

OIKONOMICS

Revista d'economia, empresa i societat

REpte DE FUTUR

Blockchain i les criptomonedes: el cas bitcoin

José Miguel Domínguez Jurado

Professor titular d'Economia Aplicada (Universitat de Cadis)

Ricardo García Ruiz

Professor col·laborador del Grau d'Informació i Documentació (UOC)

RESUM L'objectiu d'aquest article és explicar com un procés informàtic, la *blockchain* o cadena de blocs, permet generar la confiança necessària per a la creació, l'acceptació i l'ús cada vegada més generalitzat de les monedes digitals, sota un nou concepte o paradigma de diners no sostinguts per cap ens estatal o supranacional: les criptomonedes. Per entendre aquest procés, en primer lloc, s'exposen els aspectes tècnics de funcionament de la cadena de blocs i s'explica com aquest procés ha aconseguit generar confiança a l'usuari. En segon lloc, s'analitza la seva implementació en la variant més coneguda de totes, el Bitcoin, així com les dades relacionades amb l'expansió i ús de les principals criptomonedes, en un mercat que en els últims dos anys s'ha multiplicat per 65 i ha aconseguit el mig bilió de dòlars. El treball es tanca amb l'exposició de les principals conclusions i reflexions.

PARAULES CLAU bitcoin; divises digitals; compra de divises; *blockchain*; sistema de pagaments

«Blockchain» and cryptocurrencies: Bitcoin

ABSTRACT *The main aim of this article is to explain how a computer process, the «Blockchain» or chain of blocks, can generate the necessary trust for the creation, acceptance and increasingly widespread use of digital currencies, under a new concept or paradigm of money not maintained by any state or supranational entity: cryptocurrencies. In order to understand this process, the technical aspects of how the blockchain operates and how it has managed to generate confidence in the end user are explained first. Secondly, its implementation will be analyzed through the best known of all, Bitcoin, and through the data related to the expansion and use of the main cryptocurrencies in a market that in the last two years has multiplied by 65, reaching half a trillion dollars. This work closes by exposing the main conclusions and reflections.*

KEYWORDS *bitcoin; digital currency; currency market; blockchain; payment system*

Introducció

El desenvolupament tecnològic ha contribuït de manera decisiva en la transformació de l'economia i el progrés de la humanitat. Si la fita més important va ser la pròpia revolució industrial, avui dia estem assistint a una altra revolució l'origen de la qual ha estat la invenció dels ordinadors, el desenvolupament del programari, la interconnexió a escala mundial i el seu ús massiu des de principis del segle XXI. Això ha augmentat les possibilitats de crear nous productes i serveis, i ha obert la porta a transformacions de gran importància que permeten parlar d'una nova economia que convisqui amb l'actual o, fins i tot, pugui arribar a substituir-la en el futur.

Entre aquestes innovacions es troba la *blockchain*, una eina desenvolupada dins del camp de la criptografia i la gestió de xarxes informàtiques. La *Blockchain* és un sistema tecnològic que té entre els seus objectius principals generar confiança als seus usuaris, i la forma en què es concep impedeix, com a mínim a priori, exercir cap control per part d'usuaris o organitzacions, cosa que està suposant una revolució.

El procés més conegut basat en la *blockchain* s'està expandint ràpidament i és el d'emissió d'una moneda virtual, anomenada «criptomonedes», que ha donat lloc al creixement del mercat de criptomonedes en nombre, en valor de capitalització i

en volum de transaccions. És un comportament que, en els darrers mesos, podria qualificar-se d'explosiu pel seu intens creixement; fins i tot la pròpia banca tradicional està operant amb criptomonedes (Rivero, 2017; Leal, 2017).

Però el seu paper no queda aquí: les possibilitats d'aplicació de la *blockchain* en altres parcel·les de l'economia i el dret poden ser innombrables, ja que aquesta estructura d'arxius és molt adequada per assegurar escrits de valor crític, enregistraments produïts de forma continuada i que tinguin valor legal, com ara operacions de pagament, però també molts altres tipus d'escriptura, com per exemple títols de propietat, patents, diplomes, etc. (Ammous, 2016; Pilkington, 2015).

Partint de la definició i dels aspectes tècnics del funcionament de la *blockchain*, és fàcil entendre la confiança que genera en els seus usuaris. El fet de no dependre d'una institució o organització que la recolzi dota els processos que utilitzen aquesta tecnologia de gran llibertat, tant en la seva creació com en la seva implementació, per no dir que, en molts casos, el fet de poder eludir el control es converteix en el *leitmotiv* d'alguns productes.

No obstant això, un procés tan innovador no està exempt de problemes i, per tant, cal reflexionar sobre les perspectives de futur de la *blockchain* aplicada a altres camps, en general, i a les criptomonedes, en particular.

1. Fonaments de la cadena de blocs (*blockchain*)

La *blockchain* és una base de dades de creació col·lectiva, els components històrics de la qual no poden ser modificats. Es crea, es difon i s'hi accedeix mitjançant una xarxa distribuïda sense nodes privilegiats.

Aquesta definició amaga un procés de funcionament i creació complex, que atorga les garanties de seguretat necessàries perquè les accions que s'hi realitzin siguin confiables i acceptades pels seus usuaris. Els seus avantatges són evidents, especialment quant a la integritat de les dades i la certificació. No hi ha forma de canviar la informació emmagatzemada en un bloc *blockchain* (Lemieux, 2016), i això es pot aplicar en l'àmbit d'acreditació i de seguretat jurídica.

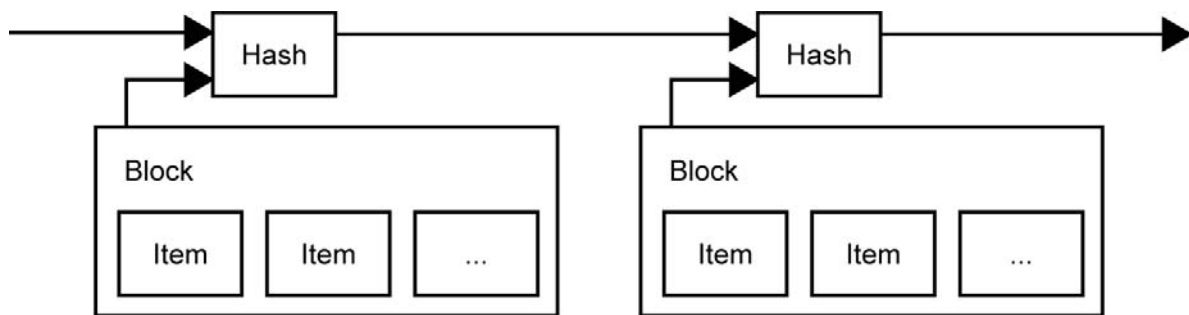
El procés de construcció d'una *blockchain* garanteix la seva seguretat, integritat i independència. A més, genera ocupació: els «miners», que s'encarreguen de les operacions necessàries de creació i consolidació de blocs, obtenen una remuneració com a recompensa.

La *blockchain* es defineix com «una base de dades distribuïda», i les seves característiques més destacades són les següents:

- Operar descentralitzadament, P2P¹, sense la supervisió de cap autoritat central (Swan, 2015). Cada node té una còpia pròpia de la *blockchain* i contribueix a la construcció i al manteniment de les operacions.
- La base de dades únicament admet addicions en ordre cronològic; és impossible canviar o esborrar informació ja registrada.
- És un registre certificat criptogràficament, i això assegura la consistència de totes les dades registrades o emmagatzemades, i validades per la majoria dels nodes de la xarxa (Nakamoto, 2008). Aquesta característica permet a la *blockchain* servir de certificació d'integritat per a qualsevol transacció.

La *blockchain* està formada per blocs d'informació. En el cas de les criptomonedes són majoritàriament les transaccions monetàries vàlides. Els blocs s'enllacen unívocament en una cadena. Cada bloc inclourà un **hash**² del bloc anterior, s'hi encadenarà i mantindrà la consistència i unicitat.

Gràfic 1. Funcionament de la *blockchain*



Font: Nakamoto, 2008

Un bloc està format per uns registres de dades, i la forma i el significat d'aquestes dades depenen de la seva aplicació. En el cas del Bitcoin i d'altres sistemes de pagament, aquestes entrades són les transaccions monetàries: cada bloc en conté entre 1.000 i 3.000. Un bloc conté un encapçalament amb la seva suma de control i un identificador del bloc anterior (amb la seva pròpia suma de comprovació). Es pot verificar qualsevol bloc navegant fins al bloc inicial de la cadena. La suma de comprovació d'un bloc sempre es comprova en cada accés per detectar qualsevol

1. P2P és l'acrònim de *peer to peer*, o xarxa entre parells; les computadores es connecten i comuniquen entre si sense servidor central, aprofitant, optimitzant i administrant l'ample de banda de la xarxa.
2. Una suma de comprovació (*hash*) és un nombre calculat a partir del contingut del bloc. Qualsevol modificació intencional del bloc canvia la suma de comprovació de manera imprevisible. Dos blocs diferents sempre tenen un *hash* diferent.

canvi en el seu contingut després de la seva construcció. Una modificació del bloc, inclosa la capçalera, amb la seva nova suma de comprovació, implica modificar el seu identificador. (Stahr, 2014)

1.1. Construcció d'una cadena de blocs

El procés de creació és competitiu i obert: això li confereix la seva independència. La competència es basa en quin miner aconseguirà el tancament del bloc, ja que solament el primer que tanqui el bloc de forma correcta i validada serà remunerat. És obert per l'estructura de treball en xarxa.

La veritable originalitat del Bitcoin i les criptomonedes derivades, que els dona les seves qualitats úniques i la seva complexitat, és que s'ubiquen en una xarxa *peer to peer* oberta, sense servidor central ni nodes privilegiats. Qualsevol persona pot unir-se a la xarxa sense haver de demanar permís. El programari utilitzat és de lliure accés. L'usuari pot descarregar, instal·lar i executar el programari sense necessitar autorització. Encara que hi ha una plataforma preferida de distribució (Github) i un programari recomanat per diverses instàncies (Bitcoin.org, 2011; Hartikka, 2016; ethereum.org, 2018), qualsevol persona pot proposar un programari nou o emprar una plataforma diferent (Tormey, 2017).

El procés de generació de la *blockchain* s'articula en tres àmbits:

- Difusió de l'escriptura entre nodes: les operacions són visibles per a tots els operadors.
- Construcció dels blocs.
- Construcció de la cadena.

Com a primer pas, cada nova creació d'un node entra al sistema per un node de la xarxa, verificant que la seva estructura és correcta i vàlida d'acord amb les entrades ja gravades. En el cas del Bitcoin, es verifica per mitjà de les transaccions anteriors que al compte hi ha una quantitat com a mínim igual a la suma total a pagar, i que l'autor de la transacció està autoritzat. Si es compleixen aquestes condicions, l'escriptura del node queda en espera en una llista local i distribuïda a tota la xarxa. En cas contrari, es rebutja.

Cada tipus d'anotació requereix el seu protocol de validació, que defineix les entrades vàlides al sistema. Aquest protocol s'executa successivament en les etapes de construcció i validació dels blocs. Cada sistema pot contenir un directori de protocols de validació, i cadascun d'ells està associat amb un codi a la part superior de cada seqüència d'ordres, la qual cosa permet realitzar anotacions a la mateixa cadena de blocs sobre transaccions de diversos tipus.

En rebre cada missatge es comprova la validesa formal i la legitimitat de la seva informació. La naturalesa oberta de la xarxa imposa un principi fonamental de seguretat: cada node assumeix que la resta del sistema pot ser defectuós o fraudulent. Tot el sistema està dissenyat robustament sota la suposició que està constantment essent atac per defraudadors altament qualificats.

Després d'això, les entrades no vàlides s'han eliminat, i cada anotació vàlida i legítima s'ha copiat a la xarxa distribuïda i és degudament validada en cada etapa de la seva trajectòria des del seu punt d'entrada.

En la segona etapa, els miners col·loquen les entrades en la seva llista d'espera local i les organitzen amb la finalitat de facilitar l'accés a les entrades individuals. Tots els miners treballen simultàniament i trien lliurement quins registres incorporen a cada bloc en construcció. S'acaba el bloc afegint una capçalera amb la suma de comprovació i l'identificador del bloc anterior.

El cost computacional d'aquesta operativa és intencionadament molt alt. La suma de comprovació compleix normes molt estrictes que requereixen molts recursos informàtics, però la seva verificació s'ha de poder comprovar fàcilment per tots els nodes: es diu «prova de treball». Aquest requisit limita el minat individual (grups de forma cooperativa), ja que perquè els seus blocs siguin acceptats necessiten molta capacitat de càlcul. (IBM Bluemix, 2017)

Existeix remuneració per motivar el minat. En el cas del Bitcoin, la remuneració es fa automàticament mitjançant la inserció del bloc en una transacció especial que acredita al miner un nombre de Bitcoins ja creats per a aquest propòsit, quan finalment s'afegeix el bloc. Si un miner ha construït un bloc vàlid, ho transmet als seus veïns, que, al seu torn, ho retransmeten a tots els nodes de la xarxa després de comprovar la validesa de totes les seves entrades. Quan un miner rep un nou bloc, cessa de construir el seu bloc actual, ja que no s'acceptarà, i comença a construir un altre bloc nou.

La construcció de la cadena. Per a cada nou bloc rebut, cada ordinador d'un node complet executa un protocol establert, ja sigui per rebutjar aquest bloc quan no sigui vàlid o presenti aquest contingut a l'escriptura local, afegir-lo al final de la cadena local després d'una comprovació final de totes les entrades o posar-lo en espera. Cada bloc conté l'identificador del seu bloc antecessor a la *blockchain* del miner que la va construir. El predecessor és el bloc terminal de la cadena local, i després s'hi afegeix d'una verificació final de la seva validesa. En cas contrari, serà retingut en cua i serà l'extrem d'una branca secundària de la *blockchain*. (Crosby, 2016; Ateniese *et al.*, 2017)

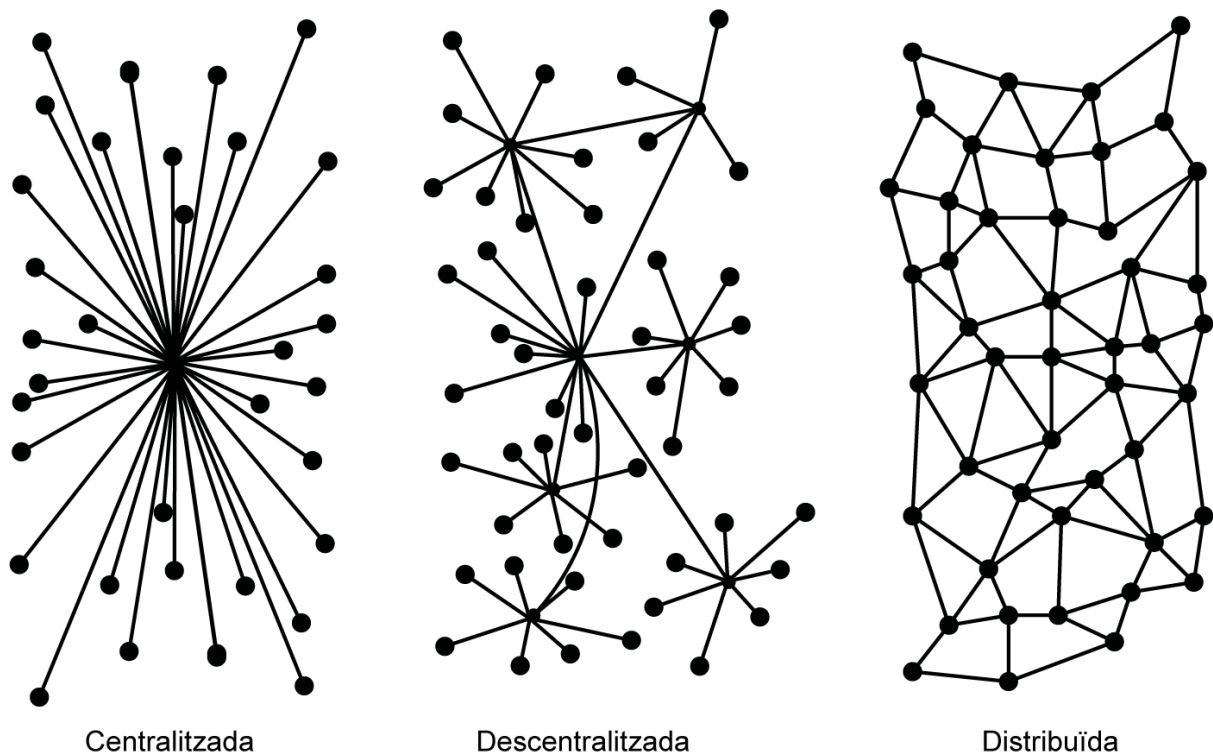
Unicitat i consistència. El protocol incorpora un mecanisme de consens com a part vital del sistema. La regla del Bitcoin és mantenir la branca amb major treball de construcció. A la capçalera de cada bloc hi ha un valor numèric del treball realitzat per a la seva construcció: la suma d'aquest valor per a cada branca indica el

treball conjunt realitzat. Si la suma del valor d'una branca secundària és superior al valor de la suma de la branca principal actual, llavors aquesta branca secundària es convertirà en la nova branca principal. El programari realitzarà els ajustos i les validacions de blocs que calguin. Aquest protocol crític i complex és el veritable cor del sistema.

Totes les còpies de la *blockchain* es mantindran idèntiques, ja que s'apliquen les mateixes regles de validació d'entrades i de blocs.

Les milions d'entrades creades es troben registrades en milers d'arxius idèntics en llocs diferents, inalterables, i que poden consultar-se gratuïtament. (IBM Blue-mix, 2017; Kehrl, 2016)

Gràfic 2. Diferències gràfiques entre sistemes de xarxes



Font: Les tres topologies de xarxa segons els gràfs de Paul Baran.

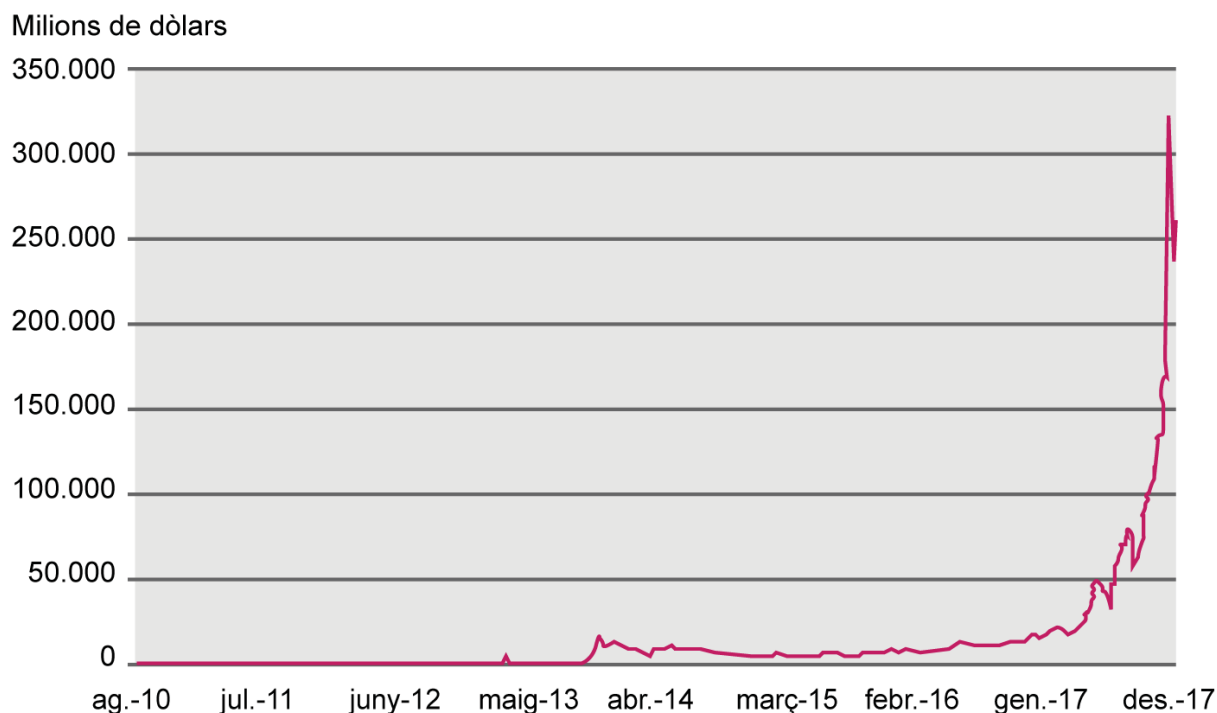
2. Les criptomonedes: el cas del Bitcoin

Actualment el Bitcoin és la més coneguda i més utilitzada de les moltes criptomonedes existents. Abans de la seva aparició ja existien precursors de monedes electròniques com, per exemple, les tecnologies desenvolupades per David Chaum i Stefan Brands (moneda electrònica), Adam Back (hashcash), Wei Dai

(b-money), Nick Szabo (bit-gold) (Brands i Chaum, 1993; Chaum i Brands, 1997; Back, 2002).

El mercat de criptomonedes, fins molt recentment, ha estat pràcticament monopolitzat pel Bitcoin. Parlar de capitalització del mercat era sinònim de parlar de capitalització del Bitcoin. El gràfic 3 mostra l'evolució del seu valor des de la seva primera cotització fins a l'actualitat.

Gràfic 3. Capitalització del mercat de Bitcoins

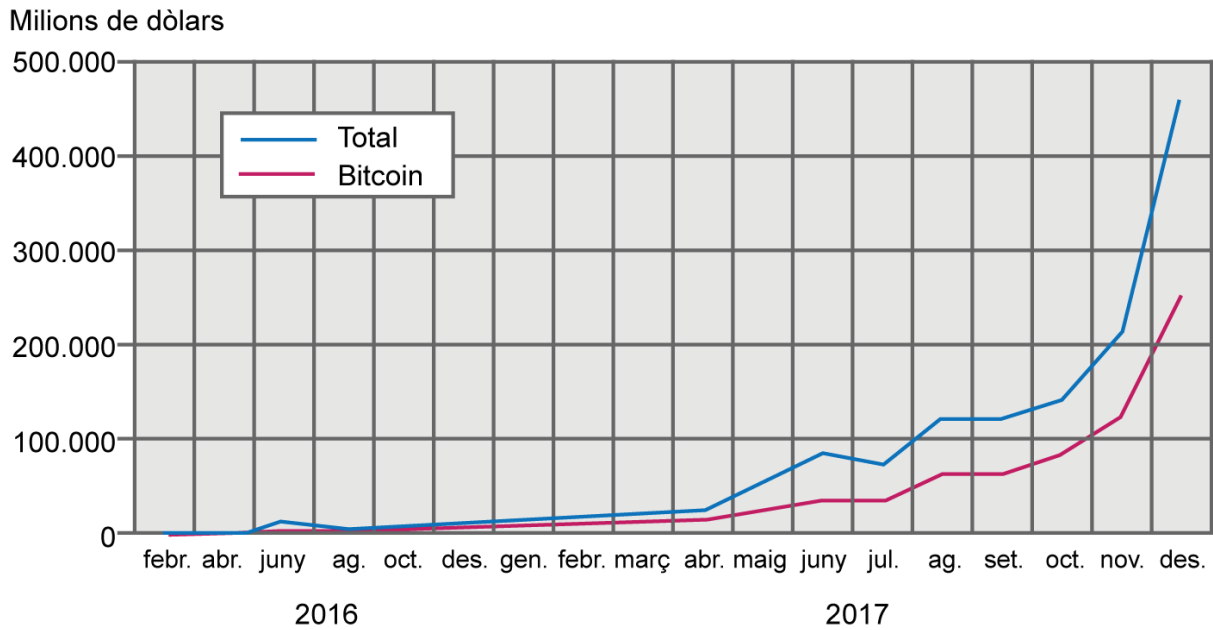


Font: elaboració pròpia sobre la base de blockchain.info.

Com a elements més destacables, cal indicar que l'any 2013 marca l'enlairament del Bitcoin i l'inici d'un període d'expansió de la seva capitalització que dura fins al desembre de 2014, quan aconsegueix els 14.000 milions de dòlars. Després d'aquest màxim, el seu valor decreix gradualment durant el 2014, especialment al desembre i al gener de 2015, i arriba a perdre més del 80% del seu valor de capitalització. Aquest toc d'atenció va establir el mercat durant tot l'any 2015, i el mercat va mostrar signes de recuperació a finals d'any, quan el valor rondava els 6.500 milions.

L'any 2016 va mostrar signes de força i es va incrementar progressivament el valor de capitalització, la qual cosa va permetre recuperar el nivell de 2014 i tancar amb un volum de capitalització proper als 15.000 milions. A partir d'abril de 2017 es va iniciar un procés explosiu.

Gràfic 4. Capitalització del mercat de criptomonedes i Bitcoins



Font: elaboració pròpia sobre la base de coingecko.com.

El gràfic 4 presenta l'evolució del valor mitjà mensual de la capitalització del mercat total i del Bitcoin. Se'n poden destacar tres fases: la primera, de lenta expansió del mercat fins l'abril de 2017, condicionada pel monopoli del Bitcoin. A partir d'aquesta data s'inicia una segona etapa amb un notable increment de la tendència i, per tant, del creixement del mercat, encara que amb una evolució irregular. Cal destacar una pèrdua d'importància relativa del Bitcoin pel naixement i l'expansió d'altres criptomonedes. A partir de setembre de 2017 s'inicia una tercera fase caracteritzada per un creixement explosiu, pràcticament exponencial, però es veu clarament que el pes relatiu del Bitcoin decreix, motivat pel fort creixement d'altres criptomonedes que estan guanyant quota de mercat. Alhora, es detecten grans irregularitats a causa de forts moviments especulatius.

Taula 1. Capitalització del Mercat (% de mitjana mensual)

	Bitcoin	Etherum	Ripple	Bitcoin Cash	Cardano	Litecoin	Altres
gener	89,22 %	5,39 %	1,45 %			1,21 %	2,73 %
febrer	89,40 %	5,67 %	1,21 %			1,03 %	2,70 %
març	80,01 %	13,21 %	1,20 %			0,89 %	4,70 %
abril	71,64 %	16,57 %	4,71 %			2,01 %	5,07 %

	Bitcoin	Etherum	Ripple	Bitcoin Cash	Cardano	Litecoin	Altres
maig	55,42 %	20,15 %	15,13 %			2,44 %	6,85 %
juny	47,05 %	31,45 %	11,95 %			2,06 %	7,50 %
juliol	52,00 %	26,70 %	9,85 %			2,93 %	8,51 %
agost	52,75 %	23,28 %	6,02 %	6,35 %		2,13 %	9,47 %
setembre	53,38 %	22,24 %	6,07 %	6,57 %	0,00%	2,50 %	9,24 %
octubre	60,11 %	19,90 %	5,93 %	4,06 %	0,46%	2,05 %	7,50 %
novembre	61,17 %	16,18 %	4,13 %	8,67 %	0,40%	1,74 %	7,70 %
desembre	56,26 %	13,46 %	6,43 %	7,94 %	1,70%	2,71 %	11,51 %
31/12/17	43,60 %	13,88 %	16,36 %	8,09 %	3,36%	2,39 %	12,34 %

Font: elaboració pròpia sobre la base de coingecko.com.

Així doncs, tot i que el Bitcoin és el que marca la fortalesa i l'evolució del mercat, la creació i expansió d'altres criptomonedes ha reduït la seva importància en conjunt, amb un descens continuat des de març de 2017, que el va portar al juny fins al 52,00% de la quota de mercat, tot i que a finals d'any es va recuperar fins al 56,26% (taula 1). A aquest fet s'hi va afegir l'escissió del Bitcoin en tres criptomonedes: Bitcoin, Bitcoin Cash i Bitcoin Gold.

Amb tot, el Bitcoin va tancar l'any (31 de desembre de 2017) amb una posició de domini, amb el 43,62% de la quota de mercat, per davant, en ordre d'importància, de Ripple (16,36%), Ethereum (13,88%) i dues monedes de nova creació: Bitcoin Cash (8,09%) i Cardano (3,36%), que van aconseguir aquestes quotes en el curt espai de temps de 5 i 3 mesos, respectivament, des de la seva creació.

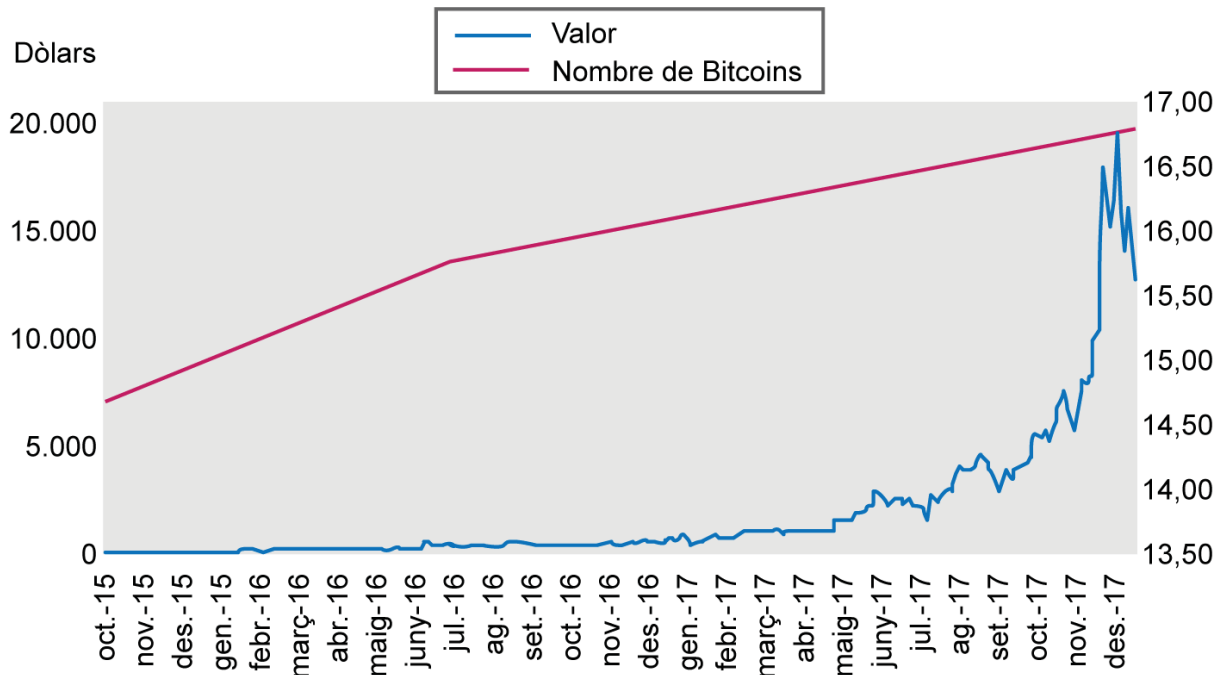
Les particularitats del Bitcoin en comparació de les monedes tradicionals i d'altres criptomonedes es poden resumir en els següents punts:

- No necessita un Banc Central: és una moneda electrònica, descentralitzada, suposadament anònima, no recolzada per cap govern o entitat legal. Les comprovacions les realitzen els usuaris de la xarxa Bitcoin.
- El procés d'emissió és automàtic, predictable i no està al servei de cap usuari privilegiat.
- El valor d'un Bitcoin és determinat pel mercat de divises mitjançant el seu ús.
- No es basa en béns materials, sinó en el valor que els individus li atorguen.

El procés de creixement del Bitcoin limitarà la seva oferta a uns 21 milions, la qual cosa, juntament amb la seva demanda creixent, fa que el seu valor s'hagi disparat en els darrers mesos. La seva cotització el 31 de desembre de 2017 era d'aproximada-

ment 14.000 dòlars per Bitcoin, i va arribar gairebé als 20.000 dòlars durant alguns dies del mes. El gràfic 5 mostra l'evolució temporal del valor del Bitcoin. Així doncs, l'oferta de Bitcoins no s'ajusta a la riquesa intercanviada per mitjà d'aquesta criptomoneda, sinó que estaria més a prop del concepte de metalls preciosos com l'or. fet que va portar algunes persones a definir el Bitcoin com l'or digital. (Popper, 2016)

Gràfic 5. Bitcoins: valor de mercat i nombre



Font: elaboració pròpia sobre la base de coingecko.com.

Conclusions i reflexions finals

La *blockchain* es podria definir com una tecnologia informàtica on un conjunt d'actors registren les transaccions efectuades entre usuaris. Com que és una xarxa descentralitzada, ningú pot, a priori, exercir cap tipus de control, i per tant ofereix la confiança necessària per a l'acceptació d'una criptomoneda. A més de ser el suport de processos econòmics i legals, la *blockchain* està creant noves professions (miners) i activitats econòmicament remunerades amb criptomonedes.

L'exemple més conegut i el referent del mercat de criptomonedes ha estat el Bitcoin, que, després d'un període d'incertesa i de dubtes després de la seva creació, a partir de 2013 ha iniciat una onada expansiva. En paral·lel, han aparegut noves monedes amb un intens creixement de la seva capitalització, cosa que ha fet que el Bitcoin perdi pes relatiu en el conjunt.

L'any 2017 ha estat crucial en el creixement i la consolidació d'aquest mercat, que ha expandit el valor de capitalització fins al mig bilió de dòlars, dominat pel Bitcoin, atès que representa pràcticament la meitat del mercat. No obstant això, després d'aquest fort creixement, es preveuen forts processos especulatius.

El Bitcoin està programat per arribar a un límit màxim d'unitats, entorn els 21 milions, la qual cosa condiciona el seu preu a l'alça als mercats, valor que en els últims tres mesos del 2017 s'ha multiplicat per 4 i ha arribat a assolir gairebé els 20.000 dòlars, per la qual cosa ha estat necessari fraccionar la moneda en unitats menors d'intercanvi (satoshi).

Per tant, cal preguntar-se si les criptomonedes estan en condicions de substituir, com a mínim a priori, el sistema de moneda tradicional basat en la participació d'un tercer (banc o banc central) capaç d'assumir una funció de regulador (Sandoval, 2017; ethereum.org, 2018). Alguns estats, com és el cas de Dinamarca, ja plantegen la retirada de la moneda tradicional i l'adopció d'aquest tipus de monedes, però sota la seva supervisió.

Els dos grans problemes als quals s'enfronta Bitcoin són la col·lusió dels miners i l'especulació. Si un grup majoritari de miners es possessin d'acord es convertiria la xarxa en el que podria denominar-se un «Banc Central Privat», cosa poc probable però possible. Els riscos d'especulació són evidents i deriven precisament del fet de no disposar d'una producció real que recolzi la criptomoneda: tal com ha sorgit podria desaparèixer. El ciutadà no especialitzat ja s'està interessant de forma creixent degut a aquest últim augment de preus, potser més amb finalitats especulatives que en l'ús en si d'aquesta moneda com a mecanisme de pagament (Arce Martínez, 2016; Asensio Grau, 2014; Elwell, Murphy i Seitzinger, 2013; Gallén, 2016; Grinberg, 2011; Gutiérrez Hernández, 2015; Europa Press, 2016; Unitat Editorial Informació Econòmica, 2017).

Com a anotació final, no hem d'oblidar que la forma de treball de la *blockchain* transcendeix a altres camps econòmics i del dret, ja que té el potencial de canviar en essència el teixit mateix de la nostra societat a nivell global. Pot fer això, per exemple, donant a milers de milions de persones l'accés a un sistema financer global i, a més, en l'aplicació de molts altres usos no financers encara desconeguts, però que estan sorgint en aquest mateix moment. (Popper, 2016).

Referències bibliogràfiques

- AMMOUS, S.H. (2016). «Blockchain Technology: What is it Good for?» [en línia]. [Data de consulta: 20 de maig de 2017] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832751>
- ARCE, D. (2016). «Transformación de la forma tradicional de banca hacia el mundo digital» [en línia]. [Data de consulta: 7 de juliol de 2017] <<http://repositorio.upct.es/handle/10317/5900>>
- ASENSIO, Y. (2014). «Bitcoin: La nueva moneda virtual que está revolucionando el mundo de las divisas digitales» [en línia]. [Data de consulta: 7 de juliol de 2017] <<http://repositori.uji.es/xmlui/handle/10234/112560>>
- ATENIESE, G.; MAGRI, B.; VENTURI, D.; ANDRADE, E. (2017). «Redactable Blockchain – or – Rewriting History in Bitcoin and Friends» [en línia]. [Data de consulta: 25 de juny de 2017] <<http://eprint.iacr.org/2016/757.pdf>>
- BACK, A. (2002). «Hashcash - A Denial of Service Counter-Measure» [en línia]. [Data de consulta: 25 de juny de 2017] <<http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.15.8>>
- BITCOIN.ORG (2011). «Bitcoin.org's Codebase» [en línia]. <<https://github.com/Bitcoin-dot-org/Bitcoin.org>>
- BRANDS, S.; CHAUM, D. (1993). «Distance-Bounding Protocols». *Advances in Cryptology – EUROCRYPT '93*. Berlin, Heidelberg: Springer Berlin Heidelberg, pág. 344-359 [disponible en línia]. [Data de consulta: 25 de juny de 2017] <http://link.springer.com/10.1007/3-540-48285-7_30>
- CHAUM, D.; BRANDS, S. (1997). «Minting» electronic cash». *IEEE Spectrum*. Vol. 34, núm. 2, pág. 30-34 [disponible en línia] [Data de consulta: 25 de juny de 2017]. ISSN 00189235. DOI 10.1109/6.570825. <<http://ieeexplore.ieee.org/document/570825/>>
- CROSBY, M. (2016). «BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review*. Núm. 2 [disponible en línia]. [Data de consulta: de 25 de juny 2017]. <<http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf>>
- ELWELL, C. K.; MURPHY, M. M.; SEITZINGER, M. V. (2013). «Bitcoin: Questions, Answers, and Analysis of Legal Issues». Congressional Research Service. Informing the legislative debate since 1914 [disponible en línia]. [Data de consulta: 7 de juliol de 2017] <<http://www.a51.nl/storage/pdf/R43339.pdf>>
- ETHEREUM.ORG (2018). «Ethereum» [en línia]. <<https://github.com/ethereum>>
- EUROPA PRESS (2016). «Santander y otros grandes bancos lanzan 'su Bitcoin' utilizando la tecnología blockchain». *elEconomista.es*. [en línia]. [Data de consulta: 7 de juliol de 2017]. <<http://www.eleconomista.es/empresas-finanzas/noticias/7782103/08/16/Economia-Santander-se-une-a-cinco-entidades-para-promover-el-uso-de-dinero-digital-entre-entidades-financieras.html>>

- GALLÉN, P. (2016). «¿Por qué están creando los bancos su propio 'Bitcoin'?» *El Mundo* [en línea]. [Data de consulta: 7 de juliol de 2017] <<http://www.elmundo.es/economia/2016/08/24/57bdc58746163fca1b8b457c.html>>
- GRINBERG, R. (2011). «Bitcoin: An Innovative Alternative Digital Currency». *Hastings Science & Technology Law Journal*. Vol. 4, pàg. 160 [en línea]. [Data de consulta: 7 de juliol 2017] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857>
- GUTIÉRREZ HERNÁNDEZ, P. (2015). «El Bitcoin ¿presente y futuro del dinero? : sus características e implicaciones» [en línea]. [Data de consulta: 7 de juliol de 2017] <<https://repositorio.comillas.edu/jspui/handle/11531/4523>>
- HARTIKKA, L. (2016). «Naivechain - a blockchain implementation in 200 lines of code» [en línea] <<https://github.com/lhartikk/naivechain>>
- IBM BLUEMIX (2017). «Blockchain basics». IBM Bluemix Docs [en línea]. [Data de consulta: 25 de juny de 2017] <https://console.bluemix.net/docs/services/blockchain/ibmblockchain_overview.html>
- KEHRLI, J. (2016). «Blockchain Explained». Netguardians [en línea]. [Data de consulta: 25 de juny de 2017] <<https://www.netguardians.ch/news/2016/11/17/blockchain-explained-part-1>>
- LEAL, A. (2017). «Banco Central Europeo define a blockchain como 'fuerza transformadora' financiera». Criptonoticias.com [en línea]. [Data de consulta: 3 de juliol de 2017] <<https://criptonoticias.com/bancos/banco-central-europeo-define-a-blockchain-como-fuerza-transformadora-financiera/#axzz4lkKrlFRL>>
- LEMIEUX, V. L. (2016). «Trusting records: is Blockchain technology the answer?» *Records Management Journal*. Vol. 26, núm. 2, pàg. 110-139 [en línea]. [Data de consulta: 24 de juny de 2017]. ISSN 0956-5698. DOI 10.1108/RMJ-12-2015-0042. <<http://www.emeraldinsight.com/doi/10.1108/RMJ-12-2015-0042>>
- NAKAMOTO, S. (2008). «Bitcoin: A Peer-to-Peer Electronic Cash System». Pág. 9 [en línea], [Data de consulta: 24 de juny de 2017] <www.bitcoin.org>
- PILKINGTON, M. (2015). «Blockchain Technology: Principles and Applications» [en línea]. [Data de consulta: 20 de maig de 2017] <https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660>
- POPPER, N. (2016). «Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money» [en línea]. [Data de consulta: 13 de desembre de 2017]. <<https://hrglkeyl.updog.co/aHJnbGxrZXIsMDA2MjMjUwWA.pdf>>
- RIVERO, J. (2017). «Banco Central de China abre Centro de Investigación de Monedas Digitales». Criptonoticias.com [en línea]. [Data de consulta: 3 de juliol de 2017]. <https://criptonoticias.com/bancos/banco-popular-china-centro-investigacion-monedas-digitales/#axzz4lkKrlFRL>
- SANDOVAL, J. (2017). «DECENT lanzó su plataforma blockchain para distribución de contenido audiovisual». Criptonoticias.com [en línea]. [Consulta: 3 de juliol]

- de 2017] <<https://criptonoticias.com/aplicaciones/decent-lanzo-plataforma-blockchain-distribucion-contenido-audiovisual/#axzz4lkKrIFRL>>
- STAHR, D. (2014). «Sledování obarvených Bitcoinů v transakčním grafu». dspace.cuni.cz [en línia]. [Data de consulta: 25 de juny de 2017]. <https://dspace.cuni.cz/bitstream/handle/20.500.11956/68852/BPTX_2013_1_11320_0_348269_0_142918.pdf?sequence=1>
- SWAN, M. (2015). «Blockchain : blueprint for a new economy» [en línia]. S.I.: O'Reilly Media. [Data de consulta: 20 de maig de 2017]. ISBN 9781491920473. <<http://www.goodreads.com/book/show/24714901-blockchain>>
- TORMEY, J. (2017). «Blockchain Wallet API V2». London: GitHub. 0.26.0. [en línia]. <<https://github.com/blockchain/service-my-wallet-v3>>
- UNIDAD EDITORIAL INFORMACIÓN ECONÓMICA (2017). «Bitcoin, ¿ganará el combate contra la banca española?» *Expansión* [en línia]. [Data de consulta: 7 de juliol de 2017]. <<http://www.expansion.com/promociones/native/2017/04/27/>>



José Miguel Domínguez Jurado
josemiguel.dominguez@uca.es
Professor titular d'Economia Aplicada
(Universitat de Cadis)

Doctor en Economia per la Universitat de Cadis. Màster en Impactes Territorials i Ambientals de la Globalització per la Universitat Internacional d'Andalusia. Llicenciat en Ciències Econòmiques i Empresariales per la Universitat de Màlaga. És professor d'Economia Aplicada i imparteix diverses assignatures relacionades amb l'Anàlisi Econòmica en estudis de grau i d'Economia Regional en estudis de màster oficial. Col·labora com a docent en programes per a alumnes d' universitats dels Estats Units en assignatures d'Economia Regional i Urbana. Ha sigut investigador principal de l'UCA en el projecte PRESPO de INTERREG de la Unió Europea, i ha participat en altres projectes d'àmbit nacional i internacional.



Ricardo García Ruiz

rgarciarui@uoc.edu

Professor col·laborador del Grau d'Informació i Documentació (UOC)

Doctor en Economia per la Universitat Internacional de Barcelona. Màster en Societat de la Informació i del Coneixement per la UOC. Enginyer Informàtic per la UOC. Màster en Tècniques Avançades d'Estadística Aplicada per la UNED. Expert en Mètodes Avançats d'Estadística Aplicada per la UNED. Actualment col·labora com a professor col·laborador en els estudis de grau d'Informació i documentació, en les matèries de *Big Data* i Minería de Dades.

Els textos publicats en aquesta revista estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement 3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los, comunicar-los públicament i fer-ne obris derivades sempre que reconegueu els crèdits dels obris (autoria, nom de la revista, institució editora) de la manera especificada pels autors o per la revista. La llicència completa és pot consultar a <http://creativecommons.org/licenses/by/3.0/es/deed.ca>.

