

Blockchain i criptomonedes: benvinguts al nou paradigma digital

El canvi tecnològic modificarà el sistema de pagaments tal com el coneixem, i, probablement, la tecnologia *blockchain* tindrà un paper molt destacat en aquest procés i facilitarà l'aparició de monedes digitals. Quines són les claus de les tecnologies que permetran aquesta transformació? Quines criptomonedes tenen més possibilitats d'èxit?

La tecnologia *blockchain*

Els avanços en criptografia, combinats amb el potencial de transmissió i d'emmagatzematge de dades, han possibilitat l'aparició de les anomenades **tecnologies de registres distribuïts** (DLT, per les sigles en anglès).¹ Es tracta de bases de dades de les quals existeixen múltiples còpies idèntiques distribuïdes entre els participants a la xarxa, que s'actualitzen de manera sincronitzada i consensuada. El gran atractiu de les DLT és que permeten gestionar i compartir dades de manera segura i guardar tota la informació sense que es pugui alterar. El tipus més conegut de DLT és el *blockchain*, que organitza la informació per blocs i que sovint es compara amb un llibre que no es pot esborrar.

La tecnologia *blockchain* es basa en tres ingredients fonamentals:

- Gràcies a la criptografia, cada bloc d'informació s'identifica de manera única.
- Els participants de la xarxa han d'aprovar i de validar tota la informació que entra a la xarxa.
- El registre és inalterable i immutable i, per aquest motiu, extremadament complicat de piratejar o de modificar.

La tecnologia *blockchain* facilita l'aparició de criptomonedes, ja que, en crear un registre compartit de totes les transaccions i en establir un mètode descentralitzat de validació, facilita l'intercanvi digital de diners entre usuaris de manera directa (les infraestructures de pagaments tradicionals compten amb un intermediari central, ja sigui el banc central, una companyia de pagaments digitals, una plataforma mòbil...). L'aplicació més coneguda del *blockchain* al món financer és la liquidació de pagaments (en les transferències internacionals, les criptomonedes poden jugar un paper valuós de moneda pont), tal com ho il·lustra la primera figura.

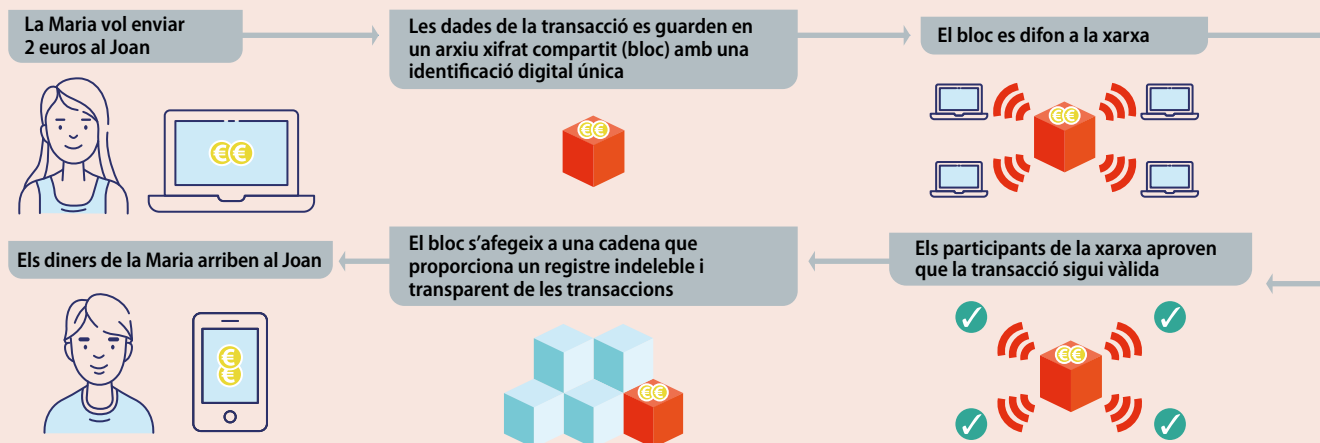
Blockchain, una tecnologia que evoluciona ràpidament i que pot acabar facilitant el desenvolupament d'aplicacions d'ús massiu

Un dels àmbits en què més es treballa és la millora de l'escalabilitat dels sistemes de pagament que tenen *blockchain* com un dels seus ingredients fonamentals. Les primeres iniciatives que van sorgir eren xarxes totalment descentralitzades i públiques. En aquests casos, atès que tots els participants han de validar les transaccions, el nombre de transaccions que es poden processar s'alenteix de forma considerable (un clar exemple és el de Bitcoin, que processa 7 transaccions per segon, en relació amb les 65.000 de Visa) i les despeses d'energia són molt elevades. Una de les solucions que s'explora és l'ús de xarxes permissionades, en què un administrador controla la xarxa i decideix qui hi pot participar. El seu avantatge és que són més escalables i permeten validar les transaccions de forma molt més ràpida, tot i que són més vulnerables a intents d'alteració i de pirateig.

Més enllà del *blockchain*

És important aclarir que, al sector financer, els avanços tecnològics van molt més enllà de les criptomonedes i de les DLT i que han permès millorar l'agilitat i el funcionament dels sistemes de pagament existents. Un bon exemple d'això són els avanços espectaculars en el pagament amb mòbils. Com hem vist, la tecnologia *blockchain* té molt potencial, tot i que seria possible emetre una moneda digital sense la necessitat de recórrer a ella. De fet, una autoritat amb poders de centralització de processos com un banc central podria arribar a plantejar-s'ho desenvolupant una infraestructura basada en els sistemes de pagaments que ja funcionen en l'actualitat.

Funcionament de la tecnologia *blockchain*



Font: CaixaBank Research.

1. Distributed ledger technologies.

Els principals àmbits en què l'ús de les criptomonedes pot ser beneficiós són:

- **Transaccions financeres internacionals.** Malgrat que la tecnologia *blockchain* no és l'única alternativa que s'estudia en aquest àmbit, és una candidata clara per millorar l'eficiència dels pagaments internacionals per la **reducció de costos que pot implicar i per una major velocitat de les transaccions en relació amb sistemes amb una elevada centralització operativa.**
- **Reducció de l'economia submergida.** Malgrat que una de les principals propietats de les criptomonedes és l'anonimat de les transaccions, es podrien dissenyar mecanismes que facilitessin la identificació de les activitats il·legals. Per exemple, que els pagaments en determinats àmbits o de determinada quantia no fossin anònims.
- Poden promoure la **inclusió financera** en països subdesenvolupats o emergents, on una part important de la població està desbancaritzada (però podria emmagatzemar criptomonedes en un moneder digital vinculat al telèfon mòbil).

No totes les criptomonedes són iguals

Segons la definició del BIS,² les criptomonedes es distingeixen perquè són **electròniques** i perquè **permeten l'intercanvi d'igual a igual** sense una tercera part que exerceixi tasques d'intermediació. Però hi ha molts tipus de criptomonedes. L'anomenada «flor dels diners» ens ajuda a classificar les diferents monedes, i també les criptomonedes, en funció de les seves propietats en els àmbits més rellevants: el tipus d'emissor de la moneda (banc central o un altre), l'accessibilitat (universal o restringida), la forma (electrònica o física) i el mecanisme de transferència (d'igual a igual o centralitzat). Per exemple, en funció de l'emissor, hi ha tres grans classes de criptomonedes:

- **Criptomonedes privades:** emeses per un particular o per una entitat privada.
- **Criptomonedes dels bancs centrals.**
- **Solucions híbrides (criptomonedes sintètiques):** el banc central és l'emissor, però un conjunt d'entitats privades s'encarregaria de la interacció amb el client i de la innovació (a les economies avançades, els bancs comercials serien el candidat natural).

Criptomonedes dels bancs centrals i criptomonedes privades: pros i contres

A priori, si un banc central acaba emetent una **criptomonedes**, i compta amb un marc regulador ben definit i no hi ha dubtes sobre la seguretat, és **molt probable que sigui acceptada com una forma de pagament d'ús generalitzat**. En tenir el suport d'una institució pública que no pot fer fallida, el fet que un comunicat dels estalvis i de les transaccions passi a fer-se amb la versió «cripto» de la moneda no hauria d'afectar el valor d'aquesta moneda. En canvi, les criptomonedes privades ho tenen més difícil a l'hora de mantenir un valor estable, ja que aquest valor depèn, entre altres factors, del grau d'acceptació o d'ús que tinguin, i, com aquest valor pot canviar de manera sobtada, el seu valor sol ser més volàtil.

De tota manera, estan apareixent propostes que intenten esquivar aquest desavantatge. Les anomenades *stablecoins* o monedes estables pretenen salvar aquest escull fixant el que, al capdavant, constituïria un tipus de canvi fix entre la criptomonedes i un actiu de valor estable (com podria ser una divisa d'un país avançat). La libra, la criptomonedes proposada per Facebook, se situa dins aquesta família de criptomonedes.³

Se sol argumentar a favor del desenvolupament de criptomonedes amb el suport d'un banc central que podrien ser un complement de les eines tradicionals de la política monetària. Per exemple, la fixació d'un tipus d'interès sobre la moneda digital ampliaria el rang d'instruments dels quals disposa el banc central.⁴

No obstant això, la introducció de criptomonedes emeses pels bancs centrals també presentaria riscos, ja que podrien contribuir, si més no en part, a una desintermediació de l'activitat financera:

- Si una part dels dipòsits bancaris de les llars i de les empreses es convertissin en criptomonedes no gestionades per intermediaris financers, l'oferta de fons disponibles per atorgar crèdits disminuiria. Això tendria a encarir el crèdit i, a més a més, atorgaria més protagonisme als bancs centrals com a proveïdors estructurals de liquiditat al sistema.
- L'existència d'aquestes criptomonedes de bancs centrals incrementaria la volatilitat dels fluxos entre dipòsits bancaris i criptomonedes en temps d'incertesa o de dubtes sobre la solidesa d'alguna entitat financera, i això provocaria un risc per a l'estabilitat financera.
- El grau de desintermediació financera depèn de forma crítica de qui allotgi els moneders digitals de les criptomonedes. Si qui els allotja és el banc central, els particulars podrien tenir comptes directament al banc central, la qual cosa agreujaria el risc de desintermediació i d'inestabilitat financera. També hi hauria la possibilitat que els allotgessin entitats desvinculades dels bancs comercials. Això no eliminaria la intermediació financera, però plantejaria reptes importants: com es regularien aquestes entitats?, estarien els moneders protegits per una garantia de dipòsits?...

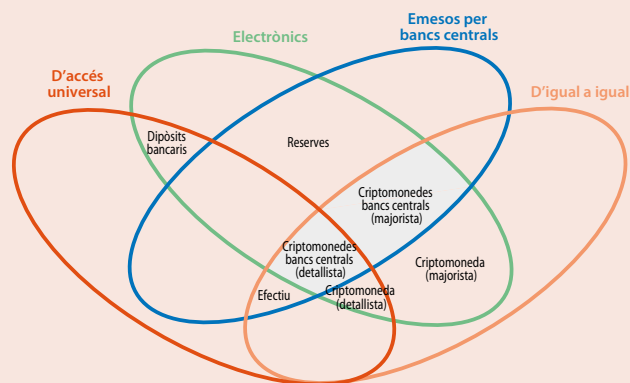
Javier Garcia-Arenas

2. Vegeu Committee on Payments and Market Infrastructures (2015), «Digital currencies», BIS.

3. Vegeu l'article «[Libra, la criptomonedes de Facebook](#)», en aquest mateix Dossier.

4. Per a més detalls, vegeu l'article «[La política e-monetària de la nova economia digital](#)», en aquest mateix Dossier.

La flor dels diners: taxonomia



Font: CaixaBank Research, a partir del diagrama del BIS.