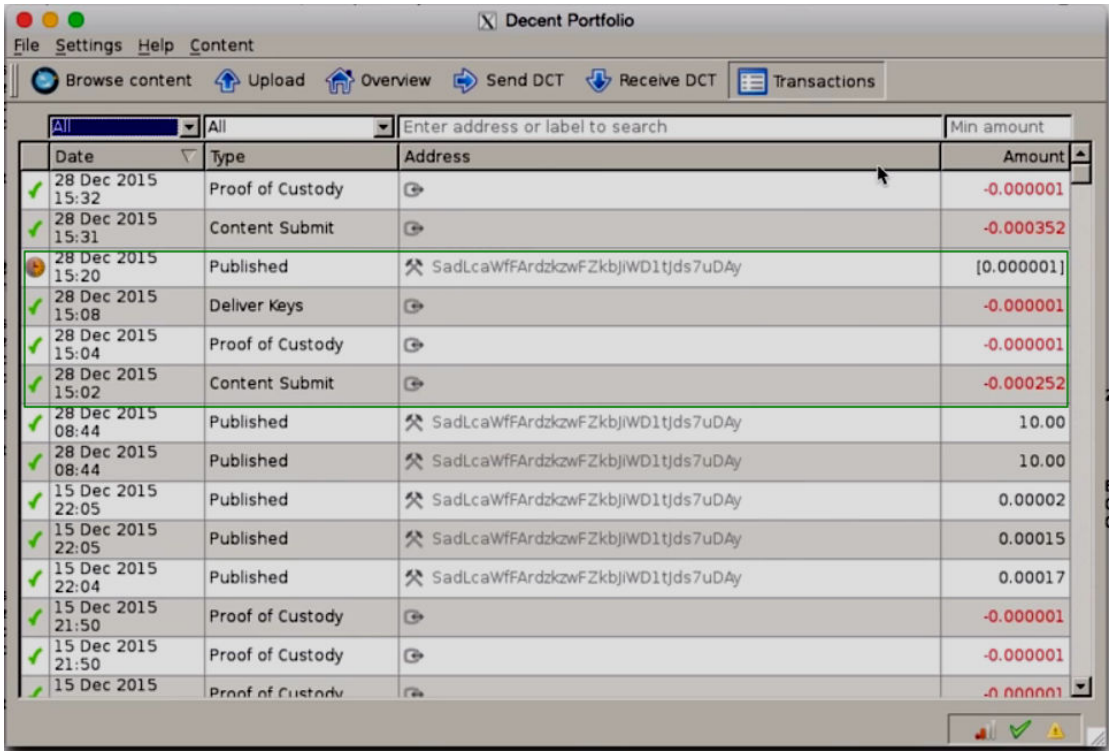


Ilustración 23: De la plataforma Decent

3.4. Difusión

Como ya señalada, la web sigue siendo el canal de soporte de las cadenas de bloques públicas o híbridas.

Para el **acceso de los usuarios,** el emisor (medio de comunicación o periodista independiente) podrá utilizar una página web común con el típico formulario de acceso con *login* y *password*. Este podrá ser la clave criptográfica que identifique el cliente en la cadena de bloques. Según el contrato podrá ver luego los enlaces a los documentos a los cuales podrá tener acceso o, si es un proveedor de contenidos, pasar a la página y formulario destinados a "cargar" y codificar este contenido.

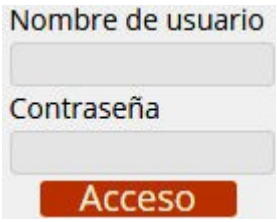


Ilustración 24

> "La autenticación es complementaria a la confidencialidad y el paso previo que nos permite o no conectar con la cadena. Una vez que la conexión ha sido realizada, es posible el acceso a la información, pero no antes. La autenticación de usuarios en las cadenas públicas es un mero intercambio de parámetros de conexión, puesto que todos los ordenadores tienen el mismo derecho a usar la cadena y, por ende, a conectarse." (Preukschat, p.230)

Nada impide que el emisor siga publicando sus titulares en las redes sociales ya que los puede enlazar a esa página de acceso. Si quiere que el contenido solo pueda ser conocido por un destinatario determinado ("mensaje secreto"), deberá recurrir al sistema de clave pública y clave privada (criptografía asimétrica), que también se usa en las cadenas de bloques. Esto podría posiblemente ser útil en un sistema de suscripción (*"paywall"*) en que la clave se dé a conocer a todos los suscriptores y solo a ellos cuando se suscriben al servicio, la clave privada - que es como una contraseña - siendo la que autoriza el pago cuando la ingresa el suscriptor.

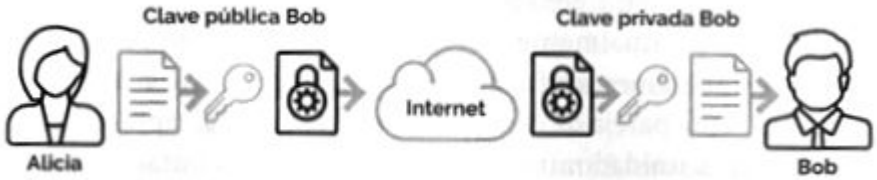


Ilustración 25: Claves pública y privada
(De Nuñez, en Preukschat, p.209)

La clave privada es un número aleatorio de 256 bits que cualquier persona puede generar y no contiene ningún dato personal. A partir de esta clave, se genera la clave pública, pero lo inverso es imposible (con la clave pública es imposible descubrir la clave privada). Así, cualquiera puede encriptar un contenido con la clave pública que se le da a conocer pero solo el destinatario puede decodificar el mensaje. Esta clave se puede generar cuando un destinatario se registra como suscriptor.

Adams y Jourdan, de la Universidad de Ottawa, han demostrado la posibilidad de generar claves públicas y privadas que sean fáciles de usar en múltiples dispositivos[20], e Irving y Holden han demostrado que se puede incluir el proceso de control en la operación de la cadena de bloques en el caso de fichas médicas. Sin duda, lo mismo es posible para cualquier tipo de mensaje digital.

20 Adams, C. & Jourdan, G.V. (2014): "Digital signatures for mobile users". IEEE Xplore, http://ieeexplore.ieee.org/document/6900969/

El *smart contract* podría tener en una capa extra el *script* (programa) que ofrezca la opción de verificación de un eventual contenido de acceso público, con una sencilla interfaz como la siguiente, inspirada de un software de *checksum*.

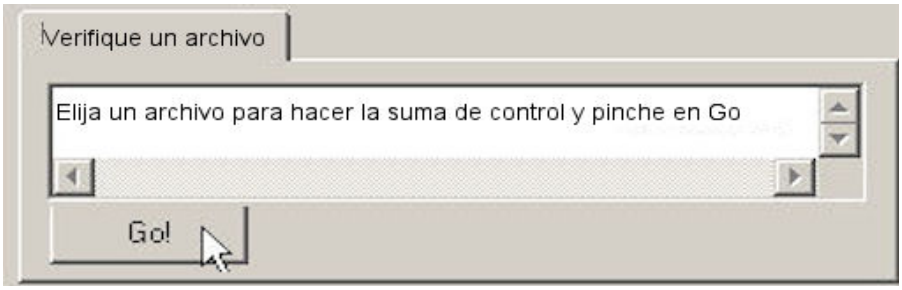


Ilustración 26: Opción de cálculo de suma de control

Es posible también recurrir a un navegador especializado como Brave, aunque podría ser difícil lograr que se universalice pronto. *"Su principal característica es que permite ver contenidos sin publicidad distribuyendo bitcoins a las webs de contenidos desde el navegador del lector según el tiempo que dedica a cada página"*, algo que no le ha gustado a periódicos importantes como The New York Times o The Washington Post, que se quejaron al CEO de Brave. (Preukschat, p.87)

Existen sin embargo proyectos de protocolos descentralizados que apuntan a reemplazar el protocolo HTTP de la web, como Blockstack, Permacoin, Storj e IPFS (*Inter Planetary File System*). El funcionamiento sería parecido al sistema de descarga de archivos (muchas veces pirateados) BitTorrent, uniendo los usuarios en una red de relaciones P2P. Blockstack, por ejemplo, tiene un nuevo sistema de servidores de nombres (DNS) basado en una cadena de bloques con dominios .id. Los actuales navegadores podrían ser compatibles con este sistema en el futuro. (Preukschat, p.122)

3.5. Resumen operativo

En el gráfico 27 reunimos las diferentes etapas de la operación del sistema. Suponemos que la identificación codificada del autor (ID) se ingresa en el bloque génesis mientras la de un lector se ingresa en algún bloque posterior. Los eventuales antecedentes relativos al autor pueden ser tratados como una "obra" más. La obra original se identifica criptográficamente (SHA) para incluir en el bloque mientras la versión no encriptada se maneja como elemento anexo (que se podrá verificar con *checksum,* no incluido en el gráfico) y su lectura podrá dar origen a un cobro para el lector y un pago para el autor, que se agregan en la cadena de bloques. La ilustración 28 entrega otra visión del ciclo.

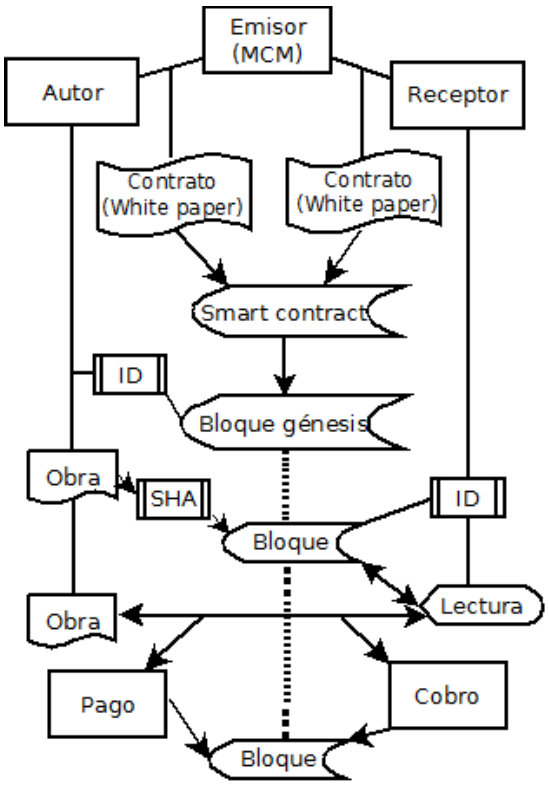


Ilustración 27: Descripción del sistema (Producción propia)

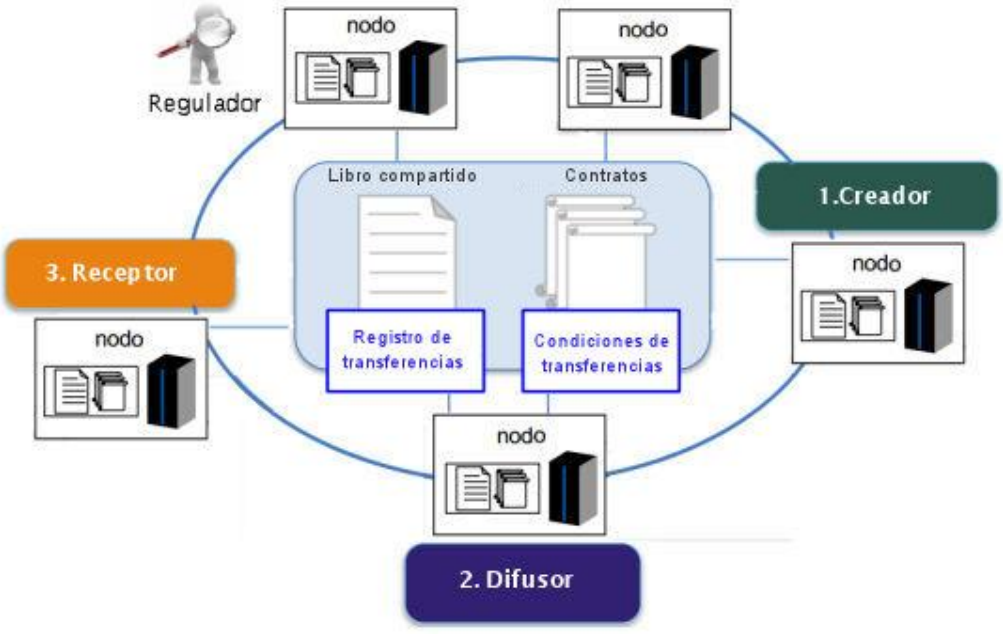


Ilustración 28: Ciclo de uso (adaptado de Altoros)

4. Periodismo y medios

4.1. El ejercicio de la profesión

Como señaló Henrik Kaufholz, periodista del diario danés Politiken y presidente del Centro Europeo para la Libertad de Prensa, con la cadena de bloques los periodistas *"podrán ejercer su profesión de forma totalmente anónima, garantizando su independencia y siendo remunerados por ello."* (Criptonoticias, 21/01/2017). Covadonga Fernández agrega que *"Los periodistas podrán desarrollar su trabajo en plataformas tipo Uber -pero sin intermediarios- y ser remunerados directamente por los usuarios con criptodivisas."* (Retina, El País, 14/6/2017)

> "La relación entre las salas de redacción y los periodistas independientes está en problemas. Por un lado están las redacciones, que continúan despidiendo y reducen los presupuestos. Por otro lado están los nuevos periodistas, aburridos de trabajar a tiempo completo en un medio tradicional." (Stanford.edu, 22/6/2017)

Los periodistas podrían depender cada vez menos de un medio particular (y los medios deberían abrirse a los aportes de *freelancers*, especialmente para temas especializados.

> "Blockchain también permitirá a cada periodista definir su propio modelo de negocio en cada contenido, porque esta tecnología permite crear reglas de utilización para cada producto periodístico. Así, cualquier periodista podrá programar con *smart contracts* las condiciones concretas en las que quiere que se consuma su contenido." (Retina, El País, 14/6/2017)

4.2. Los medios de prensa

Ante el reto de la viabilidad económica, el sistema de cadena de bloques podría ser una solución para los medios que buscan la forma de rentabilizar su negocio. No solo tendrían una forma de remunerar los periodistas de acuerdo a lo que aportan, también podrían *"ofrecer a los anunciantes una estrategia integral para llegar por los diferentes canales a las audiencias y hacerlo, además, de distinta manera a cada una de ellas, ofreciendo distintas narraciones que las conecten con los productos o servicios ofertados por los anunciantes"*. (El Economista, 21/3/2017)

Sin embargo, los medios se encuentran con otro tipo de reto: el de transformar su estructura y su forma de operar hacia un modelo más descentralizado:

> "*Blockchain* promete democratizar todos los mercados aún más que internet y llevarnos a entornos más colaborativos y descentralizados. Tal vez sea éste el reto que *Blockchain* plantea a los medios de comunicación, es decir, cómo llevar a cabo su producción de bienes y servicios (noticias y entretenimiento, fundamentalmente) de una manera más colaborativa y descentralizada. Hay que tener en cuenta que, hasta ahora, la lógica del funcionamiento de los medios de comunicación ha sido justamente la contraria, actuando como focos centralizadores de lo que estaba más o menos disperso: el medio centralizaba todo un flujo de información que está difuso, que surgía aquí y allá, y lo centralizaba bajo su marca, dando una especie de certificado de «existencia». ¿Seguirá esto siendo así?" (El Economista, 21/3/2017)

> "Aunque aún existen muchas dudas sobre cómo puede aplicarse esta tecnología en los medios tradicionales, está claro que puede ser una herramienta fundamental para conocer la trazabilidad de los productos periodísticos. Lo que significará que, tanto el medio que publica el contenido, como el creador del mismo, puedan conocer en todo momento quién reproduce sus trabajos, dónde y cuántas veces, lo que les permitirá cobrar derechos de autor por ello." (C.Fernández, en El País, 14/6/2017)

4.3. Otros medios

Ya hay editoriales que se están interesando por la cadena de bloques: *"El director de Experiencia del Grupo Prisa, Alberto Barreiro, ha indicado que su compañía está empezando a explorar las aplicaciones de Blockchain para los medios tradicionales."* (La Vanguardia 23/01/2017). *"Prisa, primer grupo editorial español en explorar la integración de blockchain en su modelo de negocio"* tituló Criptonoticias (21/01/2017). La cadena de bloques permite gestionar con facilidad los derechos de autor de los contenidos, con lo cual los editores podrán establecer una relación más de igualdad con las plataformas digitales en que puedan aparecer dichos contenidos. Las agencias de noticias, sin duda, seguirán.

> "Los grupos editoriales y agencias de noticias tienen dificultad para escalar por los costes fijos. Con la barrera de la contratación rota ya se pueden crear agencias de noticias totalmente digitales. Serían modelos de negocio que conectan a periodistas con medios.
> Gómez Toribio[21] añadió que *blockchain* permite controlar el ciclo de vida de las publicaciones, desde que se escribe el contenido hasta que se publica en un medio. Esto permitirá medir el beneficio que genera cada contenido y remunerar al periodista en función de ello. «Medir la eficiencia por periodista y por artículo permitirá que los medios ajusten su operativa y que sean mucho más eficientes, pero transformará radicalmente la profesión de periodista»." (Criptonoticias, 21/01/2017)

La estación de radio WBUR de Boston, con su proyecto BizLab, empezó a experimentar con música en cadena de bloques. (Niemanlab.org, 1/9/2016). Singular DTV, una plataforma de contenidos digitales, articulada sobre la red de Ethereum, ha anunciado que está construyendo *"una nueva industria descentralizada del entretenimiento"*. Propone que la audiencia se convierta en productora de los contenidos que le gustaría ver (recurriendo al *crowdfunding*). Así, sólo llevaría a cabo los proyectos en los que la audiencia ha mostrado un interés previo. (Retina, El País, 14/6/2017)

4.4. Una internet diferente

Tim Berners-Lee considera que internet está bajo una gran amenaza de parte de personas que *"quieren controlarla a escondidas con leyes preocupantes"* (FayerWayer, 9/06/2013). Para hacerle frente propone un modelo descentralizado y se encuentra trabajando en el desarrollo de una plataforma de fuente abierta llamada *Solid*, en el marco del *"Decentralized Information Group"* del laboratorio de computación del MIT (*Laboratory for Computer Science and Artificial Intelligence, CSAIL*). (Wired, 4/4/2017). Apunta a una comunicación de persona a persona (P2P), sin servidores centrales. El sistema de cadena de bloques va en esta dirección, aunque hoy involucra aún plataformas, principalmente para ofrecer el servicio a personas e instituciones que no pueden desarrollar su propio servicio.

21 Alberto Gómez Toribio, CTO de *blockchain* en Barrabés Biz

En la introducción, reprodujimos varios comentarios acerca del papel que podrían jugar las cadenas de bloques en el desarrollo de una internet diferente y más segura. Conviene subrayar que sería una alternativa frente a otro proyecto de "internet segura", conocido como "*handle system"*, un sistema que se "cocina" en *"oscuras salas traseras de la gobernanza de Internet"* (NewScientist, 10/8/2017). ¿De que se trata?

La internet no se creó pensando en un sistema mundial de comunicación abierto a miles de millones de usuarios. Se creó desde un inicio como sistema distribuido para la intercomunicación de computadores[22]. Se considera que la explosión de la internet de las cosas (IoT) causaría una suerte de apocalipsis, tanto por la cantidad de datos como la abolición prácticamente total de la privacidad.

Una solución propuesta es el *"handle system"*. Sus promotores se inspiran en el sistema que creó Robert Kahn - co-desarrollador del protocolo TCP/IP - a principios de los años noventa y es el que utilizan las revistas académicas para dar a los documentos de investigación una identidad inmutable, incluso si se traslada a otro sitio web: el DOI. El interés por este sistema es tal que países como Rusia, China y Arabia Saudita se unieron para tratar de lograr que la ONU lo adopte como estándar general, lo que ha alertado a los especialistas:

> "Robert McDowell, ex comisionado de la Comisión Federal de Comunicaciones de Estados Unidos, ha dicho que el *handle system* podría convertirse en una «toma autoritaria del poder del Internet». Esto se debe a que no sólo regula dispositivos y documentos, sino que cualquier cosa puede ser un objeto digital, incluyendo personas. McDowell advierte que esto podría conducir a «la vigilancia en tiempo real y el seguimiento de cada dispositivo y persona conectada a la web». Cualquier persona que controle este registro se convierte en el guardián de acceso a toda la información, recursos y dispositivos en Internet. Entonces, ¿qué sucede cuando el guardián te cierra? El sistema de control le permite denegar el acceso a cualquier dispositivo sin un identificador válido. Eso no tiene que ser una bombilla inteligente. También podría ser su computadora portátil, su teléfono inteligente, su cuenta de Twitter, o incluso usted. ¿Y quién decide si un identificador es válido? Su gobierno, con todas sus potenciales debilidades autoritarias. Por el momento esto se hace bloqueando el acceso a ciertas direcciones de Internet a nivel nacional, eliminando su dirección en línea para todos en un país. Bajo el *handle system*, un gobierno podría individualizarlo personalmente, revocándole el acceso a las páginas que no quiere que vea." (Adee & Miller, NewScientist, 10/8/2017)

El sistema de cadena de bloques tendría las mismas ventajas de seguridad (datos no modificables e identificación única) pero con la enorme ventaja de ser distribuido, de escapar de los controles centralizados y de ser encriptado, legible sólo por los destinatarios que cuentan con la clave de lectura. Pero es algo que no gustará a los gobiernos que quieren establecer control sobre los contenidos.

22Que se haya creado como sistema distribuido para asegurar la resistencia de las redes en el caso de ataques nucleares, en el contexto de la Guerra Fría, es un mito según Steve Crocker, máxima autoridad de ICANN y uno de los pioneros en la creación de Arpanet.

Conclusión

Hemos visto las múltiples promesas del *blockchain* y también algunos de sus problemas. La banca es, sin dudas, el sector más interesado y adelantado, debido a la seguridad que ofrece. ¿Porqué, entonces, no está más avanzada en otros sectores? ¿Sólo por las limitaciones de velocidad o de extensión de las cadenas que hemos señalado? Mientras lo técnico es solucionable, son otros los factores que hoy frenan los avances, nos dicen en TICbeat:

> "Muchas instituciones están invirtiendo en esta tecnología para incorporarla en sus procesos, por el ahorro de costes y la seguridad que garantiza, entre otras ventajas. Entonces, ¿por qué está costando tanto implementarlo?
> Pues no tanto por cuestiones técnicas sino sobre todo legales; y es que la cadena de bloques plantea una serie de desafíos y vacíos legales que ni si quiera los sectores industriales que están ahondando en ella saben bien cómo resolver." (TICbeat, 10/8/2017)

La promesa de las cadenas de bloques es la posibilidad de desintegrar el cuasi monopolio de Facebook y Google, democratizando los mercados aún más que internet y liberando a los actores de la información, como sugirió Jonathan Taplin, director del Laboratorio de Innovación de la Annenberg School for Communication and Journalism, de la Universidad del Sur de California, en su artículo *"Google, Facebook y Amazon son monopolios; es hora de desintegrarlos"* (The New York Times, 27/4/2017).

Como ningún gobierno ni institución puede controlar una cadena de bloques, otra de sus ventajas es la protección de la libertad de prensa, sobre todo para periodistas que se encuentran en lugares y circunstancias en que su labor puede ser amenazada. Esta tecnología permite garantizar su anonimato y ocultar el origen de la información, sin repercutir en el menoscabo de su veracidad (Retina, El País, 14/6/2017). En Australia, una *app* política llamada Flux ya está usando la votación por bloques para tratar de transformar el proceso político.

> "Uno de los futuros previstos en la Revolución *Blockchain* es una «segunda era de la democracia»: una en la cual la tecnología *blockchain* puede crear las condiciones para un voto digital justo, seguro y conveniente, que galvanice a la ciudadanía eliminando tantos de los bloqueos sistémicos de votación que asolan nuestra sistema actual. Poner a la democracia en una cadena de bloques es complicado, pero *startups* como *Follow My Vote* y *Settlemint* ya están diseñando marcos centrados en fichas basadas en cadenas de bloques que sirven como votos, dejadas en billeteras digitales para cada candidato." (PC Magazine, 29/8/2017)

¡No es una promesa para pasado-mañana! Australia la ha tomado tan en serio que se enseña en escuelas:

> "Los estudiantes de la Escuela Primaria Wooranna Park en Victoria, Australia, están recibiendo clases sobre tecnología *blockchain* y *bitcoin* , a través de un programa llamado *«School on the Blockchain»*. El proyecto permite que los alumnos de 11 y 12 años aprendan sobre la tecnología de las monedas virtuales, manteniéndose a la vanguardia en relación con el tema, el que, a juicio de los impulsores de la iniciativa, será imprescindible en el futuro." (El Mercurio, 14/8/2017)

Y en Finlandia, el Servicio de Inmigración ha estado dando a los solicitantes de asilo que no tienen cuentas bancarias tarjetas Mastercard prepagadas junto con una identidad digital única almacenada en una cadena de bloques. El titular de la tarjeta puede pagar por las cosas en los terminales de Mastercard, o ingresar un número en un formulario web para hacer pagos en línea. La empresa MONI, que diseñó el sistema, se encarga del apretón de manos criptográfico necesario para ejecutar la transacción de moneda digital, así como la conversión de la moneda digital de nuevo a la moneda legal. La compañía tiene planes para lanzar un producto de consumo pronto en toda Europa. Las mismas Naciones Unidas están explorando el uso de esta tecnología para ofrecer identificación legal a más de mil millones de personas que no tienen documentos oficiales. (MIT Technology Review, 5/9/2017). Si Mastercard ya se embarcó allá y si varios grandes bancos internacionales ya preparan su propia plataforma, no hay duda de que se podrá pronto usar este sistema en todas partes.

¡Falta que los medios de comunicación exploren en serio esta alternativa, y luego! Más pronto que tarde dependerán de esta tecnología y se enfrentarán a las nuevas compañías tecnológicas que ya han empezado a desarrollar este modelo de negocio. Que lo deseen o no.

> Es probable que el lector se haga muchas preguntas, especialmente si se plantea la posibilidad de empezar a usar este sistema. El mismo autor se hace aún varias preguntas, pero contestarlas supone entrar a estudiar aspectos más técnicos (y aún más difíciles de explicar fuera de un marco ingenieril) y, sobre todo, entrar en el área práctica. ¡Ojalá se formen equipos multidisciplinarios para desarrollar proyectos pilotos, especialmente en las escuelas de periodismo!

Bibliografía

Adams, C. & Jourdan, G.V. (2014): Digital signatures for mobile users, IEEE Xplore, http://ieeexplore.ieee.org/document/6900969/

Adee, S. & Miller, C.. (2017): We can stop hacking and trolls, but it would ruin the internet, NewScientist, 10/8/2017, https://www.newscientist.com/article/mg23531383-300-we-can-stop-hacking-and-trolls-but-it-would-ruin-the-internet/

Barabas, Ch., Narula, N. & Zuckerman, E. (2017): Defending Internet Freedom through Decentralization: Back to the Future?, The Center for Civic Media & The Digital Currency Initiative, MIT Media Lab. http://dci.mit.edu/assets/papers/decentralized_web.pdf

Camerinelli, E. (2016): How I Explained Blockchain to My Grandmother, Finextra.com. https://www.finextra.com/blogposting/12378/how-i-explained-blockchain-to-my-grandmother

Condliffe, J. (2017): Dividir Bitcoin o no dividir Bitcoin, esa es la cuestión, MIT Technology Review, 3/8/2017. https://www.technologyreview.es/s/8513/dividir-bitcoin-o-no-dividir-bitcoin-esa-es-la-cuestion

Emerging Technology (2017): Los comercios que aceptan Bitcoin filtran datos que permiten desanonimizar las compras, MIT Technology Review, 29/8/2017. Ref: arxiv.org/abs/1708.04748

https://www.technologyreview.es/s/9061/los-comercios-que-aceptan-bitcoin-filtran-datos-que-permiten-desanonimizar-las-compras

Faife, C. (2017): Blockchain for Journalism: How a Big Funding Idea is Starting Small, Coindesk.com, 22/1/2017. https://www.coindesk.com/blockchain-for-journalism-how-a-big-funding-idea-is-starting-small/

Fernández, C. 82017): ¿Blockchain para un periodismo colaborativo y descentralizado? Retina, El Pais, 14/6/2017. https://retina.elpais.com/retina/2017/06/14/tendencias/1497438132_314400.html

Guest Writer (2017): How an Unlikely New Jersey Duo Is Using the Ethereum Blockchain to Reshape Journalism, Cryptocoinsnews.com. 2/5/2017. https://www.cryptocoinsnews.com/unlikely-new-jersey-duo-using-blockchain-reshape-journalism/

Gupta, M. (2017): Blockchain for Dummies, IBM, John Wiley & Sons. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN

Herreros, P.: Blockchain: Qué es y por qué te cambiará la vida, http://comunicacionsellamaeljuego.com/que-es-blockchain/

Iles, M. & col. (2017): Civil: Self-Sustaining Journalism, https://medium.com/@Join_Civil/civil-self-sustaining-journalism-a5caa49005c3

Irving, G. & Holden, J. (2017): How blockchain-timestamped protocols could improve the trustworthiness of medical science, F1000 Research, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4866630/ > improve trustworthiness.pdf

Laurence, T. (2017): Blockchain For Dummies, Publ. For Dummies.

Lichterman, J. (2017): This startup is trying to create a set of blockchain-based marketplaces for journalism, NiemanLab, 21/6/2017. http://www.niemanlab.org/2017/06/this-startup-is-trying-to-create-a-set-of-blockchain-based-marketplaces-for-journalism/

López Morales, T. y López Bueno, O. (2017): Qué es un minero de bitcoin... y por qué llegas tarde al negocio, El País.com, 28/7/2017.

Marvin, R. (2017): Blockchain: The Invisible Technology That's Changing the World, PC Magazine, 2/8/2017. https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor

Morell, J. (2016): Cómo crear un smart contract mediante términos y condiciones, Blog Términos y Condiciones, 21/9/2016. https://terminosycondiciones.es/2016/09/21/como-crear-smart-contract-mediante-terminos-condiciones

Mougayar, W. (2016): The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, Wiley.

NN.: Welcome to Hyperledger Fabric (full documentation) http://hyperledger-fabric.readthedocs.io/en/latest/

Preukschat, A. & col. (2017): Blockchain: La Revolución Industrial de Internet, Ediciones Gestión 2000 (Grupo Planeta).

" (2017): Cómo el Blockchain puede ser un aliado de los medios de comunicación, El Economista, 21/3/2017. http://www.eleconomista.es/tecnologia/noticias/8235723/03/17/Internet-del-Valor-o-como-el-Blockchain-puede-ser-un-aliado-de-los-medios-de-comuni

Tapscott, D. (2016): Blockchain Revolution: How the blockchain is changing money and business, Penguin ISBN: 978-0241237854
https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business

Toffler, R. (2017): Blockchain Blueprint: The Complete Guide to Blockchain Technology and How it is Creating a Revolution, CreateSpace Independent Publishing Platform.

Toll-Messia, J. & alt. (2017): The Hubii Network - A blockchain-based decentralised content marketplace. https://www.hubii.network/hubii-network-whitepaper-en.pdf

Tual, S. (2014): How to get started: your first dapp, under one hour, Ethereum Community Forum. https://forum.ethereum.org/discussion/1402/how-to-get-started-your-first-dapp-under-one-hour

Vollstädt, E. (2015): ¿What are DApps?, Bitnation, https://blog.bitnation.co/what-are-dapps/