

Aplicaciones de la *Blockchain* más allá del Bitcoin

La tecnología *Blockchain*



Ajuntament de
Barcelona



Barcelona
Activa

Índice

1 INTRODUCCIÓN A LA TECNOLOGÍA <i>BLOCKCHAIN</i>	3
1.1 QUÉ ES LA CADENA DE BLOQUES	3
1.1.1 DESCENTRALIZADO	3
1.1.2 INMUTABLE	4
1.1.3 SEGURO	4
2 FUNCIONAMIENTO DE LA TECNOLOGÍA <i>BLOCKCHAIN</i>	5
2.1 ¿CÓMO FUNCIONA UNA <i>BLOCKCHAIN</i> ?	5
2.2 BENEFICIOS DE LA <i>BLOCKCHAIN</i>	5
2.3 TIPOS DE <i>BLOCKCHAIN</i>	6
3 CASOS DE USO DE LA <i>BLOCKCHAIN</i>	7
3.1 APLICACIÓN DE LA <i>BLOCKCHAIN</i> EN SECTORES	7
3.1.1 SECTOR FINANCIERO	7
3.1.2 TERCER SECTOR	7
3.1.3 LOGÍSTICA	8

1 INTRODUCCIÓN A LA TECNOLOGÍA *BLOCKCHAIN*

1.1 QUÉ ES LA CADENA DE BLOQUES

Para hablar de lo que es la cadena de bloques (*blockchain*) y entender cómo es de disruptiva esta tecnología, es bueno empezar haciendo un repaso del pasado y de la evolución de las tecnologías y los servicios en Internet.

En los primeros días de Internet, los servicios eran:

- Por un lado, centralizados tanto física como jerárquicamente, es decir, tanto en relación con la distribución física como en relación con el poder que tenían las personas usuarias.
- Por otro lado, eran caros de mantener, pues estaban al alcance de muy pocas compañías que pudieran darles soporte técnico y venderlos.
- También eran poco escalables, ya que no permitían democratizar estos servicios y estaban en manos de muy pocos.

Y, en definitiva, solo los usaban las grandes corporaciones, como por ejemplo IBM.

Hoy en día, con la nube, los servicios se vuelven:

- Descentralizados físicamente.
- Centralizados jerárquicamente. Seguimos dependiendo de servicios que ofrecen compañías que tienen todo el poder de decisión y de mantenimiento.
- Baratos de mantener. Hoy en día cualquier persona puede contratar un servidor y levantar una página web con un coste prácticamente nulo.
- Muy escalables. Y es que podemos combinar muchos servicios de bajo coste para hacer nuevas aplicaciones. Además, están en manos de miles de personas.

Y ya no solo están en manos de grandes corporaciones, sino que los usan las empresas y muchos usuarios y usuarias finales.

Con la cadena de bloques, podemos concebir un Internet:

- Descentralizado (tanto físicamente como jerárquicamente).
- Inmutable.
- Y seguro (tanto por lo que respecta a la infraestructura como al software).

1.1.1 DESCENTRALIZADO

Explicado con más detalle, decimos que un servicio está descentralizado físicamente cuando todos los actores están distribuidos geográficamente y jerárquicamente y cuando todos los actores tienen poder de acción y decisión sobre la red.

1.1.2 INMUTABLE

Por otro lado, hablamos de inmutabilidad. Cuando hacemos una inserción de datos en una cadena de bloques, estos datos no podrán ser modificados. Un cambio de datos anteriores invalida todos los siguientes. Esto nos permite obtener un registro en el que toda la información queda guardada para siempre y nunca se podrá trampear.

1.1.3 SEGURO

Por último, nos referimos a dos niveles de seguridad. En cuanto a la infraestructura, al ser descentralizada, mientras quede un nodo activo la red seguirá funcionando. Por otro lado, definimos la seguridad en relación con el *software*, pues la criptografía impide la falsificación de datos.

Siguiendo esta visión, en 2008 nace **bitcoin** como la primera aplicación de esta tecnología. Bitcoin sale como un papel de investigación y es la primera versión de igual a igual de un sistema de pagos distribuido. El 4 de enero de 2009 se sella el Genesis Block de bitcoin, que es como se llama el primer bloque de una cadena que contiene mucha información relevante sobre cada cadena de bloques, y se inicia la red bitcoin como la primera cadena de bloques de la historia.

Con esta información previa, somos capaces de definir qué es una cadena de bloques.

No existe ninguna definición estándar sobre qué es esta tecnología, pero la podemos entender como un registro inmutable y distribuido de datos que, a su vez, es integrable y programable.

En un terreno informal y como primera definición que nos puede ayudar a entender realmente qué es una cadena de bloques, imaginemos un archivo Excel que tenemos compartido en Google Drive. Las columnas serían los bloques y las filas serían datos que irían almacenados en cada bloque. Cuando dos personas actualizamos a la vez este archivo, que actúa como registro, vemos que los datos se van modificando. Una cadena de bloques sería lo mismo, pero en lugar de ser de Google, el mantenimiento haría la red. Es decir, habría un modo en el que ambos nos pondríamos de acuerdo para escribir en el mismo registro sin que haya confrontaciones. Esto se conoce como consenso. Y en la cadena de bloques se consigue mediante un algoritmo informático que ejecutan todos los ordenadores que participan en la red.

2 FUNCIONAMIENTO DE LA TECNOLOGÍA *BLOCKCHAIN*

2.1 ¿CÓMO FUNCIONA UNA *BLOCKCHAIN*?

Una vez que hemos entendido qué es la cadena de bloques y la capacidad de disrupción que puede tener para los servicios actuales, podemos entender cómo funciona y, por tanto, cuando es una buena opción usar esta tecnología. También es importante distinguir los tipos de cadena de bloques, ya que cada arquitectura se adecua a distintos casos de uso.

El primer paso para entender cómo funciona una cadena de bloques pasa por una transacción. Cuando un individuo de la red se dispone a realizar una operación candidata a ser escrita en el registro, se inicia una transacción. Esta escritura puede ser de cualquier clase, es decir, puede ser tanto una transacción de una criptomoneda como del registro de la propiedad de una vivienda. Esta transacción se lanza a la red P2P a la espera de ser validada e incluida en el registro.

El segundo paso consiste en la generación de un bloque. Cada cadena de bloques tiene un tiempo de bloque, que es el tiempo aproximado que tarda una cadena de bloques en generar un nuevo bloque, que se modifica según varios parámetros. Para generar un bloque, otro individuo de la red realiza cálculos muy complejos hasta que es capaz de generarlo y confirmar las transacciones. Este individuo incluye la transacción del individuo anterior en este nuevo bloque y recibe la recompensa de bloque, además de las comisiones de las transacciones que están incluidas.

A continuación, los demás individuos de la red validan tanto las transacciones del nuevo bloque como las de su generación y fijan, así, las transacciones incluidas como las recompensas por el minero que ha generado el bloque.

Por último, hay que entender el concepto de concatenación de bloques. Cada vez que se genera un nuevo bloque, se genera incluyendo la firma digital del bloque anterior, de modo que podemos concatenar un bloque con el anterior mediante un identificador único y formando un registro inmutable de la historia de la red. Si cambiáramos un bit de uno de los bloques, cambiaría el identificador del mismo bloque y, por tanto, el siguiente ya no encajaría con el anterior y se invalidarían todos los bloques sucesores.

2.2 BENEFICIOS DE LA *BLOCKCHAIN*

Gracias a estas características y estructura de datos, la cadena de bloques presenta una serie de beneficios muy interesantes para muchos negocios:

En primer lugar, podemos conseguir una optimización de procesos, pues la confianza entre dos partes que garantiza este registro nos permite ahorrar costes y tiempo de intermediación en las transacciones.

En segundo lugar, tenemos una alta auditabilidad, porque, al mantener toda la historia de la red y mantenerla inmutable, la auditabilidad está garantizada por diseño.

También decimos que el *down time*, es decir, el tiempo en el que la red no está operativa, es prácticamente cero, ya que mientras quede un nodo activo la red seguirá funcionando.

Además, no necesitamos una copia de seguridad, *backup*. Al tener el mismo registro en todos los nodos de la red, no necesitamos que cada parte mantenga *backups* adicionales.

Finalmente, tenemos una alta seguridad contra el ataque. La cadena de bloques añade a las capas de seguridad actuales las ventajas de la criptografía más avanzada.

A pesar de estas ventajas que aporta la cadena de bloques, hay que asegurarse de necesitamos un registro de este tipo antes de seleccionarlo para un proyecto. Algunas de las preguntas que nos tenemos que hacer son las siguientes:

- ¿Necesito una base de datos?
- ¿Tiene que tener compartido el derecho de escritura?
- ¿Los escritores tienen confianza entre sí?

La cadena de bloques, por ejemplo, tiene mucha relevancia en entornos de máxima desconfianza en los que los actores se desconocen o tienen intereses diferentes. También en entornos en los que se requiere máxima transparencia entre distintas partes y siempre en procesos bastante claros y definidos, de modo que se puedan codificar fácilmente.

2.3 TIPOS DE *BLOCKCHAIN*

Una vez identificada esta necesidad, también debemos saber que hay varias arquitecturas de cadena de bloques. A grandes rasgos, podemos distinguir entre cadenas de bloques públicas y privadas:

Las cadenas de bloques públicas, como es el caso de bitcoin, tienen una arquitectura que permite a todos los actores participar, realizar y validar transacciones. Toda la información registrada es pública y se puede consultar.

En segundo lugar, tenemos las cadenas de bloques privadas, las cuales siguen siendo distribuidas e inmutables, pero no tienen por qué ser necesariamente transparentes ni descentralizadas. Estas cadenas de bloques son más útiles cuando la información es privada y se quieren gestionar los permisos y poderes que tienen los actores.

Así pues, podemos concluir que realmente en pocas ocasiones merece la pena utilizar esta tecnología, pero en los casos de uso que apunta realmente sí que ofrece una gran mejora

respecto de las tecnologías que existían y permite aportar un valor completamente diferenciado.

3 CASOS DE USO DE LA BLOCKCHAIN

Hablemos ahora sobre los casos de uso de la cadena de bloques en los distintos sectores.

3.1 APLICACIÓN DE LA *BLOCKCHAIN* EN SECTORES

3.1.1 SECTOR FINANCIERO

El primer sector que nos viene a la cabeza cuando hablamos de la cadena de bloques es de la banca y las finanzas.

Mediante las criptomonedas, que no son más que activos que se sostienen gracias a una cadena de bloques, aparecen casos de uso como los siguientes:

En primer lugar, un medio de pago. Las criptomonedas permiten realizar pagos sin personas intermediarias, es decir, permiten a dos personas que no se conocen y desconfían completamente entre ellas enviarse dinero sin pasar por ningún intermediario como podría ser un banco.

En segundo lugar, tenemos los micropagos. Como que los costes de mantenimiento quedan repartidos en la red, enviar dinero en una cadena de bloques tiene una comisión muy baja. Esto permite hacer micropagos en el ámbito internacional, lo cual hasta el momento era un proceso muy complicado por todos los intermediarios que se necesitaban.

Otro caso de uso de las criptomonedas es la representación de derechos. Se emplea para proporcionar liquidez y transacción a los derechos. Por ejemplo, podemos observar el caso de uso de una votación. Con el DNI, por ejemplo, podemos identificar a una persona en la cadena de bloques. Esta persona tiene la capacidad de votar y registrar su voto. Nadie podrá cambiar este voto, ya que es inmutable, y a la vez, transparente, de modo que podemos asegurarnos de que nuestro voto es válido. Además, podemos confiar en que cada persona solo ha podido votar una vez y que todos los votos tienen el mismo valor. Una votación es un caso muy sencillo, pero tiene todos los puntos para que se pueda aplicar una cadena de bloques. Es un proceso claro y definido, todas las partes desconfían las unas de las otras y se necesita transparencia. Con una cadena de bloques tendríamos unas votaciones seguras, automáticas y se podría votar desde cualquier lugar.

3.1.2 TERCER SECTOR

Otro sector que puede aprovechar esta tecnología es el tercer sector.

Primeramente, la tecnología de la cadena de bloques permite aportar una transparencia inigualable para las donaciones que los miembros de las ONG puedan hacer. También permite demostrar una gestión transparente de los fondos a todos los miembros y una auditabilidad infalible de cara a organismos reguladores. Por otro lado, permitiría las microdonaciones, así como una democracia líquida dentro de la organización.

3.1.3 LOGÍSTICA

Finalmente, otro sector en el que la cadena de bloques ha tomado mucha fuerza es el de la logística. La tecnología de cadena de bloques aporta transparencia, inmutabilidad, confianza entre las partes, velocidad en la detección de errores y consenso entre las partes implicadas. Esto implica una evolución disruptiva en este sector, ya que podemos resolver algunos de los problemas más críticos. Consultamos, por ejemplo, la trazabilidad de productos en la logística, un factor esencial en este sector. La cadena de bloques resuelve este problema en tres ámbitos. En primer lugar, todos los datos que registramos referentes a la trazabilidad de un producto permanecerán inmutables, de modo que todos los participantes de la red tienen la confianza de que la información se mantendrá intacta en el tiempo. Esto elimina la necesidad de la supervisión de un tercero o de auditorías de la información. En segundo lugar, aseguramos la integridad de las reglas contractuales. Si codificamos estas reglas dentro de la cadena de bloques, podemos garantizar que siempre estarán operativas y se respetarán sin la necesidad de auditorías. Finalmente, en el caso de tener que presentar pruebas del flujo de una transacción como la firma de un contrato, las pruebas pueden extraerse de forma casual en el orden que han sucedido.

Finalmente, podemos combinar varias aplicaciones para crear soluciones más complejas. Por ejemplo, Everledger combina las ventajas que aporta la cadena de bloques en la logística con la representación de activos reales en la red. Tomando las propiedades básicas de los diamantes, podemos identificarlos y representarlos en la cadena de bloques. Una vez insertados en la cadena de bloques, podemos registrar todas las modificaciones que sufre ese diamante desde que se extrae hasta que llega a la tienda, pasando por todos los distribuidores y transportistas. Así pues, finalmente, escaneando un simple código QR o consultando un número identificador, podemos trazar todo el recorrido de ese diamante en concreto hasta su origen y podemos comprobar de forma verídica que no estamos comprando un diamante de sangre.

De este modo, podemos ver que la tecnología de cadena de bloques está presente en muchos sectores, que cada vez estará en más y que revolucionará por completo el funcionamiento de estos, cambiará muchos modelos de negocio y creará modelos nuevos que hasta ahora no podíamos ni imaginar.

Descubre todo lo que Barcelona Activa puede hacer por ti.

Acompañamiento durante todo el proceso de búsqueda de empleo barcelona.cat/treball

Apoyo para poner en marcha tu idea de negocio barcelona.cat/emprenedoria

Servicios a las empresas e iniciativas socioempresariales barcelona.cat/empreses

Formación tecnológica y gratuita para la ciudadanía barcelona.cat/cibernarium

Barcelona Activa presente en los barrios

1. Sede Central Barcelona Activa Porta 22

Centro para la Iniciativa Emprendedora Glories

Incubadora Glories

2. Convent de Sant Agustí

3. Ca n'Andalet

4. Oficina de Atención a las Empresas Cibernarium

Incubadora MediaTIC

5. Incubadora Almogàvers

6. Parque Tecnológico

7. Nou Barris Activa (próxima apertura)

-Trabajo en los barrios

-Antenas Cibernarium

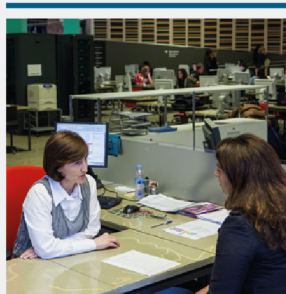
-Puntos Barcelona Treball

-Puntos de Orientación para la Búsqueda de Empleo

-Puntos de inserción sociolaboral A prop Jove

-Punto de Defensa de los Derechos Laborales

Descobreix tot el que Barcelona Activa pot fer per a tu



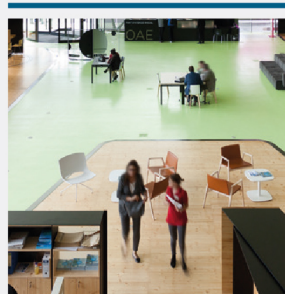
Acompanyament durant tot el procés de recerca de feina

barcelona.cat/treball



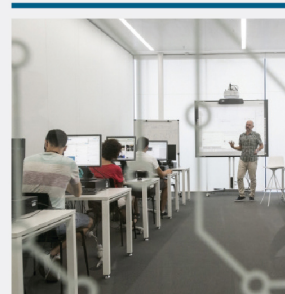
Suport per posar en marxa la teva idea de negoci

barcelona.cat/emprenedoria



Serveis a les empreses i iniciatives socioempresarials

barcelona.cat/empreses

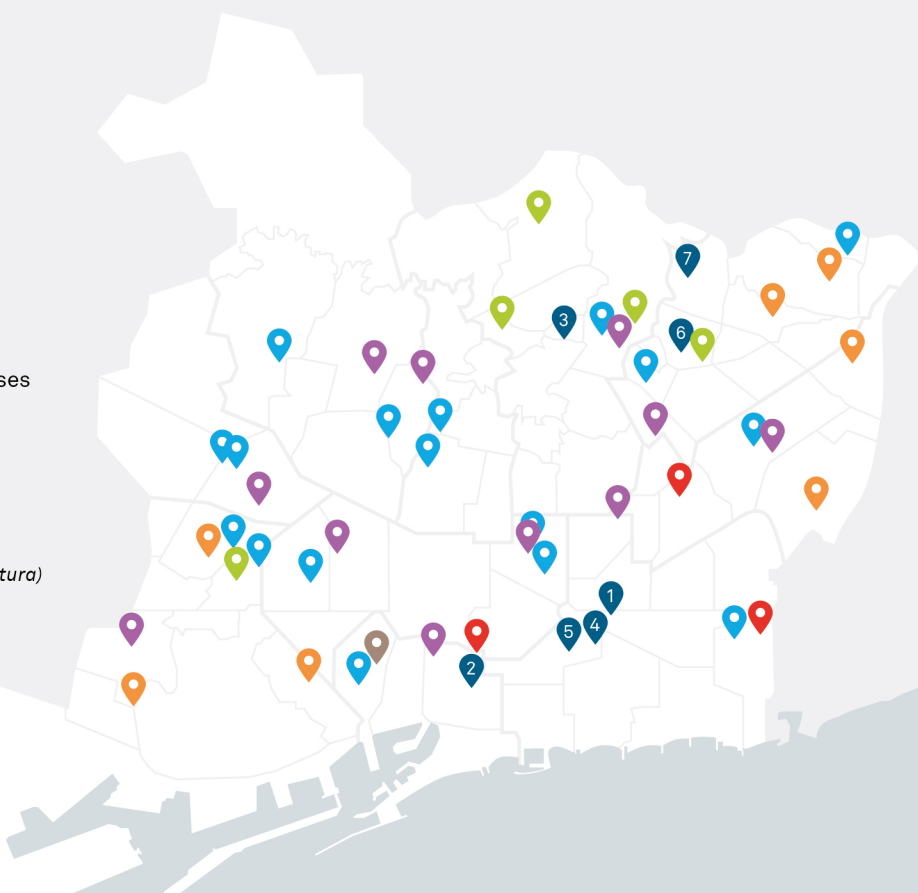


Formació tecnològica i gratuïta per a la ciutadania

barcelona.cat/cibernarium

Barcelona Activa present als barris

- 1 Seu Central Barcelona Activa
Porta 22
Centre per a la Iniciativa Emprenedora Glòries
Incubadora Glòries
- 2 Convent de Sant Agustí
- 3 Ca n'Andalet
- 4 Oficina d'Atenció a les Empreses Cibernàrium
Incubadora MediaTIC
- 5 Incubadora Almogàvers
- 6 Parc Tecnològic
- 7 Nou Barris Activa (*propera obertura*)
- Treball als barris
- Antenes Cibernàrium
- Punts Barcelona Treball
- Punts d'Orientació per a la Recerca de Feina
- Punts d'inserció sociolaboral A prop Jove
- Punt de Defensa dels Drets Laborals



 **Barcelona Activa**

**Ajuntament de
Barcelona**



© Barcelona Activa

Última actualización 2018

Cofinanciado por:



UNIÓ EUROPEA

Fons Europeu de Desenvolupament Regional

Síguenos en las redes sociales:



barcelonactiva.cat/cibernarium



[barcelonactiva](https://www.facebook.com/barcelonactiva)



[barcelonactiva](https://twitter.com/barcelonactiva)



[company/barcelona-activa](https://www.linkedin.com/company/barcelona-activa)