

COMPARACIÓ DEL CONSUM ENERGÈTIC ENTRE EL SISTEMA FINANCER TRADICIONAL I LA XARXA BLOCKCHAIN


**Universitat
de Girona**


Pau Biosca Díaz
Tutor: Dr. Ricard Rigall I Torrent
Doble Grau en Economia i Filosofia
Curs 2021-2022

Índex

Índex	I
Agraïments	II
1. Introducció.....	1
2. Què és una cadena de blocs?	1
2.1 Tipus de verificacions.....	5
2.2 Aplicacions de les cadenes de blocs	6
2.3 Limitacions i riscos de les cadenes de blocs	8
3. Consum energètic i sostenibilitat de les diferents cadenes de blocs.	11
4. Com funciona el sistema financer tradicional?	14
5. Consum energètic del sistema financer tradicional.....	15
6. Comparació del consum de la xarxa blockchain amb el sistema financer tradicional.	18
7. Conclusió.....	21
8. Bibliografia.....	23

Agraïments

En primer lloc, m'agradaria donar les gràcies, a tota la gent que ha estat al meu costat donant-me mostres d'ànim i afecte, les quals m'han ajudat a continuar endavant quan no tenia massa clara la visió.

Especialment, també, agrair al meu tutor que m'acceptés el treball. Atès que no es tracta d'una temàtica molt estesa pel món acadèmic i es podria arribar a considerar, fins i tot, un valor atípic.

Finalment, fer menció al professorat que m'ha acompanyat al llarg d'aquests anys a la FCEE, els quals m'han aportat el necessari per tenir bons fonaments juntament amb un pensament crític.

1. Introducció

Ja fa anys que la tecnologia blockchain està deambulant per la xarxa, però està sent en aquests darrers en què està obtenint més renom i rellevància. Tant les grans fortunes com els petits inversors han vist en aquesta una possibilitat d'inversió. Fet que ha portat a crear una mena d'imatge de mercat borsari que engloba tot l'ecosistema.

Però aquesta funcionalitat no és la que tenia pensada Satoshi Nakamoto. El creador de Bitcoin fou clar i concís a l'hora d'explicar quina era la finalitat d'aquesta xarxa. El que buscava era crear una alternativa al pagament en línia que oferien les institucions financeres tradicionals. A fi de millorar diferents aspectes com la privacitat i la seguretat, tot sense comptar amb la participació de tercers. (Nakamoto, 2008)

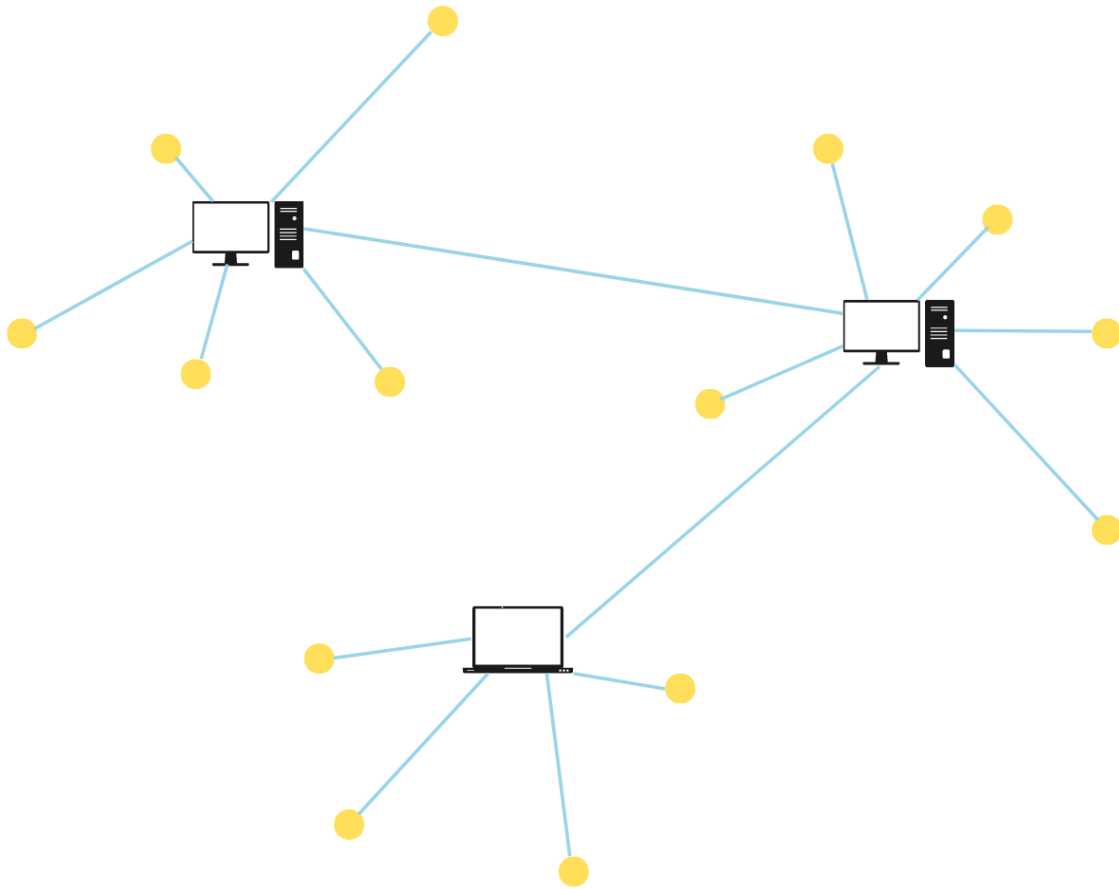
Tanmateix, Bitcoin està actualment operatiu i permet realitzar transaccions. Però el sistema que el sosté ha augmentat considerablement la seva mida i ara hi ha innumerables projectes que miren més enllà d'operar com si fossin bancs descentralitzats. Ara bé, aquesta nova tecnologia difereix en molts aspectes del sistema financer tradicional. Essent un d'ells el consum d'energia. El qual conforma l'eix central d'aquest treball, en el que es comparará el cost energètic d'aquesta tecnologia amb la despesa elèctrica que comporta el sistema financer tradicional.

2. Què és una cadena de blocs?

Una cadena de blocs, de l'anglès *blockchain*, és un sistema que combina xarxes d'igual a igual (P2P), les quals funcionen de manera descentralitzada, és a dir, sense cap servidor, com es mostra a la Figura 1. Cada dispositiu connectat a la xarxa rep el nom de node, que opera com a servidor, d'una banda, i com a client per l'altra (Schollmeier, 2001). Un dels principals avantatges d'aquest tipus de connexió entre diferents dispositius és que no requereix cap intermediari i, per tant, qualsevol node pot iniciar una transacció i d'igual manera rebre-la. I és aquesta una de les virtuts de la tecnologia blockchain, el fet d'eliminar tota mena de centralització. D'aquesta manera, són els mateixos usuaris de la xarxa qui fan possible el funcionament del sistema.

Figura 1

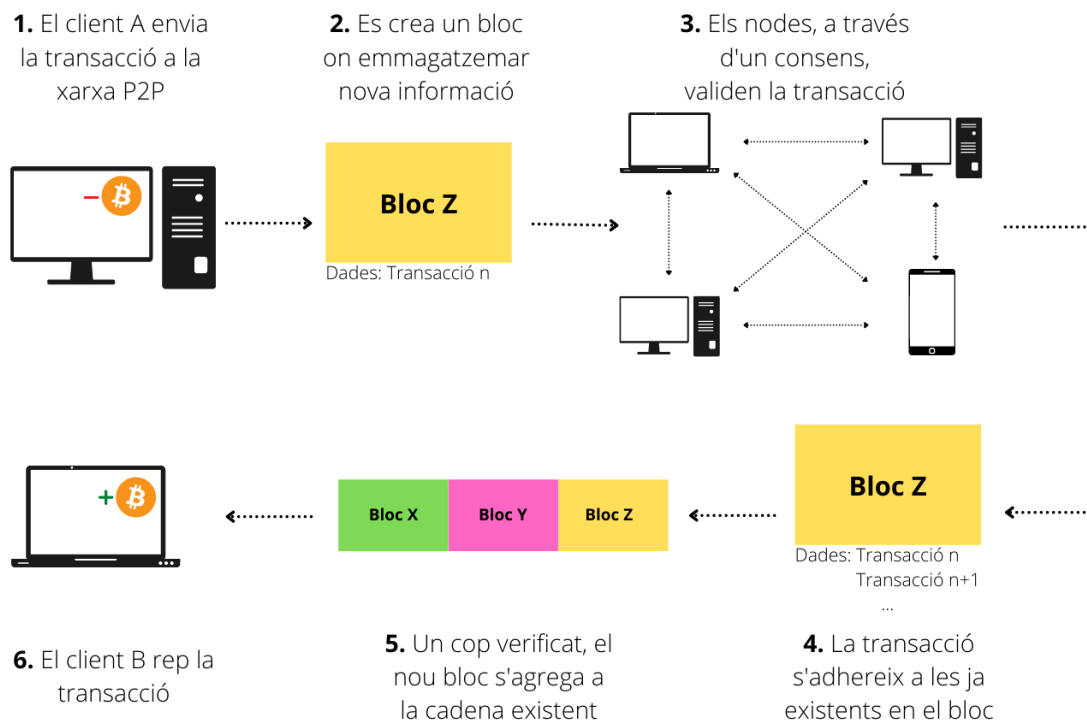
Il·lustració d'un sistema descentralitzat



Ara bé, aquest és solament l'entorn en el qual es desenvolupa aquesta tecnologia. Per explicar què és, però, és necessari saber com funciona. El principi bàsic recau en el fet que hi ha un bloc original sobre el qual es va afegint nova informació, fet que crea un nou bloc, i així successivament. D'altra banda, aquest sistema s'utilitza principalment per a realitzar transaccions, encara que no sigui la seva única funcionalitat. D'aquesta manera, un node du a terme una transacció, la qual és enviada a la xarxa P2P. Seguidament, els diferents nodes de la xarxa han de validar aquest intercanvi, el que esdevé en un nou bloc. Però abans de res, s'ha d'arribar a un consens per tal de validar l'operació. Punt que es detallarà a l'apartat següent. Un cop s'ha validat, la transacció s'agrupa amb altres per formar un nou bloc a la cadena, que queda connectat a l'anterior (Ghiro et al., 2021). Aquest procés està il·lustrat de manera conceptual a la Figura 2.

Figura 2

Funcionament d'una xarxa blockchain



Aquesta és l'explicació bàsica de com funciona una blockchain. Però es fa necessari aprofundir en el seu funcionament per poder entendre quina és la manera de verificar les transaccions. Fase del procés en la que es concentra gran part de la despesa energètica. (punts 3-4 de la Figura 2).

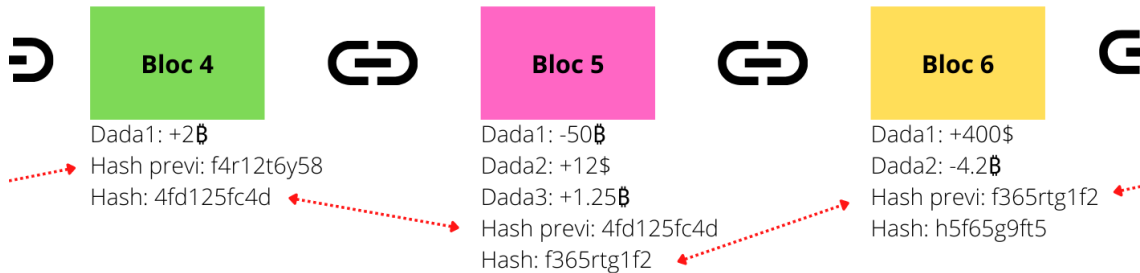
Així doncs, a partir del primer bloc, la informació necessària de l'anterior s'encrypta mitjançant una funció resum (*hash* en anglès). D'aquesta manera s'aconsegueix que tot hash sigui únic. Cal apuntar que un cop s'encrypta, ja no és reversible, és a dir, mitjançant una d'aquestes claus d'enciptació no es poden obtenir les dades que l'han format. D'altra banda, apuntar que aquests processos requereixen una capacitat de càlcul bastant petita, on qualsevol ordinador actual té suficient capacitat de processament per a executar la tasca. D'aquesta manera les dades queden emmagatzemades de manera encryptada a la cadena de blocs (Chen et al., 2019).

A la Figura 3 hi ha un exemple de l'estructura d'una xarxa blockchain on es mostra que el hash recull informació del bloc anterior com les transaccions o el conjunt de dades que emmagatzemi el bloc. En conseqüència, un nou bloc tindrà la informació dels anteriors que hagin estat connectats a aquest. És a dir, fent servir l'exemple, la dada que hi ha al

Bloc 4 s'encrypta i el resultat d'aquest resum, juntament amb altres dades, forma el hash 4fd125fc4d, el qual passarà a formar part del Bloc 5 i així successivament.

Figura 3

Estructura simplificada d'una xarxa blockchain



Tanmateix, es pot entendre que un dels usos d'aquesta tecnologia és la capacitat de recollir els moviments i transaccions que es donen en una determinada xarxa, de manera semblant a un llibre major de comptabilitat. D'aquí se segueix la connexió que guarda aquesta amb la tecnologia de llibre major distribuït (Distributed Ledger Technology o DLT en anglès). La qual permet compartir informació de manera descentralitzada. A més, conté moltes semblances amb la xarxa blockchain atès que aquesta última és un tipus de DLT, essent però, una tècnica d'emmagatzematge de dades més genèrica (Schueffel, 2017). Així, en relació amb els diferents tipus de ledgers, la manera de verificar les dades de cadascun d'ells determinarà si es tracta d'un centralitzat o descentralitzat.

En el descentralitzat, qualsevol persona que accepti el protocol de consens de la xarxa pot procedir a realitzar verificacions. Açò comporta una sèrie de particularitats, ja que no hi ha cap control d'usuaris i són anònims. Se'n deriva, llavors, una falta de confiança a la xarxa que s'ha de contrarestar a l'hora de verificar les dades per tal de mantenir la seguretat de la informació. (Rejeb et al., 2021)

Altrament, estan els ledgers centralitzats, els quals tracten de millorar el rendiment de les operacions a canvi de tenir major control sobre els usuaris. Aquests són els utilitzats per grans corporacions com les entitats financeres. No requereix un procés de verificació exhaustiu perquè en aquest tipus de xarxa solament poden modificar les dades les entitats responsables o autoritzades. (Tripoli i Schmidhuber, 2018)

2.1 Tipus de verificacions

Hi ha molts tipus de xarxes blockchain, i una de les diferències més importants entre elles, a banda del tipus de governança, són els diferents protocols de consens.

En primer lloc, s'analitzarà el protocol de Prova de Treball (PoW en anglès). És el més utilitzat en l'actualitat, atès que les dues criptodivises amb major capitalització de mercat (Bitcoin i Ethereum, respectivament) les utilitzen per verificar les transaccions de les seves xarxes i crear nous blocs. Aquest mètode és el que permet evitar la manipulació del llibre major, atès que seria rebutjada per part dels participants, els quals reben el nom de miners.

Aquest protocol permet la detecció de qualsevol alteració anòmala a la cadena mitjançant la verificació dels hashes dels blocs. Però com s'ha apuntat anteriorment, aquesta és una tasca accessible per a qualsevol ordinador, per la qual cosa es requerirà un esforç addicional. A més a més, és la mateixa xarxa la que estableix la dificultat i, per tant, aquesta depèn del tipus de blockchain en el que s'estigui executant l'operació (Ankalkoti i Santhosh, 2017). Encara que, a termes generals, es tracta d'operacions amb un alt requeriment de potència computacional.

Així mateix, pel que respecta a la mineria, és a dir, a la tasca que realitzen aquells que proven de verificar les transaccions i afegir nous blocs a la cadena, en aquest protocol es tracta d'una tasca més aïna competitiva. Cada miner té una capacitat computacional diferent i com més gran sigui aquesta, més probabilitats hi ha de què acabi rebent la recompensa per registrar les transaccions en el següent bloc (Hayes, 2016). Però un miner amb molt poca capacitat computacional també pot acabar trobant la solució al trencaclosques que imposa la xarxa, i quedar-se amb els beneficis d'haver minat un bloc. (Kroll et al., 2013). Cal mencionar també, que la unitat d'aquesta potència computacional és el hash per segon (H/s), és a dir, la potència que té un dispositiu o conjunt d'aquests per a resoldre els trencaclosques que proposen les xarxes PoW i afegir un nou bloc a la cadena.

D'altra banda, el segon protocol més utilitzat és el de Prova de Participació (PoS en anglès). Es va crear com una alternativa al PoW, buscant millores en eficiència i usabilitat en general. Però per a aconseguir aquesta comesa, fou necessari canviar la manera de verificar les dades de la xarxa. D'aquesta manera, no es premia la quantitat de treball invertida, sinó que es valora la quantitat de monedes que es tinguin acumulades. És a dir,

amb aquest protocol, la probabilitat d'obtenir una recompensa per validar un nou bloc, augmenta de manera proporcional respecte a la quantitat de moneda que es tingui de la blockchain en qüestió. (Chohan, 2018).

Com exemplifica Saleh (2021), en una hipotètica blockchain on hi ha 10 monedes circulants, de les quals el jugador A en posseeix 8, aquest té una probabilitat de 8/10 (80%) de ser seleccionat per afegir un bloc a la xarxa i, per tant, guanyar una moneda. En cas que acabi essent escollit, tindrà 9 monedes i l'oferta augmentarà a 11. Pel que en una segona adjudicació, la probabilitat del jugador A passarà a ser de 9/11 (81,81%). D'altra banda, en cas que no hagués estat escollit en primera instància, però, passaria a tenir una possibilitat de 8/11 (72,72%).

A través d'aquest exemple, Saleh (2021), a banda de facilitar la comprensió d'aquest mètode de verificació, també tracta d'explicar que en aquest tipus de xarxa, la informació es va actualitzant amb cada nou bloc i amb això, les probabilitats dels participants varien en temps real.

Ara bé, aquest era únicament un exemple il·lustratiu. Cada tipus de xarxa conté una sèrie de requisits i condicions de participació particulars. En conseqüència, poden ser diferents segons quins siguin els seus objectius, com també passa a les xarxes PoW. On cadascuna guarda diferents peculiaritats que s'associen a la finalitat amb la qual es vulgui disposar la xarxa.

2.2 Aplicacions de les cadenes de blocs

L'interès en aquesta tecnologia ha estat en augment al llarg d'aquests últims anys, fet que ha portat que s'expandeixi cap a altres àmbits allunyats de la tecnologia. Com apunten George i Jaoude (2019), la recerca relacionada amb la blockchain ha augmentat al voltant d'un 32% del 2015 al 2018, essent "aplicacions" el terme més nombrós a les publicacions. Dintre d'aquest camp, destaquen les relacionades amb la Internet de les coses (IoT en anglès), energia, atenció sanitària i finances, respectivament.

Açò dona lloc a plantejar-se la quantitat d'utilitats que es poden derivar d'aquesta tecnologia. Pilkington (2016) destaca algunes com els contractes intel·ligents, proveïdors d'identitat digital, sistemes de votació o diferents implicacions per a la indústria financera. Com també menciona diferents aplicacions en un àmbit no tan concret com són

la millora de la transparència de les cadenes de subministrament o la inclusió social en el món desenvolupat.

Però aquestes són algunes de les aplicacions que destacaven anys enrere. Actualment, existeixen diferents enfocaments com la biomedicina, el sector energètic o la indústria agroalimentària. Ara bé, encara que hi hagi moltes aplicacions, no sempre tenen el suport o la repercussió que es mereixen i acaben en res (Labazova et al., 2019).

Ara, per una banda, es destacarà una de les aplicacions més rellevants i de més renom, la qual compta amb bons fonaments, que han permès que es continuï desplegant i millorant tant amb prestacions com amb diferents implicacions. D'altra banda, es tractaran propostes innovadores amb bones perspectives de futur com les que s'han anomenat anteriorment.

En primer lloc, cal tractar els contractes intel·ligents. Aquests són un programari allotjat a la xarxa blockchain, amb la funció d'executar acords entre dues o més parts de manera automàtica. Cobreix les demandes d'un contracte bàsic i pretén reduir els costos, resultant, per tant, més eficient. S'executen seguint una sèrie de condicions que es programen amb anterioritat i la seva capacitat depèn d'aquesta última. (Alharby i van Moorsel, 2017)

Pel que respecta a les funcions que ofereixen aquests contractes, cal destacar els préstecs, dipòsits de garantia i gestió d'herències i donacions com explica Echebarría (2017). O, d'altra banda, també consta de potencial, com apunten Alharby i van Moorsel (2017), per poder gestionar drets musicals, comerç electrònic o fins i tot es pot combinar amb el IoT, on cada desenvolupador acabaria posant els límits a les possibilitats que s'ofereixen. De fet, Christidis i Devetsikiotis (2016) plantegen diversos exemples de la sinergia entre aquests i la blockchain apuntant a diverses aplicacions i la millora en termes d'eficiència que podria suposar per al sector manufacturer o al de transports de mercaderies.

En segon lloc, mencionar les aplicacions de la blockchain en el sector energètic. Hi ha a la xarxa nombrosos estudis sobre la implementació d'aquesta tecnologia en el camp de l'energia, entre els quals destaca l'extensa revisió que realitza Andoni et al. (2019). Aquesta analitza la implementació de la blockchain per a les diferents parts del procés, des del moment en el qual surt dels generadors fins quan arriba a les cases i s'ha d'efectuar el pagament. Considera els avantatges que podria comportar per al proveïdor perquè reduiria costos, però sobretot analitza quin impacte podria tenir sobre el consumidor. Pel

que respecta als avantatges que podria suposar per a aquest últim, destaca les facilitats que podria suposar per a l'autoconsum i la democratització de l'energia, de manera que s'acabaria afavorint el consum d'energies renovables. D'altra banda, la grandària del mercat elèctric es podria reduir considerablement eliminant intermediaris, el que implicaria un augment d'eficiència en el sector.

Seguidament, com expliquen Agbo et al. (2019) a la seva revisió, aquesta tecnologia ofereix moltes aplicacions en el sector sanitari. Algunes fins i tot ja s'han implementat a països com Estònia, com apunten els autors. En aquest cas, la xarxa blockchain s'encarrega de gestionar i emmagatzemar els historials clínics de la població millorant la seguretat, interoperabilitat i la privacitat de les dades. Però els autors revisen més aplicacions, assenyalant les que tenen més estudis al darrere, com ara les cadenes de subministraments de les farmacèutiques o les implicacions a la investigació. En tots dos casos, despunta el seguiment que es pot realitzar de les dades. En el primer cas, per controlar les receptes falses i les irregularitats que es podrien donar des del procés de fabricació fins que arriba al consumidor final. I en el cas de la recerca mèdica, es podria millorar la gestió de dades i la interoperabilitat entre diverses institucions i estudis atès la privacitat que aporta aquesta tecnologia.

Finalment, es revisaran breument els usos en el sector agroalimentari. Per una banda, podria aportar transparència als processos de producció i transport, mentre que també milloraria la traçabilitat del producte. D'altra banda, com apunten Kamilaris et al. (2019), que analitzen extensament les virtuts esmentades, recalquen que per poder portar a terme tots aquests canvis, seria necessària també un canvi en la infraestructura del teixit productiu. Així mateix, reforcen la idea que per a incentivar aquesta digitalització, és necessari realitzar-la a gran escala, no solament a un punt concret de la indústria. Amb tot, consideren que un bon punt de partida podria ser l'administració pública, atès que és la cara més visible i podria servir com a un model.

2.3 Limitacions i riscos de les cadenes de blocs

Un cop s'han revisat algunes de les virtuts d'aquesta tecnologia, és moment d'analitzar quines són les seves principals limitacions i riscos.

Existeixen principalment 2 riscos, entre els quals es troben l'accés a les claus privades i els atacs informàtics. Pel que respecta al darrer, hi ha diversos atacs que poden rebre les

xarxes blockchain. Alguns són compartits amb les xarxes tradicionals, com els atacs DDos i d'altres que es deriven del procés de verificació dels blocs, com és el cas dels atacs del 51%, entre d'altres.

En el cas d'aquests últims, són diferents per a cadascun dels protocols. Pel que respecta als PoW, aquests atacs es podrien donar si una entitat o una sèrie de persones aconseguix el control de més del 50% de poder de computació total de la xarxa. Aquest fet podria permetre a l'atacant desorganitzar la xarxa mitjançant la modificació de transaccions. Cal dir, però, que ja hi ha diverses solucions sobre la taula com presenten Sayeed i Marco-Gisbert (2019). I també esmentar, primerament, que seria necessària molta potència computacional per poder fer front a tota una xarxa, fet que dificultaria l'atac. I, en segon lloc, que la xarxa premia més el fet de ser honestos, és a dir, no és eficient atacar-la, sinó treballar juntament amb ella.

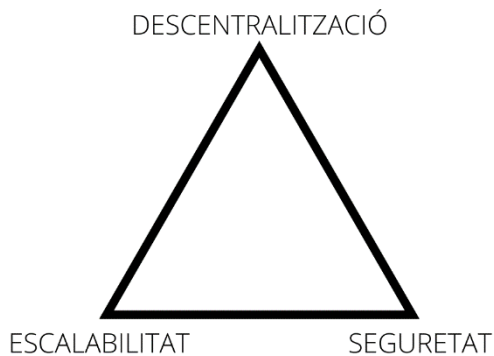
Aquest atac també es podria donar a blockchains amb un sistema de verificació PoS, però de diferent manera. Seria necessari que un usuari o un grup d'usuaris tinguessin en possessió més del 50% de la moneda circulant. (Zhang et al., 2019) D'aquesta manera aconseguirien desestabilitzar la xarxa. Tanmateix, arribar fins a aquest punt comporta moltes dificultats. Suposaria adquirir més de la meitat de l'oferta total d'una divisa, fet que resultaria molt costós i, per tant, inviable.

En segon lloc, la blockchain utilitza una criptografia asimètrica, en la qual cada usuari té una clau que el converteix en l'únic posseïdor d'una moneda o qualsevol dada. És per aquesta raó que brinda molta seguretat, mentre que la transparència la proporciona una clau pública que és el visible a tota transacció. (Zheng et al., 2017) La clau privada podria ser un avantatge, atès que l'usuari custodia els seus propis fons o dades, però també es pot convertir en un inconvenient. En cas de perdre la clau privada, no hi ha manera de recuperar-la, per la qual cosa, es perdria l'accés a l'emmagatzemat a un lloc determinat de la blockchain.

D'altra banda, pel que respecta a les limitacions, les més importants són l'escalabilitat i la ineficiència de la xarxa, la qual es tractarà al punt següent.

Figura 4

Il·lustració del trilema de l'escalabilitat



Pel que respecta a l'escalabilitat, la xarxa blockchain presenta certs problemes atès la seva infraestructura a l'hora d'assumir un creixent nombre de transaccions i usuaris, mentre s'intenta mantenir un alt nivell de descentralització i seguretat. Aquestes tres propietats són, en part, incompatibles. Fet que propicia la formació del trilema de l'escalabilitat, il·lustrat a la Figura 4. Segons Hafid et al. (2020), la seguretat és inevitable, mentre que la descentralització forma part de la naturalesa de la blockchain. Llavors, l'escalabilitat és l'única d'aquestes que es pot alterar amb vista a millorar-la.

Per portar a terreny real l'afer de l'escalabilitat, en concret, la xarxa de Bitcoin pot realitzar un màxim de 7 transaccions per segon (TPS) mentre que Visa en pot realitzar al voltant de 1700 i PayPal 193 (Hafid et al., 2020). Ara bé, aquests tempos estan estrictament relacionats amb la infraestructura i la tecnologia de verificació que s'usa en cada cas. Bitcoin utilitza PoW i el temps de confirmació dels seus blocs és de 10 minuts, un temps que resulta excessiu per dur a terme qualsevol transacció o compra.

Com apunten a Zhou et al. (2020), ja s'han proposat diversos projectes per fer front a aquest problema, cadascun dels quals està desenvolupat per aportar més eficiència i, en conseqüència, millorar la usabilitat. Però no tots ho han aconseguit, com ha sigut el cas de Monoxide o RapidChain, on solament cal fer una cerca al navegador per comprovar que s'han quedat en una proposta. I els projectes que estan en actiu com Algorand o Conflux, empen altres protocols de verificació que presenten altres limitacions a les ja esmentades i que no permeten el seu ús massiu.

3. Consum energètic i sostenibilitat de les diferents cadenes de blocs.

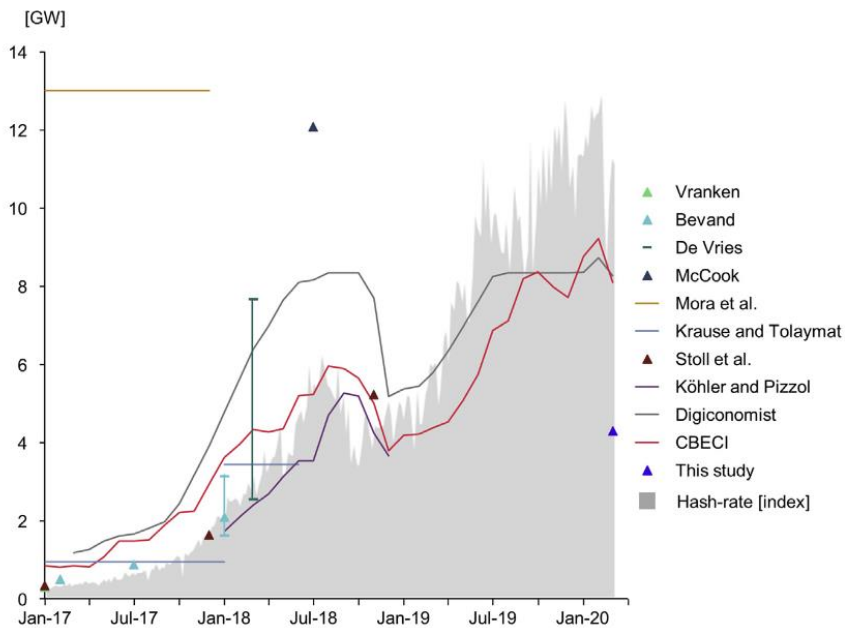
És aquí on es troba un dels punts centrals de la recerca, on s'analitzaran els diferents consums que tenen tant les xarxes blockchain amb un sistema de verificació PoW com les que el fan servir el PoS.

Primerament, es tractarà l'eficiència dels sistemes PoW, prenent com a referència blockchains com la de Bitcoin. Pel que respecta a aquesta xarxa, hi ha multitud d'estudis que han tractat d'analitzar quin és el seu consum energètic juntament amb diverses implicacions que es deriven d'aquest. Ara bé, hi ha estimacions, enquestes o exhaustives anàlisis, els quals empen diferents metodologies, proporcionant, per tant, diferents resultats. Com expliquen a Institute of Electrical and Electronics Engineers (2018), les estimacions de consum dels sistemes PoW pot variar enormement. En el cas d'una transacció de Bitcoin, la xifra oscil·la entre 200 kWh i 950 kWh. Mentre que les transaccions a la xarxa d'Ethereum, tot i tenir el mateix sistema de validació se situa al voltant de 75 kWh. Igualment, s'ha de considerar que els estudis més actuals tindran dades que mostrin menor consum atès que la tecnologia avança i és capaç de crear mecanismes més eficients per minar. A l'estudi de Hayes (2016) s'esmenta que l'eficiència de minar de Bitcoin al voltant del 2012 era de 500 watts per GigaHash cada segon (GH/s), mentre que quatre anys després, hi havien diferents dispositius capaços de minar amb una eficiència de 0,15 W per GH/s.

Pel que respecta al consum energètic, a Gellersdörfer et al. (2020) es recopilen algunes de les principals estimacions que s'han anat realitzant des de l'any 2017 fins al 2020 com es mostra a la Figura 5.

Figura 5

Estimació del consum d'energia del Bitcoin de 2017 a 2020



Nota. Adaptat d'*Energy Consumption of Cryptocurrencies Beyond Bitcoin* (p. 1844), per Gallersdörfer et al., 2020, *Joule*, 4 (9).

Es pot observar a la Figura 5 que la majoria dels estudis segueixen una mateixa tendència, excepte alguns punts aïllats. Del que se'n dedueix, que tot i haver-hi diferents metodologies i tipus d'estimacions, hi ha certa harmonia entre els resultats. Però per facilitar la comprensió d'aquests consums, s'han de comparar amb altres de manera que es tingui una noció més visual. A de Vries (2020) s'estima que anualment la mineria de Bitcoin consumeix aproximadament 87,1 TWh, que és l'equivalent al que consumeix al llarg d'un any un país com Bèlgica.

Per tant, com bé argumenten articles com el de Drusinsky (2022), està més que contrastat el fet que el manteniment de la xarxa de Bitcoin i, per extensió, del sistema de verificació PoW, és molt costós en termes energètics. Aquest mètode ofereix, com ja s'ha vist, recompenses a qui més poder de computació tingui, per la qual cosa incentiva a tenir-ne cada cop més si es volen obtenir majors beneficis. Fet que ha resultat en la creació de granges de minat, és a dir, grans espais que estan replets de dispositius, com ara targetes gràfiques, que intenten ser els primers a trobar el hash que permet verificar un bloc i aconseguir la recompensa. En conseqüència, aquestes granges se situen en zones on l'accés a l'electricitat és barat, de manera que es maximitza el benefici.

I aquesta electricitat podria venir de fonts renovables, de manera que l'impacte ambiental d'aquesta xarxa no fos tan dolent, però com s'indica a Blandin et al. (2020) solament el 39% del consum d'electricitat dels miners de xarxes PoW procedeix d'energies renovables. No obstant això, encara que fos un percentatge molt més elevat, aquesta mateixa electricitat es podria emprar per a altres tasques en què l'eficiència fos més alta o que la requerissin amb més necessitat.

Per acabar amb el sistema de verificació PoW, cal esmentar que també comporta un gran deteriorament del maquinari que s'utilitza per minar. Del que es deriva una gran quantitat de residus al llarg dels anys, al que s'ha d'afegir una capacitat de fabricació de microxips limitada o, fins i tot insuficient, atesa l'alta demanda. Conseqüentment, aquesta situació pot desembocar en escassetat de components juntament amb un augment de preus dels mateixos i un malbaratament dels recursos necessaris per fabricar-los (de Vries, 2021).

D'altra banda, el protocol de consens PoS es va crear com una alternativa al PoW, com ja s'ha explicat anteriorment, amb l'objectiu d'incrementar l'eficiència reduint el consum energètic. Tot sense comprometre la seguretat ni la descentralització. Amb aquest nou sistema, no seria necessària tanta potència computacional, resultant un nou mètode de verificació que redueix significativament els inconvenients que comporta el PoW. De fet, la segona criptodivisa amb major capitalització actualment, Ethereum, està sotmesa a una migració cap a aquest sistema (Cao et al., 2020).

I aquest pas de gegant l'ha donat Ethereum, però no ha estat el primer. Ja hi havia algunes blockchain molt importants utilitzant aquest protocol com Solana, Cardano o Algorand. Aquesta elecció es dona, en part, per la millora en el consum, i en general, per l'increment en l'eficiència que suposen les verificacions amb PoS (Cong et al., 2021).

El menor consum energètic s'aconsegueix en eliminar la competició per aconseguir la potència més gran de processament (*hashrate* en anglès) (Eshani et al., 2021). Com ja s'ha vist, el canvi de protocol comporta que per a realitzar les verificacions dels blocs es té en consideració la quantitat de divises que es vulguin habilitar per contribuir a la causa. D'aquesta manera, es contraresta l'excessiva demanda d'energia que requeria PoW.

Pel que respecta a xifres, encara no hi ha moltes publicacions que aportin claredat a aquest protocol, atès que la majoria s'han centrat en Bitcoin i el desgast que suposa el PoW. Ara bé, hi ha estudis com el de Li et al. (2020) amb una bona base, on es consideren diverses fonts amb les quals elaboren anàlisis de tota classe. Per un costat, alguns més teòrics o

quantitatius, mentre que, per l'altre, es duen a terme d'altres més qualitius o fins i tot simulacions. De tot el conjunt d'anàlisi i comparacions, es desprenen diverses conclusions que afavoreixen l'alternativa al PoW tant en consum energètic, com en escalabilitat i, fins i tot, en seguretat.

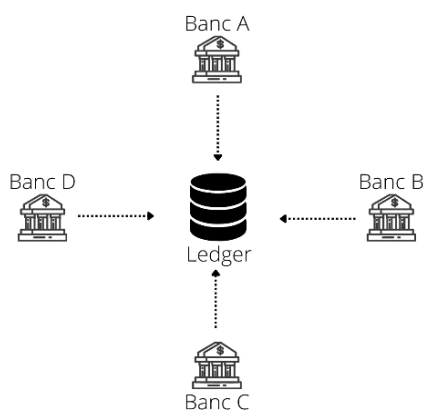
Però per poder parlar en termes numèrics i aconseguir una imatge més concreta de la millora que suposa, hi ha anàlisi com el de Kin Chan et al. (2020), el qual apunta que el consum energètic es redueix en més d'un 75%. Mentre que des de la fundació Ethereum se suggereix que aquest consum podria disminuir en més d'un 99% (Beekhuizen, 2021). Ara bé, sigui com sigui, el fet que aquest protocol redueix el consum en comparació amb el PoW està més que demostrat (Saleh, 2021). I quan Ethereum completi la seva migració a PoS, és molt probable que es comenci a estudiar amb profunditat la millora que suposa aquest tipus de verificació respecte al PoW en diferents aspectes, atesa la rellevància que té la seva blockchain a l'ecosistema.

4. Com funciona el sistema financer tradicional?

Com s'ha esmentat a finals del punt 1, la major part d'entitats financeres fan servir ledgers centralitzats per a conèixer i gravar les operacions que es produeixen en els comptes dels diferents usuaris. Però aquest ús és privat i, per tant, solament pot tenir permisos d'escriptura i demès la institució propietària (Auer et al., 2021).

Figura 6

Il·lustració d'un ledger centralitzat



Podria semblar que no hi ha gaires disparitats entre aquest ledger i el que fa servir qualsevol xarxa blockchain, però hi ha diferents punts on destaquen cadascun d'ells. Pel que respecta als ledgers centralitzats, com el que es mostra a la Figura 6, poden permetre's unes verificacions de dades més laxes. És a dir, les mesures de seguretat a l'hora d'editar i confirmar les modificacions en el llibre major són

baixes, atès que tenen un accés a la seva xarxa molt restringit. Com a conseqüència poden realitzar gran nombre de transaccions per segon de manera ràpida i eficient.

Aquest tipus de ledgers acaben essent els últims responsables del conjunt de dades que es dipositen, ja sigui d'una entitat financera, d'una asseguradora o de qualsevol empresa. Per això, es necessita en últim terme, dipositar confiança absoluta en una tercera part. Aquesta centralització, com esmenta Allen et al. (2019), està en la línia del sistema capitalista actual. El qual no es pot entendre sense un govern central, estructures radials de tota mena o una tendència cap a la simplificació i la uniformitat.

D'altra banda, la confiança en aquest tipus de serveis està força interioritzat al conjunt de la població. No s'havia ofert gairebé cap alternativa fins ara, per la qual cosa, es presentava com l'única opció. Es va passar de tenir els diners guardats cadascú a casa seva, a cedir la custòdia a una entitat en la qual s'ha de confiar cegament.

Quant al funcionament d'un ledger centralitzat, un exemple pot facilitar l'explicació i mostrar de manera més evident les diferències amb els ledgers distribuïts com la blockchain. Un client del banc A es disposa a realitzar una transferència a un client del banc B. Quan fes l'operació, a la seva compta personal se li ha descomptat l'import Z, però no és ell qui ha canviat els registres del banc per realitzar-la. Realment, el client del banc A ha fet una petició perquè es processi la transferència al client del banc B. Aquesta petició es completarà quan les ordres arribin al ledger centralitzat, el qual donem per suposat que comparteixen els dos bancs, i les processa.

5. Consum energètic del sistema financer tradicional

Ja s'ha comentat la transparència que ofereix la xarxa blockchain, tant per a comprovar qualsevol transacció, com a l'hora de facilitar l'accés a les dades que permeten calcular estimacions del consum d'una xarxa. Per contra, el sistema financer tradicional posa moltes traves a l'hora d'alliberar informació pròpia, siguin dades de consum energètic o el nombre de centres de dades, entre altres. Es dedueix, llavors, que per aquesta raó, no hi ha gaires estudis al respecte, o almenys, no tants com de la xarxa blockchain.

Ara bé, a l'hora de calcular el consum de la blockchain, com ja s'ha explicat, s'ha de calcular la quantitat d'energia que fan servir els validadors. Però per calcular el consum del sector financer tradicional, a banda dels validadors o les bases de dades, s'ha de considerar l'energia que es fa servir als milers de sucursals o caixers automàtics que hi ha arreu del món, atès que formen part del sistema. Aquest sector també comporta, com

apunta Cocco et al. (2017), un afegit de despeses que van més enllà de l'operativitat de la xarxa bancària, com el gas, l'aigua o el paper i tinta que es fa servir a les diferents sucursals i oficines. Seguint l'article, es destaquen també els residus que es produeixen en el conjunt del sistema financer incloent la producció de moneda i bitllets. Per extensió, com més intermediaris i complex és el sistema, més consum energètic, més contaminació i menys eficiència en termes generals.

Aquest resumit desglossament de despeses que comporta el sistema financer tradicional, també podria ser un factor que afecta negativament a la quantitat d'estudis que mostren el consum d'aquest sistema. Primer, no és fàcil delimitar on acaben aquestes despeses, és a dir, també s'hauria de comptabilitzar la despesa que suposa el transport dels treballadors a les oficines i sucursals? En segon lloc, cal destacar la dificultat per obtenir totes aquestes dades. S'haurien de demanar dades a molts bancs de diferents països per poder aconseguir una mostra que permeti realitzar un bon estudi. Dades que no sempre serien accessibles atès les polítiques de moltes institucions. Finalment, sembla que a aquestes institucions no els interessen brindar molta informació. Tampoc hi ha publicats gaires estudis interns, per la qual cosa es dona a entendre que no hi ha molt d'interès per part de les institucions en saber quin és l'impacte en termes energètics dels seus negocis, o almenys, no han demostrat el contrari.

Ara bé, que no hi hagi moltes dades, no significa que no hi hagi cap estimació. Pel que respecta a les transaccions, a Institute of Electrical and Electronics Engineers (2018), s'estima que Visa utilitza aproximadament 200 kWh per validar 100.000 transaccions. El que equival, per fer-se una idea, al consum d'una nevera moderna al llarg d'un any. Però, com s'ha explicat, hi ha més factors a tenir en compte a banda de les transaccions. A Ernst i Young (2020) es calcula mitjançant dades facilitades pel *DZ BANK Group* el seu consum energètic anual. L'últim informe és el de 2020, i s'apunta que el consum energètic total és de 33.093.498 kWh. Ara bé, tot i no indicar quin consum hi ha recollit, és a dir, tot i no especificar què hi ha inclòs al total, també hi ha altres dades, que en estar calculades a banda, s'entén que no estan incloses en el consum energètic total. És el cas del consum de la calefacció, la qual se situa en 18.015.789 kWh.

Tot seguit, un cop es tenen les dades de les transaccions, es poden comparar amb les del consum total d'una cadena financera. És cert que la validació de les transaccions no suposen un alt consum, però aquest es dispara notablement quan afegim la infraestructura física com les oficines i sucursals. Tot i això, s'ha de tenir en compte que aquesta despesa

representa la del segon banc més gran d'alemanya en ingressos (Ernst i Young, 2020) i que comptava amb 33.188 empleats el 2020. Per situar aquesta dada, el grup CaixaBank actualment compta amb aproximadament 49.762 treballadors (Principales datos, 2022).

Passant a l'àmbit global, destaquen dos estudis diferents. El primer és el de McCook (2014), el qual inclou en el conjunt del sistema financer els caixers automàtics i les diverses sucursals que estima que hi ha arreu del món. Per resumir la metodologia del seu estudi, primerament calcula una aproximació tant del nombre de caixers automàtics com de sucursals. Després, elabora i aplica diferents models per saber quina és la despesa de cadascuna de les parts. I per acabar, suma totes aquestes, situant el consum del sistema financer mundial en 650.000.000.000 kWh. L'equivalent aproximadament a més de 2,5 vegades el consum anual d'un país com Espanya (International, 2022).

En darrer lloc, l'estudi més recent és el de Rybarczyk et al. (2021), el qual difereix bastant amb l'anterior en la metodologia, i com a conseqüència, també en el resultat final. Aquesta anàlisi calcula estimacions, d'una banda, dels centres de dades bancàries, les diferents sucursals i els caixers automàtics. A les quals s'afegeix la despesa que suposen les xarxes a través de les quals es produeixen les transaccions electròniques o amb targeta de crèdit. En canvi, no es comptabilitza el consum de cap classe de calefacció, com si ho fa l'estudi anterior. Tot i això, sumant el conjunt de dades estimades, acaben oferint un consum anual de 263,72 TWh (el que equival a 263.720.000.000 kWh). Per fer la comparació, equival a una mica més del consum elèctric anual d'un país com Espanya.

Ara bé, tot i tenir algunes dades, no es pot explicitar què està inclòs exactament en les estimacions. A l'estudi de McCook (2014) no es fa menció al consum dels centres de dades, els quals a l'estudi de Rybarczyk et al. (2021) s'estima que tenen un consum d'aproximadament 239 TWh a l'any. Aquesta dada es pot contrarestar amb els resultats de l'article de Masanet et al. (2020) publicat a la revista *Science*, el qual apunta que el consum elèctric dels centres de dades al llarg de l'any 2018 fou de 205 TWh. Aquesta última estimació no encaixa amb la que proporciona l'estudi de Rybarczyk perquè, tot i que hi hagi un marge d'error en ambdós, segons aquest darrer, el consum de base de dades del sistema financer supera al conjunt d'aquestes bases que calculen a l'article de la revista *Science*. S'entén, llavors, que aquest darrer inclou, a banda dels centres de dades d'institucions financeres, altres de grans corporacions com Google, Amazon o Microsoft a més dels governamentals. Pel que sembla que aquestes dades poden fins i tot contradir-

se. No poden tenir més consum els centres de dades financers que el conjunt global, els quals també inclouen a aquests últims.

6. Comparació del consum de la xarxa blockchain amb el sistema financer tradicional.

Per tal de comparar el consum energètic del sistema financer tradicional amb el de la blockchain, es reduirà aquesta darrera a la xarxa de Bitcoin per diverses raons. En primer lloc, perquè és la que més estudis té al darrere i, per tant, la que més dades i estimacions ofereix. I, en segon lloc, perquè és la moneda amb major capitalització actualment que compta amb la blockchain que més consum energètic suposa.

Així doncs, pel que fa a l'estimació del consum del sistema financer tradicional a escala global, es disposa de dues dades. La primera de 650 TWh i la segona de 263,72 TWh. La diferència és significativa entre ambdues, de manera que es podria sostenir que el consum està distribuït entre els dos valors. Ara bé, tal vegada es podria valorar si s'aproxima més al valor superior o a l'inferior.

Amb les dades anteriorment esmentades del *DZ BANK Group*, tant de treballadors com de consum elèctric i calefacció, es pot realitzar una comprovació per saber quin és l'impacte de la calefacció en la totalitat del consum. De manera que es podrà extrapolar a l'estudi de Rybarczyk et al. (2021) per tal de valorar les dues estimacions en condicions més semblants.

D'aquesta manera, amb la realització d'un simple càlcul, s'extreu que el consum de la calefacció representa al voltant d'un 54% del consum total d'electricitat a l'informe d'Ernst i Young (2020). Aquesta dada es pot contrastar amb el publicat per IDAE (2020), on s'estima que la calefacció representa de mitjana el 47% del consum d'energia de la llar. Així mateix, per arrodonir la xifra i situar-la entre les dues, es pot establir en un 50%. Ara sí, donades aquestes dades, es pot aplicar a l'estimació de Rybarczyk et al. (2021) l'augment que suposaria la calefacció de les oficines i altres sucursals, la qual situaria el consum total en 358,5 TWh. Amb tot, aquesta dada encara segueix lluny de la proporcionada per McCook (2014), encara que ja es pot situar un marge més ajustat que queda entre 358,5 TWh i 650 TWh.

Altrament, pel que respecta al consum de la xarxa blockchain de Bitcoin hi ha també diverses dades provinents de diverses anàlisis amb diferents metodologies. L'estudi de de Vries (2020), com s'ha comentat anteriorment, estima el consum en 87,1 TWh. D'altra banda, Rybarczyk et al. (2021) estima que el consum és de 113,89 TWh. Mentre que a Drusinsky (2022) s'estima en 135 TWh.

Es pot observar, llavors, com les estimacions de la xarxa blockchain de Bitcoin segueixen certa tendència amb menys biaixos que les del sistema financer tradicional, el qual deixa un marge considerable entre l'estimació més alta i la més baixa. Fet que es pot deure a molts factors, com ja s'ha explicat als primers paràgrafs del punt anterior. No obstant això, aquests estudis s'han acabat publicant, dels quals diversos mitjans n'han fet ressò, i dels que cap entitat financera n'ha dit res al respecte, ni afirmant ni desmentint. És a dir, tal vegada estiguin més o menys encertats tant en la metodologia com en les estimacions finals, però no hi ha altres dades que mostren el contrari.

Aquestes entitats tenen la suficient capacitat per portar un control de les seves despeses elèctriques o de treballadors entre altres. Igual que es duen a terme estudis interns o auditories financeres, també es podrien realitzar en l'àmbit de l'eficiència elèctrica, com ha demostrat el *DZ BANK Group*. Ara bé, recau sobre aquestes entitats la possibilitat o no d'efectuar la recollida i posterior publicació d'aquestes dades.

No és cap secret que, a termes generals, les institucions privades no destaquen per la seva transparència. Per una banda, no hi ha gaires publicacions que facin referència a quin és el consum del conjunt d'aquestes institucions. Però, d'altra banda, tampoc faciliten informació perquè es puguin calcular estimacions més acurades. Caldria preguntar-se llavors, per què?

La xarxa blockchain ofereix transparència, i tot i que no hi hagi disponible una xifra exacta de quina quantitat d'energia consumeix, almenys les diferents estimacions apunten més o menys, cap a un punt en concret. És més, les estimacions que es realitzen utilitzen bases de dades públiques, com són el nombre de transaccions o la potència total de minat. Després, la maquinària que s'empra per acomplir la comesa, entre altres dades, s'extreu d'estudis i enquestes com les de Blandin et al. (2020), les quals compten amb una gran mostra, fet que ajuda a donar-li credibilitat i reputació a l'estudi. Per contra, els que fan referència al sistema financer tradicional, no fan servir grans mostres perquè no disposen d'accés a les dades necessàries per portar a cap unes estimacions acurades. No es faciliten.

D'aquesta manera, s'han de fer grans extrapolacions i usar referències d'anys diferents intentant estimar una sèrie de dades que mai han tingut xifra.

Ara bé, un cop arribats a aquest punt, cal qüestionar-se si és just comparar una xarxa que dona servei a més de 5.000.000.000 de persones com és la del sistema financer tradicional (McCook, 2014) amb la xarxa de Bitcoin que actualment dona servei al voltant de 82.500.000 persones (Bitcoin Wallets, 2022).

És cert que hi ha una diferència abismal entre el nombre de persones a les quals dona servei el sistema financer tradicional enfront de les carteres de bitcoin que hi ha. I amb les dades que s'han pogut recopilar, es pot considerar que el consum més gran de les institucions tradicionals, sigui més o menys elevat, és raonable, atès que ofereix suport a milers de milions de persones. Però la tecnologia blockchain encara té alguna cosa a dir al respecte. Al principi d'aquest punt s'ha explicat per què s'ha emprat la xarxa de Bitcoin per a la comparació. Aquesta utilitza un dels protocols menys eficients com és el PoW. No obstant això, hi ha molts més, com el ja anomenat PoS entre d'altres (Bada et al., 2021), tots ells amb menor consum i major eficiència que el PoW. Tanmateix, Bitcoin és la criptomoneda més important per ser la primera a sortir a la xarxa i de la que tothom en parla.

En últim terme, es pot al·legar que, primer, tot i les limitacions que ofereixen els estudis referents als consums del sistema financer tradicional, no hi ha millors fonts que n'indiquin de diferents, per la qual cosa es consideren com úniques referències. Segon, i en conseqüència, que el consum d'aquest és més elevat que el de la xarxa de Bitcoin i per extensió, de la xarxa blockchain. Aquesta última afirmació se sosté gràcies a la següent inferència. En primer lloc, Bitcoin domina actualment la capitalització de mercat de criptomonedes amb sistema de verificació PoW, seguit, respectivament, d'Ethereum, Dogecoin i Litecoin, entre d'altres. Després, a més capitalització de mercat, més interès hi ha per la moneda en qüestió i més elevat és el seu valor, per tant, més rendible resulta minar la moneda en qüestió, i augmenta el nombre de validadors. En segon lloc, el principal indicador del consum d'energia és el hashrate, com s'ha explicat amb anterioritat, el poder de computació. Aquest és d'aproximadament 200.000.000 TH/s a Bitcoin (Bitcoin Hashrate, 2022), mentre que el d'Ethereum se situa al voltant de 1.100 TH/s (Ethereum hashrate, 2022) i les dues restants es troben en una mitjana de 500 TH/s cadascuna (Litecoin Hashrate, 2022). En tercer lloc, tot i que el hashrate disminueix amb la capitalització de mercat, suposant que cadascuna de les següents 6 criptomonedes més importants en PoW

consumeixen també una mitjana de 500TH/s, sumarien juntament amb les ja anomenades (exceptuant Bitcoin) un hashrate total de 5100TH/s, el que suposa un 0,00255% del hashrate de Bitcoin. Per tant, tenint en compte aquestes premisses, juntament amb què el sistema PoW és el que més energia consumeix i que la resta, com ja s'hi ha arguït, tenen menor consum, es pot extreure que tot i haver comparat la xarxa de Bitcoin, amb les dades de les quals es disposen, actualment el sistema financer mundial té major consum que el conjunt de la xarxa blockchain.

7. Conclusió

No s'entenen les criptodivises sense Bitcoin, però tal vegada el futur exigeixi canviar aquest fet. La criptomoneda més rellevant no té cap valor intrínsec, és a dir, no té cap funcionalitat real, més enllà d'efectuar transaccions de manera molt poc eficient o en tot cas, com a reserva de valor. Però, encara que tot comencés amb Bitcoin, no acaba amb ell. La xarxa blockchain obre les portes a un nou espai de desenvolupament de projectes i propostes que fa uns anys ni es plantejaven. Molts dels quals tenen de marge de millora i que aniran avançant de la mà amb la tecnologia oferint noves funcionalitats i millorant en eficiència.

Recollint el més important, s'ha conclòs que el sistema financer tradicional comporta una despesa elèctrica més elevada que la de la xarxa blockchain, però cal dir que no és una comparació entre iguals. Aquesta última dona servei a un nombre molt reduït de persones en comparació amb el sistema tradicional. Encara que hi ha moltes propostes i projectes que aposten per una gran escalabilitat per solucionar aquest problema (Zhou et al., 2020). D'altra banda, com s'ha explicat al punt 1.2, les possibilitats que ofereix la xarxa blockchain són altre segell diferenciador d'aquesta tecnologia, que permet des d'aplicacions en l'àmbit financer fins a l'àmbit mèdic o industrial.

Ara bé, encara que el consum de la xarxa blockchain sigui menor, no significa que sigui petit. Xarxes com les de Bitcoin, en ser PoW, no són eficients, com s'ha demostrat al llarg de l'escrit. Pel que la migració cap a un altre sistema de verificació de blocs com el PoS és una opció més que viable i, per tant, recomanable. Finalment, cal dir que aquesta tecnologia és relativament nova si la comparem amb el sistema financer tradicional, que va néixer a l'antiga mesopotàmia (Davies, 2016) i ha anat evolucionant i adaptant-se als nous temps. En els quals mai havia tingut cap adversari en el seu camp, fins ara. Amb tot,

es pot entendre que la blockchain és competidora perquè hi ha corrents de pensament que així ho defensen, com també està la postura contrària, on les dues estan dissenyades per conviure i maximitzar l'eficiència una de l'altra creant fins i tot certa sinergia.

Sigui com sigui, la blockchain encara té problemes a solucionar com el trilema de l'escalabilitat, la seva eficiència o la implementació en diferents sectors de la societat, entre d'altres. D'altra banda, però, aquesta tecnologia pràcticament acaba de néixer i consta d'una gran capacitat de millora, un potencial emergent que dia a dia avança amb nous projectes, funcionalitats i actualitzacions.

8. Bibliografia

- Abou Jaoude, J., & George Saade, R. (2019). Blockchain applications - Usage in different domains. *IEEE Access*, 7, 45360–45381.
<https://doi.org/10.1109/ACCESS.2019.2902501>
- Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare 2019, Vol. 7, Page 56*, 7(2), 56.
<https://doi.org/10.3390/HEALTHCARE7020056>
- Alharby, M., & van Moorsel, A. (2017). Blockchain-based Smart Contracts: A Systematic Mapping Study. *Fourth International Conference on Computer Science and Information Technology (CSIT-2017)*, 125–140.
<https://doi.org/10.5121/csit.2017.71011>
- Allen, D. W. E., Berg, A., Berg, C., Markey-Towler, B., & Potts, J. (2019). Some economic consequences of the GDPR. *Economics Bulletin*, 39(2), 785–797.
<https://ideas.repec.org/a/ebl/ecbull/eb-18-00834.html>
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, 100, 143–174. <https://doi.org/10.1016/J.RSER.2018.10.014>
- Ankalkoti, P., & Santhosh, &. (2017). A Relative Study on Bitcoin Mining. *Imperial Journal of Interdisciplinary Research (IJIR)*, 3(5).
- Auer, R., Monnet, C., & Shin, H. S. (2021). Permissioned Distributed Ledgers and the Governance of Money. *SSRN Electronic Journal*.
<https://doi.org/10.2139/SSRN.3770075>
- Bada, A. O., Damianou, A., Angelopoulos, C. M., & Katos, V. (2021). Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption. *Proceedings - 17th Annual International Conference on Distributed Computing in Sensor Systems, DCOS 2021*, 503–511.
<https://doi.org/10.1109/DCOSS52077.2021.00083>

- Beekhuizen, C. (2021, May 18). *Ethereum's energy usage will soon decrease by ~99.95%* / *Ethereum Foundation Blog*. Ethereum Foundation Blog.
<https://blog.ethereum.org/2021/05/18/country-power-no-more/>
- Blandin, A., Pieters, G. C., Yue Wu, Anton Dek, Thomas Eisermann, Njoki, D., & Taylor, S. (2020). 3rd Global Cryptoasset Benchmarking Study. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.3700822>
- Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020). Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digital Communications and Networks*, 6(4), 480–485.
<https://doi.org/10.1016/J.DCAN.2019.12.001>
- Chen, Y. C., Chou, Y. P., & Chou, Y. C. (2019). An image authentication scheme using Merkle tree mechanisms. *Future Internet*, 11(7).
<https://doi.org/10.3390/FI11070149>
- Chohan, U. W. (2018). Proof-of-Stake Algorithmic Methods: A Comparative Summary. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.3131897>
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303.
<https://doi.org/10.1109/ACCESS.2016.2566339>
- Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. *Future Internet 2017, Vol. 9, Page 25*, 9(3), 25. <https://doi.org/10.3390/FI9030025>
- Cong, L. W., He, Z., Li, J., Thank, W., Baldimtsi, F., Bonneau, J., Bouvard, M., Chowdhry, B., Diamond, D., Halaburda, H., Jiang, W., Lyandres, E., Li, Y., Lowery, R., O'hara, M., Panayotov, G., Saleh, F., Tinn, K., Yang, L., ... Zhang, X. (2021). Decentralized Mining in Centralized Pools. *The Review of Financial Studies*, 34(3), 1191–1235. <https://doi.org/10.1093/RFS/HHAA040>
- Davies, G. (2016). *A History of Money* (D. Connors, Ed.; 4th ed.). University of Wales Press. <https://www.bookdepository.com/es/History-Money-Glyn-Davies/9781783163090>

- de Vries, A. (2020). Bitcoin's energy consumption is underestimated: A market dynamics approach. *Energy Research and Social Science*, 70. <https://doi.org/10.1016/J.ERSS.2020.101721>
- de Vries, A. (2021). Bitcoin boom: What rising prices mean for the network's energy consumption. *Joule*, 5(3), 509–513. <https://doi.org/10.1016/J.JOULE.2021.02.006>
- Drusinsky, D. (2022). On the High-Energy Consumption of Bitcoin Mining. *Computer*, 55(1), 88–93. <https://doi.org/10.1109/MC.2021.3123781>
- Echebarría, M. (2017). Contratos electronicos autoejecutables (smart contract) y pagos con tecnología blockchain - Dialnet. *Revista de Estudios Europeos*, 70, 69–97. <https://dialnet.unirioja.es/servlet/articulo?codigo=6258551>
- Ernst & Young. (2020). *Sustainability Report 2020*. https://www.wertewelt.dzbank.de/content/wertewelt/en/home/reports_und_downloads.html
- Eshani, G., Rajdeep, D., Shubhankar, R., & Baisakhi, D. (2021). An Analysis of Energy Consumption of Blockchain Mining and Techniques to Overcome It. *Lecture Notes on Data Engineering and Communications Technologies*, 62, 783–792. https://doi.org/10.1007/978-981-33-4968-1_60
- Ethereum Network Hash Rate Chart | Etherscan*. (s.d.). Recupera't el 23 d'abril de 2022 de <https://etherscan.io/chart/hashrate>
- Gallersdörfer, U., Klaaßen, L., & Stoll, C. (2020). Energy Consumption of Cryptocurrencies Beyond Bitcoin. *Joule*, 4(9), 1843–1846. <https://doi.org/10.1016/J.JOULE.2020.07.013>
- Ghiro, L., Restuccia, F., D'Oro, S., Basagni, S., Melodia, T., Maccari, L., & lo Cigno, R. (2021). A blockchain definition to clarify its role for the internet of things. *2021 19th Mediterranean Communication and Computer Networking Conference, MedComNet 2021*. <https://doi.org/10.1109/MEDCOMNET52149.2021.9501280>
- Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access*, 8, 125244–125262. <https://doi.org/10.1109/ACCESS.2020.3007251>

- Labazova, O., Dehling, T., & Sunyaev, A. (2019). From Hype to Reality: A Taxonomy of Blockchain Applications. *2nd Hawaii International Conference on System Sciences (HICSS 2019)*. <https://ssrn.com/abstract=3250648>
- Li, A., Wei, X., & He, Z. (2020). Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems. *Sustainability 2020, Vol. 12, Page 2824, 12(7)*, 2824. <https://doi.org/10.3390/SU12072824>
- Litecoin Hashrate Chart - LTC Hashrate - CoinWarz*. (s.d.). Recupera't el 18 d'abril de 2022 de <https://www.coinwarz.com/mining/litecoin/hashrate-chart>
- Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating global data center energy-use estimates: Growth in energy use has slowed owing to efficiency gains that smart policies can help maintain in the near term. *Science*, 367(6481), 984–986. https://doi.org/10.1126/SCIENCE.ABA3758/ASSET/70886364-447C-470D-ACB4-E0C17FB2276E/ASSETS/GRAPHIC/367_984_F3.JPEG
- McCook, H. (2014). *An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network*. https://www.academia.edu/10701244/Relative_Sustainability_2nd_Edition
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*. <https://www.debr.io/article/21260.pdf>
- Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. Xavier Olleros & Majlinda Zhegu (Eds.), *Research Handbooks on Digital Transformations* (pp. 225–253). Edward Elgar Publishing Ltd. <https://doi.org/10.4337/9781784717766.00019>
- Principales datos*. (s.d.). Recupera't el 21 d'abril de 2022 de <https://www.caixabank.com/es/sobre-nosotros/nuestro-negocio/principales-datos.html#>
- Rejeb, A., Rejeb, K., Keogh, J. G., Rejeb, A., Rejeb, K., & Keogh, J. G. (2021). Centralized vs. decentralized ledgers in the money supply process: a SWOT analysis. *Quantitative Finance and Economics 2021 1:40*, 5(1), 40–66. <https://doi.org/10.3934/QFE.2021003>

- Rybarczyk, R., Armstrong, D., & Fabiano, A. (2021). *Galaxy Digital Mining On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question*.
- Saleh, F. (2021). Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies*, 34(3), 1156–1190. <https://doi.org/10.1093/RFS/HHAA075>
- Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences 2019, Vol. 9, Page 1788*, 9(9), 1788. <https://doi.org/10.3390/APP9091788>
- Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *Proceedings - 1st International Conference on Peer-to-Peer Computing, P2P 2001*, 101–102. <https://doi.org/10.1109/P2P.2001.990434>
- Schueffel, P. (2017). Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph - A High-Level Overview and Comparison. *SSRN Electronic Journal*. <https://doi.org/10.2139/SSRN.3144241>
- Tripoli, M., & Schmidhuber, J. (2018). *Emerging Opportunities for the Application of Blockchain in the Agri-food Industry Agriculture*. https://www.researchgate.net/publication/327867089_Emerging_Opportunities_for_the_Application_of_Blockchain_in_the_Agri-food_Industry
- Bitcoin Wallets*. (s.d.). Recupera't el 21 d'abril de 2022 de <https://www.blockchain.com/charts/my-wallet-n-users>
- Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, 52(3), 51. <https://doi.org/10.1145/3316481>
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564. <https://doi.org/10.1109/BIGDATAACONGRESS.2017.85>
- Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: a Survey. *IEEE Access*, 8, 16440–16455. <https://doi.org/10.1109/ACCESS.2020.2967218>

COMPARACIÓ DEL CONSUM ENERGÈTIC ENTRE EL SISTEMA FINANCER TRADICIONAL I LA XARXA BLOCKCHAIN

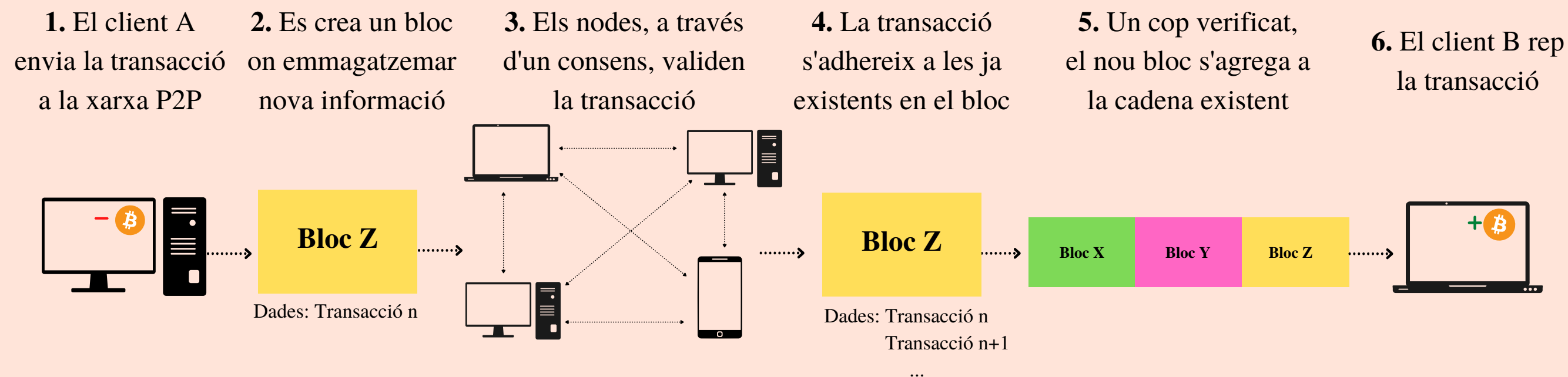
Metodologia

- Metanàlisis de diversos estudis seleccionats a partir d'una revisió sistemàtica.

Què és la blockchain?

- És un sistema que combina xarxes P2P que operen de manera descentralitzada.
- Funciona de manera que es va escrivint informació en nous blocs, la qual és verificada pels participants de la xarxa.
- Hi ha diferents tipus de verificacions, entre les quals destaquen PoW i PoS
- Característiques destacades:
 - Seguretat
 - Transparència
- Té diverses aplicacions. Entre d'altres:
 - Contractes intel·ligents
 - Aplicacions al servei sanitari
- També presenta riscos i limitacions
 - Atacs informàtics i responsabilitat individual
 - Escalabilitat i ineficiència

Funcionament d'una xarxa blockchain



Consum de la blockchain

- Les característiques lligades a cada xarxa determinen les possibilitats d'aquesta, però dintre de les limitacions del sistema de verificació

LA XARXA DE BITCOIN (PoW)

- Baixa eficiència i alt consum energètic
 - Màxim 7 transaccions per segon
 - Consum entre 87,1 TWh i 135 TWh

XARXES PoS

- Millora en eficiència i consum
 - Disminueix entre el 75% i el 99%

El sistema financer tradicional

- Utilitzen sistemes de dades centralitzats
 - Ràpids i eficients
 - S'ha de delegar confiança en un tercer
 - Menys seguretat i privacitat

CONSUM D'ENERGIA

- Dificultats per calcular estimacions
 - Poca transparència amb les dades
 - Estructura críptica. Què s'ha de comptabilitzar?
- Estimacions resultades de diferents metodologies
 - Entre 358,5 TWh i 650 TWh

Consideracions

- La blockchain dona servei a 82.5 M de persones
- El sistema financer tradicional dona servei a 5.000 M de persones
- El consum de Bitcoin representa una grandíssima part del consum total de la xarxa blockchain

Conclusions

- Consum màxim de Bitcoin --> 135 TWh
- Consum mínim del sistema financer --> 358.5 TWh
- Per extensió, el sistema financer tradicional té un consum més elevat que la xarxa blockchain
- Ni ofereixen servei al mateix nombre de persones, ni les mateixes funcionalitats