Revista de Comptabilitat i Direcció
Vol. 27, any 2018, pp. 11-31

Tecnologia blockchain, una nova era per a l'empresa

LUZ PARRONDO
UPF-Barcelona School of Management

Data de recepció: 20/01/2018
Data d'acceptació: 20/02/2018

RESUM

Des del 2009, blockchain ha servit com a una tecnologia de registres potencialment transformadora que s'espera que sigui tan revolucionària com internet. Originalment desenvolupada com una metodologia per registrar transaccions de criptomonedes, la funcionalitat de blockchain ha evolucionat en una gran quantitat d'aplicacions, tals com banca, mercats financers, comptabilitat, cadenes de subministraments, sistemes de votació i serveis governamentals. Aquest document té com a objectiu explicar en què consisteix la tecnologia blockchain alhora que proporcionar una discussió inicial sobre com blockchain podria permetre un ecosistema empresarial en temps real, verificable i transparent. A més, blockchain té el potencial de crear empreses digitals a través de contractes intel·ligents que permeten automatitzar i democratitzar la presa de decisions.

Classificació JEL: O30, O33

PARAULES CLAU

Blockchain, xarxa de registres distribuïts, tecnologia, empresa.

ABSTRACT

Since 2009, blockchain has served as a potentially transformative record technology that is expected to be as revolutionary as the

Internet. Originally developed as a methodology for registering cryptocurrency transactions, blockchain's functionality has evolved into a large number of applications, such as banking, financial markets, accounting, supply chains, voting systems and government services. This document aims to explain blockchain technology while providing an initial discussion on how this innovation could allow a real-time, verifiable and transparent business ecosystem. In addition, blockchain has the potential to create digital companies through intelligent contracts that allow automation and democratization of decision-making.

Classification JEL: O30, O33

KEYWORDS

Blockchain, distributed ledger technology, technology, business.

1. Introducció

La tecnologia blockchain és la base tecnològica de bitcoin, descrita per primera vegada per l'anònim Shatoshi Nakamoto, en el llibre blanc *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008). És una base de dades distribuïda on cada node o usuari a la xarxa executa i registra transaccions agrupant-les en forma de blocs. És una forma segura, transparent i descentralitzada de registrar transaccions que no es limita únicament a les monedes digitals, tot i que va saltar a la fama quan el 2013 bitcoin va experimentar una pujada del 1.000%. La capacitat de blockchain de registrar **tot tipus de transaccions** persona-a-persona de manera eficient, segura, verificable i immutable significa que pot aplicar-se a tasques no financeres com la comptabilitat o la traçabilitat de productes en la cadena de subministraments. Podria ajudar a resoldre finalment el problema de pirateria de música i vídeo i permetre que els mitjans digitals siguin legítimament comprats, venuts i heretats. Des d'un vessant social, pot ser utilitzada en la transmissió de vots, per ajudar a certificar si un producte és d'origen ètic, si la roba es fabrica en tallers legals o si les donacions arriben a la destinació esperada. També presenten oportunitats en tota mena de serveis públics, com pagaments de la salut i el benestar i fins i tot per a la verificació documental en el registre de la propietat. Tot això de forma transparent, segura i prescindint d'intermediaris que validin la identitat de les parts, la titularitat dels actius o la validesa en una transacció.

La crisi del 2007 va destruir la confiança en els intermediaris financers i va ser el detonant per desenvolupar una tecnologia amb capacitat de desplaçar el control de les operacions des dels bancs fins als usuaris, i així reduir la necessitat d'un intermediari validador. Aquesta desintermediació podria significar una transparència més gran i una democratització dels sistemes financers, econòmics i fins i tot polítics molt millor. No obstant això, no hem de desmerèixer el poder dels governs i dels gegants financers i econòmics, que actualment inverteixen en aquesta tecnologia per situar-se en l'avantguarda de la nova era.

No obstant això, la segona derivada d'aquesta tecnologia pot significar una revolució per a la innovació empresarial i els mitjans de finançament de nous projectes. La cadena de blocs té la capacitat d'incorporar aplicacions sobre la seva estructura com els contractes intel·ligents o *smart contracts* i les aplicacions distribuïdes o DApps[1]. Els contractes intel·ligents no solament defineixen les regles i les sancions entorn d'un acord, de la mateixa manera que ho fa un contracte tradicional, sinó que també fan complir aquestes obligacions automàticament. Permeten automatitzar mecanismes empresarials com pagaments, acords i registres aplanant el camí per a la implementació de les organitzacions autònomes descentralitzades (DAO). Una DAO és un contracte intel·ligent complex que dona origen a una organització digital mancada de caps o d'empleats, en la qual les decisions es prenen de forma descentralitzada i les accions s'executen de forma automàtica, transparent i sense necessitat d'intervenció humana.

Aquest article proporciona una aproximació accessible per a aquells empresaris que estiguin interessats a aprendre més sobre el desenvolupament de blockchain i el seu potencial impacte en l'empresa, l'economia i la societat. La secció dos presenta una introducció sobre com funciona la tecnologia blockchain. La tercera analitza l'impacte en l'estructura empresarial, en àrees com la comptabilitat, l'auditoria, la cadena de subministraments i el finançament. A l'apartat quatre s'explica en què consisteixen les DAO i, finalment, la secció cinc conclou i anima a la reflexió i el debat sobre aquesta controvertida tecnologia que ha premut l'accelerador en els dos últims anys.

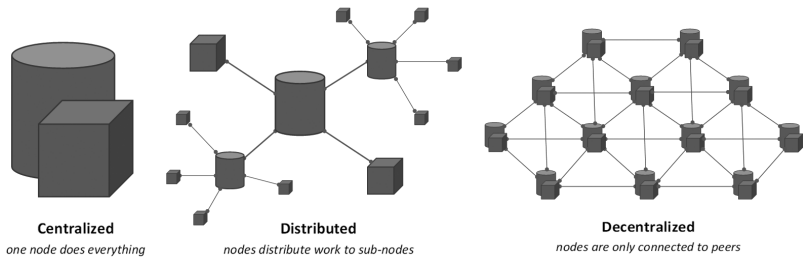
---

1. Una DApp és molt similar a una aplicació web tradicional. La interfície usa la mateixa tecnologia per renderitzar la pàgina. L'única diferència fonamental és que en lloc d'una API que es connecta a una base de dades, té un contracte intel·ligent que es connecta a una cadena de blocs.

2. Què és la tecnologia blockchain

Abans d'intentar comprendre com funcionen les xarxes blockchain, val la pena analitzar les xarxes tradicionals. Durant segles, les organitzacions han utilitzat bases de dades per registrar transaccions i informació i els governs les han usat per mantenir registres públics, com per exemple la propietat de la terra. Fins ara sempre ha estat necessària la presència d'una autoritat central, el banc o l'oficina governamental, que gestioni els canvis en les transaccions, per identificar qui posseeix el què en un moment donat. Això els permet comprovar si les noves transaccions són legítimes, que els mateixos 10 € no es gasten dues vegades i que el venedor d'una casa n'és el propietari. Atès que els usuaris confien que l'intermediari verifica les transaccions correctament, les persones poden intercanviar actius entre si malgrat no conèixer-se. La funció d'aquests intermediaris és la de proveir la confiança necessària entre les parts i la de controlar l'accés a la informació en el registre oficial. Aquests registres centralitzats i privats presenten, malgrat l'impuls que va suposar la tecnologia digital, unes ineficiències en temps i costos, així com una opacitat incapaç de frenar la proliferació de fraus i crisi de confiança.

Blockchain substitueix l'entitat central en la legitimació de les transaccions. Aquesta funció és possible gràcies a la seva arquitectura distribuïda (vegeu la figura 1) i a un sistema d'algorismes i d'incentius anomenat mineria que assegura una única veritat registral.

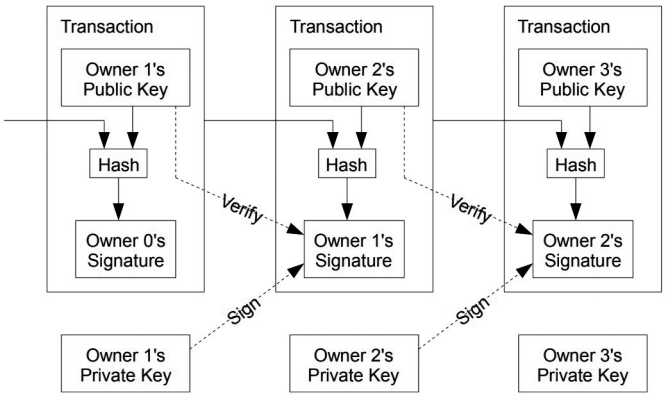


Font: *Mesh World P2P Simulation Hypothesis*, Eric Grange.

Figura 1. Tipus de sistemes.

Blockchain té el seu origen en les criptomonedes, específicament en bitcoin. Satoshi Nakamoto, en el seu llibre blanc sobre bitcoin, defineix la moneda electrònica com una cadena de signatures digitals. El propietari d'una moneda pot transferir-la a una altra persona afegint-hi, al final de la cadena, la signatura digital del codi de la transacció anterior i la clau pública

del nou propietari (vegeu la figura 2). El repte d'aquest sistema és la verificació de la propietat i la no duplicitat de les transaccions. L'única forma de verificar que la moneda pertany al transmissor i que aquest no l'ha gastada prèviament és conèixer totes les transaccions anteriors. Blockchain ofereix un sistema en el qual les transaccions són públiques i els participants confirmen que solament existeix una veritat. Aquesta veritat està codificada en una cadena en forma de blocs que no està emmagatzemada en un servidor sinó distribuïda en tots els nodes de la xarxa. Qualsevol node en el sistema pot sol·licitar que s'agregui una transacció a la cadena de blocs, però les transaccions solament s'accepten si tots els usuaris en validen la legitimitat. Aquest procés de verificació es diu mineria[2] o *mining*. Cada participant verificador o miner valida que la sol·licitud prové de la persona autoritzada. Certifica que el transmissor és el propietari i que la moneda no ha estat transmesa amb anterioritat. El poder d'aquesta tecnologia resideix en la seva extensa aplicabilitat. A més de monedes, la cadena pot transmetre qualsevol altre actiu, des d'accions i bons fins a vots o registres de propietat.



Font: *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto, 2008.

Figura 2. Tipus de sistemes.

Una vegada afegit el nou bloc en la cadena, cap usuari pot eliminar-ho. La inviolabilitat d'aquest sistema està garantida pel fet que la informació no

2. Mineria és el procés de consens descentralitzat que es produeix a la xarxa p2p amb l'objecte de validar les transaccions dels usuaris i evitar que s'incloguin despeses duplicades en la cadena de blocs; els nodes de la xarxa són recompensats amb blocs de monedes digitals. Això es pot pensar com un pagament al node a canvi del servei de crear un bloc en la cadena de consens.

es troba centralitzada en un únic custodi o intermediari, sinó distribuïda entre tots els usuaris del sistema. *Hackejar* aquests registres implica un atac simultani a tots els nodes del sistema. No pot haver-hi una «xarxa de registres falsa» perquè tots els usuaris tenen la seva pròpia versió original per contrastar.

Aquestes xarxes de registres es descriuen com «sense permís» o *permissionless*, perquè no existeix una autoritat que pugui negar el permís per participar en la verificació, l'addició i la visió de les transaccions (Pass & Shi). Malgrat l'evident controvèrsia d'aquesta característica, els seus defensors li atribueixen uns valors socials i polítics com la transparència, la redistribució del poder i l'increment de la democràcia. Posteriorment, i per exigències en molts casos empresarials, certes plataformes han configurat xarxes «autoritzades», on un grup limitat de participants té la capacitat d'accedir-hi, verificar i agregar transaccions en la cadena de registres. Els detractors d'aquesta opció adverteixen que va en contra de la idea original per la qual Shatosi Nakamoto[3] la va crear, ja que permet als intermediaris, com els bancs i els governs, perpetuar el control.

3. Classificació de les xarxes

Basant-nos en l'accés a les dades emmagatzemades, podem classificar les xarxes com a públiques o privades. En la primera, no hi ha cap restricció per a la lectura de dades per part dels usuaris; en canvi, en la segona, la lectura es limita a participants determinats.

D'altra banda, recolzant-se en la capacitat per generar i agregar nous blocs, les xarxes es divideixen en «sense permisos» o *permisionless* i «amb permisos» o *permissioned*. En les primeres no hi ha restriccions per poder realitzar transaccions i crear nous blocs, de manera que s'ofereixen monedes o actius digitals (tokens[4]) natius de la xarxa com recompensa als usuaris que vulguin realitzar la funció de miners. Són xarxes descentralitzades i un exemple és la famosa plataforma Bitcoin. Les segones són desenvolupades per entitats generalment privades, en molts casos per a l'ús intern, i els seus usuaris necessiten uns permisos, per part dels administradors de la xarxa, per interactuar amb el protocol. Són centralitzades, és a dir, controlades per l'en-

3. *Bitcoin: A Peer-to-Peer Electronic Cash System*.

4. El token és un actiu o valor generat per les empreses per a diferents propòsits. S'assimilen a les accions o els bons però també poden ser utilitzats per adquirir productes o serveis i per tant com cupons de fidelització, per exemple. Per a més informació, vegeu la secció 4, apartat «Finançament» d'aquest article.

titat i no pels usuaris i el procés de verificació no es basa en un sistema de recompenses, ja que els permisos es concentren en una de sola organització.

Donades aquestes possibles característiques, podríem dividir blockchain en tres tipus fonamentals:

- **Blockchain pública:** Una blockchain pública és una xarxa a la qual qualsevol persona pot accedir, pot crear blocs i pot participar en el procés de consens o procés de validació. Com ja hem explicat, el proveïdor de confiança en aquestes xarxes públiques és la mineria, una combinació d'incentius econòmics i verificació criptogràfica utilitzant mecanismes com *Work of Proof* (WoP) o *Work of Stake* (WoS), i aquesta última és més eficient en termes de cost energètic i computacional (Dispenza, Garcia & Molecke, 2017). Aquests mecanismes es basen en el principi que el poder de validació és proporcional a la quantitat de recursos econòmics que poden aportar. Aquestes cadenes de blocs generalment es consideren «totalment descentralitzades». Bitcoin, Ethereum, Litecoin, Namecoin són exemples de xarxes públiques.
- **Blockchain de consorci:** Una blockchain de consorci és una cadena de blocs on el procés de consens és controlat per un conjunt de nodes preseleccionats; per exemple, un podria imaginar un consorci de 15 organitzacions, cadascuna de les quals opera un node i 10 han de signar perquè el bloc sigui vàlid. La lectura pot ser pública o restringida als participants. Aquestes cadenes de blocs es poden considerar «parcialment descentralitzades».
- **Blockchain privada:** Una blockchain totalment privada és una cadena de blocs on els permisos d'escriptura es mantenen centralitzats en una organització. Els permisos de lectura poden ser públics o restringits de forma arbitrària. Les possibles aplicacions inclouen l'administració de les bases de dades o auditoria internes a una sola empresa, per la qual cosa la lectura pública pot no ser necessària en molts casos. Hyperledger és un dels projectes que més suport ha suscitat per crear blockchains privades transversals. Hyperledger està format per desenes de membres associats que pretenen desenvolupar una plataforma comuna i universal per a blockchains privades. Empreses com IBM, Intel, Cisco, JP Morgan, Wells Fargo, State Street, el London Stock Exchange Group o Accenture formen part d'aquest conglomerat.

Sembla probable que en el futur hi haurà moltes blockchains públiques i milions de blockchains privades dissenyades per a mercats específics. Totes elles variaran en protocols però usaran la tecnologia de cadena de blocs

comuna. Seria comparable a l'existència de diferents sistemes operatius: per exemple, Android i GNU/Linux comparteixen una petita part del seu codi, el nucli, però són sistemes operatius totalment diferents. Les seves llibreries són diferents, la qual cosa fa que les aplicacions de tots dos sistemes es desenvolupin de forma totalment diferent, i que, per tant, les de l'un no siguin compatibles amb les de l'altre. Així mateix, cada blockchain tindrà un mecanisme de consens diferent, un llenguatge de contracte intel·ligent específic i unes característiques úniques.

4. Terminologia

Els termes que al·ludeixen a aquesta tecnologia solen ser tres: blockchain, tecnologia de registres distribuïts (DLT) i tecnologia bitcoin, per haver-ne estat l'impulsor.

Blockchain pot al·ludir tant a la tecnologia en el seu conjunt com a les plataformes que la implementen. Acompanyar la paraula amb «tecnologia» sol ser l'adequat per al·ludir a la tecnologia en un context ampli, i aquest, al seu torn, és un terme que sol usar-se en les cadenes públiques. Existeix certa polèmica en si s'hauria de dir, o no, blockchain en les plataformes privades. No obstant això, aquest ús no és limitador, ja que molts bancs el fan servir per referir-se a les seves proves i, en general, és el més utilitzat per tots els desenvolupadors i usuaris.

Tecnologia de registres distribuïts o *Distributed Ledger Technology* és sinònim de tecnologia blockchain. No obstant això, sol usar-se en l'àmbit del desenvolupament privat i més aviat allunyada de bitcoin com a criptomoneda. A diferència de blockchain, no posseeix un doble significat, perquè solament és capaç d'al·ludir a la tecnologia de forma completa.

Finalment, tecnologia bitcoin és el terme més ambigu dels tres. Pot fer referència a tres conceptes: la DLT en el seu conjunt, la blockchain de bitcoin en particular o fins i tot els protocols que han permès el desenvolupament de totes les criptomonedes. A causa d'això, no acostuma a utilitzar-se gaire.

5. Criptomonedes i tokens

La creació de bitcoin va precipitar l'expansió d'un ecosistema de monedes i tokens, totes elles considerades criptomonedes, tot i que no totes entren dins de la definició formal de *moneda*. Una moneda representa tècnicament (1) **una unitat de compte,** (2) **una reserva de valor** i (3) **un mitjà de canvi**, i atès que aquest ecosistema va ser iniciat a partir de la creació de

bitcoin, que compleix amb les tres característiques, totes es consideren criptomonedes malgrat que la majoria no ho són.

A l'hora de distingir entre criptomoneda i token, podem reduir-ho en termes generals al fet que una moneda digital és solament això, una moneda, o mitjà de pagament, mentre que un token té una funcionalitat més àmplia. Però en la pràctica, la línia entre les monedes i els tokens no és tan nítida i en moltes ocasions s'utilitzen ambdues paraules de forma confusa i intercanviable. No hem d'oblidar que la paraula *token* posseeix múltiples accepcions, des de moneda fins a fitxa i fins i tot xec-regal. Tradicionalment s'ha emprat per referir-nos a fitxes que s'utilitzen com a moneda de canvi en esdeveniments privats com per exemple concerts. Així mateix, en moltes ocasions ens referim a bitcoin com token i confonem un token amb una criptomoneda. A mesura que la tecnologia criptogràfica ha anat avançant, la distinció s'ha fet cada vegada més clara i, en aquest moment, podem considerar la següent bifurcació: (1) les criptomonedes, que inclouen el bitcoin i les altcoins[5], la funció de les quals és la de mitjà de pagament, i (2) els tokens o criptovalors, que incorporen funcions addicionals.

La majoria d'altcoins són una variant de bitcoin, construïda utilitzant codi obert de bitcoin amb alguns canvis. Però també n'existeixen d'altres que han creat la seva pròpia cadena de blocs i els seus propis protocols i han generat una moneda nadiua. Exemples d'aquestes criptomonedes inclouen Ethereum, Litecoin, Dash, Ripple, Omni, Nxt, Waves i Counterparty. La mineria de bitcoin requereix un gran poder de còmput, la qual cosa implica uns costos alts per als miners que es dediquen a aquesta tasca. L'algorisme creat pel litecoin permet que gairebé qualsevol sistema de còmput pugui realitzar mineria, sense la necessitat de grans inversions en maquinari. D'altra banda, l'altcoin Dash incrementa l'anonimat dels qui participen en la xarxa i millora la velocitat de les transaccions. Una diferència més entre les diverses criptomonedes en relació amb bitcoin, en un àmbit ja no tècnic, és el del propòsit de la moneda digital. L'altcoin Ripple va sorgir per servir com a intermediari per a tota transacció d'unitats de valor, és a dir, està dissenyat per connectar diferents sistemes de pagament. El nínxol al qual apunta és al del canvi de divises, un aspecte que el bitcoin no integra.

D'altra banda, els tokens són un actiu o un valor que se situa sobre una cadena de blocs determinada. En aquest cas, les plataformes més freqüents són Ethereum[6] o Wave. Els tokens poden representar bàsicament qualsevol

5. Altcoins són monedes alternatives al Bitcoin.

6. Vegeu: Ethereum White Paper <https://github.com/ethereum/wiki/wiki/White-Paper>.

actiu que sigui fungible i negociable: des de participacions en projectes empresarials fins a mitjans de pagament. Un exemple de tokens són els *Energy Efficiency Coins* (EEcoin). Aquest és un cas que, com hem esmentat anteriorment, pot dur a confusió. Malgrat que en la seva denominació apareix la paraula *coin*, no fa referència a una moneda sinó a un token a través del qual es pot participar en un ecosistema blockchain d'energies renovables votant i proposant nous projectes. Els propietaris de tokens tenen dret a votar i hi poden comerciar, però no tenen els drets d'un accionista, encara que pugui semblar equiparable[7]. La funció més habitual dels tokens és la de recaptar fons per a projectes específics, cosa que ens recorda molt més al *crowdfunding* que a les IPO. No obstant això, de vegades es pot recompensar amb participació en beneficis als posseïdors de tokens, o bé poden utilitzar aquests tokens per comprar els productes i els serveis de l'organització.

Crear tokens és un procés molt senzill, ja que no s'han de modificar els codis d'un protocol en particular ni crear una cadena de blocs des de zero, tot el que s'ha de fer és seguir una plantilla estàndard en la plataforma blockchain. Aquesta simplicitat n'ha potenciat l'ús entre les empreses que, com explicarem en seccions posteriors, els utilitzen per a campanyes de fidelització o per a recaptació de fons a través d'una oferta inicial de monedes o *Initial Coin Offering* (ICO).

6. Impacte en l'empresa

El camí cap al futur demana acoblar diferents entitats productives, la digitalització sustentada a les noves tecnologies i la possibilitat de democratitzar no només la informació sinó també els actius de valor. La digitalització és la base de l'anomenada indústria intel·ligent, portada de la mà del IoT (Internet de les Coses), la comunicació Machine to Machine (M2M), el Cloud, Big Data, Machine learning, etc.

A totes aquestes tecnologies ara s'uneix la tecnologia blockchain. Aquesta cadena de blocs proporciona un nou univers de comunicació, d'interacció i de confiança a les empreses. La introducció de noves aplicacions

7. El llibre blanc d'EECoin especifica: «EECoin is not a security, future, or share, it is not a guarantee of ownership in a company or any underlying assets, or a claim against any consumer rights as guaranteed by EnLedger. The goal of this structure is to offer the public a way to participate in an energy-efficient blockchain network and to provide capital to renewable energy projects, increasing price competition for renewable energy assets and thereby enabling society to directly provide a market incentive for production of renewable forms of energy as opposed to nonrenewable ones».

industrials requereix un grau creixent de seguretat i de protecció de la privadesa; la prova d'existència o d'origen i la traçabilitat guanyen cada vegada una importància més gran. Confiar en els registres temporals i en la integritat de les dades pot ser un requisit crucial. Per això, blockchain té el potencial de canviar la forma en què l'empresa digitalitzada s'aproxima al futur, amb una seguretat més gran i una qualitat en les dades.

Els principals avantatges d'aquesta tecnologia són:

- Intercanvi sense intermediació de tercers: És possible l'intercanvi d'actius entre dues parts sense la supervisió de tercers, reduint riscos considerablement.
- Inviolabilitat: Blockchain pot resistir atacs maliciosos millor, ja que manca d'un punt central feble, en utilitzar-se xarxes descentralitzades.
- Transparència: Les dades sota blockchain estan globalment disponibles, són verificables i es transmeten en temps real.
- Control de l'usuari: Els usuaris poden controlar totes les seves transaccions i la informació.
- Immutabilitat: Cada transacció és immutable; no pot ser eliminada o modificada.
- Simplificació del sistema comptable: En afegir cada transacció a una simple comptabilitat pública, reduïm la complexitat de múltiples comptabilitats.
- Transaccions eficients: Blockchain atorga una seguretat més alta, rapidesa i eficàcia. Aquesta productivitat fa que es redueixin despeses generals i costos intermediaris innecessaris, en requerir menys seguiment i control.

L'impacte d'aquesta aplicació tecnològica pot abastar totes les àrees d'una empresa des de la comptabilitat, passant per la cadena de subministraments, la innovació, el finançament i fins i tot la fidelització de clients.

7. Comptabilitat i auditoria

No seria la primera vegada que una nova forma de registrar les transaccions canvia el món. En els seus inicis, la comptabilitat es basava en registres d'una única entrada. Amb el desenvolupament del comerç, aquest sistema ha esdevingut obsolet. Al voltant de l'any 1400, al nord d'Itàlia va sorgir una nova tècnica de comptabilitat, més tard coneguda com a comptabilitat de doble entrada. Va ser un gran pas en el desenvolupament de l'empresa i l'economia modernes. Aquest avanç tecnològic va permetre l'accés i el se-

guiment de la informació financera a tota part interessada més enllà del propietari. Pot semblar un fet irrellevant, però Werner Sombart, un sociòleg alemany que va morir el 1941, va argumentar que la doble entrada comptable va marcar el naixement del capitalisme. Després de 500 anys sense grans canvis, la comptabilitat torna a mostrar-se obsoleta (*The End of Accounting and the Path Forward for Investors and Managers*, 2016).

El canvi que la comunitat comptable estava esperant arriba de la mà d'aquesta revolucionària tecnologia. Si la doble entrada va rescatar la informació comptable del cap del comerciant, la cadena de blocs l'allibera dels confins d'una organització. Per definició, blockchain és un llibre de registres distribuït o, en altres paraules, un llibre major distribuït (*Distribuded Ledger Tecnology*). El fet que la signatura digital sigui criptogràfica confereix al registre una poderosa força probatòria i a la pràctica elimina el problema comptable de la veracitat o l'existència registral. Aquest problema es resol compartint els registres: cadascun dels nodes del sistema té una còpia original. Això condueix a dos parells d'entrades dobles connectades per la llista central de rebuts; tres entrades per a cada transacció (Dai & Vasarhelyi, 2017).

El registre distribuït representa un enorme desafiament per a la comptabilitat més enllà de la triple entrada i d'una visibilitat més gran que aquest llibre major distribuït proporciona (Ijiri, 1989). La capacitat de blockchain per registrar múltiples transaccions en temps real és increïblement poderosa. A això se li uneix la possibilitat d'afegir contractes intel·ligents per automatitzar els processos empresarials, com els de pagaments i els de seguiments de control. Per exemple, es podria emetre una ordre de compra contra aquest contracte, factures contra aquesta ordre de compra, pagaments contra aquestes factures, etc., rastrejant qualsevol problema que sorgeixi en el camí. Hi hauria una identificació única relacionada amb el contracte, l'ordre de compra o les factures en aquesta cadena que uniria en un únic bloc informatiu totes les peces independents.

Tenir un llibre de comptabilitat que mostri fàcilment tota la cadena de transaccions relacionades no solament proporcionaria excel·lents registres d'auditoria, sinó que també permetria, a ambdues parts d'una transacció, tenir actualitzacions d'estat en temps real. Cada vegada que s'actualitza la blockchain amb un nou registre, ambdues parts de la transacció poden veure l'actualització immediatament.

8. Cadena de subministraments o *supply chain*

Un altre aspecte important dins del món empresarial i el comerç és la cadena de subministrament. L'escala i la complexitat d'aquests processos

condueix a uns costos transaccionals alts, desajustaments freqüents i errors manuals. Les «cadenes de custòdia» completes, que proven els orígens de cada producte o material, encara estan fragmentades en totes les organitzacions i són vulnerables al frau i a l'error, fins i tot entre les empreses certificades. Les aplicacions basades en blockchain tenen el potencial de millorar les cadenes de subministrament en proporcionar una infraestructura per registrar, certificar i rastrejar a un cost baix els béns transferits entre parts distants, que estan connectades a través d'una cadena de subministrament però que no necessàriament confien entre si. Tots els productes s'identifiquen de forma única a través de registres transferits des del seu origen fins a la seva destinació final a través de blockchain. Cada transacció és verificada i marcada amb el temps en un procés xifrat però transparent que dona visibilitat a les parts implicades com a proveïdors, transportistes o compradors. Els termes de cada transacció romanen irrevocables i immutables, oberts a inspecció per a tots o per als auditors autoritzats. Aquí també els contractes intel·ligents podrien implementar-se per executar automàticament pagaments i altres procediments. Ja existeixen empreses que utilitzen aquesta tecnologia en la seva cadena de subministraments. Everledger permet a les empreses i als compradors rastrejar la procedència dels diamants des de les mines a les joieries i combatre el frau d'assegurances o de documentació. L'empresa social Provenance ha desenvolupat una plataforma de dades en temps real que reuneix i verifica l'origen d'un actiu assignant-li un passaport digital que pot rastrejar-se al llarg de tota la cadena de subministrament fins que arriba a la seva destinació. El gegant Wal-Mart està provant blockchain per a la seguretat alimentària. S'espera que un registre precís i actualitzat basat en blockchain pugui ajudar a identificar el producte, l'enviament i el proveïdor, per exemple, quan ocorre un brot, i d'aquesta manera obtenir detalls sobre com i on es van conrear els aliments i qui els va inspeccionar.

9. Noves vies per als negocis

Moltes són les empreses que veuen en les criptomonedes unes utilitats que van més enllà del simple mitjà de pagament. Chanticleer Holdings Inc., empresa matriu de diverses franquícies de menjar ràpid als Estats Units (BGR, Little Big Burger i American Burger, Just Fresh i alguns restaurants Hooters), utilitzarà la tecnologia blockchain per implementar un programa de recompenses per lleialtat per als clients de les seves cadenes de menjar. El client rebria criptomonedes natives anomenades Merits, les quals podria intercanviar amb altres clients o utilitzar-les per consumir els seus productes

i serveis. Transforma les recompenses tradicionals del consumidor en una cosa que el consumidor pot controlar.

Un inconvenient d'aquest sistema de recompenses és que són fragmentats i segmentats, cosa que provoca ineficiències i rigideses. Hem de recordar que tant les criptomonedes com els punts de lleialtat tradicionals suposen un deute per a les empreses i per tant n'incrementen el passiu. La solució a aquest problema implica substituir els sistemes de lleialtat privats per sistemes universals. Elements coin és una criptomoneda amb base en codi obert acceptada per diverses organitzacions i d'ús universal. Aquest model, els elements, es poden intercanviar per diners fiduciaris i per altres monedes digitals i així reduir el deute de les empreses i incrementar el control dels usuaris. També cal destacar que aquests usuaris posseiran tota la informació sobre les seves transaccions i les organitzacions tindran les dades de les seves respectives interaccions amb els consumidors. El potencial d'aquesta informació en mans de les plataformes és inesgotable.

10. Finançament

És evident que les empreses no han desaprofitat el potencial de les criptomonedes i ho han fet des de diversos enfocaments. Un dels sectors, on les empreses han explotat més aquest potencial, és el sector financer. Al marge de l'eufòria despertada per bitcoin, i el seu gran *boom* especulatiu, les empreses han vist en aquesta tecnologia una nova forma de finançament empresarial més flexible i veloç. Especialment ara que encara es troba poc regulada, comparada amb els mitjans de finançament convencionals.

L'oferta inicial de monedes, també coneguda com a ICO (*Initial Coin Offering*), és un mecanisme de recaptació de fons en el qual els nous projectes empresarials es financen a través de la venda de tokens criptogràfics a canvi de diners o moneda digital (Venegas, 2017). La creació de tokens és molt senzilla; es fa possible mitjançant l'ús de plantilles en plataformes blockchain com Ethereum i de contractes intel·ligents autoexecutables que no necessiten cap tercer per operar. Els tokens es creen i distribueixen al públic a través d'una ICO per finançar el desenvolupament d'un projecte específic.

Les ICO s'han comparat amb dues formes tradicionals de finançament: (1) les ofertes públiques inicials (IPO), en les quals els inversors compren accions d'una empresa, i (2) el model *crowdfunding*, on, com en les ICO, el finançament està lligat a un projecte determinat. En tots dos casos les diferències són significatives i molt lligades a la regulació i a la protecció de l'inversor.

La principal diferència entre el model ICO i IPO és la supervisió reguladora. En una IPO, les empreses han d'incloure un document legal declarant la seva finalitat, a més de complir certs estàndards de transparència. En segon lloc, una empresa solament pot emetre les accions si compleix una sèrie de requisits, com un mínim de guanys o un bon historial. Cap d'aquestes dues condicions és necessària en les ICO. En tercer lloc, les accions atorguen propietat sobre els guanys futurs de l'empresa, els tokens no atorguen propietat sobre el projecte al qual van lligats. Hi ha moltes formes en què els propietaris de tokens poden obtenir beneficis futurs, i això depèn de com estigui estructurada la moneda. Algunes monedes generen valor en tenir participació en els ingressos futurs dels projectes, mentre que altres tenen el valor del seu ús dins de l'ecosistema; com més gran sigui l'ús, més valor tindran. Finalment, la durada de l'oferta és major en les IPO i l'accés als inversors és limitat, mentre que en les ICO està obert a qualsevol persona. Aquestes són importants diferències que un inversor hauria de tenir en compte abans d'adquirir tokens (vegeu: *Crypto ICO vs. Stock IPO: What is the difference?*, 2017).

Respecte a la seva comparació a *crowdfunding* és molt més encertada. Malgrat que podríem considerar les ICO com el *crowdfunding* 2.0, val la pena tenir en compte algunes diferències. Quan s'introdueix un producte en plataformes de *crowdfunding* com Indiegogo, els inversors i els compradors saben exactament què esperar quan el projecte acabi. Per exemple, quan el tauler impulsat amb monopatí elèctric o el rellotge intel·ligent Pebble van iniciar les seves campanyes de finançament col·lectiu, els inversors van poder dir, immediatament, si el producte valia una certa quantitat de diners comparant els productes amb altres al mercat. Per contra, és pràcticament impossible predir el resultat d'una ICO, especialment si els usuaris no entenen l'operativa i les implicacions de la seva inversió. Les ICO en si mateixes no es basen en cap valor de mercat al món real, la qual cosa fa difícil valorar-les. El «producte» associat a aquest *crowdfunding* 2.0 és el token en si mateix. L'empresa, a través de la seva bona gestió, pot revalorar els tokens i així proporcionar plusvàlues al seu propietari al mercat criptogràfic. De la mateixa manera, la mala gestió pot desplomar el valor del token a zero. Tampoc existeix una regulació que impedeixi a l'empresa desaparèixer amb tots els diners recaptats[8]. Molts són els qui adverteixen dels perills d'invertir en tokens. Malgrat aquests advertiments, aquest mercat està creixent expo-

8. La majoria de les ICO s'executen amb un descàrrec de responsabilitat que no garanteix la devolució als inversors; si el preu del token associat cau a zero, per negligència o accions malicioses de l'equip de desenvolupament, és probable que no hi hagi gaire recurs legal on acudir.

nencialment. La raó és senzilla: a major risc, major benefici (però no oblidem que també major pèrdua). La simplicitat a l'hora de generar els tokens, així com la falta de regulació i les grans expectatives dels inversors entorn d'un fenomen altament associat al bitcoin, ha ajudat a disparar l'emissió d'aquestes ICO. Hi ha qui hi veu l'oportunitat de recaptar una quantitat injustificada i possiblement fraudulenta de capital, mentre que altres argumenten que és una innovació en el model tradicional de finançament de risc. Algunes d'aquestes ICO han estat reeixides, però altres han estat fraudulentes o excessivament opaques, i han portat els seus compradors a pèrdues milionàries (Zetzsche, Ross P. Buckley1, & Föhr, 2017).

La decisió de la SEC pot haver proporcionat certa claredat sobre l'estat dels tokens d'utilitat versus seguretat; no obstant això, encara hi ha feina per fer en l'àmbit legal. Ara com ara, i fins que s'imposin uns límits legals addicionals, les empreses continuaran aprofitant aquest nou fenomen. El setembre del 2017, la Xina va amenaçar de declarar les ICO il·legals. El Banc Popular de la Xina va advertir que castigaria estrictament les noves ofertes i que penalitzaria les infraccions legals de les ja finalitzades. El regulador va ordenar a les empreses retornar la recaptació, encara que no va especificar com es retornarien els diners als inversors.

11. Noves formes d'organització: les DAO

DAO és l'acrònim en anglès d'Organització Autònoma Descentralitzada, que és un nou tipus d'organització que podria ser comparable amb una societat digital, però sense cap mena d'entitat legal adscrita. Va ser proposada originàriament per Vitalik Buterin el 2014, qui després passaria a ser el cofundador d'Ethereum. Aquesta organització està creada amb codi informàtic, és a dir, és una entitat que solament existeix en la blockchain i que a més està controlada directament pels propietaris (posseïdors de tokens), sense necessitat que existeixi una direcció centralitzada (Jentzsch, 2017). La DAO és en si mateixa un contracte intel·ligent complex basat en codi font autònom, que automatitza totes les funcions dins d'una organització i les seves directrius solament poden modificar-se si un tant per cent dels membres hi estan d'acord. A més, porta amb si una participació comunitària, de tal forma que no són únicament els (inexistents) directors els que tenen poder de decisió, sinó que tota la comunitat en possessió de tokens participa en les votacions o introdueixen propostes per ser votades (Venegas, 2017).

L'operatiu funciona de la següent manera. Els desenvolupadors de codi escriuen els contractes intel·ligents que executarà l'organització. Hi ha un període de finançament inicial, en el qual els inversors agreguen fons a la

DAO mitjançant la compra de tokens que representen la «propietat»: això es denomina crowdsale, o una oferta inicial de monedes (ICO). Quan finalitza el període de finançament, la DAO comença a funcionar. Els titulars de tokens poden fer propostes sobre com invertir els fons i votar per aprovar o denegar les propostes. Els requisits per participar en una DAO són escassos, poden reduir-se a tenir connexió a internet. Encara que alguns països, com els EUA, protegeixen fortament els inversors i obliguen els compradors de tokens a complir certs requisits, la majoria dels països no disposen d'aquesta protecció. Les DAO manquen de directors o empleats i no tenen un objectiu empresarial específic. La simplicitat en les decisions, l'anonimat, la seguretat i la reducció de costos són els seus grans pilars. Els defensors d'aquest tipus d'organitzacions al·leguen que fomenten la innovació i la professionalitat en basar les decisions en el valor dels projectes i no en l'interès personal dels individus i les seves lluites de poder.

Alguns exemples de DAO són SuperDAO o Solar DAO (Solodukha, 2017). El projecte SuperDAO té com a objectiu crear productes i serveis disruptius a través de la cooperació virtual d'innovadors sense limitacions geogràfiques a través de programari de codi obert. Per contra, Solar DAO té un objectiu específic. Opera com un fons d'inversió per construir plantes solars fotovoltaiques. Ven tokens als usuaris, els quals poden mantenir-los per obtenir dividends[9] o poden comerciar amb ells als mercats criptogràfics. A través dels contractes intel·ligents, els pagaments es fan automàtics sense revelar la identitat del propietari del token.

12. Conclusions i debat

És innegable que l'any 2017 ha estat l'any de les criptomonedes, especialment del bitcoin i sembla probable que els propers siguin els anys de la blockchain. Fins al moment, moltes són les companyies que s'han revalorat en incloure-hi alguna innovació relacionada amb blockchain o amb criptomonedes. Per exemple, les accions de l'empresa Chanticleer es van disparar un 50% després de l'anunci del seu programa de recompenses amb blockchain i la seva capitalització de mercat es va elevar de 8 milions a 12 milions

9. Solar DAO white paper: «Solar DAO token ownership will allow users to: 1. Invest in solar plants worldwide efficiently by circumventing issues related to ownership, audits and selection of contractors 2. Take part in PV plant construction, starting from as low as $1 3. Own assets (tokens) safely and anonymously 4. Receive dividends from the investments made and profit from the value increase of tokens 5. Sell tokens on the exchange market as needed».

de dòlars. Recentment, les accions de Long Island Iced Tea (una companyia fabricant de te gelat) es van revalorar més del 500% després d'haver canviat el seu nom a Long Blockchain Corp. Cosa semblant van experimentar algunes companyies d'Israel dedicades a la mineria de metalls preciosos, energia solar i tabac, respectivament, després d'haver anunciat la seva integració a l'ecosistema blockchain.

No obstant això, hi ha raons per ser prudent. La confiança entre els participants depèn de la confiança en la tecnologia blockchain, però això no està completament lliure de vulnerabilitats, inclosos els errors accidentals i els atacs maliciosos en les aplicacions que s'estableixen sobre la cadena de blocs. L'automatització tampoc eliminarà els conflictes d'interès o la corrupció. Encara que els defensors de blockchain promulguen que és inviolable, ningú està exempt de fallades. La primera iniciativa de DAO promulgada per Ethereum va rebre un dur cop en ser víctima del robatori de més de 150.000 ethers, 30 milions de dòlars (vegeu: <https://www.coindesk.com/understanding-dao-hack-journalists>), i va donar origen a un gran debat ideològic que va dividir la comunitat Ethereum en dues. En un costat es van situar els defensors d'acceptar el robatori i no fer res, complint així amb les directrius originàries d'immutabilitat del codi (*code is law*). D'altra banda ho van fer els defensors de retrotreure la cadena fins al bloc previ a la funció que va permetre la substracció. És important remarcar que l'error de codificació estava en la DAO i no en la cadena de blocs subjacent. No obstant això, molts poden argumentar que aquesta diferència no afecta el fet que l'aclamada inviolabilitat queda totalment en dubte. Finalment, els fundadors i altres col·laboradors d'Etherum van decidir retrotreure el codi, la qual cosa va donar lloc a dues cadenes de blocs paral·leles (vegeu la figura 4). Les dues cadenes van persistir. La cadena que va conservar les normes antigues es va batejar com Ethereum Classic[10] (ETC), i la nova cadena que es va crear a partir de la retroacció es va dir simplement Ethereum (ETH).

10. Al llibre blanc d'Ethereum Classic es pot llegir: «Ethereum 'Classic' is the original unmolested Ethereum block chain of the Ethereum platform. We believe in decentralized, censorship-resistant, permissionless blockchains. We believe in the original vision of Ethereum as a world computer you can't shut down, running irreversible smart contracts. We believe in a strong separation of concerns, where system forks are only possible in order to correct actual platform bugs, not to bail out failed contracts and special interests. We believe in censorship-resistant platform that can be actually trusted - by anyone.»

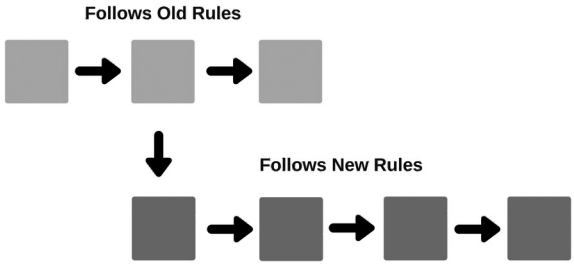


Figura 3. Escissió de la plataforma: Ethereum (vermell) i Ethereum Classic (blau).

Aquesta decisió també ataca un altre dels pilars fonamentals de blockchain: la immutabilitat del codi. Si bé no és possible per als *hackers* modificar el codi, ja que no poden accedir a tots els nodes simultàniament, sembla que és possible per a les plataformes alterar la cadena.

Des d'un enfocament més conceptual, aquells que veuen en la tecnologia una forma de democratitzar la creació de valor eliminant els intermediaris, juntament amb els seus abusos i imperfeccions, poden veure's decebuts. Una primera temptativa va ser l'economia col·laborativa. Desgraciadament, aquest ecosistema comença a mostrar senyals de fracàs en el seu objectiu inicial. En lloc d'eliminar o reduir intermediaris oligopolistes, aquests són substituïts per gegants com Uber, que no necessàriament milloren la situació inicial. Per a molts, blockchain pot ser finalment la solució a aquest problema. Un sistema no solament descentralitzat, sinó distribuït, en el qual els intermediaris ja no són necessaris i les regles del joc no venen marcades per la decisió arbitrària d'un organisme interessat. La idea és vàlida, però qui ens garanteix que aquesta opció no presentarà els mateixos errors que la seva predecessora. Els bancs han estat el primer objectiu d'aquest pla de desintermediació, iniciat a partir de la crisi financera de 2007-2008[11]. Com a reacció, aquest sector està utilitzant la tecnologia blockchain pròpia per tal de perpetuar el seu domini en les transaccions financeres. Fintech és la forma en què es denomina la tecnologia aplicada a les finances. L'agost del 2017, per exemple, Barclays, Credit Suisse, Banc Imperial Canadenc de Comerç (CIBC), HSBC, Banc MUFG i State Street Bank, sis de les entitats financeres més grans del món, es van unir per crear una moneda digital basada en la tecnologia blockchain. La resistència no només es produeix en el sector financer. Plataformes com Hyperledger creen cadenes privades adaptades a les necessitats de les organitzacions i no al contrari. Xarxes tancades,

11. Satoshi Nakamoto va llançar el seu *Bitcoin paper* el 2009, després de la crisi financera de 2007-2008.

amb permisos i controlades per un grup de participants que no difereixen en gran manera de l'actual concepte d'intermediació.

D'altra banda, si bé blockchain promet un món en el qual els intermediaris que coneixem no són necessaris, encara poden ser possibles. Per exemple, a partir de la creació d'internet, les agències de viatges no eren necessàries. Qualsevol pot reservar els vols, els hotels i el viatge complets sense necessitat d'aquelles, però això no implica que desapareguin. El fet que puguem fer un contracte directament no implica que tinguem els coneixements o el temps necessari per dur-ho a terme. Aquests costos incentiven l'ús d'intermediaris malgrat no ser necessaris. Fins i tot en el supòsit d'eliminar antics intermediaris, aquests probablement serien substituïts per nous. Un possible candidat serien les plataformes blockchain, com Ethereum o Hyperledger, que, igual que Uber en l'economia col·laborativa, no necessàriament millorarien la situació.

Com a reflexió final cal remarcar el fet que encara que blockchain no aconsegueixi revolucionar l'economia i la societat, és indubtable que tindrà un impacte substancial en moltes àrees i cal estar preparats per als desafiaments i les oportunitats que presenta.

Referències bibliogràfiques

AZIZ (2017). *Crypto ICO vs. Stock IPO: What's the Difference?* Disponible a: <https://masterthecrypto.com/crypto-ico-vs-stock-ipo/>.

BUTERIN, V. (2014). *A Next Generation Smart Contract & Decentralized Application Platform (White Paper).* <http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>.

DAI, J. i VASARHELYI, M. A. (2017). «Toward Blockchain-Based Accounting and Assurance». *Journal of Information Systems,* 31(3), 5-21.

DISPENZA, J.; GARCÍA, C. i MOLECKE, R. (2017). «Energy Efficiency Coin (EECoin) A Blockchain Asset Class Pegged to Renewable Energy Markets». Disponible a: <https://www.enledger.io/Energy_Efficiency_Coin_Whitepaper_v1_0.pdf>.

IJIRI, Y. (1989). «Momentum accounting and triple-entry bookkeeping: exploring the dynamic structure of accounting measurements». *American Accounting Association*.

JENTZSCH, C. (2017). «Decentralized Autonomous Organization to Automate Governance». file: <///C:/Users/LUZ/Downloads/WhitePaper%202.pdf>.

LEV, B. i GU, F. (2016). *The End of Accounting and the Path Forward for Investors and Managers*. ISBN: 978-1-119-19109-4.

NAKAMOTO, S. (2008). «Bitcoin: A Peer-to-Peer Electronic Cash System». *White Paper*.

PASS, R. i SHI, E. (sense data). «Hybrid consensus: Efficient consensus in the Permissionless Model». *DOI: 10.4230/LIPIcs.DISC.2017.39* URL: <http://drops.dagstuhl.de/opus/volltexte/2017/8004/>.

SOLODUKHA, D. (2017). «Solar DAO» *(White Paper).* <https://solardao.me/files/wpeng.pdf>.

VENEGAS, P. (2017). «Initial Coin Offering (ICO) Risk, Value and Cost in Blockchain Trustless Crypto Markets». Disponible a SSRN: <https://ssrn.com/abstract=3012238>.

ZETZSCHE, D. A.; ROSS P. BUCKLEY1, D. W. i FÖHR, L. (2017). The ICO Gold Rush: «It's a Scam, It's a Bubble, It's a Super Challenge for Regulators». *University of Luxembourg Law Working Paper No. 11/2017; UNSW Law Resear.*