Treball de Fi de Grau

Grau en Enginyeria en Tecnologies Industrials

Implementación de la tecnología Blockchain a entidades del tercer sector

MEMORIA

Autor: Sara Fuertes
Director: Joaquin Fernández

Convocatoria: Juny 2018

Escola Tècnica Superior
d'Enginyeria Industrial de Barcelona

Resumen

La confianza social constituye un pilar fundamental para las entidades del tercer sector. Sin embargo, las organizaciones sin ánimo de lucro no siempre han utilizado todos los instrumentos a su alcance para transmitir confianza al donante y garantizar transparencia. Con el propósito de proporcionar a estas entidades una herramienta que aumente la confianza de sus donantes, en este trabajo se estudia la viabilidad de la implementación de la tecnología Blockchain al sector de las ONGs.

La metodología seguida para realizar este trabajo se divide en tres fuentes de datos:

- En primer lugar, el *Bitcoin: A Peer-to-Peer Electronic Cash System*, el documento original donde el creador de Blockchain explicó su funcionamiento. Junto con otras fuentes que hacen referencia al mismo.
- En segundo lugar, los diferentes artículos de prensa donde se ha encontrado información sobre los últimos avances de Bitcoin y Blockchain, así como de los proyectos en los que éstos se están implementando.
- Finalmente, las entrevistas realizadas a personal de dos organizaciones sin ánimo de lucro (AFANOC y Oxfam Intermón).

Con toda la información bien documentada, se ha analizado el sistema de donaciones actual de AFANOC y Oxfam Intermón. En este análisis, se ha podido observar que sus sistemas de trazabilidad y registro de donaciones aún son escasos y disponen de diversos intermediarios que les suponen un coste adicional. Consecuentemente, la implementación de Blockchain presenta grandes ventajas puesto que otorga más transparencia a las entidades del tercer sector y les permite trazar y monitorizar acuradamente todas las transacciones de los donantes.

Asimismo, se ha determinado que Blockchain presenta ventajas más relevantes cuando se aplica a entidades que trabajan en un marco internacional. Y, puesto que los datos comentados en las entrevistas han sido limitados, se ha concluido que ámbitos como el hackeo de bases de datos o el detalle de los movimientos financieros, requerirán de estudios posteriores.

Sumario

Glosario

Criptomoneda: subconjunto de monedas digitales. No tienen representación física.

Libro de caja distribuido: base de datos en la que partes de ésta se almacenan en múltiples ubicaciones físicas y el procesamiento se distribuye entre diversos nodos. Los sistemas de cadena de bloques se denominan libros de caja (*ledgers*) distribuidos.

Minería Bitcoin: acto de procesar transacciones en el sistema de moneda digital; los registros de transacciones Bitcoin actuales – identificados como bloques - se añaden al registro de transacciones pasadas, conocido como la cadena de bloques (Blockchain).

Red *peer-to-peer* (P2P): red entre ordenadores en la que algunos o todos los aspectos funcionan sin clientes ni servidores fijos, sino un conjunto de nodos que se comportan como iguales entre sí. Cada nodo puede recibir y mandar transacciones a otros nodos y la información se va sincronizando en la red a medida que se va transfiriendo.

Hash/hashing: transformación de una cadena de caracteres en un valor, generalmente, más corto o una clave que representa la cadena original.

Billetera digital (*Wallet*): se trata de una aplicación de *software*, en general, para un teléfono inteligente que se utiliza como una versión electrónica de una cartera física.

Contrato inteligente: programa de computadora que controla directamente la transferencia de monedas o activos digitales entre partes bajo ciertas condiciones; almacenados en la tecnología Blockchain.

Tercer sector (economía social): sector de la economía que se encuentra a medio camino entre el sector privado y el sector público. Hace referencia al conjunto de organizaciones microeconómicas que se caracterizan por tener unos rasgos comunes basados en la "ética social".

Introducción

Objetivos del proyecto

Es bien sabido que las entidades del tercer sector, para poder llevar a cabo actividades y proyectos de ayuda, necesitan de la confianza social. En la medida que consiguen apoyo social, tienen acceso a más recursos y legitimidad para cooperar en cualquier ámbito cultural o social que requiera ayuda. Sin embargo, es muy complicado conseguir esta confianza social y, paradójicamente, muy fácil de perder. Por este mismo motivo, existe una inquietud generalizada en el tercer sector para tratar de ser lo más transparentes posibles.

Son varios los casos que ha habido los últimos años de organizaciones sin ánimo de lucro fraudulentas, entre otros escándalos. Cada vez que se publica uno de estos casos en la prensa, la confianza en el tercer sector cae en picado. Por esta razón cada vez son más las herramientas y hábitos de gestión que impulsan estas entidades para probar el buen uso de sus fondos (códigos éticos, auditorías, certificaciones, etc). Sin embargo, parece que ninguno de estos métodos es lo suficientemente robusto para asegurar al donante que su dinero no ha sido lanzado a un pozo sin fondo. En este contexto surge Blockchain, como una alternativa al trazado y registro de donaciones, entre otros aspectos.

Este trabajo presenta el objetivo principal de estudiar la viabilidad de la implementación de esta tecnología en entidades del tercer sector para aumentar la confianza suscitada por éstas a sus donantes. Asimismo, se presentan los siguientes objetivos específicos orientados a la consecución del objetivo principal:

- Estudiar el funcionamiento teórico de la tecnología de bloques.
- Analizar ámbitos y proyectos donde ya se haya implementado el sistema de cadena de bloques.
- Determinar las principales ventajas e inconvenientes de la aplicación de Blockchain en dos entidades del tercer sector.

- Analizar la viabilidad de la tecnología de bloques como herramienta de mejora en dos entidades del tercer sector.

Alcance del proyecto

Con el fin de llevar a cabo un trabajo que cumpla con los objetivos descritos, se pretende realizar un análisis enteramente conceptual sobre la implementación de la tecnología de bloques al tercer sector. Por tanto, hay que tener en cuenta que el alcance de este proyecto es meramente teórico. En otras palabras, aunque Blockchain es una tecnología que se puede programar si se conoce debidamente su código, en este trabajo no se estudiarán los fundamentos informáticos de Blockchain sino la metodología seguida por su creador para darle forma y otorgarle todas las funciones de las que dispone hoy en día. Las ventajas e inconvenientes de dichas funciones aplicadas a entidades del tercer sector, serán el foco de estudio de este trabajo.

1. Metodología Blockchain

1.1. Criptografía como base principal del Blockchain

1.1.1. Orígenes de la criptografía

La criptografía consiste en escribir con procedimientos o claves secretas o de una manera enigmática, de tal forma que lo escrito sea únicamente inteligible para aquél que sepa descifrarlo. Las primeras civilizaciones llevaron a cabo diferentes sistemas para poder mandar mensajes ocultos durante las campañas militares. De esta manera, en caso de que se interceptase al mensajero, la información que éste llevaba no caía en manos del enemigo. Pero no es hasta el siglo V a.C. que se tiene constancia del primer método criptográfico. Este sistema era conocido como "Escrítala", un método de transposición basado en un cilindro que servía como clave en el que se enrollaba un mensaje para poder cifrar y descifrar.

Figura 1.1 Prototipo de una escrítala

1.1.2. Desarrollo de la criptografía

A lo largo del siglo XIX, es cuando realmente se desarrolla y tiene un papel importante la criptografía. Durante la Primera Guerra Mundial, los alemanes utilizaron el cifrado ADFGVX. Y en la Segunda Guerra Mundial, los gobiernos comprendieron la relevancia de la criptografía para la codificación y descodificación de la información. Hecho que permitió al matemático británico Alan Turing[i], considerado padre de la criptografía, descifrar los códigos de *Enigma*; una máquina utilizada por los alemanes que automatizaba considerablemente los cálculos necesarios para cifrar y descifrar los mensajes que se enviaban. Este fue uno de los motivos principales que, tras la Segunda Guerra Mundial, provocó un desarrollo considerable de la criptografía.

En la década de los 70, con el desarrollo de la computación, surgieron los sistemas de clave asimétrica. En 1976 se creó el Algoritmo Diffie-Hellman cuyo sistema permitía una obtención más segura de las claves de cifrado (Anexo 2.2.). A este algoritmo le siguieron otros como el algoritmo RSA o la criptografía de curva elíptica que proponían romper las claves encriptadas en dos: una privada, conocida únicamente por su propietario y otra pública, de conocimiento público (Anexo 2.3.). Además, hay que tener en cuenta que una clave permite cifrar y la otra descifrar el mensaje, así que ambas son necesarias para transmitir la información. Sin embargo, no es necesario que emisor y receptor del mensaje conozcan las dos claves.

Es importante entender que cada clave pública tiene su par clave privada ya que la primera se obtiene, siguiendo una operativa relativamente trivial, de la segunda. Por el contrario, la obtención de la clave privada dada la clave pública resulta un cálculo computacional intratable, especialmente si se trabaja con valores a gran escala.

1.1.3. Algoritmos en la encriptación y desencriptación

Para poder desarrollar los cálculos necesarios para los sistemas de clave asimétrica, se transforman los mensajes en cadenas numéricas a partir de procesos estandarizados como el Código ASCII y posteriormente, se encriptan mediante una operación computacionalmente sencilla pero muy difícil de invertir. Es en este momento, cuando entra en juego la aritmética modular (Anexo 2.1.). La obtención de una clave de encriptación elevando un número a una potencia carece de utilidad puesto que, por muy alto que sea este número, resultará fácil de descifrar mediante el cálculo del logaritmo inverso. Por el contrario, si se encripta en módulo *m*, descifrarlo requeriría el cálculo del logaritmo inverso discreto, operación para la que no existe algoritmo de cálculo y escapa a la operativa de los sistemas de computación actuales cuando se trabaja con módulos y exponentes elevados.

1.2. El ciberpunk como detonante del Blockchain

El concepto de ciberpunk presenta una gran variedad de definiciones puesto que guarda relación con aspectos muy diversos. No obstante, en relación con el tema que trata esta memoria, quizás la definición más acertada se encuentre en la misma etimología de la palabra: ciberpunk se compone de cibernética y de punk, o lo que es lo mismo, relaciona la alta tecnología y las redes informáticas con un carácter rebelde y reivindicativo que, generalmente, busca lograr un cambio social o político. Es por tanto, un movimiento que defiende la libertad de expresión y el acceso a la información a la vez que su privacidad.

El lema del ciberpunk es: "la información quiere ser libre" y la consecución de este lema se basa en tres elementos: hacking[1], cracking[2] y criptografía. Hackear para que la información sea libre; y el cifrado y la criptografía como medio para proteger al individuo de las redes de control. Este movimiento fue el principal impulsor de la creación de Bitcoin y fundamental para el desarrollo de la cadena de bloques. Si bien es cierto que, antes de que apareciese y se consolidara Bitcoin muchos ciberpunks fracasaron en sus intentos de crear una divisa digital ("más libre" que la tradicional); durante la década de los 90 quedó claro que las semillas que harían florecer la tecnología Blockchain ya estaban sembradas.

Así pues, estos diferentes intentos fallidos de diversos ciberpunks, dieron paso a que el 31 de octubre de 2008 Satoshi Nakamoto[3] publicara, en una lista de correo sobre criptografía, un documento llamado *Bitcoin: A Peer-to-Peer Electronic Cash System*[ii]. Como su nombre indica, este escrito proponía un sistema de dinero electrónico "peer-to-peer", independiente de intermediarios. No obstante, no fue hasta casi un año más tarde cuando se generó el primer bloque de Blockchain. Éste recibe el nombre de bloque Génesis y marcó el inicio de Bitcoin. Finalmente, el 8 de enero de 2009, fue

[1] Hacking: práctica en la que una persona con sólidos conocimientos informáticos es capaz de introducirse sin autorización a sistemas ajenos.
[2] Cracking: práctica en la que una persona accede **ilegalmente** a sistemas informáticos ajenos para apropiárselos u obtener información secreta.
[3] Satoshi Nakamoto es un pseudónimo, se desconoce quién o quienes fueron los verdaderos creadores de este sistema.

cuando se llevó a cabo la primera transacción de la criptomoneda. Envuelto en un contexto de una importante crisis financiera mundial, nació i empezó a consolidarse este nuevo sistema como una alternativa a los mercados financieros tradicionales.

1.3. Definición de Blockchain

Para entender bien el término Blockchain, resulta útil introducir antes el concepto de Bitcoin tal y como Satoshi Nakamoto lo presentó al mundo. Como se comentaba con anterioridad, Bitcoin es un sistema de pago electrónico peer-to-peer que permite a un individuo hacer una transacción instantánea a cualquier persona sin pasar por ningún intermediario previo (como suelen ser los bancos). Además se realiza una validación de la misma mediante un consenso entre todos los usuarios, dando así, validez y seguridad al sistema. Se trata pues, de un libro mayor de contabilidad donde, mediante cifrado, quedan registradas de manera pública y permanente todas las transacciones. Y más interesante aún, como se analizará más detenidamente en las próximas páginas, el sistema está diseñado de tal manera que imposibilita la manipulación de los registros sobre los valores transferidos.

¿Dónde está entonces la cadena de bloques o, en inglés, Blockchain? La cadena es todo el sistema que hay detrás de Bitcoin y que hace que el proceso descrito anteriormente sea posible. Así pues, y sin entrar aún en detalle, la cadena de bloques es este gran libro de cuentas donde los registros (bloques) se van enlazando y, mediante diversas herramientas matemáticas, garantizan la seguridad y fiabilidad de las transacciones. En otras palabras, Blockchain es como una especie de Excel del Bitcoin. Una gran base de datos distribuida y segura que muestra la historia y la ubicación de cada transacción realizada. En el caso de Bitcoin, la información que queda registrada son las transacciones con moneda virtual. Sin embargo, a efectos prácticos, cualquier aspecto tangible o intangible pude ser registrado con el mismo sistema.

Como se verá más adelante, una vez definida la transacción y añadida a la red *peer-to-peer* para su validación y registro, se aporta al sistema una información bidireccional: por un lado temporal, manifestada en cada uno de los bloques de transacciones validados (aproximadamente cada 10 minutos en el caso de Bitcoin) y por otro lado de valor, como parte de todo el sistema registrado de transferencias.

1.4. Funcionamiento de la cadena de bloques

1.4.1. Principales flujos de información y acción del sistema

Una vez vista la idea general de que Blockchain consiste en esta enorme red de ordenadores que envían, reciben y verifican transacciones, seguidamente se verá su funcionamiento punto por punto.

El primer paso de la cadena de bloques reside en la voluntad de dos partes de realizar una **transacción**. Pongamos el caso de dos propietarios: Owner1 y Owner2 que deciden intercambiar una unidad de valor que, siguiendo la línea de Bitcoin, consistiría en una moneda digital.

Esta transacción se transmite por la red a todas las computadoras participantes, denominadas **mineras**. Cada nodo minero va empaquetando todas las transacciones que va recibiendo durante un periodo de tiempo determinado. Finalmente, se crea lo que en Blockchain recibe el nombre de **bloque**.

Seguidamente, cada nodo trabaja sobre el bloque que ha construido, y compite junto con el resto de computadoras, con el fin de poner una “etiqueta” o “referencia” al mismo. Esto se realiza a partir de la ***proof-of-work***, procedimiento que se describirá más adelante.

Cuando un nodo, de todos los que se disputan por tener éxito en la ***proof-of-work***, consigue llegar al resultado correcto, ya puede transmitir su bloque resuelto al resto de ordenadores que participan en la cadena.

A continuación llega el momento de la **verificación**. Las computadoras participantes, a partir de más cálculos matemáticos, deben determinar si ese bloque es válido, con base a unas reglas previamente acordadas. El consenso se alcanza cuando aproximadamente un 51% de las computadoras han verificado la transacción. Sólo entonces ésta se considera válida y cada nodo añade el bloque verificado a su cadena.

Inmediatamente después de aceptar un nuevo bloque, cada nodo comienza a trabajar en la construcción del siguiente y éste se estampa temporalmente con un **hash** criptográfico (concepto que también se desarrollará más tarde). Cada bloque contiene además referencia al hash de los bloques previos, creando de esta manera una "cadena" de registros que no puede ser falsificada, a no ser que se "convenza" a todas las computadoras de la red que los datos adulterados en un bloque y en todos los previos, son ciertos. Tal operación se considera casi imposible.

Finalmente, se llega a la parte de **ejecución**, donde la unidad de valor se mueve de la cuenta de Owner1 a la de Owner2.

Una simplificación del proceso descrito se muestra en la imagen siguiente:

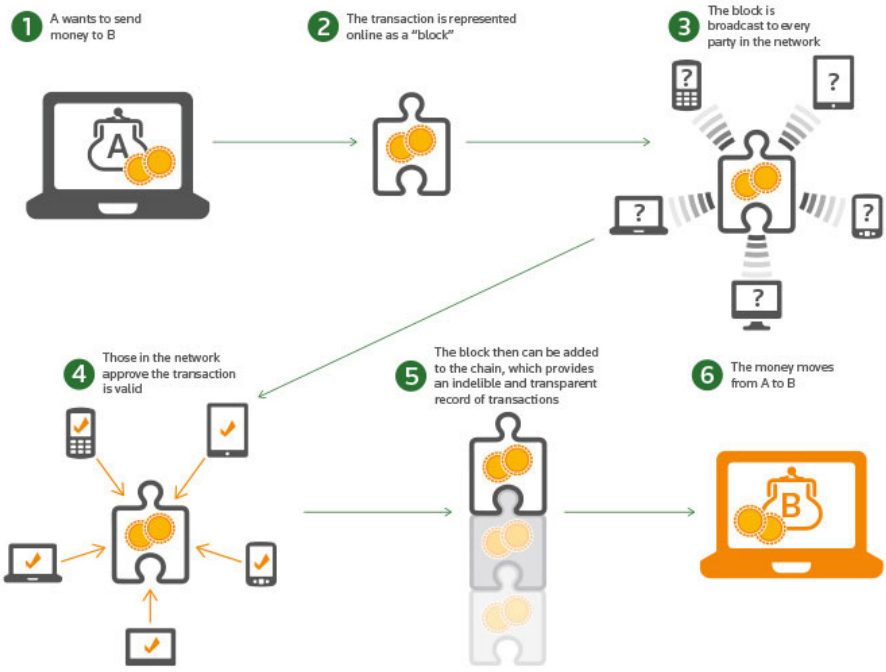

Figura 1.2 Esquema del proceso seguido por la cadena de bloques para realizar una transacción

Llegados a este punto, ya se tiene una idea global de qué es Blockchain y de cuál es su metodología general. A continuación, se verá la parte más técnica de su funcionamiento.

1.4.2. Sistemas de privacidad

En los puntos 2.1.2. y 2.1.3. de esta memoria se introducían los conceptos de clave pública y clave privada cuya aplicación es vital en el sistema de la cadena de bloques. Aunque más adelante se explicará con más detenimiento el funcionamiento del sistema de clave asimétrica en Blockchain, en las próximas líneas ya aparecerán estos conceptos y se verán algunas de sus ventajas y funciones.

Para explicar debidamente el sistema de privacidad en que se basa Blockchain, es conveniente tener en consideración que una de las principales características de esta tecnología es que no existen intermediarios, y por tanto, el modelo clásico de privacidad financiera queda obsoleto. El modelo tradicional permite mantener todas las transacciones fuera del alcance público, ya que existe una autoridad o un tercero que conoce las identidades de los participantes en la transacción, haciéndola posible. No obstante, en Blockchain, esta figura desaparece. Para poder mantener la privacidad de los participantes, la tecnología de bloques rompe el flujo de información en otro punto. En el modelo propuesto por Satoshi Nakamoto todas las transacciones deben comunicarse públicamente para su correcta validación. De manera que, sin necesidad de acudir a un intermediario, se asegure que todas ellas son veraces y correctas. En este modelo, el único aspecto de la cadena que se mantiene en secreto son las claves públicas, o más concretamente, la identidad de los propietarios de dichas claves.

A continuación se muestra el sistema clásico de privacidad, en contraposición al sistema propuesto por Nakamoto comentado en el párrafo anterior.

Figura 1.3 Funcionamiento clásico de privacidad en un sistema financiero.

Figura 1.4 Sistema de privacidad en las transacciones seguido por Blockchain

Como se venia diciendo, la única manera de garantizar lo descrito y mantener el anonimato de los participantes, es hacer que las transacciones sean públicas pero dejando a salvo la identidad última de los que participan mediante la referencia a sus respectivas claves públicas, que no deberían tener correlación directa con las identidades físicas respectivas. Por tanto, las claves públicas son, en Blockchain, un elemento no sólo de propiedad, en tanto que sirven como referencias para la propiedad del valor que se quiere transferir; sino también de privacidad. Por otro lado, la clave privada servirá para la movilización y transferencia de valor mediante la firma digital.

¿Si no existe una tercera parte que dé las claves públicas y privadas, cómo es posible que cada usuario tenga su propia clave pública sin que ésta coincida con ninguna otra? La respuesta está en que las claves públicas se obtienen de manera aleatoria, sin necesidad de una autoridad de control, puesto que la probabilidad de generar aleatoriamente claves coincidentes resulta despreciable. Considerando un sistema de claves públicas de hasta 256 bits, esta probabilidad es del orden de $1/2^{256}$. Para poder tener una idea general de la magnitud que abarca esta operación exponencial, basta con recordar la leyenda del rey de la India que explica como, cuando un habitante de su reino consiguió desarrollar un juego que le entretuvo, el monarca se comprometió a ir rellenando las casillas de dicho juego, un tablero de ajedrez, con granos de arroz de manera exponencial (2^n). De tal manera que, sin saberlo, se había comprometido a darle una cantidad ingente de arroz. Por ejemplo, sólo contando el arroz de la casilla

64 ya tenía que entregarle 2^{64} granos, cifra que equivalía a la cosecha mundial de 500 años, aproximadamente.

En el caso que nos ocupa, la función exponencial con la que trabajamos es la inversa, y por consiguiente, $1/2^{256}$ es una posibilidad ínfima, hecho que garantiza que la participación en Blockchain se pueda dar de forma totalmente anónima. De esta manera, eliminando la figura de una autoridad central necesaria para registrarse como usuario, es posible dotar al sistema de total autonomía.

1.4.3. Funciones hash criptográficas

Para comprender mejor el procedimiento de validación de bloques, es preciso entender más detalladamente las funciones hash criptográficas.

Estas funciones unidireccionales tienen la particularidad de que son ideales para su uso en sistemas que confían en la criptografía para garantizar la seguridad. Para entender conceptualmente su aplicabilidad en Blockchain basta con saber que una función hash se usa como herramienta para resumir un texto determinado y, de esta manera, agilizar y disminuir el cálculo computacional de cada nodo en el momento de transferir y procesar información.

Como pasa con los datos informáticos, los hashes son números no muy grandes, escritos en sistema hexadecimal. Expresado de manera más técnica diríamos que el funcionamiento de la funciones hash consiste en algoritmos que, dada una cantidad arbitrariamente grande de datos, convierten este dato en un Hash de longitud fija, como se muestra en el ejemplo de la figura 1.5. Como se ha introducido en el primer párrafo, esto conlleva una gran ventaja y es que cuanto menor sea el texto con el que hay que trabajar, menor será el coste computacional de las operaciones posteriores a realizar.

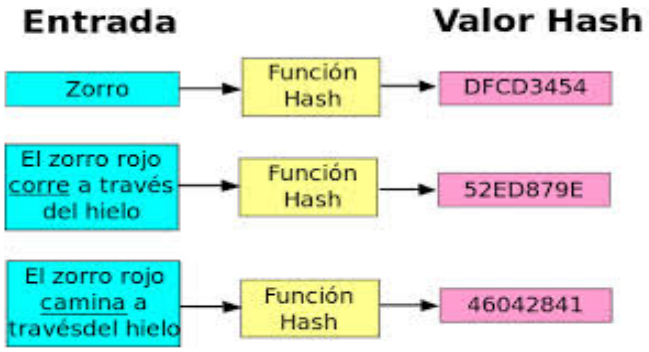

Figura 1.5 Ejemplo de funcionamiento de las funciones hash criptográficas

En el primer párrafo se hacía referencia a este tipo de funciones como funciones unidireccionales. Esto es debido a que una de sus características fundamentales es que un Hash es relativamente fácil de crear a partir de una entrada. Sin embargo, es prácticamente imposible deducir el contenido de la entrada solamente leyendo el valor Hash.

En el caso de Bitcoin, Nakamoto usa el algoritmo de encriptación ECDSA (Elliptic Curve DSA) para generar hashes de los mensajes de Blockchain. Aunque no se entrará en detalle sobre la parte más matemática que abarcan este tipo de algoritmos, a continuación se hablará de la compleja implementación de las funciones Hash en la cadena de bloques. Precisando más las líneas anteriores, se puede decir que estas funciones son de gran utilidad en Blockchain para dos procesos:

- El primero, como herramienta de preparación de resúmenes de textos de longitud aleatoria que requieran ser firmados.
- Y el segundo, como herramienta clave en el proceso de consenso del *proof-of-work*, que será el que permita añadir bloques a la cadena de manera sencilla y segura.

1.4.4. Firmas digitales

Como se hará evidente en las líneas que siguen, la cadena de bloques es, en realidad, una cadena de firmas digitales donde se precisa de la firma digital de participantes

anteriores a la cadena para poder realizar nuevas transacciones. Como ya se ha visto anteriormente, un hash se puede entender como el resumen de un mensaje y es sobre éste donde se aplica la firma digital, siguiendo el proceso que ahora se describirá.

El uso de las claves públicas y privadas en Blockchain no es para nada trivial. Hay que entender que cifrar un mensaje con la clave privada equivale a firmarlo puesto que únicamente el poseedor de la clave privada podría haber cifrado ese mensaje. Se hace evidente que cuando firmamos a mano un texto en una hoja estamos poniendo de manifiesto que cierta propiedad de ese papel es solamente nuestra. Asimismo, cuando en Blockchain cifras algo con tu clave privada estás manifestando tu autoría: únicamente tu puedes haberlo cifrado. De la misma manera que firmar un papel a mano no mantiene en secreto el contenido del papel, cifrar con la clave privada no otorga confidencialidad al mensaje, en otras palabras, no le añade secreto. Sin embargo, sí asegura la autenticación: sólo tu pudiste haberlo cifrado. Equivale por tanto, a haberlo firmado.

Una vez firmado el mensaje, y por tanto, cifrado con la clave privada, cualquiera puede descifrarlo usando la clave pública par de esa clave privada. Esto equivale a verificar una firma.

A continuación se verá el procedimiento concreto que sigue Blockchain por lo que respecta a la implementación de las claves pública y privada. Para facilitar la comprensión de este proceso puede ser de gran ayuda imaginarse el sistema de clave asimétrica de manera análoga a como funcionan actualmente las cuentas bancarias. Por un lado, la clave pública sería como el IBAN de una cuenta, puesto que ésta es la dirección que mostramos públicamente a aquellos que nos quieran mandar dinero. Por otro lado, la clave privada correspondería al pin que tu cuenta te pide para poder realizar una transferencia a otro usuario; código que sólo la persona que envía el dinero conoce.

Así pues, en Blockchain, cuando un sujeto (al que llamaremos Owner2 siguiendo el ejemplo de la figura 1.6) desea realizar una transferencia, debe firmar esta transacción con su clave privada y enviarla a la clave pública del receptor, en este caso, Owner3. Tanto esta transacción como el saldo disponible que queda en la dirección de Owner3 pueden ser comprobados por todo el mundo, ya que son públicos. Sin embargo, el único que podrá hacer una nueva transferencia con ese dinero es Owner3 ya que tiene la clave privada, par de la clave pública donde están las divisas virtuales. De este párrafo, se puede concluir que cada firma es únicamente válida para una transacción específica.

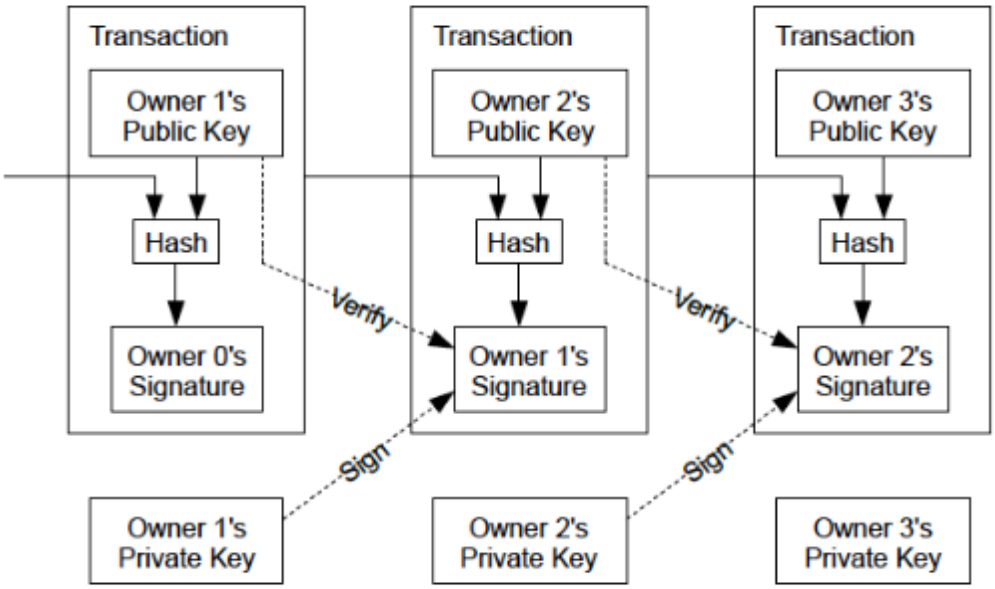

Figura 1.6 Ejemplo del proceso de firma digital en una transacción de Blockchain

La tecnología de la cadena de bloques incluso va más allá. Debido a que, en la práctica, los algoritmos de cifrado asimétrico son bastante lentos, normalmente no se utilizan para cifrar todo el mensaje, sino un resumen del mismo. Llegados a este punto, entran en juego las funciones hash criptográficas que se han comentado en apartados anteriores. En esencia, una transacción consiste en la concatenación de la transacción anterior y la clave pública del beneficiario de la transmisión (Owner3) que conjuntamente constituyen el hash criptográfico o resumen del mensaje que será firmado con la clave privada del propietario anterior, Owner2. Esto demuestra que el propietario de la clave privada realmente tiene la intención de llevar a cabo dicha transacción y da garantía de que ésta no será alterada.

Una vez realizado este paso y por tanto, aceptada la transacción, el receptor adquiere el valor que puede descifrar mediante su clave pública que, a su vez, se corresponde con la dirección donde se han transferido las monedas. El receptor podrá, al mismo tiempo, transferir de nuevo el mensaje, firmándolo con su clave privada, y así sucesivamente. De esta manera se va conformando una red de transacciones fundamentadas en la firma digital.

Finalmente, una de las ventajas de todo este sistema es que como todo el mundo conoce la clave pública de Owner2, cualquier participante de la red puede comprobar que la transacción es valida, verificando que la firma de Owner2, es decir, su clave privada, se corresponde efectivamente con su identidad, es decir, su clave pública.

Ya para acabar, se plantea la siguiente pregunta: si un atacante, Owner Z, descifrase usando la clave pública de Owner3, el mensaje que éste había cifrado con su clave privada, y luego, este mismo atacante, decidiese cifrar de nuevo el mensaje con su clave privada ¿qué ocurriría?

La respuesta es sencilla, en el momento en que los destinatarios tratasen de verificar la firma de Owner Z sobre el mensaje “atacado”, o lo que es lo mismo, descifrar el mensaje usando la clave pública de Owner3, aparecería un texto sin sentido alguno puesto que no se puede descifrar un texto cifrado con una clave privada mediante una clave pública que no le corresponde. Por este motivo, cuando un sujeto cifra algo con su clave privada, luego no puede decir que no lo firmó. Esta propiedad del cifrado asimétrico se conoce como no repudio, ya que jamás puedes repudiar tus mensajes.

1.4.5. Servidor de sellado de tiempo

Si bien, todo este sistema deja un cabo suelto puesto que no hay nada que impida a uno de los owners transferir varias veces los mismos bitcoins. Si Owner1 entrega un lápiz a Owner2, el primer sujeto ha transferido la propiedad de ese objeto y sólo podrá recuperarlo si Owner2 accede a devolvérselo. Pero no existe ninguna manera de poder

gastar ese objeto físico de nuevo si no lo recuperamos previamente. Cuando hablamos de dinero físico (monedas o billetes) aumentamos un grado la dificultad de este proceso. Es bien sabido que un billete se puede falsificar y, por tanto, Owner1 podría gastar dos veces "un mismo billete", si consigue hacer una buena copia del mismo. Sin embargo, en la actualidad, existen muchos sistemas de control que buscan erradicar estas prácticas. Llegados a este punto, conviene preguntarse qué ocurre con las divisas virtuales. ¿Se pueden realizar copias de estas e incurrir en un doble gasto?

La respuesta es sí. Para representar digitalmente una unidad monetaria de un euro, de la misma forma que ocurre para los ficheros audiovisuales (música, videos, etc), únicamente se requieren bits. En Bittorrent (un sistema para compartir ficheros digitales como películas), un archivo que se comparte con otro nodo es una copia íntegra del fichero original. Si el fichero se descarga un millón de veces en diferentes ordenadores habrá un millón de copias del mismo. Esta característica funciona perfectamente para la obtención y difusión masiva de ficheros audiovisuales. En cambio, en el caso de Bitcoin, no interesa que se puedan generar unidades de un mismo bitcoin de forma infinita, puesto que no podríamos saber si Owner1 ha gastado esa unidad anteriormente. Por este motivo, hasta el momento la idea de crear un sistema de pagos digitales siempre había requerido del uso de una estructura centralizada, en tanto que se requería de un agente externo que confirmase si la cantidad monetaria transferida era válida o, si en su defecto, se trataba de una copia.

Sin embargo, Satoshi Nakamoto da con la manera de evitar el doble gasto en sistemas de pago digitales con una estructura P2P. ¿Cómo lo hace? Activando un servidor de marcas de tiempo que establezca la prevalencia de la primera transacción registrada. En otras palabras, se programa Blockchain para que la única transmisión considerada válida sea la primera. Para conseguirlo, se establece que la única manera de asegurar la unicidad de una transacción de un valor concreto es tener un registro de todas las transacciones previas y que, por ende, deberán ser anunciadas públicamente para que esta comprobación sea efectiva y libre de intermediarios.

El procedimiento que hace posible todo el sistema descrito en el párrafo anterior es un servidor de marcas de tiempo, es decir, una especie de traza temporal donde se registran, en un hash, todas las transacciones realizadas hasta ese instante. De tal manera que, en todo momento, se puede verificar que no se esté incurriendo en un doble gasto ya que todos los nodos tienen acceso a la información del resto y la pueden validar.

1.4.6. *Proof-of-Work*

Otra herramienta que garantiza la eficiencia del sistema de marcas de tiempo anterior, es la *proof-of-work.* Este sistema previene la difusión masiva de mensajes no deseados mediante un trabajo computacional previo.

Este mecanismo consiste en ir cambiando la función hash hasta conseguir un resultado en binario que empiece con un número *n* de bits a cero. El esfuerzo necesario para conseguir lo descrito es exponencial en *n* puesto que por cada bit cero adicional requerido, el tiempo medio de trabajo se duplica. Así pues, en el caso de Bitcoin, en cada bloque de transacciones existe un nuevo campo llamado *nonce* que funciona como un contador, modificando su contenido hasta que el hash no tenga un resultado que encaje con el requerido. La consecución de este resultado no tiene una solución directa sino que se obtiene mediante iteración. Una vez se consigue la respuesta, la prueba de trabajo se dará por correcta permitiendo que el bloque se añada a la cadena. A partir de ese momento, el contenido de ese bloque no podrá ser modificado sin volver a realizar este esfuerzo. De hecho, para poder variar la información del bloque, se requeriría rehacer el trabajo, no sólo del bloque en cuestión, sino de todos los bloques siguientes ya que estos incluirán los hashes de enlaces previos que también se verían modificados.

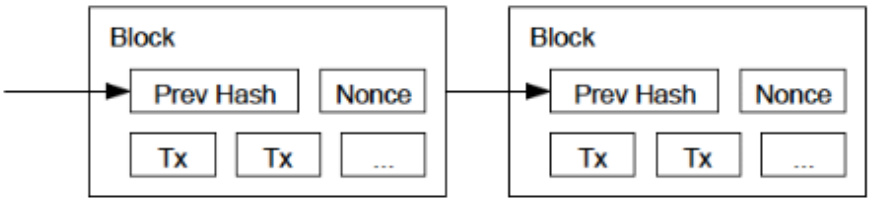

Figura 1.7 Estructura de los bloques en la *proof-of-work*

No cabe duda entonces, que para incluir un bloque de transacciones a la cadena final, se exige un importante trabajo computacional demostrable. El nivel de esfuerzo necesario se puede alterar modificando el número *n* de bits a cero que exige el hash. Se hace evidente que si yo tiro veinte dados a la vez, las probabilidades de que en alguno de ellos me salga un seis son mayores que si sólo tiro un dado. ¿Y si pudiese establecer una correlación entre el número de caras de cada dado y el número de dados que tiraré? Entonces, aumentando el número de caras de cada dado según aumente el número de dados que tiraré, podría mantener la probabilidad de 1/6 de que saliese un seis. Esto mismo es lo que consiguen los *n* bits a cero del *nonce,* puesto que garantizan que cuantos más nodos tenga la red más *n* bits a cero tendrá que cuadrar. Esta esencial variabilidad es lo que permite cambiar la dificultad del trabajo para los nodos y garantizar un ritmo de generación de bloques estable, independientemente de la potencia computacional que se tenga en cada momento.

Cogiendo una visión más global del sistema, se hace evidente que todo el trabajo computacional que requiere descubrir la combinación que permite a un bloque ser añadido a la cadena, se reparte entre los miles y miles de nodos mineros. De esta explicación se deduce que, esta gran cantidad de trabajo realizado por todo el colectivo de mineros, no es fácil de replicar por un solo nodo puesto que requeriría una potencia computacional demasiado elevada. Es decir, para que un solo nodo pudiese replicar todo el trabajo de varios nodos tendría que ser capaz de resolver un *nonce* con muchos más bits a cero de los que le corresponderían a un nodo individual. En resumen, cuantos más nodos participen en la red, más complicado será para un nodo intruso interferir en el sistema.

Hasta el momento, se han visto herramientas integradas por Blockhcain que garantizan tanto que la información registrada es difícilmente modificable, como que no habrá un abuso de poder donde un nodo tome las riendas de todo el sistema. Sin embargo, por ahora, nada garantiza que un conjunto de nodos deshonestos consigan incorporarse a la cadena y apoderarse de ella. Para facilitar la comprensión de como la *proof-of-work* soluciona también esta situación, se explicará *el Problema de los generales bizantinos.* Se trata de un experimento mental que, como ocurre en Blockchain, describe una situación en la que todos los generales (nodos en este caso), pueden comunicarse entre todos y pueden intercambiar mensajes firmados entre sí.

Supongamos un escenario de guerra en el que tenemos un grupo de *m* generales bizantinos que están asediando una ciudad desde distintos lugares y tienen que ponerse de acuerdo para atacar o retirarse de forma coordinada. Entre los generales hay sólo uno que puede cursar la orden por ser el **comandante**. El resto se dice que son **tenientes**.

Los generales se comunican a través de mensajes y las dos posibles órdenes del comandante son "atacar" o "retirarse".

Uno o más de los generales puede ser un **traidor** (al resto se les llama **leales**), por lo que su objetivo es conseguir que todos los generales leales no se pongan de acuerdo. Para ello puede ofrecer información errónea. Por ejemplo, si el comandante es el traidor, podría mandar órdenes contradictorias a los distintos tenientes. Si el teniente es un traidor podría indicar a otros tenientes, con el fin de confundirlos y que creyeran que el traidor es el comandante, que el comandante les envió la orden contraria a la que realmente les envió. […]

Si consideramos que la información se transmite de general a general mediante mensajes firmados y que todos se pueden comunicar entre todos, el escenario resultante se plantea a continuación:

Los mensajes van firmados (se trata de mensajes escritos). Al ir firmados no son modificables y por tanto los traidores no pueden alterarlos y decir que provienen del comandante. En esta situación es posible resolver el problema con sólo tres generales y uno de ellos traidor. El algoritmo de este tipo de problemas se llama SM(m) (donde SM viene del inglés Signed Messages) y es el siguiente:

> Primero el comandante envía una orden firmada a todos los tenientes. Cada vez que un teniente recibe un mensaje firmado lo guarda, hace una copia, la firma y la reenvía a todos los tenientes que no venían en la firma del documento. Según este algoritmo los generales no recibirán más mensajes cuando tengan todas las posibles combinaciones. Una vez recibidas, cada general toma la decisión basándose en la orden transmitida por la mayoría.

En este escenario los comandantes traidores son descubiertos inmediatamente ya que han firmado órdenes contradictorias.

De manera análoga, en Blockchain, la decisión de la mayoría que por defecto son los nodos honestos, se plasma en las cadenas de mayor longitud y por tanto, el sistema sabrá que tiene que quedarse con éstas. De esta manera, las cadenas de mayor longitud serán las que crecerán más rápido mientras que cualquier bloque deshonesto que quiera romper esa cadena, no prosperará.

Finalmente, hay que tener en cuenta que existen estrategias de incentivación al minado de bloques que garantizan que estos resuelvan de la manera más rápida posible los algoritmos matemáticos y que lo hagan de manera honesta, puesto que de lo contrario no se les "premiaría". No se entrará en detalle sobre estas técnicas pero basta con saber que existen y que son la base de que los nodos quieran trabajar, o mejor dicho, quieran trabajar bien.

1.5. Estructura de Blockchain

1.5.1. Los bloques

Llegados a este punto, se ha visto que cuando un nodo tiene éxito en la *proof-of-work*, o en su defecto, recibe el bloque de otro nodo con mayor éxito, dicho bloque está listo para ser incluido tras el que se encuentre en el extremo de la cadena ya existente. Como se muestra en el esquema de la figura 1.8.

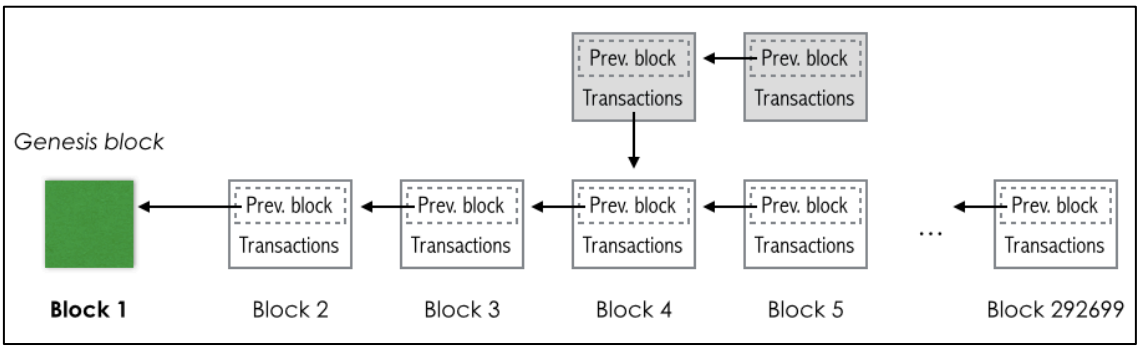

Figura 1.8 Ejemplo de los diferentes tipos de bloques que se encuentran en la cadena.

En este esquema se puede apreciar el primer bloque (bloque cero o Génesis), representado de color verde. Éste bloque encabeza la cadena y va seguido de los

bloques blancos que representan la cadena principal, la más larga. Por otro lado, los bloques grises (llamados bloques huérfanos) representan las bifurcaciones originadas por la resolución casi simultánea de la *proof-of-work* en dos nodos mineros distintos. Es decir, se puede dar el caso de que dos o más nodos resuelvan versiones diferentes del bloque en curso (puesto que pueden registrar diferentes conjuntos de transacciones). Por eso, es importante que el nodo siga trabajando sobre el bloque que ha recibido primero y mantenga la bifurcación. De esta manera, cuando se empiece a desarrollar una cadena más larga y el sistema vea que los bloques representados como grises son efectivamente huérfanos, las transacciones de éstos no se perderán. Es más, si no figuraban ya en algún otro bloque, son recuperadas y trasladas al sistema principal. Para no cometer errores, el sistema nunca elimina bloques porque aunque le llegue primero uno que más tarde "clasificará" como huérfano, debe guárdalo hasta saber cuál es la rama de mayor longitud, y posteriormente, abandonar la rama bifurcada.

Tal y como se ha ido viendo, la seguridad de esta compleja estructura de bloques es posible gracias a que todos los procesos de verificación y aceptación se producen previamente de manera independiente entre nodos. De esta forma, y a modo de resumen, el consenso que posibilita esta cadena final de bloques sólo se puede dar después de que los nodos hayan realizado las siguientes tareas:

- Verificar, de manera independiente, cada transacción.
- Agrupar, también individualmente, varias transacciones hasta crear un bloque a partir de un minado basado en la *proof-of-work*.
- Verificar, nuevamente de manera independiente, cada nuevo bloque que se quiera incluir en la red y anexarlo a la cadena de Blockchain.
- Finalmente, cada nodo selecciona independientemente, la cadena con mayor trabajo computacional acumulado y demostrado por la *proof-of-work*.

1.5.2. La red

La distribución de la red basada en elementos que actúan para verificar y transmitir la información de manera independiente, es lo que hace que el sistema sea descentralizado y distribuido. En la imagen que encontramos a continuación (Figura 1.9) se muestran las diferentes maneras en que puede presentarse una red: centralizada (sería el método de financiación actual, con los bancos como servidor central), descentralizada y, finalmente, distribuida. Como ya se ha anticipado, Blockchain se basa en las dos últimas estructuras.

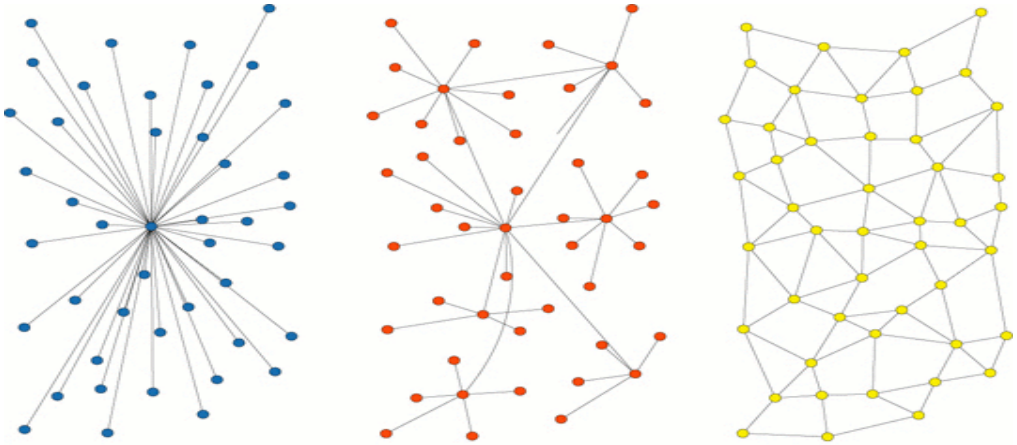

Figura 1.9 Estructura de una red centralizada, descentralizada y distribuida, respectivamente

Por un lado la tecnología de bloques sigue una disposición no centralizada ya que, como se viene repitiendo, no presenta ninguna autoridad central que organice y valide todas las transacciones. Por otro lado, presenta una estructura distribuida, en tanto que cualquier nodo partícipe puede ser receptor y emisor de información al mismo tiempo. La información se distribuye a través de todas las computadoras. Consecuentemente, todos los nodos tienen la misma información y, por tanto, la misma importancia en la red, otorgando a ésta total transparencia. En este tipo de red nadie depende de nadie para transferir la información y la libertad individual permite o no conectarse a la red. El economista David de Ugarte resume toda esta filosofía en la frase: “alguien propone y se suma quien quiere”. De modo similar a lo que ocurrió con internet, Blockchain es un sistema que nadie posee, pero del cual todos pueden ser partícipes libremente.

Todo esto además supone ciertas ventajas. Por ejemplo, el hecho de que las transferencias no tengan que pasar por un servidor central permite dotar a las transacciones de un comportamiento más ágil, que a su vez, da lugar a un abaratamiento de costes. Ya para cerrar este apartado, comentar que otra ventaja fundamental de esta tecnología es que, si se diera el caso de que hubiese algún error en la red, cayera parte del sistema o se hackeara una computadora; mientras hubiese un solo nodo funcionando correctamente, la información nunca se perdería. Esto es gracias a que toda la información no se registra y guarda en una única computadora central, sino que ésta se almacena en cada uno de los nodos participantes en la red. De igual modo que todas las células de nuestro cuerpo contienen el ADN con todas las instrucciones necesarias para el funcionamiento de nuestro cuerpo, y si una de ellas muere no se pierde información alguna ya que está presente en el resto, en Blockchain todos los nodos contienen copias de la misma información garantizando que esta no se pierda.

1.6. Blockchain más allá de las transacciones con moneda virtual

En los capítulos anteriores, la mayor parte de la explicación sobre Blockchain se ha hecho en relación a las transferencias de criptomonedas, dado que éstas han sido la aplicación principal de este sistema hasta el momento. Aún así, con el tiempo, se empiezan a vislumbrar, e incluso, consolidar, nuevas campos de desarrollo para esta tecnología.

Tras la aparición de Blockchain, los usuarios han ido adquiriendo una actitud más bien inquieta con respecto a los límites de aplicación de esta tecnología. Así pues, se ha hecho evidente que no sólo se pueden almacenar y enviar transacciones con información monetaria, sino que también se pueden guardar documentos escolares, certificados, licencias, registros médicos o incluso votos. Es más, se ha visto que, a parte de almacenar todo tipo de información, es posible registrar reglas. Este mismo hallazgo fue el que dio cobertura al desarrollo de los contratos inteligentes (*Smart contracts*).

Dicho esto, pongamos el caso de que un sujeto A se dispone a realizar una transferencia de bitcoins a un sujeto B. Hasta aquí el funcionamiento empleado es igual al que se ha descrito en esta memoria hasta el momento. Sin embargo, como se venía diciendo, Blockchain hace posible la incorporación de nuevas reglas en este juego de transferencias. Seguidamente se proponen algunos ejemplos de las condiciones que se podrían incorporar:

- el sujeto A únicamente podrá realizar la transferencia al sujeto B si dos otros sujetos, C y D, aceptan esta transacción de valor.
- la transacción de bitcoins entre los sujetos A y B únicamente se puede realizar si se hace el primer día de mes.
- o, la combinación de las dos reglas anteriores: el sujeto A sólo podrá transferir dinero a B si es primer día de mes y, los sujetos C y D aceptan previamente la transacción.

Y así sucesivamente, añadiendo y quitando limitaciones se puede ir conformando un sistema de validación y consenso, hecho a medida para cada usuario.

Si todas las partes interesadas aceptan estas reglas, éstas se actualizan en Blockchain. De esta manera, se consigue establecer contratos de alta seguridad abaratando el coste y el tiempo que supondría añadir partes que regulasen la legalidad del contrato. Y puesto que todo queda registrado, y es altamente difícil modificar los contenidos una vez aceptados por toda la red, el sistema se consolida como una herramienta de contratos segura.

Así pues, la vuelta de tuerca que Blockchain incorpora al sistema de contratos, permite a un contrato ejecutarse y validarse de manera autónoma, garantizando la seguridad de los intereses de las partes. Este nuevo enfoque, a partir del cual se usa la tecnología de bloques como una herramienta que puede ser modificada para que se adapte a los intereses específicos del usuario dentro de un gran marco de aplicaciones, es la clave de este trabajo.

2. Estudio de mercado

En el apartado anterior se ha introducido una de las principales y más genéricas aplicaciones de Blockchain. Sin embargo, en este trabajo el foco central no reside en la implementación de la cadena de bloques en los contratos, sino en la aplicación de esta tecnología en el tercer sector. Por este motivo, a continuación, se ofrece un marco global de la integración de la cadena de bloques en varios procesos vinculados con ONGs, con el fin de asentar unas bases y ver lo que se encuentra actualmente en el mercado. En apartados previos se ha podido entender detalladamente el funcionamiento global seguido por Blockchain. No obstante, aún no se han explicado de manera explícita las principales ventajas que esta tecnología puede ofrecer a ámbitos relacionados con el sector de las organizaciones sin ánimo de lucro. En los puntos que siguen, se verán de manera general algunas de ellas, aunque se detallaran con mayor profundidad en el tercer capitulo de esta memoria.

2.1. Proyectos del tercer sector basados en la implementación de Blockchain

2.1.1. Plataforma ComGo

Incluso con un impacto mayor que el de las criptomonedas, la tecnología Blockchain ha sido recibida con los brazos abiertos por el tercer sector, ya que aporta al ADN social de estas instituciones, conceptos tan agradecidos como transparencia, eficacia, certeza, confianza y seguridad, entre otros.

Un ejemplo evidente y fundamental es la posibilidad que ofrece Blockchain de seguir la trazabilidad real de cada donación desde que el donante realiza la transferencia, hasta que ésta llega a su destino final. Este hecho resulta de vital importancia para garantizar la transparencia tan buscada por muchas organizaciones sin ánimo de lucro. La desconfianza en el tercer sector se hace evidente en las magnitudes indicadas por un estudio [iii] elaborado por la Asociación Española de Fundraising (AEFr). En este documento se muestra que esta falta de confianza fue el factor principal que impidió

donar a un 56% de los españoles encuestados. Es más, en 2017, la confianza en las ONGs se desplomó 10 puntos en todo el mundo, hasta el 53% según el Barómetro Edelman[4]. En el caso de las ONGs pequeñas, la situación se agrava, puesto que el poco dinero que reciben no pueden invertirlo en publicidad que les genere notoriedad suficiente.

En este contexto de gran escepticismo, y con la implicación de IBM (International Business Machines Corporation), nace ComGo [iv]. Esta plataforma se basa en la tecnología Blockchain para ofrecer a diferentes organizaciones como Caritas y ItWillBe.org entre otras, contratos inteligentes con el fin de otorgarles transparencia y audibilidad. Además, permite que la transparencia sea constante en toda la cadena de participantes en el proceso (donantes, fundadores, auditores, ONG…), y de este modo, da una visión especifica y veraz del origen de las donaciones, cómo se gastaron y el impacto resultante.

Figura 2.1 Página principal de la plataforma ComGo (comgo.io)

Por ejemplo, en el caso de la implementación llevada a cabo en la organización ItWillBe.org que trabaja dando asistencia a 200 niños sin hogar en Surat (India); un trabajador social sólo recibe su salario cuando se compran alimentos o productos higiénicos para los niños de esta región. Únicamente entonces, la transacción es habilitada y las facturas se cargan al sistema a través del teléfono móvil del ayudante. De esta manera, la transacción queda registrada en Blockchain y es posible ver en qué momento se ha realizado.

[4] Barómetro Edelman: consiste en una herramienta que da a conocer los niveles de confianza que la población tiene en los siguientes sectores: empresarial, gubernamental, ONGs y en los medios.

En la actualidad, ComGo está implementando Blockchain en otros sectores como el de la alimentación o el farmacéutico y, al mismo tiempo, tratando de desarrollar el sistema actual de Blockchain para ONGs, haciéndolo más seguro y fiable.

2.1.2. The Responsible Cobalt Initiative

Pero la India no es el único país en vías de desarrollo al que llegan proyectos de esta índole. En la actualidad, la República Democrática del Congo es el principal país extractor de cobalto del mundo. El cobalto es un metal muy utilizado en las baterías de litio para los teléfonos móviles o vehículos eléctricos y puesto que la producción de estos últimos esta en auge, también lo está la demanda del mineral y, consecuentemente, su precio se está disparando. Sin embargo, Amnistía Internacional ya ha advertido sobre los abusos contra los derechos humanos, sobretodo de explotación infantil, relacionados con la minería de cobalto en esta parte del territorio africano. Como consecuencia, diferentes compañías, entre las que destacan Apple y Tesla, se han sumado a una iniciativa llamada The Responsible Cobalt Initiative que, impulsada por la entidad china CCCMC's [5], buscan garantizar la producción de cobalto libre de explotación de menores.

Figura 2.2 Condiciones de trabajo de los niños en las minas de extracción de cobalto de la RDC

Puesto que es necesario tener un control de toda la cadena de suministro, Blockchain se presenta como una de las soluciones más atractivas. Para conseguirlo, los responsables de esta iniciativa tienen como primer objetivo realizar un programa

[5] **CCCMC's:** Chinese Chamber of Commerce of Metals, Minerals and Chemicals Importers & Exporters.

piloto que haga uso de la tecnología Blockchain para monitorizar toda la cadena de producción del cobalto: desde la extracción mediante minería hasta la manufacturación de este metal.

Entrando un poco más en detalle, este plan piloto plantea etiquetar digitalmente todas las bolsas de cobalto selladas que cada minero extraiga del subsuelo. Esta etiqueta se actualizará en la cadena de bloques mediante un teléfono móvil y llevará información de la fecha, hora, peso e incluso una fotografía de la bolsa. En el siguiente nivel de la cadena de suministro, el comerciante que compre la bolsa deberá ingresar los detalles de la transacción en Blockchain y así sucesivamente hasta que se llegue a la fundición del metal. De esta manera, se garantiza que cualquier comprador o tercero pueda acceder a la información de cada movimiento del cobalto, implicando así a todas las organizaciones que participan en la cadena de suministro y asegurando que el producto final procede de procesos fiables y legales.

Personalmente, con las especificaciones requeridas por Blockchain descritas en el párrafo anterior, es decir, información sobre la fecha, hora, peso y fotografía de la bolsa; cuesta entender como se asegurará exactamente que el trabajador no es un menor. No obstante, esta misma información no carece en absoluto de utilidad en la trazabilidad de la cadena de suministro, sino todo lo contrario, puesto que permitiría solventar otros problemas y cuestiones controversiales de interés. A continuación se detalla un claro ejemplo.

El precio del cobalto ha ido subiendo en los últimos años y los grandes inversores se han aprovechado de ello comprando grandes cantidades con el fin de retener esta materia prima hasta que el precio esté por las nubes. Mediante el sistema de trazabilidad que ofrece Blockchain, es posible pasar de un sistema binodal, donde el propietario de la mina y el inversor acuerdan un precio de compra del cobalto; a un sistema con diversos nodos, donde todas las personas de la mina registran la fecha y la hora de las bolsas del cobalto que extraen. Tal es así que el inversor que compre el cobalto no podrá especular con el precio del producto ya que la fecha de extracción del mineral aparecerá de manera pública y permanente en el registro de Blockchain y

cualquier comprador posterior podrá saber el precio de mercado del cobalto en el momento de su extracción.

Éste es tan solo un ejemplo de cómo The Responsible Cobalt Initiative podría mejorar la trazabilidad del proceso de extracción de cobalto. Dicho proceso presenta una cadena de suministro muy compleja y son varias las grandes compañías que ya han expresado su inquietud sobre las dificultades que han tenido hasta el momento para asegurarse de que todas las partes del proceso sean seguras y legales. Así pues, el sistema de bloques aparece como una buena solución para tratar diversos de estos aspectos, la mayor parte de ellos, relacionados con la trazabilidad de la cadena de suministro de este mineral. Sin embargo, aunque en el articulo de prensa publicado en la pagina web BitcoinAfrica.io[v] se llega a puntualizar que el plan piloto incluirá monitores en el terreno que garanticen el trabajo libre de explotación infantil; no se dan datos suficientemente específicos que indiquen cómo se pretende dar esta garantía mediante Blockchain.

2.1.3. Plataforma Ethereum

Finalmente, se explicará el caso de una aplicación basada en Blockchain desarrollada por un grupo de programadores malagueños. Mediante la utilización de la cadena de bloques buscan implementar una nueva plataforma que dote de mayor transparencia la financiación de las ONGs y transmita fiabilidad a los donantes.

La ventaja de este sistema es que, a diferencia de los proyectos anteriores que buscan solventar carencias o problemas de ONGs concretas (aunque podrían llegarse a extrapolar al resto), esta aplicación desarrolla un sistema de rastreo y control de donaciones general. Es decir, un sistema que estará disponible para cualquier organización que se descargue esta app.

Partiendo de esta idea, este grupo de programados han diseñado una cartera inteligente (*smart wallet*) con acceso restringido y accesible únicamente mediante dos

claves: una en posesión del donante, que transferirá dinero como donación, y otra del profesional de la organización que esté ayudando en la tarea humanitaria en cuestión. Ambas claves son indispensables para que se lleve a cabo la transferencia de dinero. En este caso, la necesidad de recurrir a Blockchain para conseguir el proceso descrito es indudable. Recordemos que, durante el primer capítulo de esta memoria, se ha visto todo el funcionamiento del sistema de clave asimétrica, cuyas bases teóricas, constituyen la idea principal de esta aplicación.

Resumiendo el párrafo anterior, mediante los procesos intrínsecos de la cadena de bloques, se garantiza al donante que su donativo únicamente se transferirá una vez se haya alcanzado el objetivo de la donación. Por ejemplo, si se dona con el fin de conseguir asilo para un refugiado, el dinero se enviará a la cartera ubicada en el campo de refugiados, pero no se entregará al profesional hasta que no se haya transferido al donante un documento acreditando el asilo de la persona en cuestión, para que la transacción pueda ser validada y se haga efectiva. En este aspecto, este sistema de monitorización del dinero presenta una metodología muy parecida a la comentada en el punto 2.1.1. con el caso de los niños de Surat.

Este proceso garantiza a los donantes que el dinero que ellos envíen se utilice para las causas correctas; incentivando y beneficiando tanto a las personas que prestan la ayuda como a las que la reciben.

Aunque la aplicación aún está en proceso de implementación, ya se ha podido probar en un primer ejemplo. Se trata del caso de Esther, una mujer con dos hijos y cuyo esposo se encuentra en prisión condenado por malos tratos. Incapaz de sobrellevar esta situación, Esther cayó en la dependencia de los somníferos y llegó a requerir más de veinte sedantes al día que además, acabó mezclando con alcohol. Dadas las circunstancias, acabó perdiendo la custodia de sus dos hijos y terminó durmiendo en la calle.

Con la ayuda del centro solidario de recuperación de adicciones Casa de la Buena Vida, Esther ha logrado recuperarse. La aplicación creada por los malagueños participó en

este proceso inmovilizando temporalmente el dinero conseguido mediante donaciones para ayudar a Esther en su caso. Y sólo después de que ésta presentase sus analíticas de sangre, demostrando de manera fidedigna que estaba limpia, los fondos fueron transferidos. Mediante estas regulaciones, libres de intermediarios y muy seguras (como se ha visto en el capítulo 1), se garantiza al donante que su dinero irá, con toda seguridad, a la actividad a la que él lo destine.

Como se ha visto a lo largo de este capítulo, son varios los ámbitos de desarrollo de Blockchain, así como los diferentes enfoques que éste está tomando en cada uno de ellos. Se han explicado brevemente algunas de las aplicaciones más recientes o más importantes que ofrece esta tecnología. No obstante, hay que tener en cuenta que, como bien apuntan en American Banker, los diferentes proyectos con cadenas de bloques distintas están probando ser extremadamente útiles y beneficiosos pero también aportan complejidad y fragmentación; hecho que puede frenar el avance de Blockchain sobretodo en mercados consolidados.

3. Implementación de Blockchain al tercer sector

Una vez visto el funcionamiento de la cadena de bloques y algunas de las aplicaciones de esta tecnología en diferentes actividades solidarias, en las líneas que siguen, se analizará de manera conceptual la implementación de Blockchain en algunas entidades concretas del tercer sector.

Previamente a este análisis, resulta conveniente hacer una aclaración sobre cómo se enfocará esta implementación de Blockchain. A lo largo de este memoria, los nombres usados para referirse a la cadena de bloques han sido diversos. En ocasiones se ha hecho referencia a Blockchain como una metodología, mientras que en otros casos, se le denominaba tecnología. Esta distinción dista de ser trivial, de hecho, es importante tenerla en cuenta para entender bien el análisis que se hará a continuación. Así pues, Blockchain tiene la particularidad de que puede ser entendido como una metodología o una tecnología.

Entrando más en detalle, cuando se habla de la cadena de bloques como una tecnología, se puede decir que se habla de la parte más técnica de este sistema. En otras palabras, con este término se quiere abarcar la parte más tecnológica de Blockchain, la que se basa en toda la programación y el conjunto de algoritmos matemáticos que hacen posible que el sistema funcione tal y como funciona y tenga la autonomía y la seguridad que pretende proporcionar. De esta manera, si bien es cierto que el sistema presenta una gran complejidad, esta parte es parecida a programar una aplicación que realice un conjunto de funciones previamente seleccionadas y consensuadas por los realizadores de dicho programa.

Por otro lado, hablar de Blockchain como una metodología, da lugar a un concepto mucho más abstracto. En este caso, la cadena de bloques se presenta como un método de distribución de la información. Como se veía en la parte de la memoria que explica el funcionamiento de Blockchain, el sistema de cadena de bloques da un giro de 180º al sistema de financiación, y en diversas ocasiones, también al sistema de

transmisión de la información. Tal es así que se pasa de un sistema donde el flujo de dinero o información es totalmente lineal y con necesidad de un intermediario entre las partes que lo haga posible, a una estructura en que la información se encuentra en cada participante del sistema y es verificada por cada integrante de la red. En resumen, Blockchain reinventa el flujo de información tradicional que sigue una disposición lineal y le da un nuevo enfoque adoptando una estructura de red nodal; una disposición que recuerda mucho más a una estructura molecular, distribuida de manera tridimensional por todo el espacio.

Cerrando esta distinción entre Blockchain como tecnología o como metodología, cabe decir que no es que el sistema de cadena bloques se use como una tecnología o, en su defecto, como une metodología, sino todo lo contrario. Blockchain es ambos términos a la vez, simplemente depende del enfoque que se tome, se puede analizar más uno de ellos o el otro. Análogamente a la descripción de Erwin Schrödinger sobre los fotones, en la que éstos se pueden comportar como una onda o como una partícula y sin embargo, son onda y partícula a la vez; Blockchain se comporta como una metodología y como una tecnología al mismo tiempo, y su estudio dependerá del punto de vista que se coja para el análisis.

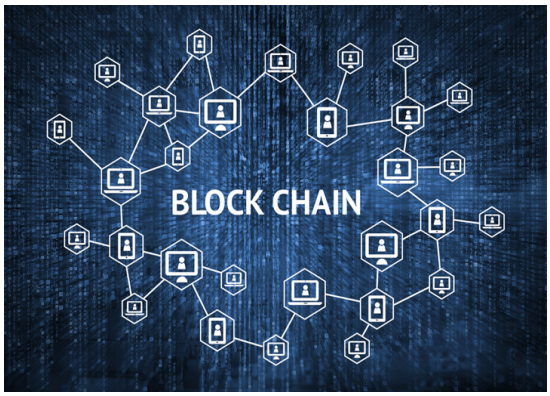

Figura 3.1 Esquema de Blockchain visto como una red de conexiones entre usuarios de una aplicación

Finalmente, como se venía diciendo al principio de este apartado, a continuación se realizará un análisis de las principales ventajas e inconvenientes que la implementación de Blockchain ofrece a entidades del tercer sector. Si bien es cierto que en este último capítulo de la memoria no se detallará la parte de programación de Blockchain en estas entidades, sino que se hará un estudio más enfocado hacia la vertiente de la metodología. Se tomará como punto final de análisis el último usuario de la cadena que pueda disponer de la aplicación de Blockchain. Dicho de otra manera, se explicará la parte más conceptual de Blockchain y como se aplicaría pero, por

ejemplo, si se está hablando de cómo un keniano participaría al final de la cadena por ser el que construye los pozos en un poblado, pero éste no dispone de un teléfono móvil para acceder a Blockchain, éste queda exento del análisis que se llevará a cabo. Así pues, el límite de implementación será el último usuario de la cadena que pueda disponer de un dispositivo que le permita ser usuario de Blockchain para participar en el sistema.

Seguidamente, se estudiará la aplicación práctica de la tecnología de bloques en dos entidades del tercer sector a las que se ha entrevistado sobre su financiación, y se determinará la viabilidad del sistema de bloques en cada una de ellas.

3.1. Aplicación conceptual de Blockchain a la asociación AFANOC

3.1.1. ¿Qué es AFANOC?

AFANOC es l'Associació de Familiars i Amics de Nens Oncològics de Catalunya. Nació en 1987 a raíz de las experiencias vividas por un grupo de padres y madres que se encontraron con la situación de tener un hijo/a ingresado en el hospital por cáncer. Envueltos en el contexto descrito, se percataron de que había diversas carencias en el día a día de la gente que padecía esta enfermedad. Carencias que aún se hacían más notorias si se considera que los tratamientos son de larga duración y, muchas veces, de pronóstico incierto. Así pues, decidieron buscar soluciones, creando programas y servicios, que mejoraran la calidad de vida de estos niños y de sus familias.

Figura 3.2 Logo de la asociación AFANOC

Uno de los proyectos más importantes llevado a cabo por esta asociación es la Casa dels Xuklis. En 2006, la Diputación de Barcelona cedió a AFANOC unos terrenos para construir la Casa dels Xuklis y se constituyó la Fundació Privada Nenes i Nens amb Càncer, responsable de gestionar el proyecto. Se trata de una casa, con 25 habitaciones y varias zonas comunes, que pretende ser un sitio donde los niños que

padezcan la enfermedad, junto con sus familias, puedan sentirse "como en casa" mientras están siendo tratados. Esta casa se encuentra al lado del hospital Vall d'Hebron en Barcelona, hecho que permite a familias que viven lejos, incluso de otros países, no sólo estar en un entorno muy agradable y familiar sino también mantenerse cerca del centro hospitalario del que reciben atención médica.

Figura 3.3 Imagen del exterior de la Casa dels Xuklis

3.1.2. Aspectos generales de la financiación de AFANOC

En cuanto a la financiación de AFANOC hay que tener en cuenta diversos aspectos. Por un lado, la fundación recibe ayudas de donantes particulares y de entidades privadas, como de l'Obra Social "la Caixa" o la Fundación ONCE. Por otro lado, también consigue donaciones de entidades públicas como es la Generalitat.

Además, en el año 2000, AFANOC fue reconocida como Entitat Declarada d'Utilitat Pública, en reconocimiento a su labor. Este reconocimiento da acceso al mismo régimen fiscal especial del que disponen las fundaciones. Concretamente, la declaración de utilidad pública comporta:

- la posibilidad de usar la mención "declarada d'utilitat pública",
- el derecho a exenciones y beneficios fiscales, así como los beneficios económicos que las leyes establezcan a su favor,
- y disposición de asistencia jurídica gratuita.

Resulta conveniente saber que, al estar declarada entidad de utilidad pública, AFANOC tiene derecho a dar certificados de donación a los donantes, hecho que supone una ventaja considerable para estos últimos puesto que les permite desgravar en sus declaraciones de renta.

Finalmente, un último dato sobre la a financiación de AFANOC a tener en cuenta es que la asociación debe rendir cuentas anuales con el Departamento de Justicia de la Generalitat de Catalunya.

3.1.3. Trazabilidad y registro de las donaciones

Hasta ahora, se ha hecho una presentación general de la asociación y se han visto, brevemente, un par de aspectos introductorios sobre su financiación. De ahora en adelante se realizará un análisis que busca determinar la viabilidad de diversos aspectos de Blockchain en sustitución, o como complementación, del sistema actual de financiación de AFANOC.

Como ya se ha visto, la asociación recibe donaciones públicas y privadas. Pero, ¿cómo se efectúan estas donaciones? La respuesta a esta pregunta está vinculada al tipo de donación que se realiza.

Por un lado, se encuentran las donaciones que hacen los socios de la asociación. Éstas se tramitan a través de un banco y de manera periódica. El socio puede escoger la cantidad que quiere donar y cada cuanto la quiere donar (mensual, trimestral o anualmente). Esta donación se realiza a través de la página web de AFANOC desde donde se transfiere el importe donado a una de las cuentas bancarias de la asociación.

Por otro lado, el resto de donaciones por lo general de carácter puntual, se suelen realizar de tres maneras distintas. La primera, a partir de la página web de AFANOC que transfiere directamente la donación del usuario a la cuenta bancaria de la asociación. Como se ha visto en el caso de los socios. En segundo lugar, en ocasiones les ocurre que algún donante, normalmente familiares o conocidos de socios, llama directamente a uno de los centros con la voluntad de donar dinero. En este caso, la persona que les atiende también les facilita el número de cuenta bancaria para que puedan realizar directamente la transferencia. Finalmente, existe la opción de donar dinero en efectivo. Esta es, sin duda alguna, la vía más difícil de trazar. Este tipo de

donativos suelen venir de gente que va a visitar alguno de los centros o que, por el motivo que sea, prefieren hacer las donaciones en metálico.

En el capítulo 1 se hablaba de Blockchain como una gran base de datos donde todas las transacciones quedan registradas. Este registro y trazabilidad dotan al sistema de una gran transparencia; característica muy buscada por todas las entidades del tercer sector. Así pues, si implementamos el sistema de cadena de bloques en AFANOC, tanto las donaciones de los socios como las de los donantes que donen mediante transferencias de cuentas bancarias quedarían registradas en el *ledger* y, además, podrían ser vistas por los usuarios en tiempo real. En tanto que el *ledger* es un documento público, los donantes no sólo podrían ver el registro de dichas transacciones sino trazar todos los movimientos de éstas y su procedencia en cualquier momento.

Teniendo en mente los aspectos descritos del funcionamiento de la cadena de bloques, resulta comprensible preguntarse cómo sigue actualmente AFANOC, toda la trazabilidad de sus transacciones. Pues bien, a día de hoy, la asociación cuelga anualmente su financiación en su página web. Estos datos también se pueden encontrar en el departamento de justicia y, en el caso de los socios, los pueden solicitar directamente a AFANOC en cualquier momento. Además, todos los aspectos relativos a la financiación se auditan, garantizando su veracidad. El hecho de que AFANOC esté declarada entidad de utilidad pública, permite mantener un registro de las donaciones de forma más sencilla. A partir de los certificados de donación que se dan a los donantes, la asociación puede llevar un registro adecuado de las donaciones. Sin embargo, hay que tener en cuenta que existen donantes que no solicitan el certificado de donación y por tanto, los datos extraídos a partir de esta fuente quedan distorsionados y pierden exactitud.

En este caso pues, más que garantizar más transparencia, Blockchain ofrecería al donante la posibilidad de tener datos mucho más específicos y actualizados que el sistema que AFANOC tiene en la actualidad. La tabla del Anexo 5.1., muestra los

balances de las cuentas de la asociación. Estos datos representan la única fuente que permite a los donantes saber dónde destinan su dinero.

Como se puede ver la tabla mencionada en el párrafo anterior, los ámbitos donde se destinan recursos son muy genéricos y además se actualizan de manera anual. Mediante el sistema de cadena de bloques, más que una solución, se estaría aportando una mejora, tanto para la asociación que tendría un registro de datos más específico y en tiempo real, como para el donante que podría seguir la traza de su donación minuto a minuto. Por tanto, pasaríamos de un sistema que sólo nos dice de manera genérica los ámbitos a los que se destina todo el dinero recaudado en donaciones cada año; a un sistema donde el donante podría ver a qué actividad concreta se destina la cantidad de dinero que él mismo haya aportado, y todo esto, de manera instantánea. En resumen, Blockchain da lugar a lo que vendría siendo una auditoría en tiempo real sobre todos los flujos de dinero de la asociación.

Finalmente, un último aspecto que falta por analizar, son las donaciones que se realizan en efectivo. Los problemas de registro y trazabilidad que acarrean las donaciones en efectivo no pueden ser solucionados mediante Blockchain puesto que este sistema no trabaja con dinero fíat, sólo con dinero virtual (Anexo 1).

3.1.4. Automatización del sistema

En el punto anterior hemos visto como Blockchain aportaba una mejora al sistema actual de donaciones de AFANOC pero no añadía novedad alguna. Sin embargo, la tecnología de bloques presenta la interesante función de que una vez se ha “subido” al sistema la transacción de dinero, los movimientos que ésta deba realizar a continuación se pueden automatizar. En el punto 1.6. de esta memoria, se ha visto un claro ejemplo donde Blockchain introducía esta función: los *Smart Contracts*. Al fin y al cabo, este tipo de contratos no deja de ser una manera particular de automatizar el sistema.

Llegados a este punto conviene recordar el caso de la plataforma ComGo cuyo objetivo principal es, justamente, la creación de contratos inteligentes que permiten trazar todo el "recorrido" de una donación, desde que el donante la realiza, hasta que los productos para los niños que viven en las calles de la India han sido comprados. Tal y como se explica en el punto 2.1.1. de este documento.

Volviendo ahora al caso concreto de AFANOC, Blockchain permitiría monitorizar el sistema de donaciones de la asociación, de tal manera que tuviera en cuenta las diferentes transacciones que los donantes realizan, y gestionase esa cantidad de dinero para cubrir los diversos gastos de la asociación. Es decir, si un día concreto se realizan donaciones que alcanzan un valor de 150 euros, el sistema cogería esta cantidad y, o bien la guardaría hasta que fuese necesaria para hacer un pago o, por el contrario, si ya existe algún servicio que deba ser pagado, la destinaría automáticamente al pago de dicha actividad.

Si bien es cierto que otras aplicaciones podrían llegar a hacer esta misma función, Blockchain va un paso más allá. Pongamos un ejemplo para entenderlo mejor. Supongamos que el sistema recoge las donaciones hechas por los donantes y se dispone a transferir de manera automática parte de ese dinero a la agencia de mantenimiento que se encarga de la limpieza de la Casa del Xuklis. La tecnología de bloques permite programar el proceso de tal manera que sólo se complete la transacción una vez algún empleado de AFANOC, haya comprobado y acreditado que la limpieza se ha efectuado debidamente. Son diversos los mecanismos usados mediante Blockchain para acreditar estas actividades. A continuación, se repasan algunos de los casos prácticos ya vistos en el capítulo anterior donde se plantean diferentes maneras de certificar la realización de actividades benéficas a través de la tecnología de bloques.

Uno de estos ejemplos se ha visto a lo largo del punto 2.1.1., donde la plataforma ComGo opta por automatizar el sistema, de tal manera que el trabajador que vaya a comprar productos para los niños de Surat, sólo reciba su salario una vez haya

acreditado, mediante las facturas correspondientes, que ha destinado todo el dinero procedente de las donaciones, a la compra de dichos productos.

Otro caso se detalla en el punto 2.1.2., con *The Responsibility Cobalt Initiative*, un proyecto que también exige una comprobación de que las actividades humanitarias son las correctas enviando información sobre cada extracción de cobalto junto con una fotografía del mismo.

Finalmente, con el caso de Esther (punto 2.1.3.), se puede ver, una vez más, que hasta que ella no presenta los análisis de sangre que confirman que ya no consume drogas, no se le ingresa el dinero recolectado a partir de las donaciones.

Un defecto de este sistema que puede presenciarse en cualquiera de estos proyectos, incluido el de AFANOC, es el que se detalla a continuación. Si bien es cierto que Blockchain permite verificar de manera segura y precisa los bienes y servicios concretos a los que se están destinando las donaciones; más allá de este punto, cuesta rastrear que ese bien o servicio en cuestión se esté destinando a una actividad benéfica. No siempre se podrá controlar el 100% de la cadena pero es conveniente estudiar bien todos los intermediarios y destinatario final por donde tiene que pasar el dinero para poder acotar al máximo este control.

Llegados a este punto, resulta interesante comentar el proyecto de AID:Tech (Anexo 3.2.) en el Líbano. Este proyecto tiene como objetivo garantizar que los refugiados sirios tengan dinero suficiente para comprar productos básicos en los supermercados locales. Para ello, AID:Tech se asoció con estos minoristas locales y, mediante Blockchain, consigue generar “bonos inteligentes” que se dan directamente a las familias y que éstas pueden canjear por productos en los supermercados. Por tanto, estudiando bien las actividades y aplicando Blockchain de manera conveniente, en algunos casos es posible asegurar un control total sobre el flujo de dinero.

Así pues, AFANOC, para implementar de manera efectiva el sistema descrito debería extender el proceso visto con el caso de la agencia de limpieza de la Casa dels Xuklis, a todas las empresas o personas que ofrezcan algún servicio a la asociación y que cobren por ello; desde los profesores que van a dar clase a los niños hasta los psicólogos o el hospital que les trata. De este modo, se da al donante, información más precisa y más fiable del fin benéfico donde se destina su dinero e incluso se le notifica y acredita exactamente del ámbito al que ha sido destinada su donación.

3.1.5. Ausencia de un intermediario que gestione las transacciones

En los párrafos anteriores se ha hecho evidente que la mayor parte de donaciones que se hacen a AFANOC se tramitan a través de un banco. La asociación dispone de cuentas en diversos bancos para que los donantes puedan realizar las transacciones. Uno de los motivos de esta segregación es el hecho de evitar más comisiones. De tal manera que, si un donante es del Banc Sabadell, no tenga que pagar comisión para hacer una transferencia a una cuenta bancaria que AFANOC tenga abierta en la Caixa. Pero a parte de estas comisiones por realizar transferencias entre cuentas de diferentes bancos, este tipo de instituciones también suelen cobrar por tener cuentas abiertas, entre otros. Es sobre estos aspectos donde AFANOC debe negociar con los bancos con los que trabaja con el fin de conseguir las mínimas comisiones, y consecuentemente, tener los menores gastos posibles. Algunos de los bancos con los que trabaja la asociación son Banc Sabadell, la Caixa o BBVA y, con cada uno de ellos, establecen unas comisiones que en el mejor de los casos pueden llegar a ser nulas.

Es en este punto donde Blockchain presenta su ventaja más destacada y el aspecto que más diferencia esta tecnología de una aplicación cualquiera. Como se ha visto en el capítulo 1 de esta memoria, una de las particularidades de la cadena de bloques es que no requiere de intermediarios o terceros que ayuden a transferir o guardar el dinero. En el punto 1.5.2. mediante la explicación de la estructura distribuida que sigue Blockchain se hace evidente que, gracias a la ausencia de un servidor central, la

tecnología de bloques permitiría a AFANOC reducir parte de sus costes, eliminando la necesidad de una entidad intermedia que valide y gestione las transacciones de dinero del donante a la asociación. Así pues, Blockchain elimina completamente el papel de los bancos; hecho que no sólo supone una reducción de costes a la asociación sino también de tiempo, en tanto que todo el tiempo invertido en negociar y hacer otros tramites con el banco desaparece.

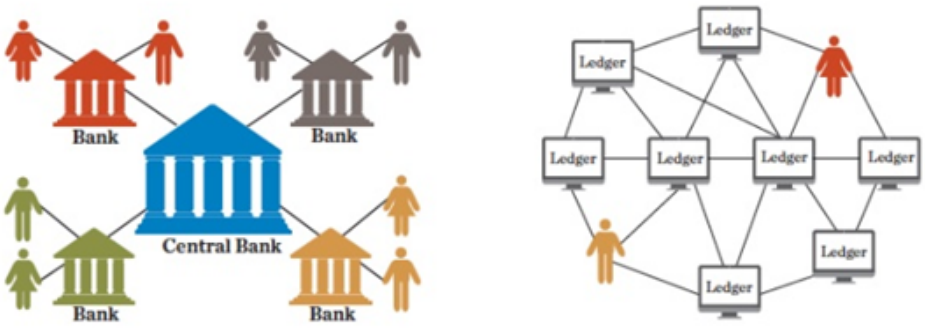

Figura 3.4 Sistema actual dependiente de un banco central (izquierda) en contraposición al sistema más contacto de conexiones entre todos los *ledgers* que ofrece Blockchain.

Recopilando más ideas vistas en el capítulo 1, conviene recordar que cuando un donante quiere realizar una transferencia mediante Blockchain, es el mismo sistema, el que verifica si esta transacción es correcta y si sigue adecuadamente "las reglas del juego". Dicha transacción se acepta en el sistema cuando el bloque más "hábil" consigue resolver un complejo algoritmo matemático, y no queda validada, hasta que un 51% de los usuarios de Blockchain la aceptan como buena. Este proceso se ha detallado más profundamente en el punto 1.4.1., donde explicábamos el funcionamiento general de la tecnología de bloques. Por tanto, haciendo uso de todas estas herramientas, Blockchain permite suplir la función que actualmente hacen los bancos, y la transferencia pasaría al sistema estando ésta validada y quedando registrada en el ledger.

3.1.6. Microdonaciones

Otro aspecto de la financiación de AFANOC que puede verse muy beneficiado por la cadena de bloques son las microdonaciones. El hecho de que los bancos cobren comisiones por efectuar transferencias hace que realizar donaciones de algunos

céntimos de euro pueda suponer un coste mayor para la asociación que el beneficio aportado por dicha donación. A parte, puesto que son cantidades de dinero ínfimas, el donante no tiene un interés especial en solicitar el certificado de donación y por tanto, el control que se tiene sobre este tipo de donaciones suele ser menor. Mediante la tecnología de bloques, donar cantidades muy pequeñas de dinero de manera casi instantánea, las 24 horas del día, desde cualquier lugar con conexión a internet, mejora la rentabilidad de las transacciones en tiempo y esfuerzo. Esta mejora puede resultar significativamente útil para grandes campañas de sensibilización lanzadas a través de las Redes Sociales, donde los donantes con tan sólo un clic pueden hacer donaciones instantáneas de pequeñas cantidades monetarias. De esta manera, tener acceso a donantes o socios más puntuales que donen grandes sumas de dinero ya no se presenta como la única opción para conseguir financiar grandes campañas de corta duración. Gracias a la tecnología de bloques, a través de un medio de difusión masiva, se puede llegar a una cantidad mayor de personas que, con donaciones menores, consigan igualmente una gran recolección de dinero.

El problema de los micropagos es una cuestión que ha resultado ser especialmente problemática durante mucho tiempo, especialmente para las ONGs. Ahora, con la implementación de Blokchain, AFANOC puede ampliar su estrategia de campañas. Una de las campañas con más impacto realizadas por la asociación, es la campaña "Posa't la gorra". En ésta, AFANOC compra gorras a un precio muy asequible y posteriormente las revende a 7 euros cada una. En este caso, el precio al que venden las gorras es suficiente como para que les salga rentable cada donación.

Figura 3.5 Cartel publicitario de la campaña Posa't la gorra de Lérida

Sin embargo, hasta ahora llevar a cabo grandes campañas de sensibilización en las que se recaudasen directamente fondos de unos céntimos de euro era complicado.

Mientras grandes ONGs tienen suficientes recursos para impulsar campañas mediáticas muy potentes, entidades benéficas que operan en un ámbito más local carecen de este presupuesto, como es el caso de AFANOC. Por este motivo, la posibilidad de financiarse mediante Blockchain aún resulta más atractiva. Hasta el momento, aprovechando la importante presencia de las redes sociales en la población y su gran capacidad de difundir masivamente mensajes a bajo coste, lanzar una campaña haciendo uso de esta herramienta ya se presentaba como una opción con mucho potencial. Sin embargo, ofrecer la posibilidad de donar 0,5 euros resulta mucho más atractivo que pedir un mínimo de 6. Así pues, el sistema de bloques pone la pieza que faltaba al puzle y brinda la posibilidad, a organizaciones más locales como es AFANOC, de realizar este tipo de campañas.

3.1.7. Anonimato en las donaciones

Hasta el momento se han visto los aspectos de Blockchain que más aportarían al sistema actual de financiación de AFANOC. Seguidamente, veremos otras características cuya mención puede resultar relevante pero cuyo impacto en la asociación es menor.

A lo largo de la entrevista realizada a la gerente de AFANOC Rosa Casals Sorribas, surgieron un par de aspectos que le hicieron cuestionar si la implementación de dichos aspectos en la organización daría lugar a un proceso viable. Por un lado, tal y como hemos visto en otros capítulos de esta memoria, se menciona repetidamente que, en Blockchain, las transacciones quedan registradas en el *ledger* y se hacen públicas para que todo el mundo pueda verlas. Esta característica, que de entrada supone la ventaja evidente de que el sistema es mucho más transparente; puede dar lugar a la siguiente pregunta: ¿si todas las transferencias se realizan de manera pública, se puede mantener el anonimato de los usuarios que las realizan, es decir, de los donantes? Esta no es una pregunta banal. Tal y como se ha comentado en el punto 1.4.2., en el sistema de financiación tradicional (del que son partícipe y elemento clave los bancos),

cualquier flujo de dinero es privado y, consecuentemente, sólo es conocido por el emisor, el receptor y el banco. Sin embargo, en Blockchain, toda la información relativa a las transacciones es pública. Tanto la cuenta del emisor y del receptor como los movimientos de dinero que se realizan en la cadena de bloques deben ser públicos para que se puedan validar las transacciones, puesto que no existe un banco que actúe como intermediario para darles validez. Sin embargo, recuperando más aspectos comentados en este punto de la memoria, recordemos que Satoshi Nakamoto ya contempló la necesidad de hacer que los usuarios mantuviesen su anonimato cambiando el punto donde se corta el flujo de información y manteniendo las claves públicas anónimas. De tal manera que, aunque todos los flujos de dinero sean públicos, no es posible conocer quién efectúa cada transacción.

Por tanto, y a modo de resumen, aún con los peculiares parámetros en que se basa la tecnología de bloques, el anonimato de los donantes se sigue garantizando. Este es un aspecto que ciertos donantes consideran realmente sustancial y, por tanto, un sistema que no diese esta garantía supondría una desventaja significativa.

3.1.8. Caída y hackeo del sistema

Un segundo aspecto crítico que surgió durante la reunión con la gerente de AFANOC, es el escepticismo que puede suscitar el hecho de que toda la financiación de la asociación dependa única y exclusivamente de una aplicación. Como se ha comentado, AFANOC dispone de varias cuentas en bancos distintos y por tanto, no depende de un servidor central. Así pues, una pregunta razonable es la que sigue: ¿si todo el dinero de la asociación se encuentra y depende de un solo sistema, Blockchain en este caso, si el sistema cae o es hackeado, se puede llegar a perder parte o todo el dinero?

A lo largo de esta memoria, se han expuesto varios ejemplos de cómo actuaria la tecnología de bloques en caso de ser hackeada o, lo que es más, se ha analizado la posibilidad de si ésta puede llegar a ser hackeada. En el punto 1.5.2. se partía de un

enfoque global de la red de nodos mineros para estudiar como respondería el sistema si, por el motivo que fuese, el funcionamiento de un nodo fallase. Tal y como se analizaba en este punto de la memoria, la estructura distribuida de Blockchain, permite hacer copias idénticas de toda la información en cada uno de los nodos mineros que participan en la red y, por tanto, aunque se pudiese alterar el funcionamiento de uno de ellos, la información (o el dinero en este caso) no se perdería.

Sin embargo, el punto anterior puede llevar a la interesante cuestión de qué pasaría si en vez de intentar atacar un nodo o, varios de ellos, atacásemos todo el sistema. ¿Es eso posible? En el punto 1.4.6. se estudiaba este mismo caso. Recordemos que el trabajo computacional que exige "engañar" a Blockchain con nueva información implica reescribir, en cada nodo, todos los hashes registrados de las transacciones anteriores. Esta tarea requiere una potencia computacional colosal y, a día de hoy, un único nodo difícilmente puede replicarla.

Al final del punto 1.4.6., se estudiaba el caso de que se intente incorporar al sistema un bloque deshonesto, y mediante la comparación con el problema de los generales bizantinos, se ha visto como la misma tecnología de bloques solventaría esta intrusión.

Finalmente, al final del punto 1.4.4. donde se hablaba de firmas digitales, también se ha considerado la situación de que un atacante hiciese uso de la clave pública del beneficiario de una transacción para descifrarla y luego quisiese cifrarlo con su clave privada para poder volver a enviar esa cantidad de dinero. Como se ha visto, tal acción tampoco sería posible puesto que el sistema dejaría un texto cifrado sin sentido.

Estos son algunos de los ejemplos por donde el sistema podría ser "atacado". Si bien, hecha la ley, hecha la trampa. Como cualquier otro sistema informático, Blockchain presenta puntos débiles por donde se le puede atacar. Sin embargo, a día de hoy ha probado ser muy robusto y, de hecho, existen proyectos de investigación que buscan fortalecer estos puntos y dar aún más seguridad a esta tecnología. Hasta la fecha, la

parte del sistema que ha resultado ser más vulnerable al hackeo han sido las claves privadas. Existen métodos para guardar de manera segura dichas claves, pero si no se protegen bien, son un blanco fácil (Anexo 4). En definitiva, en la actualidad es muy complicado interferir en el sistema de Blockchain y, como consecuencia, esta tecnología se presenta como una opción ventajosa para entidades como AFANOC (siempre y cuando conserven a buen recaudo sus claves privadas).

3.2. Aplicación conceptual de Blockchain a Oxfam Intermón

3.2.1. ¿Qué es Oxfam Intermón?

Oxfam Intermón es una organización no gubernamental española de cooperación para el desarrollo que colabora en más de 90 países. Fue fundada en 1956 como Secretariado de Misiones y Desarrollo de la Compañía de Jesús y, desde 1997, pertenecen a la confederación internacional Oxfam; una entidad que cuenta con casi dos decenas de miembros. Cada uno de estos miembros mantiene su propia identidad e independencia pero todos ellos comparten un objetivo común: erradicar la pobreza en el mundo.

Figura 3.6 logo de Oxfam Intermón

Oxfam Intermón destaca por ser un referente en el análisis y la denuncia de la desigualdad extrema y sus consecuencias. Además, son expertos en la rápida distribución de agua potable, higiene y saneamiento ante situaciones de emergencia humanitaria.

Son múltiples los proyectos en los que esta organización participa cada año, trabajando conjuntamente con más de 3000 organizaciones locales. Para Oxfam, esta cooperación es vital para que sean las mismas comunidades y personas afectadas las que puedan hacer cambios en su entorno e incidir en las causas de la pobreza.

Una vez hecha esta breve presentación sobre Oxfam Intermon, se proseguirá a implementar de manera conceptual el sistema de cadena de bloques a esta entidad.

3.2.2. Trazabilidad y registro de las donaciones

Como ya se ha introducido en el punto 3.1.3. con la aplicación de Blokchain a AFANOC, la trazabilidad y el registro de las donaciones son aspectos cuyo potencial con Blockchain es realmente significativo. A continuación se documentan los aspectos más relevantes del sistema de registro y trazado de donaciones utilizados por Intermón hoy en día.

Para ello, conviene hacer una distinción previa. Actualmente Intermón trabaja con dos tipos de ingresos (o donativos): los ingresos dirigidos y los ingresos libres.

Los primeros son aquellos que, tal y como su nombre indica, van dirigidos directamente a una cuenta bancaria específica que la organización abre para poder financiar de manera rápida y eficiente una determinada emergencia humanitaria. En este caso, el donante sabe la causa concreta a la que está destinando su donación pero desconoce las actividades o los bienes específicos a los que se entrega el dinero. Por tanto, aunque no exista un registro propiamente dicho, el donante sí tiene constancia de la causa humanitaria a la que va asignado el importe que ha donado a Intermón.

El segundo tipo de ingresos, los que también se denominan donativos libres, representan los que se recaudan para el resto de proyectos y operaciones. Es decir, los donativos que van destinados a los fondos generales de la organización y que, más tarde, ésta asignará a las actividades que los requieran. Por tanto, en este segundo caso, el donante no sólo no sabe la actividad concreta a la que va destinada su donación, sino que tampoco sabe a qué causa humanitaria se distribuye.

En las líneas que siguen se entrará un poco más en detalle sobre las cuentas de la ONG y la manera que ésta tiene de acreditar a sus donantes qué se hace con sus donativos. El sistema utilizado por Oxfam es similar al de AFANOC y consiste en publicar anualmente informes donde se detalla la cantidad de dinero destinada a cada ámbito (Anexo 5.2.). Sin embargo, como ocurría con AFANOC, estos ámbitos son muy

genéricos y no permiten tener constancia de a qué causas o actividades concretas ha sido destinado el dinero de cada donante.

Teniendo en cuenta estos datos, se hace evidente que Blockchain puede mejorar varios aspectos de este sistema. Tal y como se ha visto en el capítulo 1 de esta memoria, la tecnología de bloques permitiría al donante seguir una traza constante de sus donaciones. Como se comenta en el punto 1.3., Blockchain funciona como una gran base de datos donde todas las donaciones quedan registradas. Más allá de tener un registro permanente de las transacciones, la tecnología de bloques permitiría al donante seguir todos los movimientos de su donación. Así pues, no sólo haría posible saber a qué actividad va destinado el dinero sino que también guardaría un registro de todos los intermediarios por los que éste haya pasado. No obstante, es cierto que, tal y como veíamos en el caso de AFANOC, dependiendo de la actividad humanitaria en cuestión, la trazabilidad se puede llevar a cabo de manera total o parcial (punto 3.1.4.). Además, hay que tener en cuenta que se trabaja en países con un marco legislativo muy diferente al nuestro y que, aunque se pidan facturas, recibos o certificados, éstos no siempre son una buena garantía.

Asimismo, conviene recordar que todo este registro de datos es público. Por tanto, dado que todos los usuarios de la red pueden verificar que el dinero recaudado en las donaciones se está destinando a actividades con fines humanitarios, el sistema de la tecnología de bloques también actúa como ente auditor de las finanzas de la ONG. Puesto que organizaciones como Oxfam auditan anualmente sus cuentas y publican los correspondientes documentos en su página web, Blockchain no supone una mejora sino una manera alternativa de verificar el uso correcto de las donaciones, tal y como se ha visto con AFANOC. Sin embargo, hay que tener en cuenta que contratar una empresa auditora supone un coste adicional. Al fin y al cabo, es un intermediario más al que Intermón destina fondos y que, mediante Blockchain, se puede eliminar.

En resumen, Intermón publica informes donde acredita a qué ámbitos han ido destinados los fondos recaudados, pero su actualización y verificación se realizan únicamente una vez al año y de manera muy general. Por el contrario, Blockchain

puede trazar todos movimientos de cada donación en tiempo real y sin coste alguno, otorgando a Intermón uno de los conceptos más buscados en el tercer sector: la TRANSPARENCIA.

3.2.3. Automatización del sistema

Este apartado está íntimamente ligado al anterior. Gracias a Blockchain no sólo se pueden trazar y registrar las donaciones sino que también se pueden monitorizar. Tal y como se explica en el apartado 1.6., se pueden añadir restricciones al sistema para que éste únicamente autorice determinadas transacciones si se cumplen unos requerimientos previamente acordados. Son diversos los ejemplos vistos a lo largo de esta memoria donde se aplica esta función de Blockchain: el de la plataforma ComGo (punto 2.1.1.), The Responsible Cobalt Initiative (punto 2.1.2.), el ejemplo ya implantado con el caso de Esther (punto 2.1.3.) y el proyecto llevado a cabo por AID: Tech en el Líbano (Anexo 3.2.). En todos estos casos, se exige al sistema algún tipo de documento que acredite que los fondos se están destinando a una actividad benéfica específica.

En el caso de Intermón, habiendo analizado los documentos relativos a las cuentas de la organización y su sistema de donaciones, se hace evidente que la ONG presenta grandes similitudes con AFANOC en cuanto al sistema de registro de donaciones. Con el fin de no repetir el análisis ya hecho en la implementación de Blockchain a AFANOC, en el párrafo siguiente, se expone una de las principales diferencias entre ambas entidades.

Se trata de un factor que ya se ha introducido en otros apartados: la carencia de una legislación fiable en los países donde Intermón coopera. En el caso de AFANOC, al tratarse de una asociación pequeña que opera a escala local, sus proyectos se llevan a cabo dentro del marco legal español y, por tanto, existe menos riesgo de que certificados, facturas o documentos oficiales sean manipulados o falsificados. Sin embargo, en el caso de Oxfam Intermón, la situación es un tanto más compleja. Tal y como se explicaba en el primer punto de este capítulo, Intermón coopera en más de

90 países, muchos de los cuales no tienen un marco legislativo del todo consolidado. El hecho de que determinadas acreditaciones no siempre den una garantía absoluta, puede abrir una brecha de inquietud en los donantes y, tanto la veracidad del proceso como la eficacia de la misma tecnología, pueden salir perjudicadas. Por este motivo, es conveniente estudiar detalladamente la legislación de estos países, así como la veracidad de las garantías que se envían y registran en el *ledger* de Blockchain.

Finalmente, recordemos que en el análisis de cómo automatizar AFANOC mediante Blockchain, se expuso un caso hipotético donde se ponía en práctica la monitorización del sistema de cadena de bloques para verificar el pago a la empresa de limpieza de la Casa dels Xuklis. Durante la entrevista realizada a Oxfam Intermón, tuvimos la oportunidad de comentar un caso práctico real en el que la aplicación de la tecnología de bloques podría resultar bastante útil.

El caso surgió a raíz de comentar uno de los proyectos en los que, el responsable de finanzas de Oxfam Intermón, Iván Solà, se encuentra involucrado actualmente. El proyecto en cuestión se lleva a cabo en Guatemala y tiene como objetivo principal disminuir la hambruna en determinadas zonas de este territorio. Para ello, los miembros de Oxfam Intermón se ponen en contacto con diversas familias locales. Posteriormente, pesan a los niños y, si su peso no se corresponde con unos estándares previamente establecidos que indican que el niño esta sano, la familia en cuestión pasa a ser miembro del programa. A todos estos participantes se les entregan semillas de manera periódica para asegurar que disponen de una cantidad de alimentos mínima que cubra sus necesidades básicas de alimentación. Además, tal y como se ha explicado en el punto 3.2.1., uno de los principales objetivos de Intermón es conseguir que las organizaciones locales y la gente de los países donde cooperan, puedan desarrollar de manera autónoma el máximo de actividades posibles, es decir, que puedan ser autosuficientes. Por este motivo, Intermón no entrega directamente la comida a las familias, sino que busca darles autosuficiencia mediante un programa que les suministra semillas, les enseña a plantar y a cultivar y les hace un seguimiento para verificar el cumplimiento y la evolución del programa.

Este proyecto es un buen ejemplo donde se podría implementar Blockchain. Siguiendo una metodología similar a la usada por AID: Tech en el Líbano (Anexo 3.2.), Oxfam podría llegar a acuerdos con los vendedores de semillas locales para que las familias pudiesen canjear "bonos inteligentes" por bolsas de semillas. Este proceso resulta doblemente beneficioso puesto que, por un lado permite controlar totalmente que el dinero recaudado por Oxfam Intermón se está usando para comprar estas semillas y, por otro lado, da autonomía a las familias de este programa para que no tengan que depender de la organización para abastecerse. Un esquema de este proceso se representa en la figura 3.7.

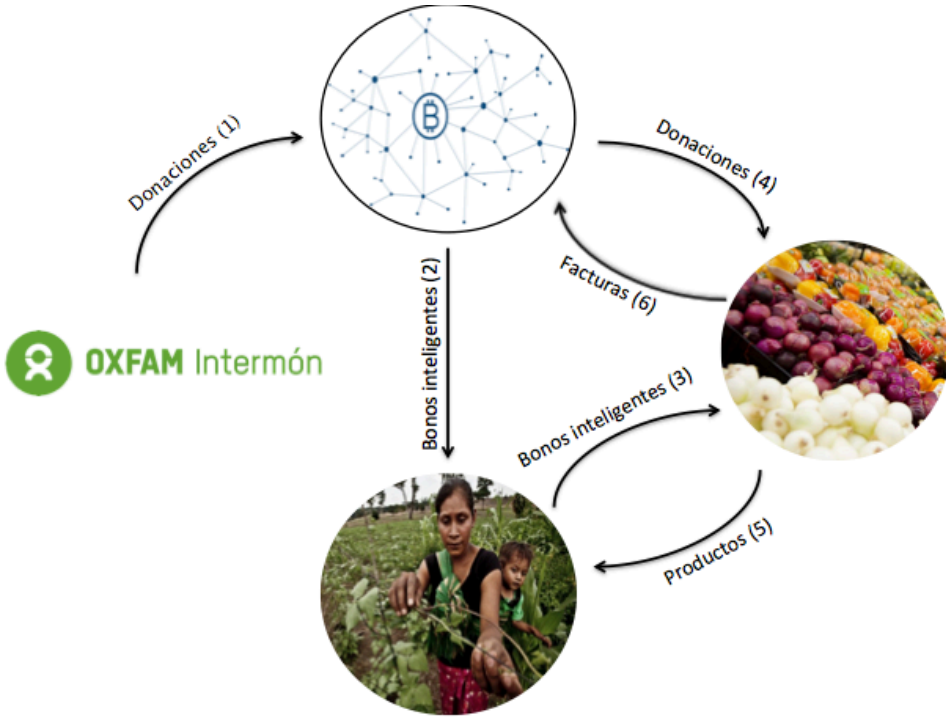

Figura 3.7 Esquema donde se muestra el sistema de donación de semillas mediante Blockchain

Asimismo, aprovechando que Intermón ya tiene integrado como parte del proceso un seguimiento de las familias que se asegura de que estén cultivando bien; se pueden recoger "pruebas físicas" de este seguimiento para subirlas a Blockchain y mantener un registro. Por ejemplo, siguiendo la línea de The Responsible Cobalt Initiative (punto 2.1.2.), se podrían subir fotografías a la red donde se viese el proceso y la continuidad del cultivo de estas familias. Un siguiente paso, más allá de hacer un seguimiento y llevar este registro, sería monitorizar el sistema de bloques para que sólo se

autorizasen las transferencias a esta causa benéfica una vez se registrasen fotografías (con fecha) donde se viese la evolución del cultivo.

Por tanto, Blockchain se presenta como una herramienta que permite al donante no sólo poder seguir el rastro de su donación sino también poder ver la evolución del proyecto al que está ayudando. Este hecho resulta muy significativo puesto que puede actuar como incentivo para fidelizar a los donantes que participan en estos proyectos, al sentirse éstos más involucrados en la causa.

3.2.4. Ausencia de un intermediario que gestione las transacciones

De manera análoga al sistema seguido por AFANOC, Oxfam Intermón distribuye sus fondos en diferentes entidades bancarias, a partir de las cuales, realiza y recibe todas las transacciones necesarias. Hay que tener en cuenta que Intermón es una organización que opera a escala mundial y, por tanto, no sólo trabaja con bancos españoles sino también con bancos de todos los países donde tiene oficinas. Algunos de los principales bancos con los que trabaja aquí en España son CaixaBank, Banc Sabadell, Triodos Bank y Fiare Banca Ética.

Las ventajas de utilizar la tecnología de bloques para eliminar los bancos como principal intermediario son muy parecidas a las vistas en el punto 3.1.5. aplicado a AFANOC. Algunos aspectos sobre el sistema de donaciones de Oxfam que difieren sobre el caso explicado en ese apartado son los que siguen:

Una primera característica a tener en cuenta es que una de las maneras que Oxfam Intermón tiene de recaudar fondos, son las grandes campañas mediáticas lanzadas para ayudar en emergencias humanitarias. Este tipo de eventos son puntuales y requieren de una gran cantidad de dinero en un lapso de tiempo muy breve. Para este tipo de ocasiones, existe un acuerdo generalizado con los bancos según el cuál no cobran ningún tipo de comisión por realizar transferencias orientadas a subvencionar la ayuda en la emergencia en cuestión. De hecho, se abre una cuenta específicamente

para dicha emergencia y todo el dinero recaudado en esa cuenta se destina directamente a actividades relacionadas con esta crisis humanitaria.

En cuanto al resto de recaudaciones benéficas, es preciso negociar con los bancos para conseguir las mínimas comisiones. Como se veía en el caso de AFANOC, si las transferencias se realizan entre cuentas bancarias de diferentes bancos, normalmente se cobraran comisiones que suelen ir a cargo del donante. Por tanto, menos en el caso de cuando se trata de donaciones directas a emergencias humanitarias, Oxfam Intermón depende del banco como intermediario y esto, conlleva un coste añadido.

Otro aspecto que Intermón tiene diferente de AFANOC es el que implica a las operadoras telefónicas como nuevo intermediario. A diferencia de la asociación, donde todas las donaciones se hacen directamente a cuenta bancaria o en efectivo; en Intermón, también se realizan grandes campañas de sensibilización vía SMS. En este caso, tener a una operadora telefónica como intermediario supone no sólo un coste económico sino también un coste temporal. Estas operadoras van acumulando dinero de todos los SMS que los donantes envían y, normalmente al cabo de un mes, mandan todo lo que hayan recaudado hasta el momento a Intermón. Por tanto, con este método, la donación ya no es inmediata (o casi inmediata) sino que presenta una brecha temporal considerable. Así pues, en este caso, la tecnología de bloques puede resultar muy ventajosa. Tal y como se detalla al final del punto 1.3., Blockchain tramita las transacciones de manera casi inmediata. Más concretamente, el sistema requiere de entre 6 y 11 minutos para verificar cada transferencia; tiempo mucho menor al que tarda Intermón en recibir las donaciones hechas por SMS.

Hasta ahora se ha visto cómo afecta la implicación de intermediarios en la parte del proceso donde Intermón recibe las donaciones. A continuación, se estudiará la presencia de intermediarios en la parte del proceso que engloba hacer llegar las donaciones a las personas necesitadas. Al colaborar en muchos países subdesarrollados, Oxfam Intermón se encuentra con la situación de que, en ocasiones, tiene que hacer llegar dinero a personas que no disponen de una cuenta bancaria. Y es en este punto donde Blockchain presenta una parte importante de su potencial. Según

el Grupo Banco Mundial[vi], a finales de 2016, había alrededor de 2500 millones de personas en el mundo que no utilizaban servicios financieros formales y el 75% de los pobres no tenían una cuenta bancaria. Por el contrario, según un informe realizado por este misma entidad, en el 2016, entre el 20% más pobre de los hogares, casi 7 de cada 10 tenían teléfono móvil. Así pues, se hace evidente que, en los países en vías de desarrollo, la tecnología móvil es mucho más accesible que las cuentas bancarias. Por este motivo, Blockchain es un instrumento con un alcance mayor que ofrece a todas estas personas la posibilidad de poder acumular y transferir dinero virtual sin necesidad de acudir a un banco.

Durante la entrevista se comentaron cuatro vías distintas que Intermón utiliza para poder hacer llegar dinero a la gente que no dispone de una cuenta bancaria. La primera, vía teléfono móvil. A partir de estos dispositivos y trabajando conjuntamente con la operadora telefónica, Intermón consigue hacer llegar a los más necesitados el dinero recaudado por las donaciones. Sin embargo, tal y como se ha visto anteriormente, esta vía supone un coste monetario y temporal. Una segunda opción es hacer llegar el dinero mediante cheque bancario. En este caso se llega a un acuerdo con el banco que permite al receptor de la donación adquirir el dinero a través de un cheque bancario aunque éste no disponga de una cuenta. No obstante, esta opción también supone un coste adicional y la implicación del banco como intermediario. En tercer lugar, existe la posibilidad de contratar una empresa externa que se encargue de hacer llegar este dinero a su beneficiario. Nuevamente, este opción supone un coste añadido en el proceso. Finalmente, una alternativa que sólo se ha usado en casos extremos es la de entregar el dinero directamente en efectivo.

En cualquier caso, tal y como apuntaba el Sr. Solà en la entrevista, este proceso siempre ha sido complejo y ha acarreado costes añadidos. Por este motivo, la tecnología de bloques se presenta como una solución mucho más optima que, pudiendo llegar a un número de personas mucho más amplio, conseguiría disminuir los costes temporales y monetarios del proceso. La viabilidad de un sistema libre de intermediarios se detalla en el punto 1.4.2. y, de manera más técnica, se evidencia en el punto 1.4.4. de esta memoria.

En resumen, dado que Intermón es una organización con una estructura mucho más grande que AFANOC, el número de intermediarios con los que trabaja es mayor. En este apartado tan sólo se han visto algunos de sus intermediarios principales, pero está claro que a lo largo de toda la cadena de suministro de ayuda participan muchos más. Por este motivo, aplicar Blockchain en los diferentes procesos puede suponer una gran ventaja y permitiría no sólo aumentar la trazabilidad y registro de las diferentes actividades sino también reducir costes.

3.2.5. Otros aspectos

En el caso de AFANOC se han estudiado otras características fundamentales de Blockchain, tales como el anonimato de las transacciones, las microdonaciones o el hackeo del sistema. El desarrollo de estos puntos para Intermón es muy similar al de la asociación, o al menos, lo que se ha podido analizar. Es decir, mientras los apartados de trazabilidad, automatización y ausencia de intermediario se han podido estudiar en profundidad para cada entidad, el estudio del resto de características de Blockchain ha resultado ser un poco menos accesible. Un análisis que llevase a resultados concluyentes sobre si la base de datos de Intermón puede ser hackeada, requiere de un estudio de la organización mucho más profundo del que se ha podido hacer para este trabajo. Lo mismo ocurre con aspectos específicos de la financiación de estas entidades. Por este motivo, se ha dejado la investigación exhaustiva acerca de estos ámbitos para un próximo trabajo.

4. Presupuesto

Con el propósito de dar una magnitud económica al coste de la implementación de un proyecto como el que se ha comentado hasta el momento, se ha hecho un estudio simplificado del coste monetario que puede suponer la aplicación de Blockchain al programa de la Casa dels Xuklis impulsado por AFANOC.

Para ello, en primer lugar se han definido de manera detallada las diferentes fases y actividades en las que estaría divido el proyecto, así como la estimación de su tiempo de implementación. Estos datos se muestran en la tabla siguiente:

ETAPA	Actividad	Planificación
Introducción al proyecto	Definición de los objetivos del proyecto	2 semanas
	Presentación de conceptos básicos de Blockchain a AFANOC	
Proceso de documentación y estudio de AFANOC	Análisis del sistema de donaciones y financiación	1 mes
	Estudio del sistema de base de datos	
	Estudio de cada actividad benéfica a la que se destinan recursos	
	Análisis de gastos en otras actividades	
Diseño del sistema aplicado a AFANOC	Diseño conceptual del sistema de trazado de donaciones	2 meses
	Diseño conceptual de la automatización de Blockchain en las actividades determinadas en la etapa dos	
	Diseño conceptual de un sistema de garantías o documentos que acrediten el uso específico de las donaciones	
	Presentación del diseño a AFANOC	
Desarrollo del prototipo	Programación del programa principal de Blockchain para trazar y registrar donaciones	4 meses
	Programación de Blockchain para monitorizar los transacciones de las actividades estudiadas en la segunda etapa	

	Programación de Blockchain para que solicite las garantías establecidas en la etapa tres que, tras ser verificadas, autorizarán las transacciones	
Implementación de Blockchain a AFANOC	Implementación de prueba del prototipo a una actividad concreta de las estudiadas en la etapa dos a partir de una primera donación "génesis"	4 meses
	Incorporación de mejoras al prototipo y corrección de errores que aún no se hubiesen detectado	
	Implementación definitiva de Blockchain a las diferentes actividades y procesos de AFANOC	
	Implementación de un acceso directo a Blockchain desde la página web de AFANOC	
Seguimiento del proyecto implementado en AFANOC	Mantenimiento del sistema	-
	Actualización del sistema con la incorporación de nuevas actividades que vayan surgiendo	
Expansión del proyecto	Marketing	-
	Página web	
	Implementación de Blockchain a más entidades del tercer sector	

Las diferentes fases que se muestran en la tabla no son totalmente independientes. De hecho, es posible que actividades de diferentes fases puedan desarrollarse simultáneamente. Asimismo, el tiempo de trabajo destinado por los responsables del proyecto a cada fase es variable. Por ejemplo, en la fase de implementación de Blockchain, los participantes en el proyecto tendrán que ir viendo cómo responde AFANOC a las diferentes incorporaciones tecnológicas que se irán introduciendo en su funcionamiento. En otras palabras, el cambio de un sistema a otro es progresivo y, por tanto, habrá que adaptarse a este tiempo de migración. Así pues, aunque se plantea la implementación del proyecto con el margen de un año, los plazos pueden variar.

Adicionalmente, se ha tenido en cuenta que es necesario un mínimo de tres personas responsables para implementar el proyecto: un programador, un ingeniero y un analista. Sin embargo, hay que tener en cuenta que también se requerirá de la cooperación del personal de AFANOC. De hecho, como mínimo, será necesaria la

colaboración de: un miembro del departamento financiero, una persona con un buen conocimiento de los actuales sistemas informáticos de la entidad y alguien que conozca bien los diferentes proyectos en los que actualmente están involucrados.

Pese a que la cantidad de recursos destinados y las horas trabajadas en cada fase no son constantes, tal y como ya se explicado; se ha estimado un promedio de trabajo de 12 horas semanales. Por tanto, considerando que el precio de mercado de un ingeniero está valorado sobre los 60 euros/h, el gasto total en salarios al final del año sería de 34.560 euros. Por otro lado, se considera que AFANOC habilitaría espacios y recursos para que los trabajadores pudiesen implementar Blockchain a su entidad. De esta manera, no sólo se permitiría a los trabajadores trabajar cerca del entorno en el que tienen que implementar la tecnología de bloques, sino que también haría posible un abaratamiento de costes.

Ya para cerrar este último capítulo, cabe añadir que este esbozo de presupuesto sería extrapolable a Oxfam Intermón o a otras entidades del tercer sector donde se quiera aplicar la cadena de bloques. Sin embargo, el presupuesto de organizaciones tan grandes como es Oxfam, requeriría de un estudio previo de las diferentes actividades y proyectos en los que éstos están involucrados, así como de la magnitud y complejidad de su sistema de financiación y base de datos.

Conclusiones

A lo largo de este trabajo se ha hecho evidente el indudable potencial de la tecnología de bloques, así como sus limitaciones. En el primer capítulo se han podido estudiar las diferentes herramientas, como la *proof-of-work* o los algoritmos *hash,* que hacen de Blockchain una tecnología robusta, segura y transparente. En el segundo capítulo, se ha podido analizar la factibilidad del sistema de bloques en proyectos cuya implementación ya está dando sus frutos, como es el caso de Esther donde la monitorización de Blockchain asegura al donante que se está haciendo un buen uso de su dinero. Finalmente, se ha hecho un análisis de la implementación conceptual de la tecnología de bloques en las entidades AFANOC y Oxfam Intermón que pretende responder directamente al objetivo principal de este proyecto. De este análisis se ha deducido lo siguiente:

En primer lugar, gracias al estudio comparativo llevado a cabo entre ambas organizaciones, se deduce que la aplicación de Blockchain puede tener un impacto mayor en una entidad multinacional que en una organización local. Por aspectos tales como la problemática de hacer llegar dinero a personas que no disponen de una cuenta bancaria, o la gran versatilidad de proyectos en los que éstas están involucradas. Desde un punto de vista opuesto, también se ha podido constatar que la participación de ONGs en países del tercer mundo, supone una dificultad añadida al proceso de obtención de garantías fiables que acrediten dónde se está haciendo llegar el dinero. Por tanto, si bien es cierto que Blockchain presenta ventajas muy significativas en organizaciones que operan en ámbitos internacionales, la implementación de esta tecnología en estos casos es mucho más compleja.

A lo largo del trabajo, los aspectos de Blockchain que más se han podido analizar han sido las mejoras aportadas a AFANOC y Oxfam Intermón en cuanto a la trazabilidad, registro y automatización de las transacciones. El análisis realizado sobre el método de financiación actual en ambas entidades, hace evidente que Oxfam y AFANOC no utilizan un sistema que ponga al alcance del donante datos, suficientemente precisos,

sobre la traza de sus donaciones. En este sentido, Blockchain, con su base de datos pública y cuyas transacciones se actualizan de manera casi inmediata, permite al donante realizar un seguimiento completo de sus donaciones, al mismo tiempo que otorga mayor transparencia a las entidades que lo implementan. Dando respuesta al objetivo principal de este trabajo, esta tecnología no sólo puede conseguir aumentar la confianza del donante en el tercer sector, sino también incrementar su implicación en las causas benéficas a las que aporta dinero.

Además, se ha podido concluir que, aunque la implementación de Blockchain conlleve una inversión inicial importante; gracias a la ausencia de intermediarios en la cadena de suministro, esta tecnología permitiría una reducción relevante de los costes temporales y monetarios. Sin embargo, este dato responde a una cuantificación subjetiva, en tanto que no se ha podido realizar un estudio administrativo y contable de las organizaciones en profundidad.

Así pues, pese a las importantes mejoras que la cadena de bloques aporta a las entidades del tercer sector en aspectos tales como la trazabilidad de las donaciones o la eliminación de intermediarios; conviene estudiar bien todos los ámbitos de actuación de este tecnología para poder llegar a una conclusión global suficientemente válida. Por este motivo, para un futuro trabajo, se plantea estudiar más detalladamente la financiación de AFANOC y de Oxfam Intermón, así como sus sistemas de bases de datos. Y, de esta manera, poder analizar más específicamente la viabilidad de la tecnología de bloques en estos campos.

Finalmente, añadir que un obstáculo que surgió durante la confección de este trabajo fue el hecho de que, para poder estudiar bien la implementación de esta tecnología a entidades del tercer sector, es necesario estudiar datos y casos específicos de su funcionamiento. Sin embargo, en algunos casos, en las entrevistas realizadas a las ONGs se describían procesos muy generales, obviando detalles que podían ser muy significativos.

Bibliografía

Referencias bibliográficas

[i] Andrew Hodges. *Alan Turing: The enigma*.

[ii] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [en línea]. Disponible en: < https://bitcoin.org/bitcoin.pdf >

[iii] Asociación Española de Fundraising (AEFr). Perfil del donante 2016 [en línea]. 1 Julio 2017 [Consulta: Mayo 2018]. Disponible en: < https://www.aefundraising.org/wp-content/uploads/2017/09/Perfil_donante-2016-_-resumen-ejecutivo.pdf >

[iv] Plataforma ComGo. Disponible en: < https://www.comgo.io/ >

[v] Angeline Mbogo. Pilot Scheme to Apply Blockchain Tecnology to DRC's Cobalt Industry[en línea]. 4 Febrero 2018 [Consulta: Mayo 2018] Disponible en: < http://bitcoinafrica.io/2018/02/04/apply-blockchain-technology-cobalt-industry-dr-congo/ >

[vi] Banco Mundial. Inclusión financiera [en línea]. 19 Noviembre 2016 [Consulta: Junio 2018]. Disponible en: < http://www.bancomundial.org/es/topic/financialinclusion/overview >

Bibliografía complementaria

Aida Roselló. Study of the implementation of Blockchain technology in Supply Chain Management. Febrero 2017. Trabajo de fin de máster de la universidad Taiwan Tech.

Augustín Isasa Cuartero. Blockchain y su Aplicabilidad a una Industria bajo Regulación. Junio 2017. Trabajo de fin de máster de la Universitat Oberta de Catalunya.

Christopher Cannucciari. Banking on Bitcoin [documental]. Estados Unidos, 2016. Videodisco (DVD).

José Basa. Cómo invertir en criptodivisas. El Bitcoin y su funcionamiento [Conferencia]. Forex4group.

Emily McLaughlin. Cómo funciona Blockchain: Una explicación infográfica [en línea]. Abril 2017. [Consulta: Marzo 2018]. Disponible a: <http://searchdatacenter.techtarget.com/es/cronica/Como-funciona-blockchain-Una-explicacion-infografica>.

Manuel Moreno. Tecnología blockchain (I): sistema criptográfico [en línea]. 28/09/2017 [Consulta: Abril 2018] Disponible a: < http://blognewdeal.com/manuel-moreno/tecnologia-blockchain-i-sistema-criptografico/ >.
Robert Hazlitt. Bitcoin le dio nueva vida a la revolución cyberpunk [en línea]. 15 Abril 2016. [Consulta: Marzo 2018] Disponible a: <https://www.diariobitcoin.com/index.php/2016/04/15/bitcoin-le-dio-nueva-vida-a-la-revolucion-cyberpunk/ >
Javier Pastor. Qué es blockchain: la explicación definitiva para la tecnología más de moda [en línea]. Creado: 17 Noviembre 2017. Actualizado: 10 Junio 2018. [Consulta: Junio 2018] Disponible a: < https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda >

Alex Preukschat. Criptografía asimétrica: Sistemas de Cifra con Clave Pública – Conceptos Bitcoin (II) [en línea]. 10 Enero 2014 [Consulta: Abril 2018] Disponible a: < https://www.oroyfinanzas.com/2014/01/criptografia-asimetrica-sistemas-cifra-clave-publica-bitcoin/ >

Problema del doble gasto en Bitcoin. ¿Qué es doublé spending en tecnología descentralizada? [en línea]. 27 Noviembre 2014 [Consulta: Abril 2018]. Disponible en: < https://www.oroyfinanzas.com/2014/11/que-es-problema-double-spending-doble-gasto-p2p-bitcoin/ >

Problema de los generales bizantinos [en línea]. 4 mayo 2018 [Consulta: Marzo 2018] Disponible en: < https://es.wikipedia.org/wiki/Problema_de_los_generales_bizantinos >

Alex Preukschat. ¿Qué es, qué significa y para qué sirve un Hash en Bitcoin? (IV) [En línea]. 13 Enero 2014 [Consulta: Marzo 2018] Disponible en: < https://www.oroyfinanzas.com/2014/01/hash-bitcoin-que-es-significa-sirve/ >

David Dinkins. Bitcoin es descentralizado pero no distribuido, y ese hecho probablemente contribuyó a la guerra civil de Bitcoin [en línea]. 8 Agosto 2017 [Consulta: Marzo 2018]. Disponible en: < https://es.cointelegraph.com/news/bitcoin-is-decentralized-but-not-distributed-and-that-fact-likely-contributed-to-bitcoins-civil-war >

Europa Press. La ONG 'it.willbe.org' utiliza la tecnología de IBM Blockchain para aumentar la confianza de los donantes [en línea]. 13 Marzo 2018 [Consulta: Abril 2018] Disponible en: < http://www.europapress.es/epsocial/cooperacion-desarrollo/noticia-

ong-itwillbeorg-utiliza-tecnologia-ibm-blockchain-aumentar-confianza-donantes-20180313183707.html >

Mar Calvo. Blockchain, al rescate de las ONG [en línea]. 22 Febrero 2018 [Consulta: Abril 2018] Disponible en: < http://www.blockchainservices.es/asociaciones-y-consorcios/el-blockchain-al-rescate-de-las-ong/ >

Josu Sangroniz Gómez. Criptografía de clave pública: el sistema RSA [en línea]. Noviembre 2004 [Consulta: Mayo 2018] Disponible en: < http://www.osakidetza.euskadi.eus/r85-cknoti03/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_25/15_criptografia.pdf >

Adrián Peláez Paniagua. Criptografía asimétrica o de clave pública – Certificados, Rsa, etc [en línea]. 1 Diciembre 2015 [Consulta: Abril 2018]. Disponible en: <https://www.adictosaltrabajo.com/tutoriales/criptografia-asimetrica-o-de-clave-publica-certificados-rsa-etc/ >

Jackeline Rivero. Altruismo y tecnología: 12 ONG que aceptan Bitcoin [en línea]. 30 Octubre 2016 [Consulta: Mayo 2018]. Disponible en: < https://www.criptonoticias.com/colecciones/altruismo-tecnologia-ong-bitcoin-donaciones/ >

Javier Campos. El Algoritmo Diffie-Hellman [en línea]. 22 Julio 2011 [Consulta: Marzo 2018]. Disponible en: < https://javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/ >

Angeline Mbogo. BitGive launches new charitable project and announces research partnership [en línea]. 2 June 2018 [Consulta: Abril 2018]. Disponible en: < http://bitcoinafrica.io/2018/06/02/bitgive-launches-new-charitable-project-and-announces-research-partnership/ >

Pablo G. Bejerano. Una ONG usa blockchain para evitar que los rohigya queden indocumentados [en línea]. 7 Febrero 2018 [Consulta: Abril 2018]. Disponible en: < http://www.lasexta.com/tecnologia-tecnoxplora/internet/ong-usa-blockchain-evitar-que-rohingya-queden-indocumentados_201712225a4dfbf80cf2948ad89f5f76.html >

PharmAccess. PharmAccess Partners With Aid:Tech to Transform Antenatal Care in Tanzania Through Blockchain Technology [en línea]. 4 Junio 2018 [Consulta: Junio 2018]. Disponible en: < https://www.pharmaccess.org/update/pharmaccess-partners-aidtech-transform-antenatal-care-tanzania-blockchain-technology/ >

Cristina Sánchez. Robando carteras digitales: dos “hackers” españoles desmontan la seguridad de Bitcoin [en línea]. 5 Mayo 2015 [Consulta: Junio 2018]. Disponible en: < https://www.eldiario.es/hojaderouter/seguridad/seguridad-carteras-bitcoin-hackers-criptomonedas_0_363264145.html >