

Aplicacions del Blockchain més enllà del Bitcoin

La tecnologia Blockchain



Ajuntament de
Barcelona



Barcelona
Activa

Índex

1 INTRODUCCIÓ A LA TECNOLOGIA BLOCKCHAIN	3
1.1 QUÈ ÉS LA CADENA DE BLOCS	3
1.1.1 DESCENTRALITZAT	3
1.1.2 IMMUTABLE	4
1.1.3 SEGUR.....	4
2 FUNCIONAMENT DE LA TECNOLOGIA BLOCKCHAIN	5
2.1 COM FUNCIONA UNA BLOKCHAIN.....	5
2.2 BENEFICIS DE BLOKCHAIN.....	5
2.3 TIPUS DE BLOCKCHAIN.....	6
3 CASOS D'ÚS DEL BLOCKCHAIN	7
3.1 APLICACIÓ DE BLOCKCHAIN EN SECTORS	7
3.1.1 SECTOR FINANCER.....	7
3.1.2 TERCER SECTOR	7
3.1.3 LOGÍSTICA.....	7

1 INTRODUCCIÓ A LA TECNOLOGIA BLOCKCHAIN

1.1 QUÈ ÉS LA CADENA DE BLOCS

Per parlar de què és la cadena de blocs (blockchain) i entendre com de disruptiva és aquesta tecnologia, és bo començar fent un repàs al passat i a l'evolució de les tecnologies i els serveis a Internet.

En els primers dies d'Internet, els serveis eren:

- Per una banda, centralitzats tant físicament com jeràrquicament, és a dir, tant amb relació a la distribució física com amb relació al poder que tenien les persones usuàries.
- Per altra banda, eren cars de mantenir, ja que estaven a l'abast de molt poques companyies que podien suportar i vendre aquests serveis.
- També eren poc escalables, ja que no permetien democratitzar aquests serveis i estaven en mans de molt pocs.

I en definitiva, només els usaven grans corporacions, com per exemple IBM.

Avui en dia, amb el núvol, els serveis es tornen:

- Descentralitzats físicament.
- Centralitzats jeràrquicament. Seguim depenent de serveis que ofereixen companyies que tenen tot el poder de decisió i manteniment.
- Barats de mantenir. Avui en dia qualsevol persona pot contractar un servidor i aixecar una pàgina web amb un cost pràcticament nul.
- Molt escalables. I és que podem combinar molts serveis de baix cost per fer noves aplicacions. A més, estan en mans de milers de persones.

I ja no només estan en mans de grans corporacions, sinó que en fan ús totes les empreses i molts usuaris i usuàries finals.

Amb la cadena de blocs, podem concebre un Internet:

- Descentralitzat (tant físicament com jeràrquicament)
- Immutable
- I segur (tant pel que fa a la infraestructura com al programari)

1.1.1 DESCENTRALITZAT

Explicat amb més detall, diem que un servei està descentralitzat físicament quan tots els actors estan distribuïts geogràficament i jeràrquicament i quan tots els actors tenen poder d'acció i decisió sobre la xarxa.

1.1.2 IMMUTABLE

Per altra banda, parlem d'immutabilitat. Quan fem una inserció de dades en una cadena de blocs, aquestes dades no podran ser modificades. Un canvi de dades anteriors invalida totes les següents. Això ens permet obtenir un registre en què tota la informació queda gravada per sempre i mai no es podrà tramejar.

1.1.3 SEGUR

Per últim, ens referim a dos nivells de seguretat. Pel que fa a la infraestructura, en ser descentralitzat, mentre quedi un node actiu la xarxa seguirà funcionant. Per altra banda, definim la seguretat amb relació al programari, ja que la criptografia impedeix la falsificació de les dades.

Seguint aquesta visió, el 2008 neix **Bitcoin** com la primera aplicació d'aquesta tecnologia. Bitcoin surt com un paper d'investigació i és la primera versió d'igual a igual d'un sistema de pagaments distribuït. El 4 de gener de 2009 se sella el Genesis Block de Bitcoin, que és com s'anomena el primer bloc d'una cadena que conté molta informació rellevant sobre cada cadena de blocs, i s'inicia la xarxa Bitcoin com la primera cadena de blocs de la història.

Amb aquesta informació prèvia, som capaços de definir què és una cadena de blocs.

No existeix cap definició estàndard de què és aquesta tecnologia, però la podem entendre com un registre immutable i distribuït de dades que, alhora, és integrable i programable.

En un terreny informal i com una primera definició que ens pot ajudar a entendre realment què és una cadena de blocs, imaginem-nos un fitxer Excel que tenim compartit al Google Drive. Les columnes serien els blocs i les files serien dades que anirien emmagatzemades a cada bloc. Quan dues persones actualitzem a la vegada aquest fitxer, que actua com a registre, veiem com les dades es van modificant. Una cadena de blocs seria el mateix, però en comptes de ser de Google, el manteniment el faria la xarxa. És a dir, hi hauria una manera en què ambdós ens posaríem d'acord per escriure en el mateix registre sense tenir confrontacions. Això es coneix com a **consens**. I a la cadena de blocs s'aconsegueix mitjançant un algoritme informàtic que executen tots els ordinadors que participen a la xarxa.

2 FUNCIONAMENT DE LA TECNOLOGIA BLOCKCHAIN

2.1 COM FUNCIONA UNA BLOKCHAIN

Un cop entès què és la cadena de blocs i la capacitat de disrupció que pot tenir per als serveis actuals, podem entendre com funciona i, per tant, quan és una bona opció utilitzar aquesta tecnologia. També és important distingir els tipus de cadena de blocs, ja que cada arquitectura s'adequa a diferents casos d'ús.

El primer pas per entendre com funciona una cadena de blocs passa per una transacció. Quan un individu de la xarxa es disposa a realitzar una operació candidata a ser escrita en el registre, s'inicia una transacció. Aquesta escriptura pot ser de qualsevol tipus, és a dir, tant pot ser una transacció d'una criptomoneda com del registre de la propietat d'un habitatge. Aquesta transacció es llança a la xarxa P2P a l'espera de ser validada i inclosa al registre.

El segon pas consisteix en la generació d'un bloc. Cada cadena de blocs té un temps de bloc, que és el temps aproximat que tarda una cadena de blocs a generar un nou bloc, el qual es modifica en base a diversos paràmetres. Per generar un bloc, un altre individu de la xarxa realitza càlculs molt complexos fins que és capaç de generar-lo i confirmar-ne les transaccions. Aquest individu inclou la transacció de l'individu anterior en aquest nou bloc i rep la recompensa de bloc, a més de les comissions de les transaccions que hi són contingudes.

Seguidament, la resta d'individus de la xarxa validen tant les transaccions del nou bloc com la seva generació i fixen, així, les transaccions incloses com les recompenses pel miner que ha generat el bloc.

Per últim, cal entendre el concepte de concatenació de blocs. Cada vegada que es genera un nou bloc, es genera incloent la firma digital del bloc anterior, de manera que podem concatenar un bloc amb l'anterior mitjançant un identificador únic i formant un registre immutable de la història de la xarxa. Si canviéssim un sol bit d'un dels blocs, canviaria l'identificador del propi bloc i, per tant, el següent ja no encaixaria amb l'anterior i s'invalidarien tots els blocs successors.

2.2 BENEFICIS DE BLOKCHAIN

Gràcies a aquestes característiques i estructura de dades, la cadena de blocs presenta una sèrie de beneficis molt interessants per a molts negocis:

En primer lloc, podem aconseguir una optimització de processos, ja que la confiança entre dues parts que garanteix aquest registre ens permet estalviar costos i temps d'intermediació en les transaccions.

En segon lloc, tenim una alta auditabilitat, ja que, en mantenir tota la història de la xarxa i mantenir-la immutable, l'auditabilitat està garantida per disseny.

També diem que el *down time*, és a dir, el temps en què la xarxa no està operativa, és pràcticament zero, ja que mentre quedi un node actiu la xarxa seguirà funcionant.

A més a més, no necessitem una còpia de seguretat, *backups*. En tenir el mateix registre en tots els nodes de la xarxa, no necessitem que cada part mantingui backups addicionals.

Finalment, tenim una alta seguretat contra l'atac. La cadena de blocs afegeix a les capes de seguretat actuals els avantatges de la criptografia més avançada.

Tot i aquests avantatges que aporta la cadena de blocs, cal estar segurs que necessitem un registre d'aquest tipus abans de seleccionar-lo per a un projecte. Algunes de les preguntes que ens hem de fer són les següents:

- Necessito una base de dades?
- Ha de tenir compartit el dret d'escriptura?
- Els escriptors tenen confiança entre si?

La cadena de blocs, per exemple, pren molta rellevància en entorns de màxima desconfiança en què els actors es desconeixen o tenen interessos diferents. També en entorns on es requereix màxima transparència entre diferents parts i sempre en processos força clars i definits, de manera que es puguin codificar fàcilment.

2.3 TIPUS DE BLOCKCHAIN

Un cop identificada aquesta necessitat, també cal saber que hi ha diverses arquitectures de cadena de blocs. A grans trets, podem diferenciar entre cadenes de blocs públiques i privades:

Les cadenes de blocs públiques, com és el cas de Bitcoin, tenen una arquitectura que permet a tots els actors participar, realitzar i validar transaccions. Tota la informació enregistrada és pública i es pot consultar.

En segon lloc, tenim les cadenes de blocs privades, les quals segueixen essent distribuïdes i immutables, però no han de ser necessàriament transparents ni descentralitzades. Aquestes cadenes de blocs són més útils quan la informació és privada i es volen gestionar els permisos i poders que hi tenen els actors.

Així doncs, podem concloure que realment en poques ocasions val la pena utilitzar aquesta tecnologia, però en els casos d'ús que apunta realment sí que ofereix una gran millora respecte a les tecnologies que existien i permet aportar un valor completament diferenciat.

3 CASOS D'ÚS DEL BLOCKCHAIN

Parlem ara sobre els casos d'ús de la cadena de blocs en els diferents sectors.

3.1 APLICACIÓ DE BLOCKCHAIN EN SECTORS

3.1.1 SECTOR FINANCER

El primer sector que ens ve al cap quan parlem de la cadena de blocs és el de la banca i les finances.

Mitjançant les criptomonedes, que no són res més que actius que se sostenen gràcies a una cadena de blocs, apareixen casos d'ús com els següents:

En primer lloc, un mitjà de pagament. Les criptomonedes permeten realitzar pagaments sense persones intermediàries, és a dir, permeten a dues persones que no es coneixen i desconfien completament l'una de l'altra enviar-se diners sense passar per cap intermediari com podria ser un banc.

En segon lloc, tenim els micropagaments. Com que els costos de manteniment queden repartits a la xarxa, enviar diners en una cadena de blocs té una comissió molt baixa. Això permet fer micropagaments en l'àmbit internacional, cosa que fins ara resultava un procediment molt complicat per tots els intermediaris que es necessitaven.

Un altre cas d'ús de les criptomonedes és la representació de drets. S'utilitza per proporcionar liquiditat i transacció als drets. Per exemple, podem observar el cas d'ús d'una votació. Amb el DNI, per exemple, podem identificar una persona a la cadena de blocs. Aquesta persona té la capacitat de votar i enregistrar el seu vot. Ningú no podrà canviar aquest vot, ja que és immutable i, a la vegada, transparent, per la qual cosa ens podem assegurar que el nostre vot és vàlid. A més a més, podem confiar en què cada persona només ha pogut votar una vegada i que tots els vots tenen el mateix valor. Una votació és un cas molt senzill, però té tots els punts perquè una cadena de blocs pugui tenir lloc. És un procés clar i definit, totes les parts desconfien les unes de les altres i es necessita transparència. Amb una cadena de blocs tindríem unes votacions segures, automàtiques i es podria votar des de qualsevol lloc.

3.1.2 TERCER SECTOR

Un altre sector que pot aprofitar aquesta tecnologia és el tercer sector.

Primerament, la tecnologia de la cadena de blocs permet aportar una transparència inigualable per a les donacions que els membres de les ONGs puguin fer. També permet demostrar una gestió transparent dels fons a tots els membres i una auditabilitat infal·lible de cara a organismes reguladors. D'altra banda, permetria les microdonacions, així com una democràcia líquida dins l'organització.

3.1.3 LOGÍSTICA

Finalment, un altre sector en què la cadena de blocs ha pres molta força és el de la logística. La tecnologia de cadena de blocs aporta transparència, immutabilitat, confiança entre les parts,

velocitat en la detecció d'errors i consens entre les parts implicades. Això implica una evolució disruptiva en aquest sector, ja que podem resoldre alguns dels problemes més crítics. Consultem, per exemple, la traçabilitat de productes en la logística, un factor essencial en aquest sector. La cadena de blocs resol aquest problema en tres àmbits. En primer lloc, totes les dades que enregistrem referents a la traçabilitat d'un producte romandran immutables, de manera que tots els participants de la xarxa tenen la confiança que la informació es mantindrà intacte en el temps. Això elimina la necessitat de la supervisió d'un tercer o d'auditories de la informació. En segon lloc, assegurem la integritat de les regles contractuals. Si codifiquem aquestes regles dins de la cadena de blocs, podem garantir que sempre estaran operatives i es respectaran sense la necessitat d'auditories. Finalment, en cas d'haver de presentar proves del flux d'una transacció com la firma d'un contracte, les proves es poden extreure de forma casual en l'ordre que han succeït.

Finalment, podem combinar diverses aplicacions per crear solucions més complexes. Per exemple, EverLedger combina els avantatges que aporta la cadena de blocs a la logística amb la representació d'actius reals a la xarxa. Prenent les propietats bàsiques dels diamants, podem identificar-los i representar-los a la cadena de blocs. Un cop inserits a la cadena de blocs, podem enregistrar totes les modificacions que pateix aquell diamant des que s'extreu fins que arriba a la botiga, passant per tots els distribuïdors i transportistes. Així doncs, finalment, escanejant un simple codi QR o consultant un número identificador, podem traçar tot el recorregut d'aquell diamant en concret fins al seu origen i podem comprovar de forma verídica que no estem comprant un diamant de sang.

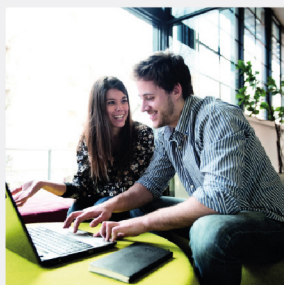
Així doncs, podem veure que la tecnologia de cadena de blocs està present en molts sectors, que cada vegada ho estarà en més i que en revolucionarà per complet el funcionament, canviarà molts models de negoci i crearà models nous que fins ara no podíem ni imaginar.

Descobreix tot el que Barcelona Activa pot fer per a tu



Acompanyament durant tot el procés de recerca de feina

barcelona.cat/treball



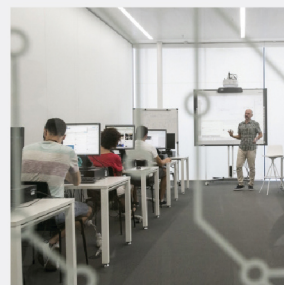
Suport per posar en marxa la teva idea de negoci

barcelona.cat/emprendoria



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
Darrera actualització 2018

Cofinançat per:



Segueix-nos a les xarxes socials:

-  barcelonactiva.cat/cibernarium
-  [barcelonactiva](https://www.facebook.com/barcelonactiva)
-  [barcelonactiva](https://twitter.com/barcelonactiva)
-  [company/barcelona-activa](https://www.linkedin.com/company/barcelona-activa)