

**Carles Gallart Olivé
Gerard Marsal Figueres**

EL BITCOIN, INVERTIR O NO INVERTIR?

TREBALL DE FI DE GRAU

Dirigit pel Dr. Antonio Rodríguez Ramos

Grau de Finances i Comptabilitat



**FACULTAT D'ECONOMIA i EMPRESA
Universitat Rovira i Virgili**

Reus

8 de juny de 2018

Resum

Quan parlem del Bitcoin, no ens referim simplement a una criptomoneda, també engloba tot el sistema innovador que hi ha al seu darrere. El present estudi no només analitza la criptomoneda i el seu sistema operatiu, sinó que a més intenta aconsellar sobre la viabilitat de la inversió en Bitcoin. El projecte està estructurat en dos grans blocs, un de caire més teòric i l'altre més pràctic. En el primer bloc, es defineix el què és el Bitcoin i el que l'envolta, així com també els fonaments del seu sistema, el *blockchain*. A més, s'han comparat els avantatges i riscos d'aquesta criptomoneda i les diferències del Bitcoin amb el diner fiduciari. Pel que fa al bloc pràctic, s'ha estudiat la correlació del Bitcoin amb els principals índexs borsaris i també el binomi rendibilitat-risc, paràmetre molt important a l'hora de realitzar una inversió. Per acabar, a les conclusions finals es dona una resposta justificada al què es pregunta en el títol del projecte: invertir o no invertir en Bitcoin?

Paraules clau: *Bitcoin, criptomonedes, blockchain, volatilitat.*

Abstract

When we talk about Bitcoin, we don't simply refer to cryptocurrencies, it also includes all the entire innovative system behind it. The present study does not only analyze the cryptocurrency and its operating system, but also tries to give advice on the viability of investment in Bitcoin. The project is structured in two big blocks, one more theoretical and the other one more practical. In the first block, we define Bitcoin and what surrounds it, as well as the bases of its system, the blockchain. In addition, the advantages and risks of this cryptocurrency and the differences between Bitcoin and the fiduciary money have been compared. Regarding to the practical block, we have studied the correlation of Bitcoin with the main stock market indexes and also the return-risk binomial, a parameter that is very important at the time of making an investment. At the end, in the final conclusions we have given a justified answer to what is being asked in the title of the project: to invest or not to invest in Bitcoin?

Key words: *Bitcoin, cryptocurrencies, blockchain, volatility.*

Sumari

1. Introducció	5
1.1. Justificació del treball	5
1.2. Objectius del treball	6
1.3. Metodologia del treball.....	6
1.4. Estructura del treball	8
2. El Bitcoin	9
2.1. Concepte.....	9
2.2. Antecedents i fets rellevants	11
2.3. El Bitcoin i les altres criptomonedes	16
3. La tecnologia <i>blockchain</i>	19
3.1. Els fonaments de la tecnologia <i>blockchain</i>	19
3.2. La “mineria”	21
3.3. Emissió de Bitcoins.....	22
3.4. Operativa del <i>blockchain</i> dins del mercat Bitcoin.....	23
4. Bitcoin vs. Diner fiduciari	26
5. Avantatges i riscos del Bitcoin	28
5.1. Avantatges	28
5.2. Riscos operatius	30
5.3. Riscos del Bitcoin anunciats per les autoritats monetàries	31
6. Anàlisi quantitatiu	33
6.1. Anàlisi de la correlació	33
6.2. Binomi rendibilitat-risc.....	35
6.2.1. Rendibilitat logarítmica diària.....	35
6.2.2. Volatilitat diària.....	36
6.3. L’anàlisi tècnica: el “doble top”	38
7. Conclusions	41
8. Bibliografia	44

1. Introducció

1.1. Justificació del treball

El desenvolupament tecnològic i la globalització de tots els sistemes financers està comportant canvis d'importància en el dia a dia de la població d'arreu del món. Països desenvolupats i subdesenvolupats reben influència directa de nous elements i infraestructures intangibles que internet en fa possible la seva existència. Internet fa eliminar completament totes les barreres culturals i financeres, comunicant a temps real diferents punts del planeta.

Per aquest motiu, i per la part que ens toca, cal esmentar la versatilitat i eficiència que aporta internet dins del sistema financer mundial, on totes les transaccions que es duen a terme són registrades als servidors informàtics bancaris. No obstant això, un gran col·lectiu amb necessitat contractual amb els bancs, veuen la ineficiència que aquests creen amb els elevats costos de transacció i control dels seus clients. D'aquí sorgeix la creació de les monedes virtuals o criptomonedes, amb l'objectiu d'evitar l'ADN bancari, que no és més que guanyar diners aprofitant-se dels diners dels clients. És a dir, la creació de les criptomonedes té l'origen en la necessitat vigent de simplificar la manera d'intercanvi de transaccions monetàries sense dependre d'un tercer.

L'augment del valor del Bitcoin (a partir d'ara BTC) ve donat gràcies a que els compradors han vist una oportunitat senzilla i ràpida de guanyar diner fàcil només tenint en compte la revalorització del seu preu. D'aquesta manera, amb l'aparició de la criptomoneda i concretament, amb l'augment de la demanda del BTC, es crea un escenari econòmic i de gran influència social que, a dia d'avui, el Banc Central Europeu (a partir d'ara BCE) i la *Federal Reserve Bank of United States of America* (a partir d'ara FED) adverteixen de l'elevat risc que aquest actiu té incorporat.

La bombolla especulativa del BTC, com es sabut per la gran majoria de la població, segueix fluctuant a valors intrínsecs que la ment humana no pot raonar. La premsa i diaris d'arreu del món informen de les grans pujades i baixades que aquest actiu pateix dia a dia i molts especuladors novells es llencen a la compra sense coneixement del que realment és aquesta criptomoneda de moda.

Hem decidit escollir el BTC com a tema del nostre Treball de Final de Grau per tal de no cometre els mateixos errors i entendre el seu complex sistema operatiu. A més, ens ha motivat la realització d'aquest treball per comprovar si les notícies referents al BTC són

del tot certes o si realment són prediccions o hipòtesis amb interessos comuns al darere.

Des d'aquí, s'origina el punt de partida del present treball, amb l'interès i la motivació per analitzar exhaustivament el BTC i entendre tot el seu funcionament per tenir una visió i valoració crítica de totes les notícies i informació que avui en dia ens arriben d'arreu.

1.2. Objectius del treball

El present treball té com a objectiu estratègic realitzar un estudi exhaustiu del funcionament, operativa i evolució del valor de la criptomoneda virtual BTC, així com la influència que està generant actualment davant una economia i sistema financer globalitzat. Per assolir l'objectiu citat anteriorment, es definiran uns objectius secundaris que facilitaran el desenvolupament del treball:

- Definir i entendre el concepte de BTC.
- Analitzar el passat i l'evolució cronològica del BTC, així com el doini que té en el món de les criptodivises.
- Estudiar la complexitat del funcionament i negociació del sistema BTC sota el sistema de cadena de blocs o *blockchain*.
- Comparar el BTC amb el diner fiduciari i veure les divergències que tenen ambdós.
- Diferenciar i reconèixer els avantatges i riscos que presenta la inversió en BTC.
- Analitzar el binomi rendibilitat-risc del BTC.
- Respondre a la pregunta "*és el BTC un actiu potencialment adequat per incloure en una cartera diversificada?*"

1.3. Metodologia del treball

La metodologia emprada per al desenvolupament del present treball ha estat un procés en el qual s'han realitzat diverses tutories amb el tutor del treball de final de grau, el Dr. Antonio Rodríguez Ramos. Moltes d'elles aprofitant la flexibilitat que ens permet el correu electrònic i d'altres presencialment, ha estat de gran ajuda per tal d'orientar les pautes a desenvolupar i establir uns objectius acords amb el tema.

En la realització del treball, vam trobar un article d'opinió publicat el mes d'abril al *Diari de Tarragona* titulat "Las criptodivisas: mas allà del Bitcoin" i escrit pel Dr. Aurelio Fernández Bariviera, professor de la Facultat d'Economia i Empresa de la universitat. Vam contactar amb ell per tal de concertar una reunió i, així, saber quina és la seva opinió respecte el BTC i les criptomonedes en general. Gràcies als seus consells, vam dissenyar correctament tota la part quantitativa i d'anàlisi numèriques, proporcionant-nos, a més, diferents articles i pàgines web que han estat molt útils per tal de realitzar una anàlisi exhaustiva.

Per tal de realitzar tota la part més qualitativa i conceptual, s'han consultat llibres especialitzats de tots els àmbits del BTC. Concretament, hem seleccionat documents des de diferents punts de vista, ja que quasi bé cada llibre ha estat enfocat cap a un gran apartat, com són el funcionament del *blockchain* i tota la seva operativa o com tot el marc conceptual i fonamental del BTC.

A més, per tal de contrastar l'evidència de la informació, s'ha complementat aquesta amb articles i publicacions extretes de les bases de dades adquirides per la Universitat Rovira i Virgili. També, per tal de consultar les opinions d'organismes internacionals i membres representants d'autoritats monetàries, s'han consultat articles específics en matèria econòmica tant de premsa com de revistes.

Per l'anàlisi quantitativa, s'han extret totes les cotitzacions de la pàgina web Investing, la qual és considerada fiable i de prestigi. Per fer l'anàlisi i la seva posterior interpretació, s'han utilitzat moltes fórmules i conceptes emprats durant el grau. És més, conseqüentment a aquesta anàlisi, s'han extret diversos gràfics d'elaboració pròpia per facilitar la comprensió de la informació. Per fer aquesta anàlisi, s'han limitat les dates de la cotització de tots els instruments financers que s'han estudiat, prenent com a data d'inici el 30 d'abril de 2013 i de final el 30 d'abril de 2018.

Finalment, per tal de citar i referenciar correctament totes aquestes fonts, hem estat assessorats per Sra. Inmaculada Gámez Candela, bibliotecària del Centre de Recursos per a l'Aprenentatge i la Investigació (CRAI) de la universitat. Gràcies a la seva ajuda i els seus coneixements tant en matèria de citar i referenciar com en la recerca d'informació, ens ha estat molt més fàcil l'obtenció i consulta de llibres i articles com l'elaboració de la bibliografia.

1.4. Estructura del treball

Pel que fa al treball com a tal, aquest està compost per dos grans blocs: una anàlisi de caire més qualitativa i una de més quantitativa.

Per una banda, l'anàlisi qualitativa té com a objectiu donar a entendre conceptualment el BTC i els fets més importants que li han fet adquirir cert renom, així com tot el seu famós sistema operatiu, conegut com a *blockchain*. A més, s'analitza la quota de mercat de les principals criptomonedes, focalitzant l'anàlisi en la criptodivisa BTC. També, es compara la criptodivisa en qüestió vers el diner fiduciari, per tal d'observar les seves divergències. Per finalitzar aquest gran bloc, es citen i es justifiquen els avantatges i els riscos que suposa invertir en BTC.

D'altra banda, l'anàlisi quantitativa és un estudi de caire numèric, on es busca respondre la pregunta proposada als objectius. Per fer-ho, s'analitza des d'una vessant pròpia la correlació entre el BTC i els principals índexs borsaris, així com el binomi rendibilitat-risc de la criptodivisa. Finalment, des d'un punt de vista xartista s'explica el gràfic de preus del BTC.

Finalment, amb tota la informació ja analitzada, s'extreuen unes conclusions d'acord amb els objectius proposats, comparant també la percepció personal inicial i final del BTC.

2. El Bitcoin

2.1. Concepte

El BTC és una moneda virtual, de les conegudes com criptomonedes, que permet realitzar transaccions entre els usuaris sense necessitat de dependre d'una administració o institució per emetre-la, processar les seves transaccions, ni emmagatzemar la informació de les comptes (Martín Fernández, 2015, p. 17).

El propòsit d'aquesta moneda virtual/digital és l'eliminació dels intermediaris en el tràfic mercantil, ja siguin financers, bancaris o d'asseguradores, i l'autonomia davant el monopoli de les autoritats bancàries centrals. En definitiva, busca ser un sistema de "persona a persona" a través d'internet emparada en la distribució d'un software lliure. Quan afirmem això, ens referim a què l'absència d'intermediació entre les parts proposa un sistema d'intercanvi monetari descentralitzat, independent de qualsevol autoritat central (com el BCE o la FED), públic i aliena a la voluntat de les parts. D'aquesta manera, el sistema Bitcoin és una xarxa completament distribuïda en la que el protagonisme total de les transaccions resideix en els usuaris i no en els intermediaris (Rosembuj, 2015, p. 17).

Les propietats més importants del sistema BTC són les següents:

- **El seu codi és obert (software lliure):**

Aquest codi utilitza llicència del MIT (*Massachusetts Institute of Technology*), la qual no té copyright. Aquesta llicència permet utilitzar, copiar, modificar i distribuir les modificacions lliurement i que qualsevol interessat pugui examinar el codi, participar en el desenvolupament del BTC o, fins i tot, crear la seva pròpia moneda virtual basant-se en aquesta. De fet, el BTC no és l'única criptodivisa que és coneix i s'utilitza, n'hi ha moltes més (en el subapartat 2.3. El Bitcoin i les altres criptomonedes s'analitza en més detall la relació del BTC amb aquestes altres criptomonedes).

Que el codi font d'aquesta criptodivisa estigui disponible per a qualsevol persona és realment important i aporta transparència al sistema, la qual cosa és fonamental per obtenir la confiança de nous usuaris, empreses i, fins i tot, governs. D'aquesta manera s'elimina la necessitat de confiar en un tercer, al contrari d'empreses privades del món de les noves tecnologies com Apple o Windows, les quals el codi dels seus productes no està disponible ni es pot consultar i els seus

usuaris no tenen altre remei que confiar que no hi hagi males praxis. Un altre avantatge és que elimina una de les majors preocupacions de moltes persones que no confien del tot amb el sistema BTC, ja que pensen que, al tractar-se d'una cosa intangible com un codi informàtic, pot ser fàcilment manipulable i convertir-se en una estafa.

El codi BTC no és inalterable, sinó que està en continu desenvolupament, rebent constants canvis i actualitzacions que serveixen per a millorar la seguretat, fiabilitat i funcionament del sistema. D'aquesta forma, com major sigui el número de persones que s'involucren en el desenvolupament del BTC, és més ràpida i eficaç la detecció d'errors o vulnerabilitats (Martín Fernández, 2015, p. 25).

- **Descentralitzat:**

No hi ha una administració o institució encarregada d'emetre BTCs, controlar les transaccions i emmagatzemar la informació dels comptes, sinó que es fa de manera distribuïda per persones de tot el món.

D'aquesta tasca s'encarrega l'anomenada "minería" i feta per les persones anomenades "miners", repartits pel planeta, que posen a disposició del sistema BTC els seus ordinadors i recursos. Tot el procés de la "minería" i de creació de BTCs està explicat en els subapartats 3.2. La "minería" i 3.4. Operativa del blockchain dins del mercat Bitcoin respectivament (Martín Fernández, 2015, p. 22-23).

- **Anonimat:**

El sistema BTC permet que les transaccions siguin anònimes, preservant la identitat d'aquelles persones que vulguin romandre en l'anonimat. Tota la informació dels comptes del sistema BTC s'emmagatzema en el que s'anomena *blockchain* (explicat en profunditat en l'apartat 3. La tecnologia blockchain). Aquest anonimat genera controvèrsia. D'una banda, limita el control dels estats, ja que els ciutadans, si la moneda del país és objecte de contínues devaluacions poden refugiar-se en el BTC. D'altra banda, certes persones afirmen que el sistema BTC és aprofitat per a realitzar activitats il·legítimes, com el blanqueig de capitals (s'ha aprofundit més en aquest tema en el subapartat 2.2. Antecedents i fets rellevants) (Martín Fernández, 2015, p. 27).

S'ha de fer una distinció bàsica entre l'anonimat i la privacitat en el context de les transaccions financeres. S'anomena una "transacció anònima" quan ningú sap qui ets i s'anomena una "operació privada" si el què compres i la quantitat pel què ho compres ens es desconegut. Podem afirmar, doncs, que les transaccions

amb BTC són anònimes, però no privades, ja que les identitats no es registren enlloc, però cada transacció realitzada és visible en el *blockchain*, que ve a ser el llibre electrònic de comptabilitat públic (Rodríguez Herrera, 2014).

- **Deflacionista**

El sistema BTC és un sistema monetari deflacionista, ja que l'emissió global està limitada de BTCs a 21 milions d'unitats. Podem dir que el BTC sigui deflacionista significa que és un bé escàs i, com passa amb l'or, un bé escàs farà que aquest tingui el que anomenem valor per ser precisament escàs. Si no ho fos, es podrien crear BTCs de forma ininterrompuda i aleatòria i això faria que mai arribés a tenir el valor que té avui en dia. Aquest raonament està explicant en detall en el subapartat 3.3. Emissió de Bitcoins (Martín Fernández, 2015, p. 17).

Aquestes són les propietats més importants que, actualment, podem afirmar d'aquest nou actiu financer tant atractiu que, cada cop més, té més importància en el món financer. Tot i així, no hem de deixar de qüestionar-nos si aquesta criptodivisa és realment com els seus creadors afirmen, ja que, com veurem en el següent apartat, el sistema BTC ha patit diversos atacs i males praxis que han fet disminuir la confiança d'aquest nou actiu financer.

2.2. Antecedents i fets rellevants

El BTC ha evolucionat molt des dels seus inicis. Tot i que fa només 9 anys des de la seva creació, aquesta criptomoneda ha guanyat rellevància en el món econòmic i financer, passant de ser un actiu completament desconegut i sense saber ben bé del cert el què era exactament a estar en boca de tothom i ser un dels actius que més se'n parla. Diaris especialitzats en economia o no, informatius de televisió, articles en revistes rellevants i un llarg etcètera de mitjans s'han fet ressò del BTC, o el què també s'anomena avui dia, "l'actiu financer de moda".

El BTC apareix per primera vegada a l'octubre de 2008 en una publicació d'un article firmat pel nom japonès Satoshi Nakamoto. Aquest article detalla el funcionament de la criptomoneda, així com les bases i normes d'aquesta (com per exemple, que està limitada a l'emissió global de només 21 milions d'unitats). No se sap realment qui s'amaga sota aquest pseudònim, si és una única persona o varies. El què sí que se sap és que, el 3 de gener de 2009, Nakamoto fou l'encarregat de crear el primer bloc minat de BTC.

Aquest primer bloc va donar una recompensa de 50 BTCs (agafant com a referència el valor del BTC a 30 d'abril de 2018 serien uns 460.000\$). Nakamoto ja no continua desenvolupant aquest sistema, ja que poc després de crear aquesta tecnologia va decidir llegar a un grup d'experts informàtics el desenvolupament de la xarxa BTC, entre els quals l'actual desenvolupador Gavin Andresen (Urquhart, 2018).

Des d'aquest moment, aquesta tecnologia, eina financera, criptomoneda o, fins i tot, ideal, no ha fet més que créixer, deixant atònits als seus detractors i confirmant alguns dels pronòstics més ambiciosos dels seus promotors.

Molt ha passat en l'ecosistema *blockchain*, doncs el BTC ha estat el causant i impulsor de l'aparició de centenars de criptomonedes. Aquestes intenten arravatar el lloc per ser la criptomoneda número 1, però, si parlem en termes financers, el BTC es nega a cedir. Totes tenen diferents fortalezes, capacitat i aplicacions, però totes elles comparteixen la inspiració que els hi donà el BTC per a desenvolupar els seus projectes, basats en la descentralització i el concepte *peer to peer* (explicat en més detall en el subapartat 3.4. Operativa del blockchain dins del mercat Bitcoin).

Un com explicat l'inici del sistema BTC, a continuació s'explica quins han estat els fets més rellevants i l'evolució que ha portat al BTC de passar de ser un desconegut a tenir el renom internacional d'avui en dia. Per facilitar la comprensió de l'evolució, hem inserit la gràfica on es veu la variació del preu del BTC.

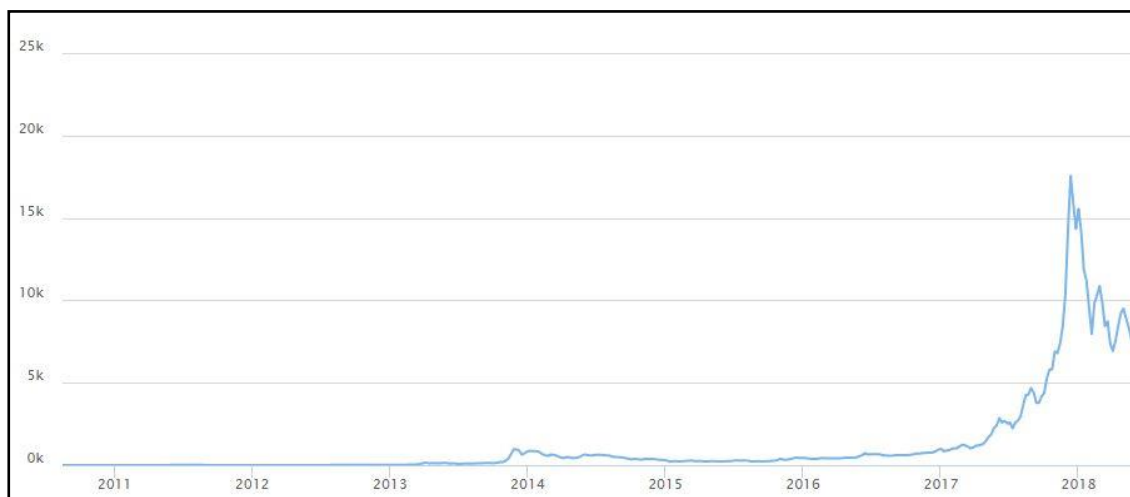


Figura 1. Evolució de la cotització del BTC. Extret de (Buy Bitcoin Worldwide, 2018)

Els antecedents ordenats cronològicament són:

- **Any 2010:**
 - Primera compra feta amb BTC al maig. Concretament fou una pizza per un valor de 10.000 BTCs (Sala, 2017).

- Es crea la primera casa de canvi el 17 de juliol, Mt.Gox, que permet per primer cop canviar de BTC a dòlars i viceversa (Martín Fernández, 2015, p. 17).
- El 15 d'agost es descobreix una vulnerabilitat greu en el protocol BTC i es generen 184.000 milions d'unitats en una sola transacció. La transacció es va detectar al cap de poques hores i es va decidir fer una bifurcació forçada del *blockchain* per a deixar de banda la cadena errònia i crear una nova xarxa per a continuar amb el projecte. Fins a dia d'avui, aquesta vulnerabilitat ha estat la més greu que ha patit mai el sistema BTC (Esparragoza, 2018).
- **Any 2011:**
 - Durant el mes de febrer, el BTC aconsegueix la paritat amb el dòlar americà.
 - La prestigiosa revista Forbes publica un article titulat "Crypto Currency", on parla per primer cop del BTC (Greenbert, 2011).
 - El juny l'organització WikiLeaks comença a acceptar donatius realitzats amb BTC, ja que un any abans les plataformes per a pagar a través d'internet com PayPal o les marques de targetes amb pagament via internet com Visa i Mastercard van bloquejar les transaccions cap aquesta organització gràcies a les pressions de les autoritats dels Estats Units. L'octubre de 2017, el fundador de WikiLeaks va revelar que l'organització ha guanyat un 50.000% de rendiment durant 6 anys des de l'inici de les donacions via BTC (Kharpal, 2017).
- **Any 2012:**
 - Comencen a sorgir diferents proveïdors que accepten el sistema BTC com a mitjà de pagament. És per això que és crea la Fundació Bitcoin, que té com a missió la promoció i estandardització de la moneda (The Bitcoin Foundation, 2016).
 - Durant el mes d'octubre, el BCE es fixa en el BTC i arriba a la conclusió que les monedes virtuals podrien tenir un impacte negatiu en la reputació dels bancs centrals si el seu ús creix considerablement i que aquest risc ha de ser considerat a l'avaluar la situació general de risc dels bancs centrals (Europe Central Bank, 2012)
- **Any 2013:**
 - Es crea el primer caixer de BTC del món creat per l'empresa Robocoin, situat a una cafeteria de Vancouver al Canadà. Actualment, hi ha uns 2.020 caixers automàtics operatius de BTC arreu del món (AFP, 2013).
 - Durant el mes d'octubre, el *Federal Bureau of Investigation* (FBI), la *Drug Enforcement Administration* (DEA) i altres agències estatals dels Estats Units van posar en marxa un operatiu per tancar el mercat negre cibernètic anomenat Silk Road, on es podia comprar i vendre armes, drogues i altres productes il·legals. En aquest operatiu, es van confiscar prop de 26.000 unitats de BTC, fet que va provar la teoria que el sistema BTC és un refugi per les

activitats il·lícites com la compra-venda d'armes, drogues o com el blanqueig de capitals (Leinwand Leger, 2014).

- A finals d'any, el preu unitari del BTC supera la barrera dels 1.000\$ i s'equipara al preu de l'unça d'or. Però l'anunci per part del Banc Popular de la Xina, el banc central xinès, de que els bancs xinesos no poden comerciar amb el sistema BTC, va comportar una ràpida baixada de la cotització fins els 600\$ per unitat de BTC (El Economista.es, 2013)
- **Any 2014:**
 - A principis d'any, Mt.Gox, la casa de canvi més important i la que gestionava el 70% dels intercanvis BTC-dòlars en aquell moment, suspèn les retirades tant de BTC com de dòlars degut a un atac informàtic. Tot i que encara està sota investigació, la companyia afirmà que es van perdre uns 750.000 BTCs dels clients de la casa de canvi i vora uns 100.000 de la pròpia empresa, en total, més del 7% de la totalitat dels BTCs. Aquest robatori, va significar aleshores una pèrdua d'uns 473 milions de dòlars d'aleshores i una caiguda de la cotització del BTC situant-se per primera vegada per sota d'altres plataformes, com per exemple el Bitsamp (Pollock, 2018).
 - A finals d'any, l'empresa tecnològica Microsoft va anunciar l'acceptació de BTCs com a mètode de pagament pels seus continguts oferts en les botigues en línia dels seus productes Windows, Windows Phone i Xbox. Les transaccions es realitzen a través de BitPay, la plataforma de servei de pagament de BTCs més important del món. Des d'aleshores, Microsoft ha estat al capdavant de les grans corporacions multinacionals que han donat suport i a l'acceptació del BTC com a mètode de pagament, fet que ha creat més confiança cap a la criptomoneda (Chansanchai, 2014).
- **Any 2015:**
 - A inicis d'any, el banc del Regne Unit Barclays es va convertir en el primer banc comercial britànic en acceptar BTCs. Aquesta estratègia formava part del pla per facilitar als usuaris a fer donacions caritatives utilitzant la criptografia fora dels seus sistemes. Concretament, es van associar al sistema BTC durant el mes d'abril amb la *startup* de pagaments via telèfon mòbil *Circle Internet Finacial* (Gautham, 2016).
 - A partir de l'agost, s'estima que prop de 160.000 comerciants d'arreu del món accepten pagaments en BTCs.
- **Any 2016:**
 - A inicis del mes de març, el Gabinet del Japó (la branca executiva del govern de Japó) va aprovar una sèrie de lleis referides a la regulació de les criptomonedes i l'ús de la tecnologia financera en el país. Aquestes lleis bàsicament han permès tractar al BTC i a la resta de criptomonedes de la mateixa forma igualitària que les monedes fiduciàries, sent així el Japó el primer país a reconèixer el BTC com a tal (Kyodo, 2016).

- A finals d'any, els Ferrocarrils Federals de Suïssa van actualitzar totes les seves màquines automàtiques de venda per a poder comprar bitllets de tren amb BTCs des del telèfon mòbil. Aquesta estratègia forma part d'un experiment de dos anys de durada per avaluar l'acceptació de la criptomoneda per part del ciutadà suís (Schweizerische Bundesbahnen, 2017).

A grans trets, aquesta ha estat l'evolució del sistema BTC des del seu inici fins a principis de l'any 2017. Durant tots aquests anys, la cotització del BTC ha augmentat de manera progressiva, arribant a cotitzar i establir-se al voltant dels 1.000\$.

Però arribats en aquest punt, des de mitjans de 2017 s'ha produït un gran augment del seu valor en els mercats internacionals. L'agost de 2017, la cotització del BTC va arribar per primera vegada a superar els 3.000\$. A partir d'aquest moment, el valor del BTC ha augmentat de forma exponencial i de manera molt més pronunciada en un període molt curt. Això és degut a les especulacions que va haver a final de 2017 pel que fa a la creació de futurs del BTC (Pozzi, 2017).

Aquesta especulació va acabar quan, a inicis de desembre de 2017, el *Chicago Mercantile Exchange Group*, el mercat de futurs i opcions més antic del món, va estrenar contractes de futurs del BTC. Això va causar un increment de valor espectacular on en dues setmanes la cotització quasi es va arribar a duplicar, ja que en data 1 de desembre de 2017 la cotització del BTC era de 10.869\$ i en data 16 de desembre del mateix any va arribar al seu màxim històric de 19.187\$ (Doncel & Pozzi, 2017).

A partir d'aleshores, la cotització del BTC ha anat disminuint de forma gradual. A data 30 d'abril de 2018, el preu de tancament ha estat 9.240\$. Tot i així, el BTC ha experimentat petits pics, però en general, des del seu punt màxim, la tendència ha sigut sempre a la baixa. Aquesta baixada va ser deguda a les vendes massives que hi van haver just després que s'assolís el màxim històric com a conseqüència de les declaracions per part de Xina, Japó i Corea del Sud (les quals deien que es prohibiria l'ús de la criptomoneda) i les futures investigacions per part de les autoritats de França i Estats Units per a coordinar una regulació del mercat de les criptomonedes (Reuters, 2018).

És per això que molts experts s'han arriscat a afirmar que el BTC és una bombolla que ja ha estallat i que tothom corre per vendre i, fins i tot, el gegant americà *Bank of America Merrill Lynch* s'ha atrevit a dir que el BTC és la major bombolla especulativa de la història, sent molt més gran que la bombolla de les tulipes a l'Holanda del segle XVII (El Economista.es & Bloomberg, 2018).

2.3. El Bitcoin i les altres criptomonedes

Tal i com s'ha comentat a l'apartat anterior, el BTC va ser la primera criptomoneda en aparèixer, tot i que no va estar sola en el món de les criptomonedes durant massa temps. Ràpidament van aparèixer noves criptomonedes, les quals totes elles comparteixen la filosofia del BTC, però amb peculiaritats operatives diferents.

Parlar de criptomonedes i enumerar-les totes ens portaria a fer un treball completament nou. Actualment hi ha més de 1.630 criptomonedes registrades i totes elles cotitzant, però, a data 30 d'abril de 2018, quasi el 70% de la quota de mercat només la tenen 5 d'aquestes criptodivises. Aquestes són l'esmentat BTC, amb un 36,72%, l'Ethereum (a partir d'ara ETH), amb una quota de mercat del 15,67%, el Bitcoin Cash (EBCH), amb el 5,59% del total de les criptomonedes, el Litecoin (LTC), amb el 1,97%, i la criptomoneda Ripple (XRP), amb el 7,76%.

Per tal de facilitar-ne més la comprensió, s'adjunta la gràfica següent:

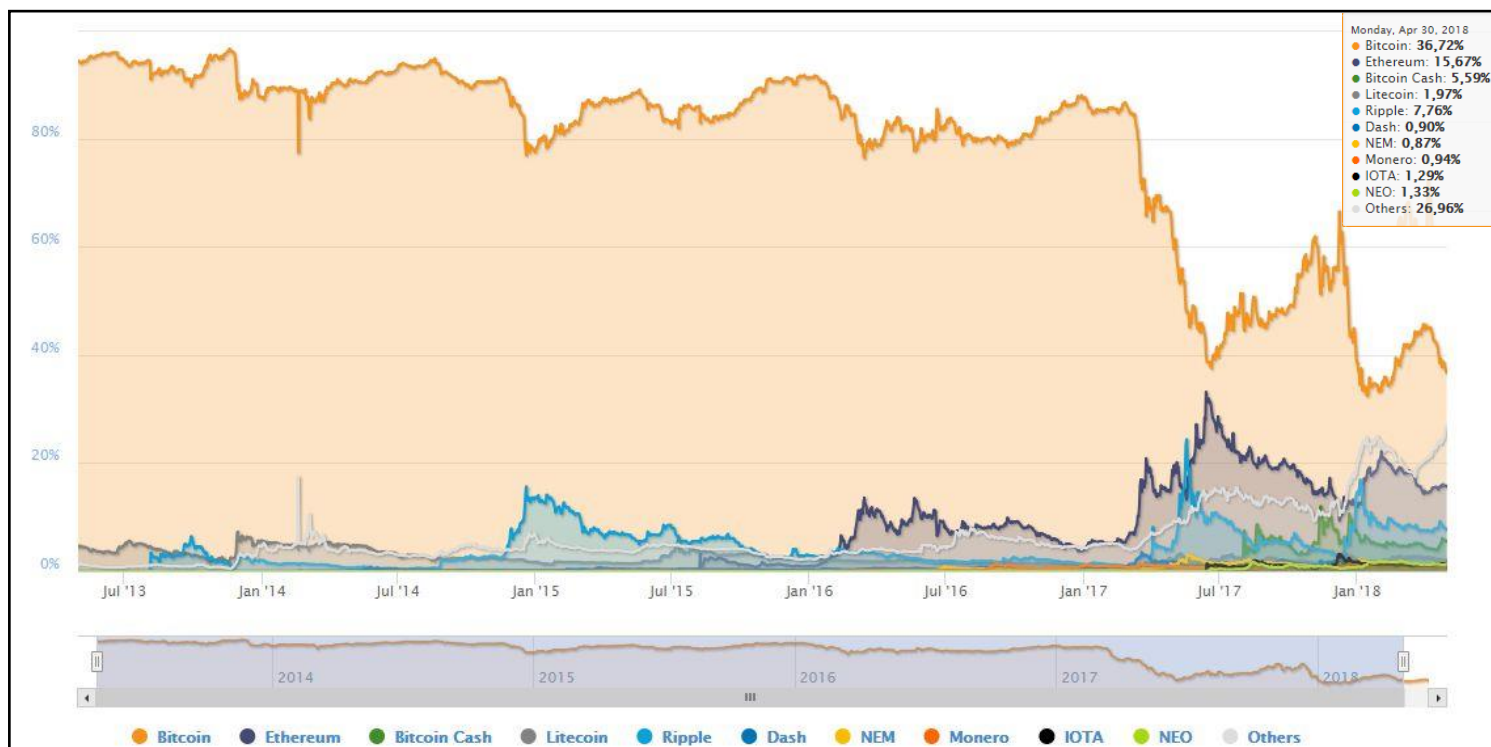


Figura 2. Percentatge de capitalització total de mercat (domini). Extret de (CoinMarketCap, 2018)

Aquesta gràfica mostra la quota de mercat que ha tingut cada criptomoneda en les dates compreses entre el 30 d'abril del 2013 i el 30 d'abril de 2018. El domini que té i ha tingut el BTC. Com es veu a la llegenda, es mostren 11 valors, dels quals 10 són criptomonedes com a tals i l'11è valor és la suma de la resta de criptomonedes (vora 1.620). Per tant, es pot comprovar que, pel que fa a quota de mercat, hi ha moltes criptomonedes

que la seva representació és pràcticament nul·la pel que fa a les criptomonedes principals. Aquestes són les que hem esmentat abans, les quals quasi tenen el 70% de la quota de mercat total.

Dins d'aquestes criptodivises més rellevants, la que sempre ha tingut el domini sobre les altres ha estat el BTC. Com es veu a la gràfica, no sempre ha tingut la mateixa. A l'inici del sistema BTC, aquest sempre ha tingut entre el 80% i 90%, molt superior que la resta. Això es degut a què sempre s'ha parlat del BTC, des de l'inici de la criptografia i tecnologia digital. Arran del BTC, se n'han creat d'altres que, poc a poc, han anat guanyant quota de mercat.

La davallada més important que ha patit el BTC va ser entre els primers sis mesos de 2017. El gener de 2017 seguia per sobre del 80% de la quota de mercat, però al juliol del mateix any va desplomar-se per sota del 40%. Aquesta davallada s'explica ja que les altres criptomonedes han anat agafant protagonisme, ja sigui perquè s'han començat a conèixer per un públic no tant especialitzat o per culpa de l'augment de valor del seu preu de mercat i el nombre de transaccions realitzades. Un exemple clar és el de l'ETH, el qual a data 1 de gener de 2017 la seva cotització rondava els 8\$/unitat i sis mesos després va arribar a quasi els 400\$/unitat (Rodríguez, 2017).

Arran dels rumors de la sortida de futurs en els últims mesos de 2017, el BTC va tornar a guanyar domini gràcies a l'especulació dels inversors. El desembre de 2017 es va situar per sobre del 60% de la quota de mercat, moment que coincideix justament amb la màxima cotització que ha tingut el BTC. Tot i així, com s'ha vist en la gràfica de l'evolució del valor, just després d'assolir el màxim històric el valor del BTC ha patit una davallada gradual tenint una tendència baixista. Aquest fet es pressuposa que té una correlació directa amb la disminució del domini que ha patit en les mateixes dates.

Una altra hipòtesi que explica aquest fet, ha estat el factor psicològic dels inversors. Després de les notícies de finals de desembre de 2017 dels països on les criptomonedes tenen major acceptació, com són la Xina, el Japó i Corea del Sud, la tendència es va revertir a baixista just després del màxim històric amb un vendes massives en pocs dies. En veure el possible esclat de la bombolla del BTC, el domini es va veure afectada en benefici de les altres criptomonedes, les quals van guanyar quota gràcies a la seva baixa cotització de mercat en comparació al BTC i als possibles inversors que venien de tenir en cartera BTCs.

El Bitcoin, invertir o no invertir?

Carles Gallart i Gerard Marsal

Per acabar, després de tota la informació recopilada, plantejem que en un futur a mig termini moltes de les criptomonedes actuals que estan cotitzant al mercat, però que tenen una quota d'aquest quasi bé nul·la, desapareixeran. Com s'ha observat, de les més de 1.630 criptomonedes, només 5 d'aquestes tenen quasi el 70% de la quota, per tant, és ineludible pensar que aquestes i algunes més es mantindran en el futur.

3. La tecnologia *blockchain*

Per tal d'entendre el funcionament i la negociació del BTC és de vital importància analitzar el sistema en que està basat tota la seva operativa de negociació i compra-venta. Molts professionals en la matèria, afirmen la gran eficiència que pot aportar al sistema econòmic mundial i molts llibres escrits per experts el comparen amb els avenços com van ser l'emmagatzematge al núvol, les xarxes socials o el correu electrònic.

3.1. Els fonaments de la tecnologia *blockchain*

La tecnologia *blockchain* va sorgir el 2008 com l'arquitectura que va permetre la creació de la moneda virtual BTC. No obstant això, en els últims anys l'ús d'aquesta tecnologia s'està implantant molt més enllà del BTC i la resta de criptodivises (Fernández, 2018).

Una *blockchain* és una base de dades que es troba distribuïda entre diferents participants, protegida criptogràficament i organitzada en blocs de transaccions relacionats entre sí matemàticament. És a dir, és una base de dades descentralitzada que no pot ser alterada. Un element molt important a tenir en compte és que, per definició, es tracta d'un sistema que permet a parts que no confien plenament unes amb les altres, mantenir un consens sobre l'existència, l'estat i l'evolució d'una sèrie de factors compartits. Per aquest fet, el consens és precisament la clau d'un sistema *blockchain*, ja que es el fonament que permet que tots els participants puguin confiar en la informació que es troba gravada en ell. La informació que conté la cadena de blocs és totalment transparent i totalment pública, de manera que qualsevol individu la pot consultar fàcilment en plataformes com l'oficial del *blockchain* entre d'altres, i observar aspectes com el saldo que té un compte del qual conec la seva direcció o l'última transacció que s'ha produït (Preukschat, 2017, p. 23-24).

Aquest sistema basat en la confiança i el consens es construeix a partir d'una xarxa global d'ordinadors que gestionen una gegantesca base de dades. Concretament, consisteix en un conjunt d'apunts que estan en una base de dades compartida online, la qual es registren per mitjà de codis les operacions, quantitats, dates i participants. Tal com hem comentat, a l'utilitzar claus criptogràfiques i estar distribuït per molts ordinadors, presenta avantatges en seguretat davant manipulacions. Per incloure un exemple, si es volgués realitzar intencionadament una modificació en una de les còpies, no seria

viable perquè s'ha de realitzar el canvi a totes les còpies al ser una base oberta i pública (Martín Fernández, 2015, p. 22).

Per tal d'aconseguir l'eficiència ja esmentada, una *blockchain* es compon de tres parts que, combinades i integrades, compleixen el seu propòsit:

- **La criptografia:**

Com a tal, entenem com un procediment que, utilitzant un algoritme amb clau xifrada, transforma un missatge sense atendre la seva estructura lingüística, de tal forma que sigui incompreensible a tota persona que no tingui la clau secreta de l'algoritme empleat. Al *blockchain*, la criptografia té la responsabilitat de proveir un mecanisme infal·libre per la codificació segura de les regles del protocol que regeix el sistema. És també fonamental per evitar la manipulació, robatori o introducció errònia d'informació a la cadena de blocs, així com la responsable de generar firmes i identitats digitals encriptades (Preukschat, 2017, p. 26).

- **La cadena de blocs:**

És la base de dades dissenyada per l'emmagatzematge dels registres realitzats pels usuaris. Totes les *blockchains* han d'actuar sota les mateixes regles o protocol per donar validesa a un bloc i, d'aquesta manera, incorporar-lo a la cadena de blocs. Una vegada realitzada l'activitat, la cadena continuarà amb l'emissió del següent bloc, sent inalterable la informació registrada per mitjà de la criptografia. Aquest funcionament, elimina la necessitat d'un tercer de confiança. La cadena de blocs és emmagatzemada per totes les computadores que componen la xarxa BTC, cosa que es tracta d'un gran avantatge ja que no es depèn només d'una màquina i, en el supòsit de que alguna d'elles deixés de funcionar, sempre n'hi hauria d'altres disponibles (Preukschat, 2017, p. 26).

- **Un consens:**

Tal com hem comentat, es tracta d'una part imprescindible entre els usuaris de la *blockchain*. Aquest consens se sustenta en un protocol comú que verifica i confirma les transaccions realitzades i assegura la irreversibilitat d'aquestes. D'igual manera, aquest consens ha de proporcionar a tots els usuaris una còpia inalterable i actualitzada de les operacions realitzades a la *blockchain* (Preukschat, 2017, p. 27).

3.2. La “mineria”

Una de les característiques principals del BTC és que no hi ha una administració o institució centralitzada encarregada d'emetre, controlar les transaccions i emmagatzemar la informació dels comptes, sinó que es fa, de manera distribuïda per persones d'arreu del món. D'aquestes tasques, s'encarrega la “mineria”, dutes a terme per persones anomenades “miners”, repartits pel món, que posen a disposició del sistema BTC, el poder computacional de les seves màquines i ordinadors (Martín Fernández, 2015, p. 22).

La “mineria”, és un sistema de consens distribuït que s'utilitza per confirmar les transaccions pendents de ser incloses a la cadena de blocs. Entre les seves funcions trobem: la protecció de la neutralitat de la xarxa, complir un ordre cronològic a la cadena de blocs i permetre un acord entre tots els equips sobre l'estat del sistema. Per la confirmació de les transaccions, aquestes hauran de ser incloses a un bloc que s'ajusti estrictament a les normes de xifrat i que serà verificat per la xarxa. Aquestes normes, bàsicament eviten que qualsevol bloc anterior es modifiqui, ja que de fer-ho, invalidaria tots els blocs següents. Així mateix, la “mineria” també crea l'equivalent a una distribució aleatòria que evita que qualsevol persona pugui incloure nous blocs consecutius a la cadena. D'aquesta manera, cap persona pot controlar el que està inclòs en la cadena de blocs o substituir parts de la cadena per a revertir les seves pròpies despeses (Rosembuj, 2015, p. 23-25).

La pregunta que sorgeix després d'entendre les tasques dels “miners” és: per què algú posa a disposició de la xarxa BTC el seu ordinador? La raó és que el sistema proporciona una sèrie d'incentius, en forma de BTCs als “miners” (Martín Fernández, 2015, p. 22-23).

En concretament, els “miners” són els encarregats d'emmagatzemar la comentada cadena de blocs, de tal manera que cadascun d'ells emmagatzema una còpia completa i la va actualitzant, agregant nous blocs. Així mateix, el procés que duen a terme els miners es el següent:

- 1) Reben les últimes transaccions que s'han produït a la xarxa.
- 2) Verifiquen la validesa de les transaccions, és a dir, que la persona que emet la transacció tingui els BTCs i que la seva firma sigui autèntica.
- 3) Les transaccions s'agrupen en un bloc candidat.
- 4) És busca una solució a un problema matemàtic molt complex. Aquesta solució és única per cada bloc i és compon d'una sèrie de caràcters alfanumèrics que

representen de manera única el bloc. Quan un “miner” troba la solució, la retransmet a la resta de “miners”, els quals comproven que tant les transaccions que componen el bloc com la seva solució siguin vàlides.

- 5) Finalment, el “miner” que ha trobat la solució per aquell bloc rep una recompensa, és a dir, un cert nombre de BTCs.

3.3. Emissió de Bitcoins

Les tasques de verificació de les transaccions i emissió dels BTCs van íntimament lligats. El protocol BTC estableix que es generi un bloc aproximadament cada 10 minuts. De manera que, el ritme de la generació de la moneda està controlat, ja que per cada bloc, s'emeten en forma de recompensa al “miner” un cert nombre de BTCs. Aquest interval de temps entre bloc i bloc es controla mitjançant la dificultat del problema que han de resoldre els “miners” per trobar la solució de cada bloc. La dificultat augmenta en funció del poder computacional de tots els “miners”. D'aquesta manera, quantes més persones i millors equips estiguin involucrats en la “mineria”, major serà la dificultat del problema i, per tant, obtenir la recompensa (Tapscott & Tapscott, 2017, p. 42-44).

A la següent gràfica, s'aprecia com el nombre de BTCs que es generen està programat, reduint-se fins arribar als 21 milions:

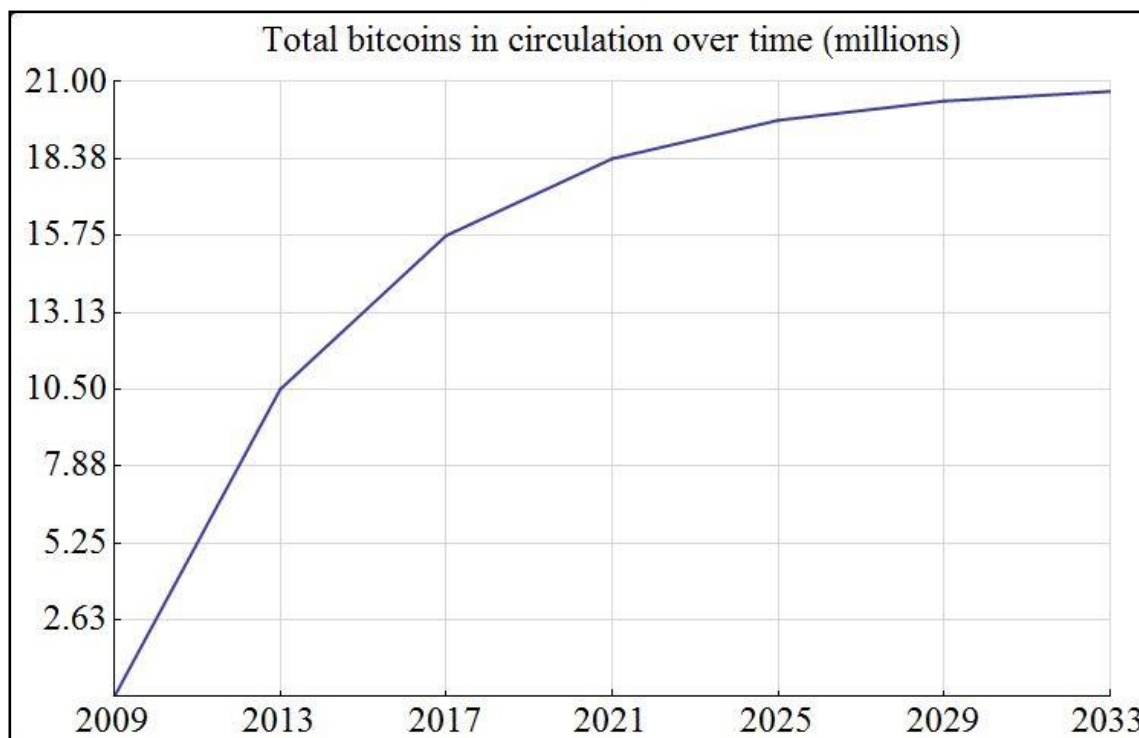


Figura 3. Evolució cronològica d'unitats de BTC en circulació. Extret de (Blockchain Luxembourg S.A., 2018)

A l'eix d'ordenades, en milions, tenim la previsió de la quantitat de BTCs que es generaran, i a l'eix d'abscisses, tenim els anys el quals s'espera que la previsió es compleixi. Com a característica peculiar, és que el BTC té un nombre màxim definit de monedes que es poden crear, concretament 21 milions d'unitats de BTCs. Això és així, perquè el creador o creadors originals, amb el pseudònim de Satoshi Nakamoto, van decidir crear una moneda deflacionària, com l'or. Una de les raons principals, és que quan un bé és escàs, de forma natural, és més probable que tingui cert valor perquè si es pogués crear BTCs de forma indefinida i descontrolada, no tindria valor com a tal. En canvi, si es limita la seva creació, augmenta la probabilitat d'obtenir cert valor.

3.4. Operativa del *blockchain* dins del mercat Bitcoin

Una vegada analitzat i comentat els fonaments d'una *blockchain* i els integrants que fan possible la realització d'aquesta, és moment d'analitzar l'operativa del *blockchain* dins del mercat del BTC.

A continuació, mostrem un esquema que mostra tota l'operativa del *blockchain*, així com tot el procediment que segueix el sistema per realitzar i validar una operació amb BTCs, des de l'inici amb la transacció inicial fins que la transacció queda concloua:

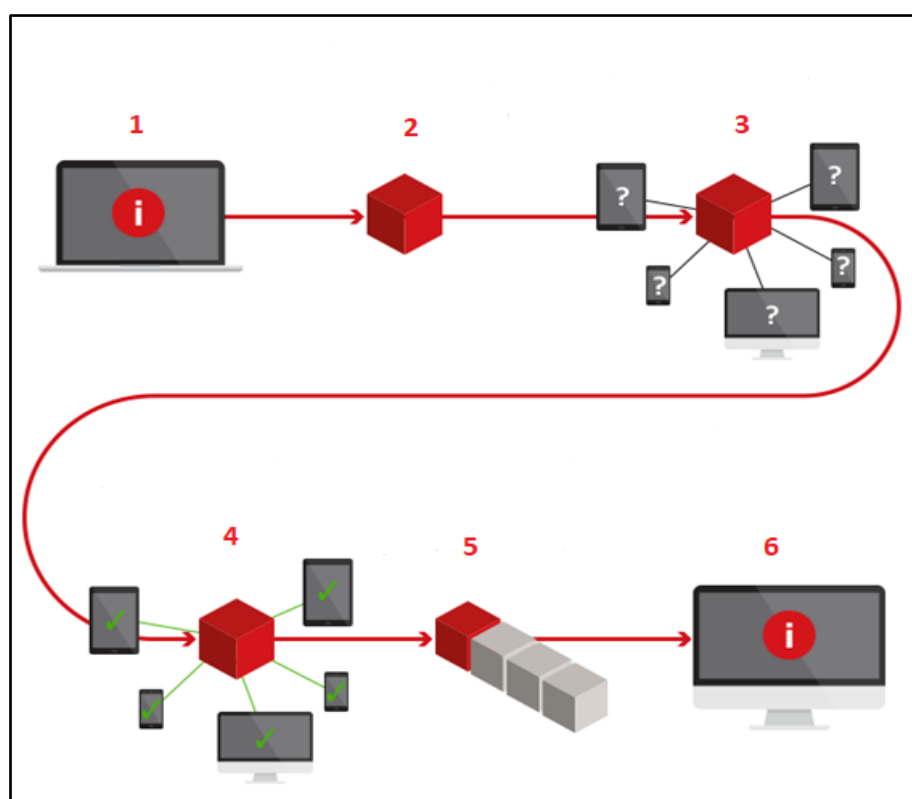


Figura 4. Procés de validació d'una transacció dins la *blockchain*. Extret de (Allen, 2018)

Tot actiu que tingui com a sistema de negociació una *blockchain*, el procediment és el que es mostra en l'esquema anterior on (Tapscott & Tapscott, 2017, p. 28):

- 1) Una vegada tenim BTCs al nostre moneder, ja podem operar amb ells. Quan realitzem un pagament, creem una transacció que conte la quantitat de monedes a transferir i la direcció del destinatari. Les transaccions, son una transferència de valors entre moneders BTC que serà inclosa dins la cadena de blocs. Aquests disposen d'un fragment secret anomenat clau privada, utilitzada per firmar les operacions, proporcionant una prova matemàtica corroborant que la transacció l'ha realitzat el propietari del moneder. La firma, també, evita que la transacció no sigui alterada per algú una vegada ha estat emesa.
- 2) Una vegada sol·licitada, el sistema registra la transacció com un bloc que haurà de ser validat pels integrants de la xarxa, que com hem vist anteriorment, s'anomenen "miners".
- 3) El sistema retransmet el bloc a totes les parts que componen la cadena, que tal com hem analitzat en l'apartat anterior, s'encarregaran de la validació del bloc.
- 4) Els "miners" s'encarreguen de buscar la solució mitjançant algorismes matemàtics. Una vegada validat el bloc, la informació d'aquest es difon per tota la xarxa d'usuaris.
- 5) El nou bloc es inclòs dins la cadena permanentment i inalterable, el qual tindrà una informació transparent de tots els moviments.
- 6) Finalment, l'operació queda realitzada.

Com es pot observar doncs, la tecnologia del *blockchain* no necessita un tercer per garantir i controlar les transaccions, sinó que directament les transaccions són realitzades directament d'un usuari a l'altre. Això és el que s'anomena el *peer to peer* (a partir d'ara P2P). La xarxa P2P és un sistema de comunicació per internet, sense la necessitat d'un tercer per garantir la operació, ni de comptar amb clients ni servidors fixes, el qual atorga flexibilitat i eficiència al sistema. Aquest sistema és bàsicament una interconnexió directa entre ordinadors connectats a la xarxa, sense la necessitat de tenir un servei intermedi. Aquest fet dóna doncs, una gran eficiència operativa ja que no existeixen comissions per realitzar les operacions i és un dels factors que els experts recolzen i donen importància (Tapscott & Tapscott, 2017, p. 28).

Les conclusions que podem extreure de la importància del *blockchain* son les següents:

- **Permet la reducció de costos:**

Encara que el *blockchain* comporta uns costos inicials d'obertura i gestió, gràcies a l'absència de tercers, les comissions són nul·les. És més, afavoreix les transaccions segures i redueix els costos associats a frauds i errors.

- **Aporta confidencialitat:**

Garanteix que la informació estigui accessible únicament al personal autoritzat. Per aconseguir-ho utilitza codis i tècnica de xifrat.

- **Aporta integritat:**

Garanteix la correcció i que es completi la informació.

- **Anonimat:**

Permet vincular un document o transacció a una persona. Per aconseguir-ho utilitza un sistema de doble clau pública i privada, per tal de preservar l'anonimat.

- **Procés a quasi temps real:**

El *blockchain* permet realitzar operacions a quasi temps real i que siguin visualitzades per les parts involucrades.

- **Opera en un entorn segur:**

La base de dades i l'entorn del *blockchain* és, com ja hem vist, molt segur gràcies al seu sistema operatiu i a la validació de les transaccions per la resta d'usuaris.

- **Permet un camí secundari:**

Per tal d'evitar la banca tradicional amb grans comissions, els experts aposten per la teoria de l'absència de tercers per realitzar operacions.

4. Bitcoin vs. Diner fiduciari

Comparar el BTC amb el diner fiduciari és interessant per analitzar les convergències i divergències entre totes dues monedes. Abans d'entrar en matèria, cal esmentar que el diner fiduciari és aquell que està sota la confiança d'una societat, és a dir, no es basa en el valor dels metalls dels quals està compost com antigament es feia, sinó en la creença general de què aquell diner té valor i és acceptat com a mitjà d'intercanvi. Per tal de mantenir la confiança, aquesta moneda està regulada per autoritats governamentals i controlada amb les lleis. En paral·lel al diner fiduciari, s'ha desenvolupat el diner virtual, que no s'ha de confondre amb el diner bancari electrònic.

A continuació, es desenvolupen les principals diferències de caire financer que s'observen entre el BTC i el diner fiduciari:

- La primera i gran diferència que afecta directament a la confiança popular és la descentralització del diner virtual. Tot el conjunt de criptomonedes de nova creació no estan sota la supervisió ni el control de cap institució governamental ni autoritat. Això no passa en el diner fiduciari, que depèn de la divisa, té un òrgan regulador al darrere. Aquest òrgan, a més supervisar-la i controlar-la, aporta confiança. Pel que fa al control del BTC, aquest es realitza indirectament mitjançant les transaccions i els seus usuaris per mitjà del sistema *blockchain* i la "mineria". La carència de control governamental i el límit definit de nombre de BTCs, impossibilita que el valor del BTC estigui influenciat pel factor inflació, ja que cap òrgan pot crear ni realitzar un control exhaustiu d'aquesta moneda virtual (Martín Fernández, 2015, p. 17).
- Les transaccions de BTC es realitzen sense la necessitat d'un tercer, gràcies a l'esmentat sistema P2P. Aquest fet, com ja hem comentat, crea una gran eficiència en el mercat perquè suprimeix els típics costos bancaris. En canvi, si parlem de transaccions de diner com a tal, les entitats bancàries actuen com a intermediaris en la majoria d'aquestes, produint una ineficiència a causa de comissions i elevats costos de gestió (Preukschat, 2017, p. 25).
- Pel que fa a la creació i emissió de la moneda, el diner fiduciari es emès pels bancs centrals mitjançant la creació de deute, el qual forma un sistema multiplicador a través dels bancs i les seves reserves. Contràriament, la creació del BTC no es realitza mitjançant institucions imprimint fons monetaris, sinó que la producció i valor del BTC es basa directament en la llei de l'oferta i demanda. És a

dir, per introduir més criptomonedes en circulació, tal com hem vist en el subapartat 3.3. Emissió de Bitcoins, es realitza mitjançant el procés de la “mineria”, on els “miners” aconseguen BTCs gràcies a oferir els seus potents ordinadors (Martín Fernández, 2015).

- Dins del sistema BTC, només podem operar via online, no existeix el diner físic com a tal. En canvi, el diner bancari o real, pot adoptar dues formes, la via tangible i l'intangible. És a dir, les transaccions amb diner fiduciari poden ser realitzades físicament amb diner físic o mitjançant plataformes electròniques.
- Cal destacar que la producció de BTC és finita, és a dir, que arribarà un dia en que ja no es crearan més BTC. En total, el seu creador va definir quantitat màxima de 21 milions de BTCs. Pel que fa el diner bancari, no té un límit definit que s'hagi de posar en circulació, sinó que els bancs centrals imprimeixen fons monetaris per tal d'adequar la seva política monetària (Martín Fernández, 2015, p. 23-24).

5. Avantatges i riscos del Bitcoin

5.1. Avantatges

Com ja hem vist, el BTC és una criptomoneda digital la tecnologia de la qual es fonamenta en la descentralització i l'absència d'autoritat de direcció, que no es altra que els seus protocols de software. El BTC, a més de les qualitats monetàries de l'or, presenta altres relacionades amb la seva naturalesa:

- **Límit d'emissió:**

La creació de BTC s'ha dissenyat de tal manera que no es generin problemes d'inflació en la seva emissió, essent 21 milions el nombre màxim definit de BTC que pot circular. L'objectiu de l'emissió definida de nombre de BTC és que quants més usuaris hi hagin, més baixa serà la taxa de creació de noves unitats i major competència per adquirir-les. És a dir, hi haurà molts usuaris interessats en comprar i vendre, però poques monedes amb què comercialitzar. D'aquesta manera, està previst que al voltant de l'any 2038 hi haurà l'oferta fixa dels 21 milions, fet que provoca que el BTC no esdevingui deflacionari i sempre acumuli cert valor (Martín Fernández, 2015, p. 49-50).

- **Moneda divisible:**

Actualment, el BTC es pot subdividir fins a 8 decimals, mentre que amb els futurs se'n poden subdividir més.

- **Aliè al sistema fiduciari:**

No es pot crear deute per mitjà d'ell, ja que el seu valor no està intervingut per cap banc central (Martín Fernández, 2015, p. 17).

- **Global:**

No pertany a cap govern ni banc central i és operatiu en tot el món, independentment de les barreres geogràfiques, culturals i polítiques.

- **Impossible de falsificar o alterar:**

Tal i com està composta tota la seva operativa, no es pot fabricar un BTC fals ni realitzar una doble despesa sense que la xarxa o detecti (Urquhart, 2018).

- **Operacions a temps real:**

De mitjana, en menys d'una hora la transacció pot estar validada i conclosa.

- **Absència de reguladors:**

Assumint que el BTC té establertes unes regles i protocol definit, hi ha una absència de reguladors que controlin l'oferta i la demanda (Rosembuj, 2015, p. 29-30).

- **Anonimat:**

Cap usuari està obligat a revelar la seva identitat, fet que fa més atractiu el BTC ja que en cap moment s'ha de revelar el teu patrimoni (Martín Fernández, 2015, p. 17).

- **Baix cost:**

Gràcies a l'absència d'intermediaris, el BTC presenta uns costos molt més inferiors que la utilització de targetes de crèdit, transferències o PayPal (Urquhart, 2018).

- **Seguretat:**

Tal com ja hem vist en apartats anteriors, el BTC presenta un sistema operatiu molt segur, gràcies a la criptografia i el *blockchain*.

- **Transparència:**

Totes les transaccions validades, queden completament gravades en un registre obert als usuaris i de lliure accés (Preukschat, 2017, p. 27).

- **Micropagaments:**

Gràcies a la seva divisibilitat i el baix cost pel que fa a les comissions, és un instrument ideal per realitzar petits pagaments.

- **Operatiu les 24/7:**

El mercat del BTC està operatiu les 24 hores del dia i els 7 dies de la setmana sense contemplar dies festius.

- **Emmagatzematge en un espai intangible i petit:**

Té la capacitat de guardar grans fortunes en un espai virtual ínfim i ser capaç de ser guardat i traslladat sense dificultat i sense presència de tercers (Rosembuj, 2015, p. 29).

Volem recalcar que tots aquests avantatges són molt útils per a tots els usuaris del sistema BTC, però també és cert que és un mitjà ideal i facilita tot el que vénen a ser activitats il·lícites com, per exemple, el blanqueig de capitals, l'evasió d'impostos i el tràfic d'armes i droga.

5.2. Riscs operatius

Tota persona que estigui interessada en invertir en BTCs hauria de conèixer, com a mínim, els següents riscs o inconvenients:

- **Les transaccions són irreversibles:**

Això significa que, si per equivocació no s'envien els BTCs a la direcció correcta, s'hauran perdut els BTCs per sempre, sense la possibilitat de reclamar a ningú (Rosembuj, 2015, p. 22-23)

- **La custòdia de la clau privada:**

Hi ha diferents maneres de guardar la clau privada amb què es pot accedir als BTCs i és per això que s'ha d'evitar per tots els mitjans perdre-la. La majoria de moneders però, ofereixen la possibilitat d'encriptar la clau privada, de tal manera que sigui indesxifrabla per qualsevol persona i evitar ser robats per cibercriminals. Per tant, si es perd la clau, no es pot anar al banc a sol·licitar-ne una de nova, sinó que, com a últim recurs, es pot demanar a unes empreses de nova creació que ofereixen la recuperació de la contrasenya. Fent ús de potents ordinadors, proven milions de combinacions tenint com a referència alguna paraula que recordis de la teva contrasenya anterior (Martín Fernández, 2015, p. 28).

- **Vulneració del protocol establert:**

Una de les raons principals que propicia que moltes persones mirin amb desconfiança el BTC és per la preocupació de què els cibercriminals vulnerin el protocol, és a dir, les regles que fan que tot l'entramat del BTC funcioni. Per posar un

exemple, que és sobrepassi la regla de la màxima oferta de 21 milions de BTCs o que la plataforma deixi d'estar operativa en un moment determinat (Martín Fernández, 2015, p. 28).

No obstant els inconvenients operatius que comporta, cal tenir clar que la seguretat del sistema BTC és fort i segur. Contràriament, el que es pot considerar insegur són els serveis d'algunes plataformes que operen amb aquesta criptomoneda. Per sort, cada vegada en queden menys i, per tant, no és correcte dir que el sistema BTC és insegur.

5.3. Riscs del Bitcoin anunciats per les autoritats monetàries

Davant l'eufòria popular del BTC, organismes centralitzats i bancs centrals han publicat inusuals comunicats advertint dels possibles riscos de les criptodivises en general. Entre aquests comunicats, tots els ens convergeixen en els mateixos riscos. Entre aquests organismes es troben el Banc d'Espanya, la Comissió Nacional de Mercats de Valors (a partir d'ara CNMV) i d'altres d'internacionals com són el *Bank for International Settlements* (BIS), el BCE o la FED. La conclusió és que tots estan d'acord que existeix una altra probabilitat de frau perquè cap autoritat monetària no té el control ni la supervisió.

Segons Randal Quarles, Governador de la FED i encarregat de la supervisió de Wall Street, alerta dels greus problemes en l'estabilitat financera que poden generar les criptomonedes pel la falta de suport institucional. Tanmateix, corrobora en la seva explicació afirmant que, sense l'ajuda d'un actiu que vingui d'un banc central o el suport institucional, no està clar com es comportarà una moneda digital privada. A més, segons Quarles, la preocupació per les criptomonedes rau en la utilització a gran escala d'aquestes, ja que pot fer trontollar el sistema monetari actual. No obstant això, el volum actual de transaccions i influència del BTC a la societat no suposen preocupacions alarmants (EFE, 2017).

Pel que fa als organismes nacionals, la CNMV i el Banc d'Espanya afirmen certament que cap emissió de monedes digitals ni qualsevol ICO, ha estat registrada, autoritzada o verificada per cap organisme supervisor espanyol. Per ser més concrets, ICO és l'acrònim de *Initial Coin Offering* i és el sistema de finançament que utilitzen les empreses *blockchain* per tal d'obtenir fons i donar valor a les monedes que ells utilitzen en els seus serveis. Els inversors obtenen criptomonedes, que poden ser utilitzats en aplicacions de la pròpia empresa, en comptes d'obtenir accions (Doncel, 2018b).

Sebastian Albella, president de la CNMV, a una intervenció durant una conferència sobre criptomonedes, va recomanar no invertir en BTCs als inversors minoristes. Albella, mostrava preocupació pels perills que aquests productes financers sense regulació poden ocasionar als inversors i va insistir en què, ni ell ni la CNMV, estan en contra de les noves tecnologies ni dels avenços com el *blockchain*, però sí del risc d'una inversió desordenada i sense informació (Doncel, 2018a).

El president de la CNMV observa dos tipus de problemes en les operacions en criptomonedes. El primer és que les plataformes comercialitzadores no estan regulades i que, per tant, les operacions amb elles no estan protegides per cap fons de garantia. I el segon problema és l'extrema volatilitat del BTC i el seu risc de bombolla. Tot i així, la CNMV i el Banc d'Espanya han creat un grup de treball que analitzarà les possibilitats i riscos d'aquesta tecnologia innovadora. D'aquesta manera, la CNMV va advertir dels perills del BTC traduint un follet, fet per l'organisme regulador dels mercats americà, que avisava del risc d'estafa que comportava invertir en aquest sector en augment (Doncel, 2018a).

Per altra banda, el Banc d'Espanya i el seu governador, Luis Maria Linde, va advertir també de l'enorme risc del BTC i altres divises digitals, basant-se en la seva extrema volatilitat i afegint que les criptomonedes no són monedes ni divises, sinó actius i va recordar que no ofereixen ni interès, ni rendibilitat ni un termini d'amortització. No obstant això, va dir subratllant que no s'han de confondre amb les *Fintech*, les quals va caracteritzar com una explosió tecnològica molt forta i molt complicada, de la qual estan començant a aprendre tant en el sentit regulador com en l'operatiu (Doncel, 2018a).

Tan en el comunicat de la FED, la CNMV i el Banc d'Espanya convergeixen en l'alerta de que les monedes digitals no estan controlades per cap banc central ni autoritat centralitzada i senyalen que aquestes criptomonedes no poden ser una alternativa a les divises actuals ni és obligatori acceptar-les com a mitjà de pagament. Així mateix, continuen corroborant la seva explicació afirmant que tenen una circulació molt limitada i oscil·lacions molt fortes del seu valor, concloent que no es poden considerar un bon dipòsit de valor ni una unitat de compte estable.

6. Anàlisi quantitativa

Una vegada entesa tota la configuració i el funcionament del BTC, és moment d'analitzar amb dades numèriques la complexitat del BTC per tal de sintetitzar la informació i extreure conclusions que donin resposta als objectius del treball.

L'anàlisi quantitativa del present treball té com a objectiu donar resposta a la pregunta proposada en el subapartat 1.2. Objectius del treball que planteja "és el BTC un actiu potencialment adequat per incloure en una cartera diversificada?"

Cal esmentar que els valors que s'han utilitzat per aquest bloc són molt amplis, cosa que ens ha portat solament incorporar al present treball els gràfics i valors que s'han extret per tal de facilitar la comprensió. Pel que fa les dates, per tots els actius financers i índex borsaris que s'han analitzat, la data d'inici de l'anàlisi ha estat el 30 d'abril de 2013 i la data de finalització el 30 d'abril de 2018.

6.1. Anàlisi de la correlació

Per tal de resoldre la qüestió proposada, la primera anàlisi que s'ha realitzat és l'estudi de la correlació entre la rendibilitat logarítmica entre el BTC i els principals índexs borsaris d'arreu del món. També comentar que per la següent anàlisi s'han adaptat totes les dades dels valors del BTC a la dels índex borsaris suprimint caps de setmana i festivitats, ja que les principals borses del món no estan operatives.

A la taula següent, es mostra el resultat de l'anàlisi numèrica obtinguda:

Variables	Coefficient de Correlació
BTC - IBEX 35	0,01235
BTC - DAX	-0,05232
BTC - CAC 40	-0,00702
BTC - DOW 30	-0,02609
BTC - NASDAQ	-0,01827
BTC - S&P 500	-0,02860
BTC - NIKKEI	0,02799
BTC - HANG SENG	0,02045
BTC - CHINA A50	0,02295

Taula 1. Correlació entre el BTC i els principals índexs borsaris. Adaptat de (Investing.com, 2018)

A la columna de l'esquerra, s'observen les variables on s'hi ha aplicat la correlació, mentre que a la columna de la dreta, es mostra el coeficient de correlació resultant.

Sense entrar en termes purament estadístics, a grans trets el coeficient de correlació mesura el grau de relació lineal entre dos variables aleatòries quantitatives. En el nostre cas, s'ha fet coincidir les dates cronològiques entre el BTC i l'índex en qüestió i utilitzant les rendibilitats logarítmiques com a base d'anàlisi, s'ha aplicat la correlació. Més endavant s'explicarà amb més detall el motiu de la preferència de la rendibilitat logarítmica en comptes de la rendibilitat simple.

El coeficient de correlació (a partir d'ara cc) pot assumir valors dins de l'interval $[-1,1]$, i la interpretació és la següent:

- Si el $cc = 1$, existeix una correlació lineal positiva perfecta. És a dir, hi ha una dependència total entre dues variables i quan una variable augmenta, l'altra també ho fa d'igual proporció.
- Si $0 < cc < 1$, existeix una correlació lineal positiva. Quan una variable augmenta, l'altra també ho fa, però no en la mateixa proporció.
- Si el $cc = 0$, no existeix correlació lineal, tot i que això no implica que siguin completament independents perquè pot existir alguna relació no lineal entre totes dues variables.
- Si $-1 < cc < 0$, existeix correlació lineal negativa, és a dir, quan una variable augmenta, l'altra disminueix, però no en la mateixa proporció.
- Si el $cc = -1$, existeix una correlació lineal negativa perfecta. Totes dues variables tenen una dependència total anomenada relació inversa, és a dir, quan una d'elles augmenta, l'altra disminueix en la mateixa proporció.

En el aquest cas, una vegada explicat breument el significat dels valors assumibles per la correlació, podem observar com tots els valors s'aproximen a 0. Alguns valors són negatius i d'altres positius, però tots s'aproximen a 0, el què indica que no existeix relació lineal entre la rendibilitat logarítmica del BTC i qualssevol dels índexs borsaris principals.

Això porta a la conclusió d'aquesta primera anàlisi, i és que només agafant com a referència aquesta, podem afirmar que el BTC és un actiu financer potencial per incloure dins d'una cartera d'inversió diversificada perquè no té dependència lineal amb cap dels principals índexs borsaris. No obstant això, hem de analitzar altres variables per tal de corroborar i matisar la hipòtesis anterior.

6.2. Binomi rendibilitat-risc

Com en tot anàlisi d'un actiu financer, el principal factor a estudiar és el binomi rendibilitat-risc. Bàsicament, el que es vol estudiar és quin retorn econòmic comporta el BTC i quin risc s'ha d'assumir per tal d'obtenir aquest retorn. A continuació doncs, s'ha realitzat una anàlisi del binomi, utilitzant mètodes matemàtics que s'ajusten als objectius establerts.

6.2.1. Rendibilitat logarítmica diària

S'ha observat l'evolució cronològica de la rendibilitat logarítmica del BTC des dels inicis fins a l'actualitat. S'ha emprat la rendibilitat logarítmica, assumint que les rendibilitats del BTC segueixen una distribució normal perquè té certs avantatges quan es treballa amb percentatges petits. La fórmula emprada ha estat la següent:

$$\text{Rendibilitat logarítmica} = \ln \left[\frac{P_t}{P_{t-1}} \right]$$

Un dels factors més importants que presenta aquesta fórmula matemàtica és que permet sumar rendibilitats en el temps. A més, permet una igualtat aproximada dels retorns quan els rendiments són petits, cosa que s'adapta al mercat del BTC al ser continu, és a dir, està obert les 24 hores del dia durant els 7 dies de la setmana. La rendibilitat logarítmica és un mètode que els analistes utilitzen en gran mesura.

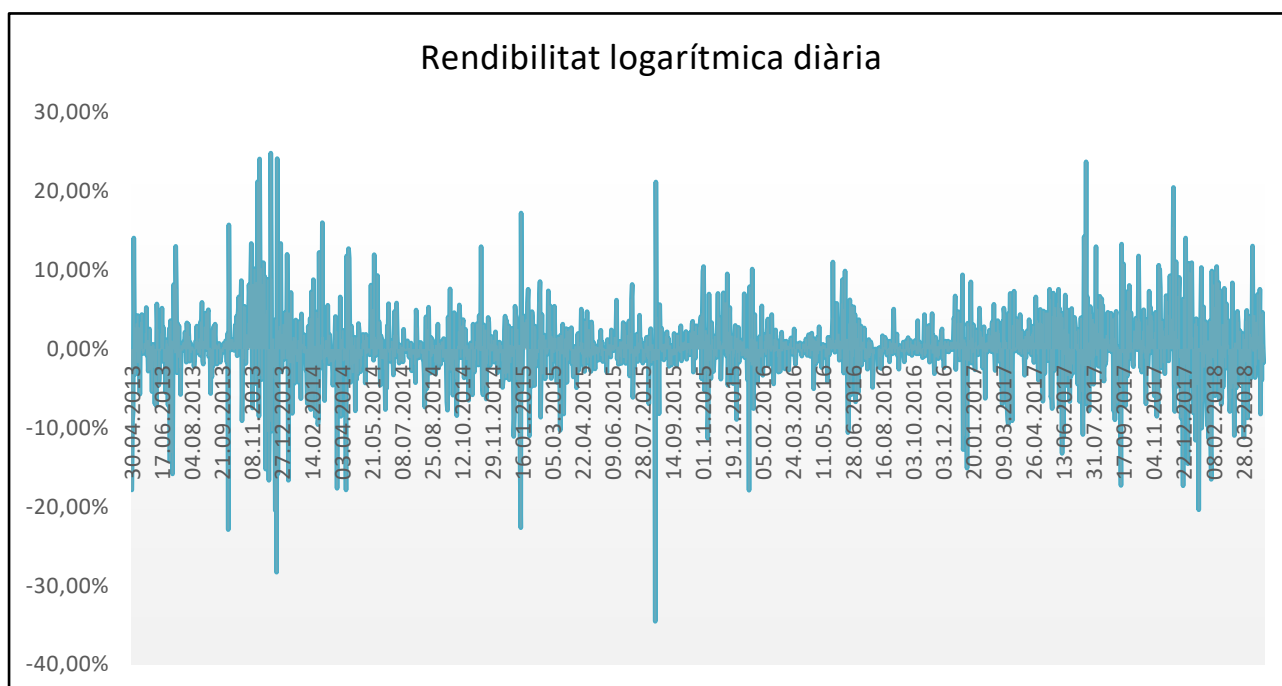


Figura 5. Rendibilitat logarítmica diària del BTC. Adaptat de (Investing.com, 2018)

El gràfic anterior dóna lloc a moltes conclusions, moltes d'elles ja advertides per les autoritats monetàries principals. Tothom està al corrent de les grans fluctuacions que el valor del BTC ha sofert. No obstant això, com es pot observar durant els primer anys de vida financera, també ha sofert moltes variacions en el seu valor. Possiblement, en valors absoluts aquets canvis es veuen més exagerats aquests últims dos anys, però en valors relatius, podem observar grans canvis de valor des dels seus inicis.

Un altra de les consideracions a esmentar és els cicles de volatilitat o nerviosisme que presenta el preu. Com es pot veure, com més amplitud té el gràfic, més nerviosisme mostra el mercat i, a la vegada, oportunitat de treure'n plusvàlues. No obstant això, la volatilitat o nerviosisme dels especuladors ve donada en cicles perquè com es veu hi ha trams on el preu varia molt fortament i d'altres que es manté a variacions més suaus. Totes aquestes etapes de nerviosisme poden venir donades per, bàsicament, notícies i fets rellevants que afecten directament al BTC.

Finalment, a partir del juny de 2017 s'observa una etapa més volàtil, sent aquesta més permanent i que afecta el valor del BTC.

6.2.2. Volatilitat diària

L'altre factor necessari d'estudi dins el binomi de tot actiu financer és el risc. En aquest apartat, s'ha analitzat des d'una vessant pròpia el risc diari que pot suposar invertir en el BTC. Concretament, la fórmula matemàtica que s'ha utilitzat ha estat la rendibilitat logarítmica entre el valor màxim i el valor mínim intra-dia del BTC. La fórmula emprada ha estat la següent:

$$Volatilitat = \ln \left[\frac{P_{max}}{P_{min}} \right]$$

Aquest càlcul, mesura l'amplitud entre el màxim i el mínim diari del preu del BTC, la qual és un bon indicador de la volatilitat diària i del nerviosisme del mercat.

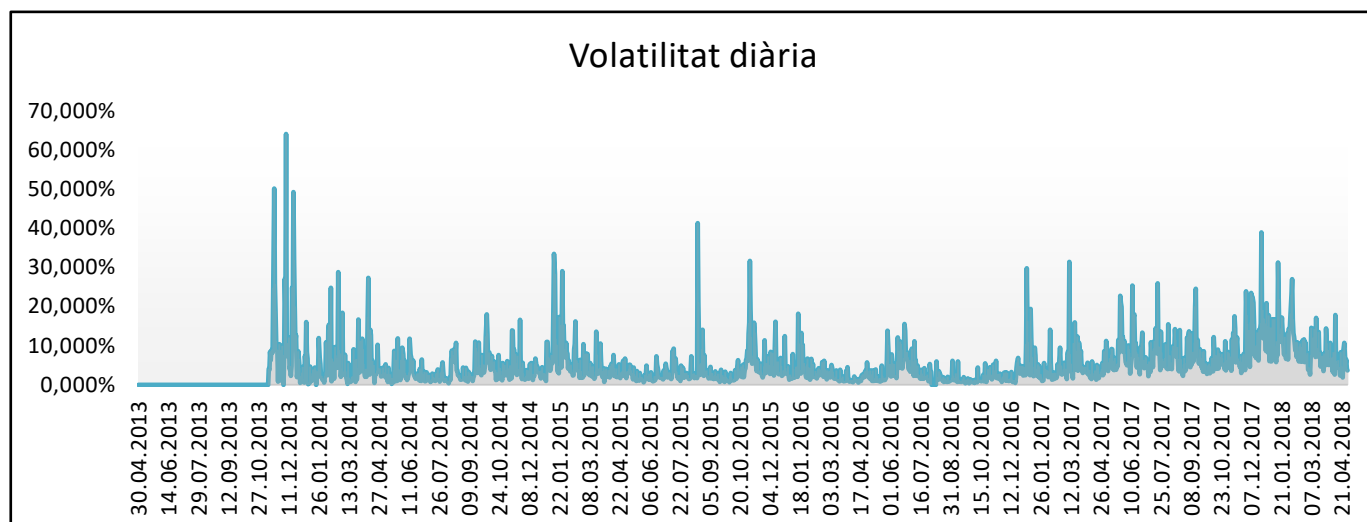


Figura 6. Volatilitat diària del BTC. Adaptat de (Investing.com, 2018)

En els primers anys de la vida financera del BTC i a causa del nul volum de transaccions, la variació diària del preu quasi bé és inexistent. No obstant això, es pot veure com a finals de l'any 2013, el BTC ja comença a sofrir grans variacions diàries del seu preu.

Durant la seva evolució, es pot observar com el BTC pateix cicles de volatilitat molt alta i altres de volatilitat més baixa. Com més alt és el punt a el gràfic, més variació de preu ha sofert el preu del BTC dins d'un mateix dia. Per tant, es pot veure com a final de 2013 va patir un cicle d'alta volatilitat, que justament coincideix en el moment on la criptomoneda es donà a conèixer. En la data esmentada, el preu encara estava al voltant dels 700\$ i va arribar a pics de revaloració d'un 65% diari.

No s'ha de menystenir el cicle de volatilitat que hi ha a mitjans de 2017 i fins a meitat de 2018, on la mitjana de rendibilitat logarítmica entre el màxim i mínim diari d'aquest últim any estudiat (30 d'abril de 2017 fins 30 d'abril de 2018) ha estat del 8,91%.

Això matisa la conclusió extreta del subapartat 6.1. Anàlisi de la correlació. Com bé s'ha dit, el BTC és potencialment adequat per a formar part d'una cartera diversificada. Però, una vegada vist com es comporta el BTC pel que fa al binomi rendibilitat-risc, es pot afirmar de l'alt risc que aquesta cartera assumiria si s'inclogués el BTC en aquesta cartera d'inversió. Per tant, el BTC podria formar part d'una cartera d'alt risc on es pot esperar un alt retorn econòmic, però al mateix temps, també s'ha d'assumir un alt risc.

6.3. L'anàlisi tècnica: el "doble top"

Una vegada analitzat numèricament la complexitat del BTC, és interessant observar el comportament del valor del BTC en termes més tècnics. A simple vista, la fluctuació del BTC en els últims dos anys correspon al que els xartistes anomenen un "doble top". Els xartistes, és el nom que s'atorga als inversors que basen la totalitat de les seves anàlisis en gràfics, per tal d'entendre les oscil·lacions històriques dels preus d'un actiu financer. L'objectiu d'aquests és extreure prediccions i especular sobre el comportament futur de l'instrument financer. De manera més formal, són els anomenats analistes tècnics.

S'ha volgut incloure aquest apartat per explicar com la fluctuació de preus del BTC coincideix amb el que s'anomena el patró "doble top". A més, es creu que la psicologia de l'inversor ha estat clau en tot els fets i antecedents que han influït en el BTC.

L'anàlisi tècnica, a grans trets, segueix els següents principis:

- No segueixen el què es diu a les notícies, sinó que segueixen el que mostra realment el mercat.
- Existeix una psicologia col·lectiva en el mercat que influeix als preus reiteradament i recurrentment.
- Aquesta psicologia produeix repeticions i, per tant, regularitats en el preu i en el volum dels actius financers que s'analitzen.

Per tant, el "doble top" és una regularitat, és a dir, una freqüent fluctuació de preus que el BTC ha patit i és clau la seva anàlisi. El "doble top" és un patró clàssic de reversió que anuncia un canvi potencial de tendència d'alcista a baixista. Aquest patró, com el seu nom indica, està compost per dos pics consecutius que són, aproximadament, al mateix nivell de preus amb una depressió moderada al mig.

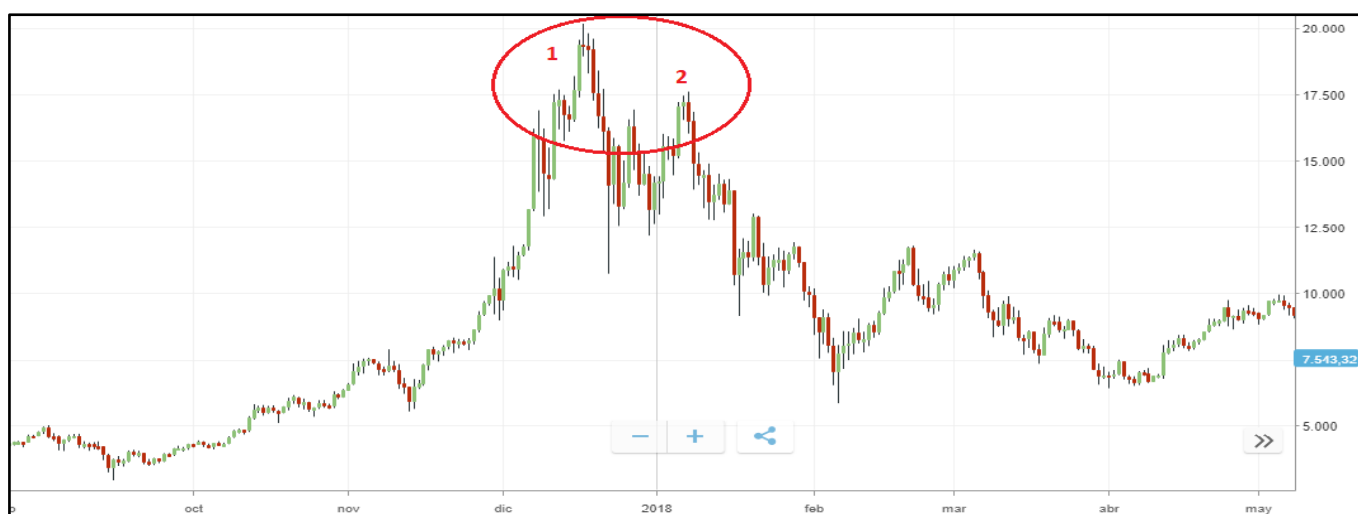


Figura 7. Gràfica del preu del BTC on es mostra el "doble top" del darrer any. Extret de (eToro, 2018)

Al gràfic anterior, es mostra l'últim gran augment de valor que va experimentar el valor del BTC al novembre de 2017, on es pot observar clarament els dos pics de preus i, en conseqüència, la tendència del patró.

Com es pot observar, el valor del BTC segueix clarament la seqüència cronològica del “doble top”, ja que la tendència després del segon pic canvia directament a baixista. Pel que fa al primer, aquest marca el valor més alt, produint successivament una disminució del valor amb un volum de negociació baix. El segon pic en el cas del BTC no va arribar a adquirir el mateix nivell ni de preus ni de volum com el primer. Finalment, una forta baixada alimentada per venda massiva dels especuladors corrobora les característiques del “doble top”.

Seguint amb l'anàlisi, el gràfic que es presenta a continuació, mostra amb una línia verda la referència de la directiu alcista (a partir d'ara DA) i amb una línia vermella la del suport (a partir d'ara S):



Figura 8. Gràfica del preu del BTC on es corrobora el “doble top” del darrer any. Extret de (eToro, 2018)

Primerament, cal comentar que el BTC, abans de la baixada del primer top, segueix una tendència alcista ja que:

- Els mínims secundaris son creixents.
- Els volums són concordants, ja que quan el preu pujava el volum pujava.

Per tal de confirmar que el valor del BTC va seguir el patró del “doble top”, s'ha inclòs a la gràfica de l'evolució de preus la DA i S. La DA sempre té pendent positiva i és la recta que uneix els mínims secundaris. Aquesta DA, marca el suport de la tendència alcista, essent cada vegada més forta quan més vegades reboti el suport en ella. Així mateix

també, és més forta com més temps durin els rebots. En el cas del BTC, la tendència alcista ja es podia veure des d'anys endarrere, però, tal com la DA mostra, la tendència alcista més forta va durar al voltant d'uns 3 mesos.

Segons patrons de l'anàlisi tècnica, un cop traspassada la DA, amb una elevadíssima probabilitat, la tendència passa a ser baixista. En el cas que s'ha analitzat, quan la DA es traspassada, es confirma que la tendència ja passa a baixista.

Per tant, la conclusió que es pot extreure d'aquest subapartat és que, a part de les notícies i fets rellevants que han influenciat la fluctuació del BTC, també afecta directament el factor psicològic dels inversors i, en molts d'ells, són partidaris d'invertir des d'un punt de vista de caire tècnic. A més, es confirma que el preu del BTC és influenciable directament per l'anàlisi tècnica perquè, amb un nul valor intrínsec, l'anàlisi fonamental no és una bona eina d'anàlisi per aquest instrument financer.

7. Conclusions

Una vegada acabat el nostre treball de fi de grau, podem afirmar que entenem millor el què és el BTC i quin és el seu funcionament. Des de l'inici d'aquest treball, ha estat un repte obtenir la informació i recursos adequats per tal de completar tots els apartats que ens vam proposar al començament. Tan és així que els apartats que vam establir des d'un inici de redactar el treball no són els mateixos que els actuals. A mesura que s'ha anat cercant la informació, hem anat modificant el treball per adaptar-lo als recursos que anàvem trobant. Això ens ha permès elaborar un treball més ambiciós i amb una part pràctica que al començament no ens havíem plantejat.

A diferència d'altres treballs realitzats durant el grau, ens hem trobat amb dos grans obstacles que ens han dificultat l'elaboració d'aquest projecte. El primer d'ells ha estat pròpiament la temàtica en sí. Els fonaments del sistema BTC són purament matemàtics i informàtics, fet que ens ha comportat un sobre esforç analitzar i entendre un camp desconegut per a nosaltres. L'altre obstacle ha estat la cerca de l'informació, ja que com que el BTC i tot el que l'envolta és relativament recent, el seu estudi no està massa desenvolupat. Amb això volem dir que hem hagut de fer una recerca exhaustiva per comparar totes les fonts obtingudes i extreure'n la informació vàlida.

Vam definir el BTC a l'inici com un dels "actius financers de moda". Hem pogut confirmar-ho a l'analitzar els antecedents i els fets més rellevants que han influenciat el valor del BTC. Gràcies a aquest estudi, hem pogut comprovar que el BTC, com la resta de les criptomonedes, han estat i són notícia constant. Tant pel que fa als professionals de la informació i comunicació (com per exemple, els mitjans audiovisuals, la premsa escrita, els analistes financers, etc.) com també per a les autoritats monetàries i reguladores, hem vist que se'n fa un ressò continu.

Pel que fa a les característiques principals del BTC, creiem que la més important és la descentralització i la no regulació d'aquest actiu financer. El sistema *blockchain* que recolza el BTC permet la creació d'una criptomoneda digital segura i fiable que afavoreix el lliure intercanvi econòmic entre persones d'arreu del món. Pel que fa al *blockchain*, certes notícies negatives pel BTC (com els ciberatacs, per exemple) i la desconeixença de la temàtica han provocat que el públic en general cregui que no és ni un sistema segur ni fiable. El que volem concloure amb això és que, un cop investigat i aprofundit, afirmem que la inseguretats ve donada per algunes de les plataformes que operen amb

BTC, no en el sistema en si. Per tant, parlar del sistema *blockchain* com insegur no és correcte.

Tot i així, un cop analitzats els riscos, tenim l'obligació de comunicar que, gràcies a l'anonimat i la desconfiança que pot generar el BTC, és un mitjà molt atractiu per als ciber-criminals i per a totes les activitats il·lícites, com el blanqueig de capitals, l'evasió d'impostos i el tràfic d'armes i droga.

Un cop comparat el BTC amb el diner fiduciari, podem concloure que les criptomonedes, a dia d'avui i sense una regulació eficaç per part dels bancs centrals, mai podran substituir i ser una divisa acceptada per la major part de la ciutadania. Això contradiu als partidaris i defensors acèrrims de la criptodivisa, que prediquen que arribarà el dia en què desapareixeran les divises convencionals i tot intercanvi es farà mitjançant les criptomonedes.

Una altra conclusió que hem extret és que el BTC ha perdut domini respecte la resta de criptodivises. Tot i que encara és manté com a líder destacat pel que fa a la quota de mercat, no té el domini que tenia a un any i mig endarrere (gener de 2017). En aquell temps, el BTC quadruplicava la quota de mercat que tenia sobre l'ETH, la segona gran criptodivisa. Actualment, la diferència entre ambdues criptomonedes s'ha rebaixat fins tenir el BTC una quota de mercat que només duplica la que té l'ETH, fet que corrobora l'increment de quota de mercat de la resta de criptomonedes en detriment del BTC.

Després de realitzar l'anàlisi quantitativa, és moment de donar resposta a la pregunta plantejada als objectius que deia "*és el BTC un actiu potencialment adequat per incloure a una cartera diversificada?*". Per tal de corroborar la incorporació del BTC dins d'una cartera, el primer que s'ha d'estudiar és la relació amb els actius que la compondran. Per aquest motiu, la conclusió que s'arriba després d'estudiar la correlació entre el BTC i els principals índex borsaris és que no hi ha relació lineal entre ells i que, per tant, el BTC és un actiu potencial a incloure dins d'una cartera diversificada.

En la posterior anàlisi, concretament en la del binomi rendibilitat-risc del BTC, dóna coherència i matisa la conclusió anterior. Específicament, el que extraiem d'aquest estudi és que, tant la rendibilitat com el risc del BTC són molt cíclics, és a dir, té cicles d'alta rendibilitat i volatilitat i altres de baixa. A més, també arribem a la conclusió que el BTC té una rendibilitat molt superior a la resta d'actius financers convencionals. No obstant, el fet de voler incloure'l en una cartera diversificada en un percentatge significatiu, elevaria en gran mesura el risc de la cartera en qüestió.

Finalment i per donar resposta al títol del present treball, hem arribat a la conclusió que, com en tots els actius financers on es vulgui invertir, s'ha de conèixer i investigar tots els paràmetres que poden influir en la seva fluctuació. En aquest cas, al tractar-se d'un actiu nou, no regulat i sense precedents, aconsellem que només hi inverteixin els inversors que coneguin i assumeixin els riscos d'aquesta inversió. Corroborem aquest consell després d'haver realitzat l'estudi del binomi rendibilitat-risc del BTC, on s'ha pogut observar que, ja des dels seus inicis, presenta una gran volatilitat.

8. Bibliografia

- AFP. (2013, octubre 30).** Primer cajero automático de bitcoins. *El País*. Recuperat de https://elpais.com/tecnologia/2013/10/30/actualidad/1383129755_439976.html
- Allen, M. (2018).** Blockchain property start-up encounters regulatory resistance. Recuperat el 19 de maig de 2018, de https://www.swissinfo.ch/eng/swissrealcoin_blockchain-property-start-up-encounters-regulatory-resistance/44141256
- Blockchain Luxembourg S.A. (2018).** Bitcoins in circulation. Recuperat el 19 de maig de 2018, de <https://www.blockchain.info/es/charts/total-bitcoins>
- Buy Bitcoin Worldwide. (2018).** Gráfico de historial del precio de Bitcoin. Recuperat el 2 de juny de 2018, de <https://www.buybitcoinworldwide.com/es/precio/>
- Chansanchai, T. (2014).** Now you can exchange bitcoins to buy apps, games and more for Windows, Windows Phone and Xbox. Recuperat el 1 de juny de 2018, de <https://blogs.microsoft.com/firehose/2014/12/11/now-you-can-exchange-bitcoins-to-buy-apps-games-and-more-for-windows-windows-phone-and-xbox/>
- CoinMarketCap. (2018).** Global Charts: Percentage of Total Market Capitalization (Dominance). Recuperat el 3 de juny de 2018, de <https://coinmarketcap.com/charts/>
- Doncel, L. (2018a, gener 24).** La CNMV recomienda a los inversores minoristas no comprar bitcoins. *El País*. Recuperat de https://elpais.com/economia/2018/01/24/actualidad/1516812109_393178.html?rel=str_articulo#1524761249269
- Doncel, L. (2018b, febrer 8).** La CNMV y el Banco de España alertan de los riesgos del bitcoin. *El País*. Recuperat de https://elpais.com/economia/2018/02/08/actualidad/1518102049_854223.html
- Doncel, L., & Pozzi, S. (2017, desembre 11).** El estreno del bitcoin en la Bolsa de futuros augura nuevas subidas. *El País*. Recuperat de https://elpais.com/economia/2017/12/11/actualidad/1512957928_348981.html



- EFE. (2017, desembre 1).** La Fed advierte del peligro del bitcoin para la estabilidad financiera. *El Economista.es*. Recuperat de <http://www.eleconomista.es/divisas/noticias/8782972/12/17/La-Fed-advierte-del-peligro-del-bitcoin-para-la-estabilidad-financiera.html>
- El Economista.es. (2013, desembre 5).** China prohíbe a las instituciones financieras las transacciones en bitcoins. *El Economista.es*. Recuperat de <http://www.eleconomista.es/divisas/noticias/5370138/12/13/China-prohibe-a-las-instituciones-financieras-las-transacciones-en-bitcoins.html>
- El Economista.es, & Bloomberg. (2018, abril 10).** El bitcoin es «la mayor burbuja de la historia» y se propaga como la gripe, según Bank of America. *El Economista.es*. Recuperat de <http://www.eleconomista.es/divisas/noticias/9060767/04/18/El-bitcoin-es-la-mayor-burbuja-de-la-historia-y-ademas-se-comporta-como-la-gripe.html>
- Esparragoza, L. (2018).** Un repaso por la historia de Bitcoin tras nueve años de minarse el bloque génesis. Recuperat el 2 de juny de 2018, de <https://www.criptonoticias.com/opinion/repaso-historia-bitcoin-nueve-anos-minarse-bloque-genesis/>
- eToro. (2018).** Gráfica del precio de Bitcoin: valor e historial de BTC en tiempo real. Recuperat el 26 de maig de 2018, de <https://www.etoro.com/es/markets/btc/chart/full>
- Europe Central Bank. (2012).** Virtual Currency Schemes. *European Central Bank*. Recuperat de <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- Fernández, A. (2018, abril 11).** Las criptodivisas: más allá del Bitcoin. *Diari de Tarragona*.
- Gautham. (2016).** Barclays, First Bank to Embrace Bitcoin with Circle. Recuperat el 1 de juny de 2018, de <https://www.newsbtc.com/2016/04/06/barclays-bitcoin-circle/>
- Greenbert, A. (2011).** Crypto Currency. *Forbes*. Recuperat de <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#740ae970353e>
- Investing.com. (2018).** BTC USD Bitfinex Historical Data. Recuperat el 26 de maig de 2018, de <https://www.investing.com/crypto/bitcoin/btc-usd-historical-data>

- Kharpal, A. (2017, octubre 16).** WikiLeaks' Julian Assange claims he made 50,000% return on bitcoin. *CNBC*. Recuperat de <https://www.cnbc.com/2017/10/16/wikileaks-julian-assange-bitcoin-50000-percent-return-thanks-to-us-government.html>
- Kyodo. (2016, març 4).** Japan OKs recognizing virtual currencies as similar to real money. *The Japan Times*. Recuperat de <https://www.japantimes.co.jp/news/2016/03/04/business/tech/japan-oks-recognizing-virtual-currencies-similar-real-money/#.Wxenq0jRDIV>
- Leinwand Leger, D. (2014, maig 15).** How FBI brought down cyber-underworld site Silk Road. *USA Today*. Recuperat de <https://eu.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/>
- Martín Fernández, J. et al. (2015).** *Todo sobre Bitcoin. Aspectos económicos, fiscales, contables y administrativos*. Madrid: Francis Lefebvre.
- Pollock, D. (2018).** El lío que era Mt. Gox: cuatro años después. Recuperat el 1 de juny de 2018, de <https://es.cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on>
- Pozzi, S. (2017, desembre 9).** El mercado de futuros de Chicago estrena contratos de bitcoin. *El País*. Recuperat de https://elpais.com/economia/2017/12/09/actualidad/1512788236_703268.html
- Preukschat, A. et al. (2017).** *Blockchain: la revolución industrial de internet* (6a.). Barcelona: Centro Libros PAPP, S.L.U.
- Reuters. (2018, gener 18).** El bitcoin cae por debajo de los 10.000 dólares, la mitad del valor que alcanzó en diciembre. *La Vanguardia*. Recuperat de <http://www.lavanguardia.com/economia/20180117/4473814646/bitcoin-cae-20-por-ciento-temor-restricciones-china-corea-sur-asia.html>
- Rodríguez, E. (2017, juliol 2).** Todo sobre Ethereum, la moneda virtual que superará al Bitcoin. *El Español*. Recuperat de <https://omicro.no.elespanol.com/2017/07/que-es-ethereum-criptomoneda/>
- Rodríguez Herrera, D. (2014).** ¿Qué es Bitcoin? *La Ilustración liberal*, 59. Recuperat de <https://www.clublibertaddigital.com/ilustracion-liberal/59/que-es-bitcoin-daniel-rodriguez-herrera.html>

Rosembuj, T. (2015). *Bitcoin*. Barcelona: Editorial el Fisco-G.L.E.T.S.L.

Sala, M. (2017, desembre 6). 113 millones por dos pizzas: el fail de la primera compra con Bitcoin. *El Español*. Recuperat de https://www.elespanol.com/social/20171206/267473674_0.html

Schweizerische Bundesbahnen. (2017). Make quick and easy purchases with Bitcoin. Recuperat el 2 de juny 2018, de <https://www.sbb.ch/en/station-services/services/further-services/bitcoin.html>

Tapscott, D., & Tapscott, A. (2017). *La revolución blockchain: Descubre cómo esta nueva tecnología transformará la economía global* (4a.). Barcelona: Centro Libros PAF, S.L.U.

The Bitcoin Foundation. (2016). The Bitcoin Foundation Manifesto. Recuperat de https://bitcoinfoundation.org/wp-content/uploads/2017/03/Bitcoin_Foundation_Manifesto.pdf

Urquhart, A. (2018). What causes the attention of Bitcoin? *Economics Letters*, 166. Recuperat de <https://doi.org/10.1016/j.econlet.2018.02.017>