ANÀLISI I APLICACIÓ BLOCKCHAIN D'ETHEREUM

AUTOR:

ERIC GARCIA MAÑOSA

GRAU:

EMPRESA I TECNOLOGIA

TUTOR:

ALBERT SALA CUBERTA

DATA:

07/06/2019

AGRAÏMENTS

Després d'aquest llarg procés, m'agradaria agrair a totes les persones properes que m'han acompanyat (familiars i docents) que han aportat els seus coneixements i suggeriments a la realització d'aquest treball. Per altra banda, agrair a totes aquelles persones, que de forma pública o anònima, han compartit, comparteixen i compartiran, el seu coneixement sobre Blockchain i Ethereum, fent possible que altres persones n'aprenguin.

RESUM

La tecnologia blockchain permet emmagatzemar dades xifrades, descentralitzar el poder sobre les dades i mantenir una xarxa de participants distribuïda. Això permet que cada un dels participants d'aquesta xarxa mantingui una còpia exacta de les dades.

Aquest fet, obliga als participants a mantenir la majoria absoluta, per tal d'obtenir el consens necessari en la presa de decisions sobre la xarxa i les seves dades. Tot aquest procés, permet democratitzar l'ús i l'accés a les dades, qüestió rellevant tenint en compte la falta d'ètica i valors de les grans corporacions i estats, els quals actuen com a gestors de dades.

Per altra banda, Ethereum sorgeix com una plataforma descentralitzada que utilitza la tecnologia blockchain per aportar les eines i un entorn on desenvolupar aplicacions descentralitzades. Aquestes, es creen amb l'objectiu de redistribuir el poder, eliminar intermediaris i despeses de gestió, i sobretot, augmentar la confiança i la privacitat dels usuaris i les seves dades.

Per últim, els contractes intel·ligents són creats davant la necessitat d'eliminar intermediaris que encareixen qualsevol classe de transacció, la necessitat de tornar a mantenir confiança en les transaccions, i l'automatització de processos quotidians.

De què tracta aquest treball? D'analitzar i comprendre les relacions i diferències entre la tecnologia Blockchain i la plataforma d'Ethereum. Així com la importància dels contractes intel·ligents en l'execució de la lògica d'aplicacions descentralitzades desenvolupades i guardades en la blockchain d'Ethereum. (Vegeu *Il·lustració 1: Esquema gràfic de la relació entre Blockchain, Ethereum i els contractes intel·ligents*).

ÍNDEX

1. INTRODUCCIÓ 1
   1.1. Motivació 1
   1.2. Objectius 2
   1.3. Estructura del Document 2
2. BLOCKCHAIN 5
   2.1. Definició de l'Origen i Conceptes 5
   2.2. Principals Elements 9
      2.2.1. Els participants i la xarxa 10
      2.2.2. Sistema criptogràfic asimètric 13
      2.2.3. Protocol i l'algorisme de consens 14
   2.3. Com Funciona 19
   2.4. Avantatges de Blockchain 24
   2.5. Inconvenients Blockchain 26
3. ETHEREUM 31
   3.1. Definició dels Conceptes i Aspectes Clau 31
   3.2. Diferències entre Bitcoin i Ethereum 33
   3.3. Evolució i Desenvolupament 37
      3.3.1. Fase Frontier 38
      3.3.2. Fase Homestead 38
      3.3.3. Fase Metropolis 39
      3.3.4. Fase Ethereum 2.0 41
   3.4. La Moneda Ether i la Unitat Gas 41
   3.5. Aplicacions Descentralitzades 43
   3.6. Contractes Intel·ligents 45
   3.7. Avantatges Ethereum 46
   3.8. Inconvenients Ethereum 47
4. APLICACIÓ PRÀCTICA D'UN SMART CONTRACT AMB ETHEREUM 49
   4.1. Les Donacions a ONG's 49
   4.2. Procediment 51
   4.3. Creació del Contracte 51
   4.4. Compilació i Execució en Remix 55
   4.5. Implementació en Ropsten 56
   4.6. Implementació en Ethereum 57
5. CONCLUSIÓ 61

6. ACRÒNIMS 64
7. ANNEX 71
8. BIBLIOGRAFIA 74
8.1. Recursos Electrònics 74

1. INTRODUCCIÓ

1.1. Motivació

Al llarg dels darrers anys la contínua exposició de les nostres dades personals i l'amenaça continua envers la privacitat i la creixent agressivitat cap a la nostra intimitat, ha generat una creixent desconfiança del públic en general, i alhora ha provocat l'eclosió de tecnologies disruptives descentralitzadores i anonimitzadores com el blockchain.

Davant aquests fets, sumant al gran desconeixement originat per la prematuritat que presenta la tecnologia blockchain, veient el potencial que té aquesta per retornar el control de les dades als seus usuaris, i al fet que molta de la informació que es troba en Internet actualment està totalment o parcialment errònia, ha provocat la necessitat d'investigar aquesta tecnologia per conèixer-la a fons.

La falta de confiança en els gestors de dades mundials com ara Facebook i Google, i la seva falta d'ètica, m'ha provocat la necessitat de conèixer i introduir-me en el món de la blockchain i els seus projectes, per observar si aquests realment poden reequilibrar la balança sobre el control de les dades i com ho poden dur a terme.

La primera gran ona de popularitat de les criptomonedes, va arrossegar a molta gent, jo el primer, la qual s'hi va entrar sense tenir un mínim de coneixement respecte a les diferents funcionalitats i el potencial real dels projectes que utilitzen la tecnologia blockchain, provocant l'extrema volatilitat que va patir el mercat borsari de les criptomonedes.

Aquest fet, juntament amb els ja mencionats, em va fer adonar que era necessari un ampli estudi de la matèria per tal de poder continuar en aquest ecosistema, i ser capaç d'integrar-me en ell i poder interactuar amb la xarxa.

És molt possible que la intel·ligència artificial o IoT siguin les principals innovacions tecnològiques actuals, però el món de la tecnologia blockchain, juntament amb la creixent desconfiança de la població, permetrà impulsar i crear un canvi de paradigma quant a la gestió de les dades i de la nostra privacitat.

I és per tant, que davant les grans innovacions tecnològiques que hi ha actualment, l'estudi d'aquest treball se centra en la tecnologia blockchain.

1.2. Objectius

Els principals objectius que es pretenen assolir amb la realització d'aquest treball, són:

- Aportar una definició vàlida de la tecnologia blockchain.
- Conèixer i destacar els elements indispensables perquè una blockchain funcioni.
- Entendre què és i com funciona el procés de validació de transaccions i creació de blocs.
- Ser capaç de detectar tant els avantatges com els inconvenients de la tecnologia blockchain i el seu potencial.
- Comprendre la necessitat d'eliminar la confiança entre participants.
- Entendre el paper clau de la tecnologia blockchain en la descentralització del poder i la distribució d'una xarxa.
- Conèixer els elements necessaris que permeten a Ethereum ser única.
- Conèixer les semblances i diferències entre Bitcoin i Ethereum.
- Entendre el funcionament intern de la plataforma Ethereum.
- Desenvolupar un contracte intel·ligent i ser capaç d'interactuar amb ell en la xarxa Ethereum.
- Comprendre la relació entre els conceptes de blockchain, Ethereum i els contractes intel·ligents.
- Conèixer i augmentar el coneixement sobre l'ecosistema de les criptomonedes i els projectes amb major potencial.

1.3. Estructura del Document

Aquest document el podem separar en 3 parts. L'estudi de la tecnologia blockchain, l'estudi del projecte Ethereum i la implementació de contractes intel·ligents, que serà possible gràcies a l'estudi realitzat en les anteriors parts.

La separació en 3 parts s'ha realitzat per entendre que és i el funcionament de la tecnologia blockchain, comprendre que és la plataforma Ethereum i quina relació té amb la tecnologia blockchain, i què són, com funcionen, i com interactuen amb la blockchain en la xarxa Ethereum.

L'estudi de la tecnologia blockchain es centra en:

- Aportar una definició suficientment clara i concisa respecte a aquesta tecnologia a partir de l'anàlisi d'un conjunt de definicions esmentades per grans experts de la tecnologia blockchain.
- Conèixer tots els elements que participen i que són necessaris per a la implementació d'aquesta tecnologia
- Entendre el procés de creació d'un bloc, com aquest s'incorpora posteriorment en la cadena de blocs i el consens necessari que s'estableix entre els diferents participants de la xarxa.
- Anomenar i destacar els avantatges i inconvenients detectats gràcies a l'anàlisi que s'ha dut a terme prèviament al llarg del mateix estudi. Per altra banda, també se'n destaquen les possibles amenaces i els elements dels quals requereix la tecnologia blockchain per a poder ser àmpliament acceptada i implementada en negocis convencionals.

La segona part del document se centra en l'estudi del projecte Ethereum, realitzant una anàlisi i un seguiment del seu desenvolupament:

- Presentar les diferents parts que conflueixen i permeten a la plataforma Ethereum connectar, interactuar i sincronitzar la informació amb tota la xarxa, seguint els principis prèviament definits en l'anàlisi de la tecnologia blockchain
- Establir les principals semblances i diferències entre Ethereum i la criptomoneda Bitcoin, els dos projectes de l'entorn de les criptomonedes amb major capitalització borsària i les més conegudes mundialment.
- Realitzar un seguiment de les diferents etapes que han sorgit en el procés de desenvolupament del projecte des dels seus inicis, i en destaca els aspectes més importants de cada una de les etapes.
- Presentar l'objectiu i les funcions que desenvolupa la moneda Ether i la unitat Gas en el desenvolupament d'aplicacions descentralitzades en la plataforma.
- Explicar la funcionalitat de les aplicacions descentralitzades, alguns exemples de casos reals aplicats i el seu potencial respecte a negocis tradicionals.
- Explicar que són i en què consisteixen els contractes intel·ligents, i els principals avantatges i inconvenients d'aquests.

- Realitzar una anàlisi sobre els avantatges i inconvenients que presenta el projecte Ethereum i la implementació de contractes intel·ligents per a les aplicacions descentralitzades.

L'última part d'aquest document se centra a presentar els principals problemes que es troben en les donacions a ONG's i en intentar pal·liar aquests a partir de la implementació dels contractes intel·ligents:

- Establir els objectius que es volen assolir amb la implementació de contractes intel·ligents en les ONG's.
- Identificar i esmentar de forma específica els beneficis que pot suposar aquesta implementació tant per l'usuari com per a l'ONG.
- Analitzar les possibles vies per implementar el contracte.
- Explicar el procediment que es durà i les eines que es requereixen per implementar el contracte intel·ligent.
- Analitzar amb gran nivell de detall el codi del contracte per entendre cada una de les seves funcionalitats.
- Detallar les opcions de compilació i execució del codi que aporta el navegador Remix per a desenvolupar codi vàlid.
- Analitzar i detallar el procediment per connectar i interactuar amb l'extensió Metamask i la xarxa Ropsten.
- Implementar el contracte en la xarxa Ethereum i interactuar amb les diferents funcions que s'introdueixen en el contracte intel·ligent.

2. BLOCKCHAIN

2.1. Definició de l'Origen i Conceptes

Una cadena de blocs, o més popularment coneguda com a blockchain, és en termes generals, una tecnologia disruptiva que permet la transmissió i l'emmagatzemament de dades en blocs, formant un "llibre major de dades".

Blockchain és una manera senzilla però al mateix temps complex, d'enviar informació d'A a B. Aquesta transmissió es pot fer mitjançant una petita despesa per a la transacció, evitant la necessitat de mantenir la confiança en el sistema o en els participants, mantenint la integritat de les dades, reduint el temps d'espera en comparació als sistemes bancaris actuals, i en molts casos a partir d'una xarxa descentralitzada i distribuïda, la qual no està sotmesa a cap política ni ideologia individual sinó a la col·laboració, consens i confiança d'un conjunt.

Aquest fenomen va sorgir arran de la crisi econòmica i financera mundial del 2007, la qual, va ocasionar la pèrdua de confiança amb els bancs i els polítics, com a principals actors en utilitzar el poder i la influència per al seu propi benefici.

La pèrdua de confiança, juntament amb les elevades despeses i els processos administratius que retarden les transferències, i la falta d'integritat de moltes bases de dades governamentals, ha provocat aquest canvi de tarannà en la forma d'interactuar dels individus, pel que fa a mantenir la confiança en els canals tradicionals per a la transmissió de valor.

La figura del Bitcoin[1], la primera criptomoneda amb èxit fins aleshores, va permetre introduir el concepte blockchain com el sistema capaç de transmetre valor de manera automatitzada, descentralitzada, distribuïda i eliminant la necessitat d'intermediaris. Els únics intermediaris són els participants de la comunitat que verifiquen la integritat i veracitat dels blocs creats.

Un aspecte molt important en una xarxa connectada a partir de la tecnologia blockchain, és que com més gran és la comunitat de participants, major dificultat d'atac o corruptibilitat tindran els blocs en qüestió. Aquest fet en una xarxa com la de Bitcoin o

[1] Delton Rhodes. A Complete History of Bitcoin (2008 – 2019 Timeline) https://blockexplorer.com/news/bitcoin-history-timeline/ [Consultat: 26 gener 2019]

Ethereum, els principals projectes respecte al nombre de persones en una comunitat i nodes en actiu[2] i [3], és pràcticament impossible.

Hi ha milers de definicions per a aquesta nova tecnologia, és així, que s'intentarà abordar al màxim d'aquestes per poder obtenir un ampli punt de vista i coneixement d'aquesta tecnologia tan innovadora.

"*Blockchain és una revolució perfectament comparable a l'aparició de l'ordinador personal, o al desenvolupament d'Internet. El blockchain és un llibre digital incorruptible i immutable de dades temporitzades, que es poden programar per enregistrar no només les transaccions financeres, sinó pràcticament tot el que té valor, i que són gestionades per un clúster d'ordinadors que no pertanyen a cap entitat. Cadascun d'aquests blocs de dades s'asseguren i s'uneixen entre si mitjançant principis criptogràfics*." - segons el gran expert de blockchain i fundador del Blockchain Research Institute, Don Tapscott i el seu fill Alex Tapscott[4].

Segons l'escriptor i periodista Matt Higginson, "*blockchain és una base de dades, la qual, és compartida entre el conjunt dels participants. Cada un d'ells, té un ordinador (node). La idea és que en qualsevol moment, de forma simultània, cada un dels membres de la xarxa guarda una còpia idèntica de la base de dades de la blockchain en el seu ordinador. Aquest és el principi essencial. La informació està disponible per a tots els participants*" [5].

En aquest sentit, convé recordar la definició oferta per Alex Preukschat, analista de criptomonedes, d'acord en el fet que: "*una blockchain, no és una altra cosa que una base de dades que es troba repartida entre diferents participants, protegida a partir del xifratge de les dades, i organitzada en blocs de transaccions relacionades entre si matemàticament*" [6].

[2] The Ethereum node explorer. https://www.ethernodes.org/network/1 [Consultat: 27 gener 2019]
[3] Global Bitcoin Nodes Distribution. https://bitnodes.earn.com/ [Consultat: 27 gener 2019]
[4] TAPSCOTT, Don; TAPSCOTT, Alex. 2017. *La revolución blockchain.* Editorial DEUSTO.
[5] HIGGINSON, Matt. Blockchain explained: What it is and isn't, and why it matters. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-explained-what-it-is-and-isnt-and-why-it-matters [Consultat: 28 febrer 2019]
[6] PREUKSCHAT, Alex. 2017. *Blockchain: la revolución industrial de internet*. Editorial Gestión 2000.

Totes les definicions presentades anteriorment, descriuen la tecnologia blockchain com una tecnologia capaç d'emmagatzemar dades.

En definitiva, aquesta tecnologia el que permet, és augmentar el valor afegit del procés d'emmagatzemar dades, gràcies al fet de mantenir l'anonimat de les dades, eliminar la necessitat de confiança entre participants i la connexió entre els participants de la xarxa, els quals comparteixen i sincronitzen les dades amb l'objectiu de mantenir la integritat de les dades de forma descentralitzada i distribuïda.

Per últim, cal destacar una frase d'una de les persones amb major influència en el món de les criptomonedes, sobretot de l'ecosistema Bitcoin i de la tecnologia blockchain com a xarxa descentralitzada i distribuïda, Andreas M. Antonopoulos, en el que crítica la situació actual en l'ecosistema blockchain "*L'ús més popular de blockchain, és anar a Silicon Valley, trobar una habitació d'hotel, parar-se davant del mirall, i dir Blockchain tres vegades. Seguidament, deu fons d'inversió sortiran de l'armari i et llançaran milions de dòlars*"[7].

Amb aquesta frase, M. ANTONOPOULOS critica l'ús i la promoció que s'està donant a aquesta tecnologia, ja que no es tenen en compte els principis pels quals es va crear. La promoció d'aquesta innovadora tecnologia en l'àmbit mundial, ha estat amb voluntat especulativa[8]. (Vegeu *Il·lustració 2: Tendència de cerca de la paraula Blockchain en Google*).

De fet, la majoria de projectes els quals no han tancat abans de complir l'any després de la primera ronda de finançament, o popularment coneguda com a ICO inicial, s'estan basant en xarxes descentralitzades i privades, les quals no són distribuïdes. Això provoca que la xarxa sigui controlada no per al conjunt sinó per al creador o creadors de la xarxa en concret, com és el cas de la popularment coneguda IBM Blockchain[9].

[7] M. ANTONOPOULOS, Andreas. 2014. *Mastering Bitcoin*. Editorial O'Reilly.
[8] Google Trends. https://trends.google.com/trends/explore?date=2015-01-01%202019-05-26&q=blockchain [Consultat: 26 maig 2019]
[9] IBM Blockchain - Enterprise Blockchain Solutions & Services https://www.ibm.com/blockchain [Consultat: 2 febrer 2019]

Cal destacar que existeixen dos tipus de blockchain, la privada i la pública. Les principals diferencies, són:

Taula 1: Taula de comparació entre cadena de blocs pública i privada

Tipus de Blockchain	**Privada**	**Pública**
Nivell d'accés i participació	Necessari el permís per poder interactuar-hi	Sense restriccions i amb anonimat
Poder de control	Una o diverses entitats	Recau en la comunitat i consens democràtic
Seguretat	Major coneixement dels participants	Mecanismes de consens i protocols de consens
Rendiment	Major velocitat de les transaccions	Menor velocitat de les transaccions
Emmagatzemament	Controlat	Lliure
Possibilitat d'atac de 51%[10] en cas de utilitzar PoW	Major, ja que hi ha menys nodes interactuant en la xarxa	Quasi nul·la (en grans comunitats) Gran (en petites comunitats)[11]

Font: Elaboració pròpia

A continuació, es presenten dos exemples de casos d'implementació de la tecnologia blockchain en negocis reals:

- **Blockchain pública**: La plataforma CryptoCribs[12] ofereix el lloguer d'apartaments. Aquesta idea funciona igual que Airbnb però, elimina els intermediaris, ja que connecta directament client amb amfitrió, la centralització de les dades d'Airbnb i la necessitat de connectar amb bancs, ja que pots pagar amb criptomonedes.

[10] AMMOUS, Saifedean. 2017. *El patrón Bitcoin: La alternativa descentralizada de los bancos centrales*. Editorial DEUSTO.
[11] Pàgina web on consultar el cost per hora que suposa realizar un atac del 51% en les principals criptomonedes. Crypto51. https://www.crypto51.app/ [Consultat: 2 febrer 2019]
[12] Pàgina web de la plataforma. CryptoCribs. https://www.cryptocribs.com/ [Consultat: 23 maig 2019]

Tot usuari que es vol registrar, necessita introduir certes dades personals, com ara el DNI, amb l'objectiu de crear un registre únic per a cada client. Aquest registre està xifrat i és accessible, només una part, per a l'amfitrió.

El protocol de la xarxa estableix diferents indicadors que permeten a l'amfitrió conèixer al seu possible hoste i "veure si és de confiança", a partir de l'anàlisi dels anteriors negocis del client amb altres amfitrions de la plataforma.

Per altra banda, qualsevol usuari pot introduir el seu habitatge en la plataforma, mentre obtingui el consens dels nodes de la xarxa i segueixi les regles establertes en el protocol[13].

- **Blockchain privada**: L'empresa IBM ha creat el projecte de Food Trust[14], amb l'objectiu de crear una xarxa de col·laboració entre els diferents participants del sector alimentari, el qual permeti mantenir la traçabilitat d'un producte des de la seva creació fins a la venda al client final.

  Aquest projecte pretén mantenir un registre immutable i compartit, de la procedència dels aliments, dades de transaccions i detalls de tots els processos per als quals passa el producte.

  Això, permet realitzar un seguiment més ràpid dels brots i augmentar la confiança de l'usuari proporcionant transparència de dades pel que fa als certificats, procedències, registres d'inspecció i qualitat d'un producte[15].

2.2. Principals Elements

A causa de l'amplitud i complexitat de les diferents definicions sobre la tecnologia blockchain, resulta necessari definir els nombrosos aspectes clau en tota blockchain per poder donar un punt de vista suficientment ampli.

[13] ERASMUS. *A Peer-to-Peer Electronic Rental System.* https://www.cryptocribs.com/images/whitepaper.pdf [Consultat: 23 maig 2019]
[14] IBM Food Trust. https://www.ibm.com/es-es/blockchain/solutions/food-trust [Consultat: 23 maig 2019]
[15] GALVIN, David. *IBM and Walmart: Blockchain for Food Safety*. https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf [Consultat: 23 maig 2019]

2.2.1. Els participants i la xarxa

La falta de confiança amb els actors en la presa de decisions, ha provocat un canvi en la tendència a l'hora de seleccionar les persones amb les qui dipositar aquesta confiança. Aquest fet, juntament amb tendència creixent pel que fa a preocupació per aspectes clau com la privacitat de les dades així com la popularitat del mercat de les criptomonedes a causa de la seva volatilitat, ha disparat el nombre de participants en les diferents comunitats blockchain.

En primer lloc, cal destacar que el conjunt de registres del qual es forma una cadena de blocs es construeix a partir d'una xarxa global d'usuaris. Podem diferenciar tres grans grups d'usuaris:

- Els usuaris que només realitzen transaccions en la cadena de blocs per a l'intercanvi de béns i comerç, sense participar de forma activa en la comunitat. Aquests també poden desenvolupar contingut en la cadena de blocs, mitjançant navegadors i extensions, sense la necessitat de tenir un node.[16]
- Els usuaris que mantenen un node, i s'encarreguen d'actualitzar-lo i sincronitzar-lo, però no d'executar proves de conceptes. Aquests també poden dur a terme les accions del grup d'usuaris anterior. Cal remarcar, que la despesa del manteniment és baixa comparada amb els miners.
- Els usuaris popularment coneguts com a miners, són els que utilitzen el hardware amb el node per executar les proves de concepte.

Com descriu TUR FÁUNDEZ, "*El terme node es refereix a qualsevol ordinador que, prèvia descàrrega i execució en el mateix d'un o diversos programes es converteix en part integrant de la xarxa descentralitzada de la cadena de blocs i immediatament passa a conservar una rèplica exacta de tots els registres integrants de la mateixa*"[17].

D'aquesta forma, la informació de la cadena de blocs es troba replicada i distribuïda entre els diferents participants de la xarxa. Tenint en compte que la cadena de blocs en qüestió, es pot descarregar de forma gratuïta a través d'Internet, qualsevol usuari, mentre

[16] No han de mantenir un node, però per altra banda, no tenen control absolut dels seus comptes, ja que utilitzen serveis de tercers per connectar-se amb les cadenes de blocs i poder llançar els seus continguts.
[17] TUR FÁUNDEZ, Carlos. 2018. *Smart Contracts: Análisis jurídico*. Editorial Reus.

compleixi un conjunt de regles preestablertes, podrà desenvolupar la funció de validar i d'emmagatzemar la informació que es va registrant al pas del temps en la xarxa.

En relació als nodes, convé destacar que el seu funcionament és com el de qualsevol xarxa P2P – Peer-to-Peer en anglès- la qual pot ser definida com una xarxa d'ordinadors que es comporten com a iguals entre ells, i actuen de forma simultània com clients i servidors respecte als altres nodes de la xarxa.

En les cadenes de blocs de caràcter públic, tots els ordinadors que estan connectats a aquella xarxa tenen, en el seu conjunt, el dret de controlar-la, ja que en aquesta tipologia de xarxes, no hi ha una jerarquia. Mentre que en una cadena de blocs de caràcter privat, és possible l'existència d'una jerarquia.

Tota cadena de blocs, està formada per una xarxa de participants. Des d'un inici, qualsevol xarxa es podia definir com a **xarxa centralitzada**, la qual és una xarxa on hi ha un node central concentrat, que disposa de tot el control sobre la resta de participants, o com a **xarxa descentralitzada**, la qual era una xarxa distribuïda on el poder requeia en el conjunt dels nodes.

Amb l'aparició dels clústers i de les piscines de mineria – o minning pools en anglès –, el poder i els mateixos nodes han tendit a agrupar-se en zones geogràfiques específiques i en poques entitats. És per això, que va sorgir el terme de **xarxa distribuïda**[18], com a xarxa massivament descentralitzada on tots els participants tenen el mateix poder de decisió dins la xarxa, per tal de diferenciar-se amb la xarxa descentralitzada.

Amb aquest nou concepte, hi ha participants que consideren que la cadena de blocs no és del tot una xarxa distribuïda, i que per tant no segueix els principis per al qual va sorgir bitcoin, mentre que d'altres mantenen que l'agrupació és fruit de la necessitat, del consens entre els participants i que originalment, la definició de xarxa descentralitzada esmenta que es basa en un conjunt de nodes centrals els quals tenen el poder sobre els nodes perifèrics.

[18] ALCÁNTARA, Jose. *Red distribuida*. https://www.versvs.net/pedia/red-distribuida/ [Consultat: 2 març 2019]

Aquest debat ha provocat una falta de consens, i ha generat opinions molt diferents en l'ecosistema[19] blockchain, a l'hora de definir quina tipologia de xarxa utilitza la tecnologia blockchain en el seu conjunt. A causa d'aquest conflicte, una de les raons per les quals estan sorgint noves propostes de protocols per tal de redirigir la forma en la qual els diferents nodes d'una xarxa es relacionen i interactuen en la transmissió d'informació.

En aquesta anàlisi es presenten els dos aspectes clau de qualsevol xarxa[20] i que ens permetran entendre el perquè de les grans diferències generades en l'entorn blockchain. Els dos aspectes claus són el control i la localització:

El **control o autoritat** sobre una xarxa, el qual el podem classificar en dues tipologies diferents:

- Centralitzat: El poder recau en un únic node que controla la resta de nodes perifèrics.
- Descentralitzat: El poder recau sobre diversos nodes, coneguts com a clústers, i altres participants, els quals tenen un gran poder de computació i per tant, capacitat per obtenir el consens necessari dins d'una blockchain.

La **localització o ubicació** dels nodes d'una xarxa, la podem classificar en dues tipologies diferents:

- Una xarxa amb nodes concentrats en una ubicació específica permet que problemes externs, com ara regulacions polítiques o afectacions en la xarxa de subministrament, afectin el correcte funcionament de la xarxa.
- Una xarxa amb nodes escampats en diferents ubicacions geogràfiques permet obtenir una xarxa distribuïda i complica qualsevol possibilitat d'afectació a la totalitat de la xarxa.

Segons aquesta classificació, podem observar com existeixen diferents possibilitats, des d'una xarxa centralitzada amb nodes concentrats, fins a una xarxa amb poder

[19] DINKINS, David. *Bitcoin es descentralizado pero no distribuido, y ese hecho probablemente contribuyó a la guerra civil de Bitcoin*. https://es.cointelegraph.com/news/bitcoin-is-decentralized-but-not-distributed-and-that-fact-likely-contributed-to-bitcoins-civil-war. PORT, Torp. *Centralized vs decentralized vs distributed networks + Blockchain*. https://medium.com/@torp_port/centralized-vs-decentralized-vs-distributed-networks-blockchain-f895416dc22 [Consultat: 16 març 2019]

[20] POENITZSCH, Julia. *What's the difference between decentralized and distributed?* https://medium.com/nakamo-to/whats-the-difference-between-decentralized-and-distributed-1b8de5e7f5a4 [Consultat: 10 abril 2019]

descentralitzat i una ubicació dels nodes distribuïda, la qual seria la tipologia de xarxa amb la qual es pot identificar la tecnologia blockchain, ja que el poder recau en els diferents clústers i participants de la xarxa i aquests, estan repartits per tot el globus.

Gràcies a la tecnologia blockchain, la informació no està concentrada en un registre de dades opac i controlat per una o diverses autoritats responsables de les dades, sinó que l'autoritat recau en el consens del conjunt de la xarxa dotant aquesta, de transparència, seguretat, integritat dels registres i amb una clara visió per a la col·laboració i compartició de coneixement.

2.2.2. Sistema criptogràfic asimètric

A causa de la falta de seguretat en la transmissió de dades a través del món digital, i de la falta de privacitat d'aquestes en vers les dades dels participants que se'n generen o que surten reflectides de les seves accions, és necessària l'aplicació d'un sistema que permeti protegir les identitats d'aquells que hi participen per tal d'equilibrar el món físic i virtual.

El registre de les transaccions que es produeix en la xarxa blockchain, es realitza a partir de l'aplicació d'una capa de seguretat, anomenada criptografia[21], la qual pot ser definida, seguint PREUKSCHAT, com "*aquell procediment que, utilitzant un algorisme amb clau —clau de xifrat—, transforma un missatge sense atendre la seva estructura lingüística o significat, de tal forma que sigui incomprensible o, almenys, difícil de comprendre, a tota persona que no tingui la clau secreta —clau de desxifrat—de l'algorisme emprat. En el context d'una xarxa blockchain, la criptografia té la responsabilitat de proveir un mecanisme infal·lible per a la codificació segura de les regles de protocol que regeixen el sistema i de generar signatures i identitats digitals xifrades i, així mateix, resulta fonamental per a evitar la manipulació, furt o introducció errònia d'informació en la cadena de blocs*"[22].

La tipologia de criptografia que s'utilitza en la tecnologia blockchain, és l'**asimètrica**. Aquesta, utilitza dues claus matemàticament relacionades de manera que el contingut que es xifra amb una (clau pública), només pot desxifrar-se amb una segona (clau privada)[23].

[21] PREUKSCHAT, Alex; NÚÑEZ, Jaime. 2017. Blockchain: la revolución industrial de internet. Editorial Gestión 2000. Criptografía y consenso aplicado a la blockchain: 203-220.
[22] PREUKSCHAT, Alex. 2017. Blockchain: la revolución industrial de internet. Editorial Gestión 2000.
[23] ROCA, Luis. *Seguridad Informática: Criptografía*. http://minubeinformatica.com/cursos/seguridad-informatica/criptografia/ [Consultat: 30 març 2019]

Ambdues creades i vinculades entre si mitjançant una funció especial. Aquestes funcions calculen la clau pública a partir d'una clau original – clau privada – que es genera de forma aleatòria[24].

D'aquesta forma, cada un dels usuaris de la xarxa, compta amb dues claus associades de forma matemàtica: una **clau pública** que es distribueix per tota la xarxa, i mitjançant la qual es xifren les transaccions i permet identificar-se amb la resta de la xarxa, i l'altra, una **clau privada** la qual manté la funció de desxifrar les dades i que permet la firma per a la realització de transaccions en la xarxa.

És a dir, l'emissor del missatge, sempre xifra les dades que vol enviar amb la **clau pública** del receptor, mentre que el receptor utilitza la seva **clau privada** per tal de desxifrar el conjunt de dades que l'hi ha enviat l'emissor.

2.2.3. Protocol i l'algorisme de consens

La causa de la falta d'acords en arribar a un únic consens en els sistemes descentralitzats es genera en el moment en què apareixen escenaris com la caiguda de participants, la violació de les normes establertes, la falta de confiança entre els participants i/o l'existència de canals imperfectes, els quals provoquen, que **l'algorisme de consens** sigui la implementació en aquests sistemes, que més possibilitats té d'aproximar-se a obtenir un consens majoritari entre els diferents participants.

Perquè tots els nodes puguin desenvolupar les funcions de forma adequada, és necessari que estiguin connectats i sincronitzats entre ells mateixos. Això, només es pot obtenir en cas que utilitzin un canal únic i idèntic de comunicació, el qual ve representat per un protocol estàndard, acceptat gràcies al consens del conjunt dels participants, en forma de software informàtic.

Cal remarcar que el protocol i l'algorisme de consens no són el mateix. Podem definir el **protocol** com el conjunt de regles primàries d'una cadena de blocs. En canvi, **l'algorisme**, és un mecanisme a través del qual les regles són seguides, i serà aquest el que li dirà al node quins passos s'han de seguir per complir les regles i produir els resultats desitjats.

[24] PREUKSCHAT, Alex; NÚÑEZ, Jaime. 2017. Blockchain: la revolución industrial de internet. Editorial Gestión 2000. Criptografía y consenso aplicado a la blockchain: 203-220.

A partir del consens de la comunitat, s'aniran realitzant modificacions i millores per adaptar el protocol a les innovacions que vagin sorgint del desenvolupament tant del protocol de consens com dels altres protocols i tecnologies que s'utilitzen.

Així doncs, la millor aproximació a la utilitat de **l'algorisme de consens**, és que assegura les regles i els principis de com s'han de comunicar els nodes d'una xarxa. Aquest fet que permet organitzar i establir relacions sense dependre de la confiança entre participants, així com assegurar que el següent bloc de la cadena és l'única versió existent i que és verídica.

Existeixen diversos tipus de **protocols de consens** que resolen els problemes de consens. A continuació, es presenten els protocols més comuns i utilitzats en l'ecosistema de blockchain i de les criptomonedes en general:

- **PoW: Proof-Of-Work o Prova de treball**: Mecanisme de consens, més utilitzat en l'actualitat, que obliga als usuaris a realitzar un treball computacionalment costós, amb la finalitat de poder fer ús d'un servei o xarxa, amb una recompensa econòmica per l'esforç[25], i al mateix temps, per evitar el mal ús d'aquest[26].

  Aquest mecanisme és el mateix mecanisme amb menys dificultat, que s'utilitza quan a l'hora d'accedir a un compte d'una pàgina d'Internet, has d'escriure el que veus en una imatge, o seleccionar unes imatges concretes, el captcha[27].

  És molt segur, senzill i fàcil d'implementar. També permet una ràpida adaptació a les necessitats del hardware, disposa d'una gran capacitat de resistència davant atacs DoS (Denegació de serveis) i com més poder de computació tens, major serà el benefici i pes de verificació que tindràs en la xarxa.

[25] Les recompenses que reben els miners, provenen de la suma de les comisions que es paguen per realizar transaccions en la moneda en qüestió més una recompensa per generar un bloc. La recompensa per generar un bloc está preestablerta en les normes. Cada criptomoneda varia. Per a més informació: MEJIA, Jose Luis. ¿A dónde van los cargos por transacción de Bitcoin? https://steemit.com/spanish/@joseluismejia/a-donde-van-los-cargos-por-transaccion-de-bitcoin [Consultat: 3 abril 2019]

[26] BOLAÑOS, Juan Francisco. *Blockchain y la Prueba de Trabajo – PoW –.* https://steemit.com/cryptocurrency/@juanfb/blockchain-y-la-prueba-de-trabajo-pow [Consultat: 31 març 2019]

[27] Com més difícil sigui, més temps s'haurà d'invertir per solucionar el problema.

Així i tot, és altament costós a nivell tant computacional com energètic perquè la major part del poder computacional es perd, ja que tots competeixen per trobar primer la solució matemàtica. Per altra banda, el sistema de recompenses de validar transaccions i minar blocs, provoca una pressió venedora del valor, ja que no hi ha cap necessitat de mantenir en possessió les monedes, i l'evolució del hardware deixa enrere la capacitat de resistència del mateix algorisme de consens.

- **PoS: Proof-Of-Stake o Prova de participació**: Mecanisme de consens que funciona mitjançant la petició de proves de possessió de les monedes. És a dir, la probabilitat de poder validar un bloc de transaccions, és directament proporcional a la quantitat de monedes que un té en dipòsit (no es poden tocar mentre mantenen en dipòsit), evitant així que la confiança vingui donada per la quantitat de treball invertit, i fent que els que posseeixen més participació en la xarxa siguin els més indicats per protegir-la i els que més hi poden perdre[28].

  Es pretén que aquest mecanisme de consens permeti incentivar a minar a nous usuaris (ja que no cal una gran infraestructura) i que per tant, sigui una xarxa més distribuïda i amb major descentralització de poder. Per altra banda, la despesa energètica és menor perquè no necessita un treball computacional tan elevat, i el grau de rendiment de la xarxa és molt major en comparació al sistema de prova de treball[29]. A diferència de la prova de treball, la participació està subjecte a la quantitat de monedes en possessió, fet que provoca que els validadors no exerceixin la pressió venedora dels incentius percebuts.

  Tot i això, l'anonimat en la xarxa és molt més complex de mantenir, no hi ha recompenses per minar blocs, només a partir de les comissions que sorgeixen per validar les transaccions executades[30]. La participació dels nodes depèn de la quantitat de monedes que tinguin en possessió, és a dir, segons la seva capacitat

[28] BUTERIN, Vitalik. *Proof of Stake FAQ*. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ [Consultat: 31 març 2019]
[29] BOLAÑOS, Juan Francisco. *Blockchain y la Prueba de Participación (PoS).* https://www.academiablockchain.com/2018/05/17/blockchain-y-la-prueba-de-participacion-pos/ [Consultat: 31 març 2019]
[30] Pensat perquè serveixi com a model d'inversió. Un usuari manté una quantitat en dipòsit, i obté un rendiment per a aquesta quantitat que prové de les comissions, ja que el cost de minar es veurà radicalment reduït. DHANANI, Shanif. *Ethereum's Proof-of-Stake May Be A Profitable Venture For Current Holders.* https://medium.com/@shanif/ethereums-proof-of-stake-may-be-a-profitable-venture-for-current-holders-183024263151 [Consultat: 20 abril 2019]

financera, i el fet de minar sense la necessitat d'un treball intensiu, pot incentivar a alguns generadors de blocs a verificar múltiples històries de blockchain, destruint el consens inicial.

- **PoA: Proof-Of-Authority o Prova d'autoritat**: Mecanisme de consens alternatiu on existeixen ja diversos nodes d'autoritat preestablerts i aprovats, que reben el nom de segelladors. En comptes de tenir una certa quantitat d'actius retinguts com a valor, s'utilitza la identitat.

  En aquest context, la identitat significa la correspondència entre la identificació personal d'un validador en el món real. Qualsevol participant que vulgui ingressar en la xarxa, haurà de passar per una votació, cosa que dóna control total sobre quins nodes poden segellar blocs en la xarxa, i permet assegurar-se de què nodes maliciosos no puguin malmetre la xarxa[31].

  A diferència de PoS, només hi ha una identitat per persona. Això significa, que has de revelar voluntàriament qui ets, a canvi de tenir dret a crear els blocs, fet que provoca que els beneficis que obtinguis en el procés de validació de transaccions i creació de blocs, siguin públics i també les accions que dus a terme.

  Les persones les quals la seva identitat està en joc per assegurar una xarxa, estan incentivades per preservar la xarxa. Com bé diu Warren Buffet,"*Es necessiten 20 anys per construir una reputació i 5 minuts per arruïnar-la*"[32].

  Permet una major eficiència en els temps de transacció i el consens en general de la xarxa, fet que afecta positivament en l'escalabilitat de les mateixes xarxes. Tanmateix, els avenços tecnològics poden ajudar a assegurar encara més les xarxes, ja que els validadors són independents entre si, i susceptibles a la intervenció de tercers.

  Així i tot, aquest sistema abandona un dels principals principis de blockchain, i és el de la privacitat, i per altra banda, és una versió lleugerament més

[31] MALDONADO, Jose. *¿Qué es la prueba de Autoridad (POA)?* https://www.criptotendencias.com/base-de-conocimiento/que-es-la-prueba-de-autoridad-poa/ [Consultat: 31 març 2019]
[32] OLMO, Lara. *10 grandes frases de Warren Buffet para los negocios (y la vida).* https://www.estrategiaynegocios.net/empresasymanagement/1113606-330/10-grandes-frases-de-warren-buffett-para-los-negocios-y-la-vida [Consultat: 31 març 2019]

descentralitzada d'un sistema centralitzat. Una de les principals preocupacions és que algunes persones simplement no es preocupen per la seva reputació, cosa que pot produir males conductes indetectables en un primer moment.

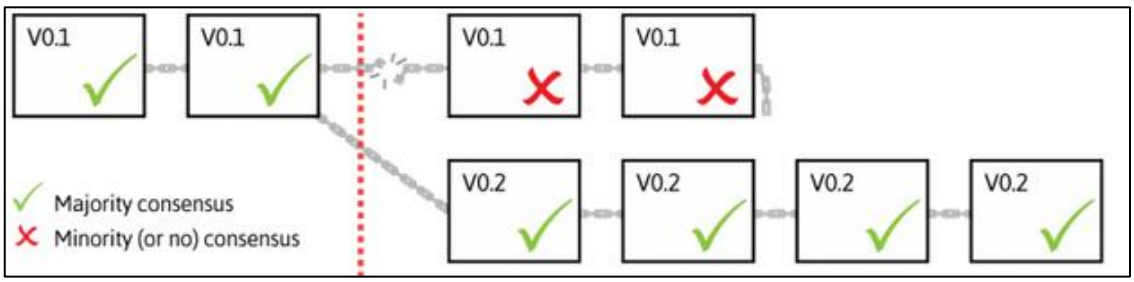
Cal destacar però, que cada cadena de blocs és diferent, i conseqüentment, les normes i el protocol de consens que s'aplica. És per això, que en l'anàlisi anterior es dóna una imatge genèrica dels diferents protocols de consens.

En cas que hi hagi propostes de millores en el protocol, les modificacions s'han de presentar a la comunitat. Tot seguit, la comunitat de la xarxa debat a través de plataformes digitals i conferències sobre la viabilitat de la proposta i la possible repercussió de la implementació en la xarxa.

Depenent de l'impacte que tenen aquestes modificacions en el protocol vigent, podem diferenciar en dos tipus de fork: un softfork o un hardfork. En la pràctica, consisteixen en el fet que un cop finalitzat el debat de la comunitat, hi haurà dues còpies similars del software que començaran a desenvolupar-se de forma independent a partir de la bifurcació de la xarxa i per tant dues blockchain separades[33].

- **Softfork**: L'actualització del protocol és compatible i no entra en conflicte amb la versió antiga del software. Per tant, es romandrà en la mateixa cadena. El nou software, V0.2, valida només una part dels blocs i ignora els altres, mentre que els nodes antics que no han actualitzat el software V0.1, podran continuar validant tots els blocs amb les regles anteriors però estaran creant una cadena més dèbil, que perdrà suport, i al final, els participants hauran d'actualitzar el software per

Il·lustració 2: Cas d'aplicació de softfork



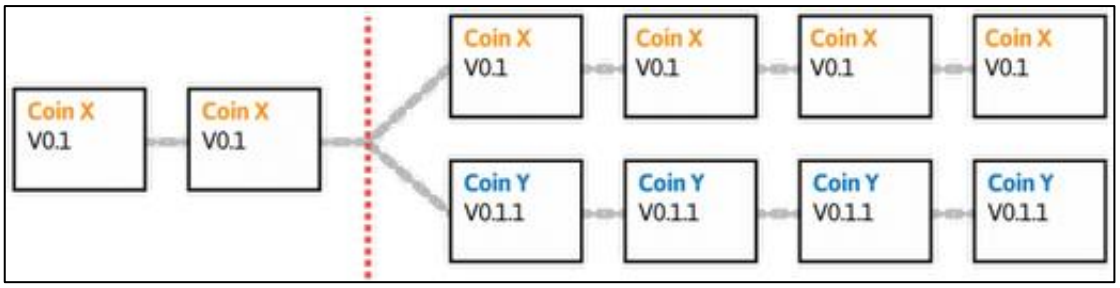
Font: Elaborat per CryptoGraphics.info

[33] LEUSSINK, Klaas. *Hard and Soft forks*. https://cryptographics.info/cryptographics/blockchain/hard-soft-forks/ [Consultat: 31 març 2019]

continuar treballant amb la nova actualització. Aquestes actualitzacions s'activen quan estan acceptades per una majoria de miners.

- **Hardfork**: Es tracta d'una bifurcació definitiva de la cadena, es comença amb una nova, però amb els registres de l'anterior, i es produeix a causa d'un canvi en les regles que fan vàlids alguns blocs que en la versió anterior serien rebutjats.
  Els nodes actualitzats amb la nova versió de la blockchain, validaran tots els blocs, però els que no acceptin els canvis, i per tant, no actualitzin el seu software, no podran validar els nous blocs de la nova blockchain i romandran en la cadena original. Aquest cas es dóna quan les millores a implementar divideixen la comunitat i aquesta, decideix dividir-se a partir de les seves actualitzacions.

Il·lustració 3: Cas d'aplicació de hardfork



Font: Elaborat per CryptoGraphics.info

Dels elements característics de la blockchain cal remarcar que un funcionament adequat de la xarxa només serà possible amb la participació d'un gran nombre de nodes, l'acceptació de les normes d'ús i del consens entre els participants.

2.3. Com Funciona

Com bé indica el seu nom, blockchain és una cadena de bocs, dit d'una altra manera, és una consecució de blocs, encadenats i vinculats amb el bloc anterior.

Tot procés comença simplement amb la realització d'una transacció. Dues parts, A i B, decideixen intercanviar una unitat de valor (sigui una moneda digital, un certificat, una propietat, etc.), és a dir, qualsevol actiu que pugui ser descrit en forma digital. Un cop realitzada la transacció, la comparteixen amb la resta de la xarxa.

- Totes les transaccions són atòmiques, és a dir, tota l'operació s'executa, o en cas d'algun error en la seva estructura, l'operació es cancel·la.
- Les transaccions s'executen de manera independent, per tant, no hi ha dues operacions que poden interactuar o interferir entre ambdues.

- Transaccions les quals es poden inspeccionar, que permet la possibilitat d'auditar i assegurar solucions a una escala molt àmplia.
- Els objectes són immortals mentre els nodes continuïn executant la blockchain. Només si està programat es poden retirar o a partir d'un softfork o hardfork.

Cada bloc és identificat amb un hash, que, com ens indica NÚÑEZ, "*és un verb que en anglès significa "picar" i moldre*", ja que la criptografia consisteix a moldre uns continguts fins a obtenir una seqüència de caràcters d'una llargada màxima[34]. Sempre que s'apliqui la mateixa funció al mateix contingut, obtindrem el mateix hash, però en el moment en què es modifiqui un sol caràcter, el hash canviarà de forma radical, gràcies a la propietat de caràcter unidireccional – una única direcció – de l'algorisme.

Les funcions unidireccionals permeten eficiència de càlcul pel que fa a velocitat d'operacions i baix cost, resistència a preimatge[35], i que sigui molt difícil generar dos missatges diferents que donin el mateix hash com a resultat.

El propòsit d'un hash, no és el d'amagar el missatge, ni el de permetre el desxiframent després, sinó el de comprovar la integritat i verificar que no hi ha hagut alteració de les dades.

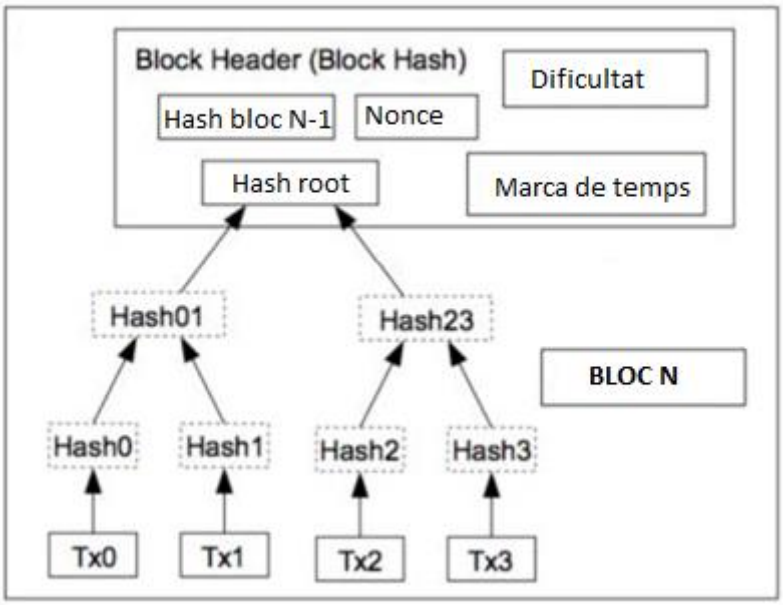
L'estructura d'un bloc comença per l'ENCAPÇALAMENT que conté un conjunt de metadades diferents sobre el bloc:

- El hash del bloc anterior. En una blockchain, cada bloc hereta del bloc anterior el seu identificador – hash –. Per a cada bloc N que la xarxa generi, haurà de contenir el hash del bloc N-1.
- Un nonce, és un nombre aleatori de 64 bits que varia en cada intent d'obtenir el hash correcte. Depenen de la dificultat establerta[36], hi haurà més o menys probabilitats d'obtenir el nonce correcte abans.
- Un marca de temps – timestamp en anglès – (quan s'ha generat el bloc).

[34] PREUKSCHAT, Alex; NÚÑEZ, Jaime. 2017. Blockchain: la revolución industrial de internet. Editorial Gestión 2000. Criptografía y consenso aplicado a la blockchain: 203-220.
[35] La resistència a preimatge, significa que és computacionalment molt difícil obtenir un missatge d'entrada que produeixi un hash predeterminat i que per tant, sigui molt complicat preveure la seqüència numèrica
[36] Per exemple, el nombre de 0 amb el que ha de començar el hash a validar.

- Una dificultat del bloc[37], és un mètode que contribueix a mantenir certa freqüència en el temps que s'utilitza la xarxa per afegir nova informació a la cadena. Per tant, si els miners sumen més hashrate per processar transaccions i disminueix el temps entre blocs afegits, s'augmentarà la dificultat del mètode.
- La Merkle Root o arrel de l'arbre de merkle. És l'encapçalament de l'arbre, és a dir, és un hash, resultat d'aplicar una funció de hash sobre els hash anteriors.

Il·lustració 4: Estructura d'un bloc



Font: Elaboració pròpia amb plantilla de blog.soydata.net

Tot seguit, hi ha l'IDENTIFICADOR del bloc, que és, el **hash del bloc**. L'altra via per identificar de forma específica un bloc, és segons el número del bloc en la blockchain[38].

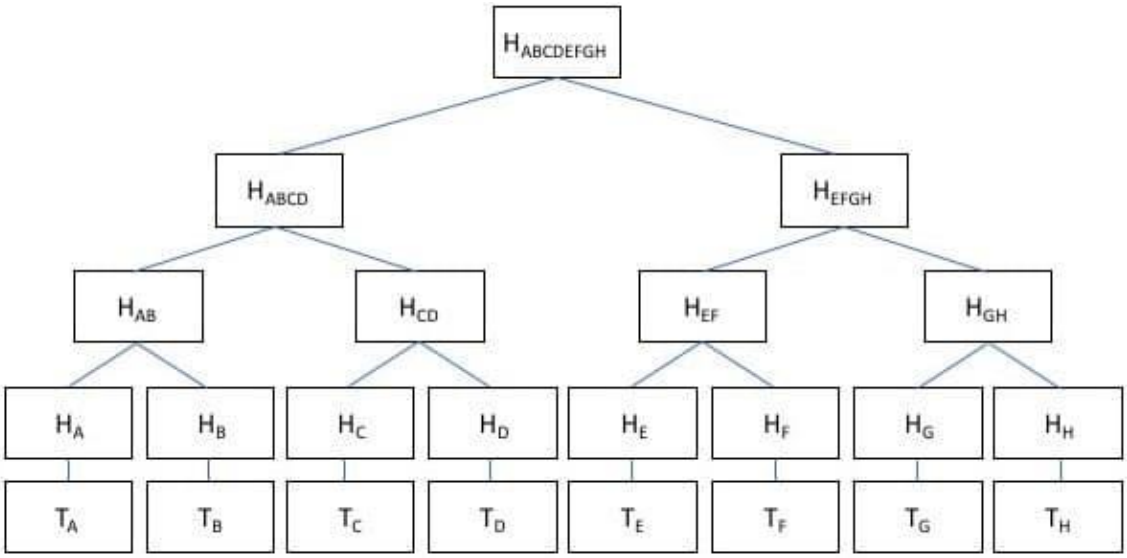
Per últim, tenim el CONTINGUT del bloc, on hi ha totes les transaccions que emmagatzema. L'estructura que guarda totes les transaccions, és el Merkle Patricia Tree.

T_A representa una transacció normal, és a dir, A envia alguna cosa a B. La transacció, s'introdueix en una funció de hash que retorna un valor de hash H_A. Després que cada transacció hagi estat modificada amb la funció de hash, el hash H_A correspost a la transacció T_A és combina amb un hash adjacent H_B, creant el nou hash combinat H_{AB}. Per tant, després de combinar totes les transaccions emmagatzemades en el contingut del bloc,

[37] PREUKSCHAT, Alex. *Hashcash.* https://libroblockchain.com/hashcash/ [Consultat: 1 abril 2019]
[38] Per buscar un bloc específic, entre d'altres opcions, pots visitar aquesta página web on trobaràs tota la blockchain de 3 de les principals criptomonedes. Blockchain Explorer. https://www.blockchain.com/es/explorer [Consultat: 2 abril 2019]

s'obtindrà un únic hash ($H_{ABCDEFGH}$) que serà el representant de totes les transaccions anomenat Merkle Root.

Il·lustració 5: Exemple de Merkle Patricia Tree



Font: Creat per Investopedia

El següent procés de creació d'un bloc, es realitzarà amb la prova de treball, ja que és el més extens i s'utilitza, de moment, en les principals cadenes de blocs[39]. Per altra banda, s'intentarà explicar de forma genèrica tot el procés de creació d'un bloc i no centrant el procés a com es realitza en la xarxa Ethereum.

Totes les transaccions són executades, firmades per una wallet (cada usuari en disposa d'una o varies), registrades i transmeses a tots els nodes de la xarxa, les quals les afegeixen a una llista d'espera sense verificar. Així, tots els integrants tenen la informació constantment actualitzada. Tot seguit, els miners escolliran les transaccions[40] sense confirmar per crear un nou bloc de transaccions.

Un cop validades les transaccions pel node (a partir d'unes normes), el miner obté el merkle patricia tree de les transaccions i genera el root hash.

[39] BOTJES, Edzo. *Pulling the Blockchain apart. The transaction life-cycle* https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3 [Consultat: 1 abril 2019]

[40] Com més gran sigui la comissió pagada per l'usuari a l'hora de realizar la transacció, major possibilitat tindrà aquest, de que qualsevol miner seleccioni la seva transacció per validar-la.

Tot seguit obté el nonce aleatori, i l'incorpora a l'encapçalament, executa l'algorisme Ethash[41] dues vegades amb les dades de l'encapçalament, i en el moment en què aquest hash compleixi les normes (com per exemple, que comenci amb 6 zeros), s'haurà obtingut el hash correcte. En cas contrari, tornarà a crear un nou nonce, i tornarà a intentar generar el hash correcte[42].

Un cop s'obté el hash correcte, el miner crea el bloc i el node afegeix el nou bloc a la cadena de blocs local. Tots els nodes actualitzen la xarxa de forma constant, i en el moment en què s'afegeix un nou bloc en cadena de blocs, el node comparteix la seva actualització amb la resta de la xarxa per a què aquests, comprovin la seva veracitat.

En aquest punt, els miners que estaven generant un bloc, tornen a començar de nou a partir de la cadena de blocs actualitzada. I els miners que han creat el bloc que ha estat finalment afegit a la cadena de blocs.

El problema sorgeix, quan dos miners emeten els seus blocs vàlids a la xarxa en pocs segons de diferència o el contingut del bloc és modificat. Aquest problema s'anomena, *El Problema dels Generals Bizantins*[43].

Alguns nodes rebran un bloc abans que l'altre (Bloc 1), i començaran a resoldre el següent bloc (Bloc 1.1, Bloc 1.2, Bloc 1.3 ...) a partir del (Bloc 1). D'altra banda, altres nodes rebran un bloc diferent abans (Bloc 2) i començaran a resoldre el següent bloc a partir d'aquest.

És en aquest moment quan la resta de nodes descarten la cadena de blocs més curta (Bloc 2), i els blocs que s'hagin generat a partir d'aquest queden eliminats. Aquests blocs s'anomenen blocs orfes. Tot seguit, els nodes s'incorporaran a la cadena de blocs més llarga, ja que serà la més acceptada per la majoria de nodes de la xarxa.

---

[41] Versió modificada de Dagger Hashimoto i mix del SHA3 i més avançat que SHA-256, que és el que s'utilitza en la prova de treball de Bitcoin. Per a més informació, visitar: RAY, James. *Dagger Hashimoto.* https://github.com/ethereum/wiki/wiki/Dagger-Hashimoto [Consultat: 21 abril 2019]

[42] En el cas de Bitcoin, aquest procés dura minuts (fins que un miner trobi el hash correcte) a causa de l'elevada dificultat.

[43] SOTO, Marvin G. *El problema de los Generales Bizantinos (PGB).* https://medium.com/@marvin.soto/el-problema-de-los-generales-bizantinos-pgb-e0cb8c4279c2 [Consultat: 20 abril 2019]

2.4. Avantatges de Blockchain

A partir de les definicions, dels principals elements i del funcionament d'una cadena de blocs presentats anteriorment, es presentarà una anàlisi més exhaustiva dels avantatges d'implementar una cadena de blocs pública:

La característica més important que ha contribuït al fet que aquesta tecnologia rebi els qualificatius de disruptiva i revolucionaria[44], és que és una **xarxa descentralitzada**[45] i **distribuïda**. Això ha permès la delegació del poder sobre el conjunt de la xarxa i que els seus participants puguin ser lliures d'escollir la seva ubicació segons les seves necessitats. Tot això, ha fet possible que la xarxa estigui sempre activa i sigui capaç de pal·liar els possibles atacs a nodes, desastres naturals, avaries dels mateixos nodes o regulacions polítiques.

Com bé s'ha esmentat anteriorment, la cadena de blocs consecutius permet mantenir la **immutabilitat de les dades**, gràcies al fet que tots i cada un dels miners de la xarxa tenen en el seu node la cadena de blocs completa i actualitzada, i per tant la modificació d'un registre en un o diversos nodes no tindrà efecte mentre no superi el 51% de la capacitat de processament de la comunitat en qüestió. A l'hora d'emmagatzemar les dades en un bloc es realitza de forma **cronològica**, és a dir, cada bloc fa referència al bloc anterior a través d'un hash generat en el procés de validació d'aquest, permetent trobar fàcilment qualsevol modificació i mantenint així la immutabilitat dels registres.

Les **normes estan establertes** en un conjunt d'estàndards que conformen un protocol per a cada cadena de blocs i s'actualitzen, a partir del consens de la comunitat a mesura que les noves necessitats sorgeixen. Aquest fet, permet mantenir certa estabilitat en els projectes i comunitats. Pel que fa a les comunitats, cal destacar que són **inclusives**, és a dir, nous participants poden accedir en qualsevol moment, ja que les úniques barreres d'entrada són, depenent de la prova de concepte aplicada, disposar de tokens de la xarxa, l'equip i la instal·lació necessaris per poder executar la pròpia blockchain.

---

[44] GARCÍA, Isra. *Blockchain: descentralización y disrupción como nunca antes en la historia.* http://www.expansion.com/blogs/economia-disruptiva/2018/01/15/blockchain-descentralizacion-y.html [Consultat: 13 abril 2019]

[45] Pàgina web per veure dades de les principals criptomonedes com el nombre de nodes públics o d'entitats que controlen un % alt del hashrate. https://arewedecentralizedyet.com/ [Consultat: 16 abril 2019]

Un dels aspectes més rellevants d'aquesta tecnologia, és que **s'elimina la necessitat de confiar** amb tercers o entitats (intermediaris)[46], mantenint només als mateixos miners, els quals l'únic incentiu que tenen és obtenir la recompensa per les despeses i temps invertits, i no el contingut de la mateixa transacció. Aquest fet, permet que les transaccions siguin en comparació als sistemes tradicionals de pagament i transaccions financeres, més **ràpides**[47], en molts casos en **temps real**, i amb una gran reducció de despeses[48]. Tot això és possible, gràcies a l'automatització del procés de transmissió[49], que per altra banda, permet reduir considerablement els riscs d'errors sistemàtics com ara l'eliminació d'errors humans[50] o l'eliminació d'embuts millorant la qualitat dels processos.

L'aplicació de criptografia en el procés de transmissió i emmagatzematge de dades, permet mantenir un gran nivell de **privacitat** i **seguretat** de les dades. A partir de l'aplicació dels diferents algorismes matemàtics, les transaccions no tenen cap valor per a tercers que no han participat en la transacció o no tenen la clau per poder desxifrar les dades. La implementació d'aquests algorismes matemàtics, permet als seus participants mantenir **l'anonimat**, el qual s'està degradant cada vegada més amb la nova era d'Internet, i per altra banda, augmentar la seguretat de les dades.

Per últim, destacar que, a l'espera de possibles futures regulacions per a la utilització de criptomonedes i/o el manteniment de la propietat de nodes que executen la cadena de blocs[51], actualment hi ha **llibertat de pagament**, és a dir, es pot enviar i rebre qualsevol

---

[46] AMMOUS, Saifedean. 2017. El patrón Bitcoin: La alternativa descentralizada de los bancos centrales. Editorial DEUSTO.

[47] MERLO, Irene. *¿Cuánto tarda una transferencia internacional en hacerse efectiva?* https://www.helpmycash.com/blog/cuanto-tarda-una-transferencia-internacional-hacerse-efectiva/ [Consultat: 13 abril 2019]

[48] L'única despesa és la comissió que es paga en el moment de realitzar la transacció. Aquesta, és molt reduïda en comparació a les comissions actuals per realitzar transaccions internacionals o a altres bancs, i va en funció a la rapidesa que vulgui l'usuari que s'efectuï la transacció, el pes en bytes d'aquesta, i depenent del mitjà que s'utilitza, una comissió per al mitjà (plataforma en línia per realitzar operacions amb monedes digitals). Per a més informació: Bit2Me Academy. *Cómo saber la comisión de una transacción Bitcoin.* https://academy.bit2me.com/como-saber-la-comision-de-una-transaccion-bitcoin/ [Consultat: 13 abril 2019]

[49] FERNÁNDEZ, Froilan. *Las criptomonedas retan al sistema bancario tradicional.* https://www.criptonoticias.com/opinion/criptomonedas-retan-sistema-bancario-tradicional/ [Consultat: 13 abril 2019]

[50] GAMALERO, Martin. *Blockchain eliminará desperdicios en la industria de la logística.* https://criptotario.com/blockchain-eliminara-desperdicios-la-industria-la-logistica [Consultat: 13 abril 2019]

[51] Legality of bitcoin by country or territory explained http://everything.explained.today/Legality_of_bitcoin_by_country_or_territory/. CASADO, Nicomedes. *Medidas y Regulaciones que vienen en camino para las criptomonedas*.

quantitat de diners de forma instantània des de qualsevol lloc del món, sense bancs ni horaris, sense fronteres, sense límits imposats. Els usuaris tenen el control total sobre els seus diners.

2.5. Inconvenients Blockchain

Un cop mencionats els avantatges que suposa la implementació de la cadena de blocs, també cal mencionar un conjunt d'inconvenients detectats, i per altra banda, les principals amenaces que estan sorgint, o que poden sorgir en un futur pròxim. Aquests, han sorgit fruit de la implementació de diversos projectes i han permès donar un punt de vista més ampli de les deficiències d'aquesta tecnologia i dels que l'implementen.

El principal problema que hi ha, és en la implementació, execució i manteniment de la infraestructura d'aquesta tecnologia. Per al correcte funcionament d'una cadena de blocs, es **requereix una gran quantitat d'energia**[52]. Energia que s'utilitza en mantenir els nodes actius, executant algorismes, els quals requereixen una gran capacitat de processament per tal de trobar els hash correctes, tenint en compte que la dificultat d'aquests augmenta segons la potència total dels nodes actius en la xarxa i les normes establertes.[53]. Si l'hi sumem al fet que la **major de la capacitat de processament es perd**, ja que només el primer a trobar el hash correcte obté la recompensa, podem concloure que la prova de treball, implementada per la gran majoria de projectes, provoca una gran ineficiència d'energia i un alt deteriorament de les mateixes instal·lacions dels nodes.

La gran esperança de la comunitat blockchain, és la d'implementar la prova de participació com a prova de concepte. La comunitat amb més probabilitat d'implementar-la, és Ethereum, i com ja s'ha demostrat últimament, estan molt lluny de fer-ho possible a causa dels problemes que comporta en termes d'escalabilitat i seguretat de les dades.

Tota cadena de blocs **requereix un gran nombre de participants distribuïts** perquè aquesta pugui ser executada de forma segura i permeti mantenir la integritat de les dades,

---

https://www.criptomano.com/medidas-y-regulaciones-que-vienen-en-camino-para-las-criptomonedas/ [Consultat: 14 abril 2019]

[52] Digiconomist. *Bitcoin Energy Consumption Index*. https://digiconomist.net/bitcoin-energy-consumption [Consultat: 6 abril 2019]

[53] SALAZAR, Jonathan. *Una sola transacción de Bitcoin utiliza la misma cantidad de energía que una casa en tres semanas.* https://tekzup.com/una-sola-transaccion-de-bitcoin-utiliza-la-misma-cantidad-de-energia-que-una-casa-en-tres-semanas/ [Consultat: 6 abril 2019]

sense que hi hagi la possibilitat d'atacs del 51%. Quines implicacions té aquest fet? Doncs implicacions rellevants, ja que si una cadena de blocs no té un gran suport, serà molt barat corrompre les dades. La desactualització és una amenaça important perquè tots els projectes s'han anat actualitzant al llarg del temps. Alguns d'ells han realitzat hardforks, com ara el que es va realitzar el 15 de Novembre a la cadena de blocs Bitcoin Cash, generant dues noves cadenes de blocs[54], Bitcoin Cash ABC i Bitcoin Cash Satoshi Vision, ambdues amb la meitat del hashrate que tenien prèviament. Tot plegat facilita i fa més barat un atac.

A diferència de perdre la cartera física o una targeta bancaria, en què en ambdós casos pots acabar recuperant part del contingut o demanar una còpia a l'entitat, amb la **pèrdua de la clau privada**, de les dades d'accés a moneders digitals, o si el servei de tercers que guarda la teva cartera deixa de funcionar, perdràs la possibilitat de tenir accés al valor que emmagatzemaves[55].

La necessitat d'haver de mantenir tota la base de dades de la cadena de blocs en cada un dels nodes que participen en la xarxa, provoca que sigui una **redundància molt costosa**. I per altra banda, s'utilitza un **mètode poc eficaç i lent** de realitzar transaccions en comparació a altres tecnologies. En realitat, l'únic aspecte a destacar, és el grau d'importància que se l'hi dóna a la confiança entre participants i a les dades que s'hi generen. El primer pas per aconseguir-ho, depèn d'eliminar intermediaris i ser conscients del valor que tenen les nostres dades.

Un dels grans problemes, és la **falta d'escalabilitat**[56] de la blockchain. Un augment de l'escalabilitat de la cadena de blocs, provocarà un augment en el nombre màxim de transaccions per segon. Aquest fet afectarà directament a la càrrega computacional i d'emmagatzemament sobre els membres de la xarxa. Com major sigui el volum de dades de la cadena de blocs, major serà el cost d'unir-se en la xarxa i menys nodes tindran la

[54] WALL, Jeremy. *Bitcoin Cash Hard Fork Aftermath: BCHABC and BCHSV Continue to Battle It Out*. https://www.investinblockchain.com/bitcoin-cash-hard-fork-aftermath/ [Consultat: 7 abril 2019]
[55] GAS, Dani. *Una quinta parte de Bitcoin está perdido, el suministro real de BTC es muy bajo.* http://infocoin.net/2018/07/07/una-quinta-parte-de-bitcoin-esta-perdido-el-suministro-real-de-btc-es-muy-bajo/ [Consultat: 6 abril 2019]
[56] CASTRO, Luis. *¿Qué es escalabilidad?* https://www.aboutespanol.com/que-es-escalabilidad-157635 [Consultat: 7 abril 2019]

capacitat suficient per mantenir el ritme. És per tant, que la xarxa tendirà cap a la **centralització del poder**.

Per últim, cal puntualitzar que s'estan duent a terme estudis per part dels estats i entitats financeres, per **regular i aplicar normatives** més dures i restrictives amb la finalitat d'obtenir un major control sobre les identitats dels participants de les xarxes i els seus moviments. Alguns països ja han prohibit l'existència de plataformes que permeten la conversió de la moneda local amb criptomonedes, per la falta de control que suposa. A escala europea, s'ha decidit promoure més que regular les iniciatives de blockchain, i ha deixat en mans dels estats la interpretació i aplicació de les regulacions pertinents[57]. En l'àmbit espanyol, una de les propostes amb major acceptació, és, com bé indica José Carmelo Llopis, incloure les criptomonedes en la Quarta Directiva, la qual serà aplicable als intercanvis de moneda virtual, sotmetent a la normativa de prevenció de blanqueig de capitals[58].

Cal una profunda reflexió per poder observar i ser conscients de tot el que ens pot aportar la tecnologia blockchain un cop sigui implementada en el nostre dia a dia[59]. És per tant, que caldrà estar atents a les possibles regulacions que es vagin implementant.

Pel que fa a les **grans amenaces a la tecnologia blockchain**, l'arribada de potents ordinadors quàntics, els quals realitzaran operacions matemàtiques per resoldre els algorismes que utilitza la criptografia en microsegons[60], i per tant, faran obsolets tots els nodes que actualment competeixen i mantenen les diferents cadenes de blocs. Principalment, hi ha dues solucions. La primera implica dissenyar cadenes de blocs resistents a la computació quàntica by default, i per tant, crear-les de zero. Mentre que l'altra opció contempla substituir els esquemes de signatura digital, o algorismes

[57] YAKUBOWSKI, Max. *Europa da pasos serios hacia adopción de blockchain*. https://es.cointelegraph.com/news/europe-takes-serious-steps-towards-blockchain-adoption [Consultat: 15 abril 2019]
[58] CARMELO, José. *¿Existe regulación de blockchain en la Unión Europea?* http://www.notariallopis.es/blog/i/1424/73/existe-regulacion-de-blockchain-en-la-union-europea [Consultat: 15 abril 2019]
[59] LEONARD, Andreu. *The Blockchain is a remainder of the Internet's Failure*. https://onezero.medium.com/the-blockchain-is-a-reminder-of-the-internets-failure-b16c58d70413 [Consultat: 15 abril 2019]
[60] IGLESIAS, Andreina. *La computación cuántica podría hacer vulnerable a la Blockchain*. https://bitcoin.es/actualidad/la-computacion-cuantica-podria-hacer-vulnerable-a-la-blockchain/ [Consultat: 11 abril 2019]

generadors de hash, en aquells nous algorismes capaços d'aplicar tecnologia quàntica[61]. Tot això, a condició que la implementació de la tecnologia quàntica sigui satisfactòria, i sigui rendible desenvolupar ordinadors capaços d'implementar aquesta tecnologia[62].

Pel que fa a **possibles alternatives** a la tecnologia blockchain, a part de les que ja s'implementen com les mateixes bases de dades o els serveis de còpia de seguretat, han sorgit noves propostes les quals s'han centrat a potenciar algunes de les solucions que aporta la tecnologia blockchain, però no en potenciar el seu conjunt. Les alternatives són: TIPS[63], una nova infraestructura de pagaments internacionals desenvolupada pel BCE que permet la realització de transaccions instantànies les 24 h del dia a un baix cost, Hashgraph[64],que és un sistema de xarxa centralitzada en comptabilitat i consens, que permet 250.000 transaccions per segon, més segura, ja que es requereix que 2/3 de la xarxa validin una transacció però privada i amb nodes estàtics i coneguts, i per últim, Atos[65] que és un sistema de xifrar modulable d'arxius que permetrà a l'usuari exercir major control sobre les seves dades. Amb aquest sistema, serà possible crear claus parcials per permetre a tercers accedir a les dades.

Aquestes propostes s'han centrat a millorar alguns aspectes concrets com la velocitat de les transaccions, l'eficiència energètica de la xarxa, el xifratge i el control de les dades, però cap d'elles s'ha centrat a mantenir la confiança i la privacitat de les dades com a base del sistema, i com a principal innovació i disrupció que comporta la tecnologia blockchain.

---

[61] Els quals de moment no existeixen. Segons els especialistes, hi ha aproximadament un 14% de probabilitats que un ordinador quàntic estigui disponible comercialment al 2026, i un 50% de cara al 2031. Per a més informació: GHEORGHIU, Vlad; GORBUNOV, Sergey; MOSCA, Michele; MUNSON, Bill. *Quantum-Proofing the blockchain*. https://www.evolutionq.com/assets/mosca_quantum-proofing-the-blockchain_blockchain-research-institute.pdf [Consultat: 11 abril 2019]

[62] VILLATORO, Francisco R. *El ruido cuántico contra el futuro de la computación cuántica*. https://francis.naukas.com/2016/11/29/el-futuro-de-la-computacion-cuantica/ [Consultat: 11 abril 2019]

[63] PIRES, Tiago. *TIPS, the new European payment system*. https://technologist.eu/tips-the-european-instant-payment-settlement/ [Consultat: 15 abril 2019]

[64] És síncrona, ja que ningú pot evitar que s'arribi a un consens, amb menys emmagatzematge de dades ja que només es guarda la transacció i menys despesa elèctrica (no hi ha prova de treball), ja que no és de codi obert sinó que és una xarxa privada. Per a més informació: CALLEJA, Carlos. *Hashgraph, la nueva Blockchain? Explicación y razonamientos*. https://steemit.com/hashgraph/@kallejo/hashgraph-la-nueva-blockchain-explicacion-y-razonamientos [Consultat: 16 abril 2019]

[65] GONZÁLEZ, Manuel. *Encriptación modulable, ¿la alternativa al "blockchain"?* https://retina.elpais.com/retina/2018/11/29/innovacion/1543493308_805539.html [Consultat: 15 abril 2019]

Tot això és possible, molt probablement, gràcies al fet que tots aquests nous projectes tenen **el suport econòmic de moltes entitats privades i fins i tot públiques**, i no d'una gran comunitat de participants els quals decideixen el futur. Sembla clar que el poder, sigui privat o públic, voldrà ser propietari i/o intermediari de la confiança dels participants d'aquella xarxa per a propòsits econòmics i/o de coneixements i control.

Per a una implementació a gran escala dels principis blockchain sobre la confiança i la necessitat d'augmentar la privacitat de les dades entre els participants, cal un gran **canvi en la mentalitat cultural** de la gent.

3. ETHEREUM

3.1. Definició dels Conceptes i Aspectes Clau

Ethereum és una plataforma, és a dir, una infraestructura informàtica, descentralitzada i distribuïda de codi obert que executa programes[66].

Ethereum utilitza l'Ether (ETH és la seva abreviatura) com a:

- **Criptomoneda** per a l'intercanvi de béns i comerç fora de la plataforma amb altres criptomonedes com Bitcoin o divises com ara el €.
- **Token** per cobrir les despeses que es generen en la mateixa plataforma i per a l'intercanvi amb altres tokens creats per finançar les aplicacions descentralitzades que es creen en la plataforma[67].

El principal objectiu de la plataforma, és proveir a qualsevol desenvolupador dels elements necessaris com ara eines i una infraestructura, per a poder crear organitzacions virtuals i aplicacions descentralitzades i per tant, no haver de crear la idea des de zero. Per altra banda, aquesta plataforma també fa la funció de facilitar l'emissió, distribució i intercanvi dels seus tokens per al finançament de projectes gràcies a l'estàndard ERC20 el qual estableix els requeriments i els límits per a qualsevol projecte.

La plataforma permet el desenvolupament de software basat en una xarxa peer-to-peer descentralitzada i distribuïda, la qual connecta els nodes de la xarxa a partir del protocol RLPx Transport. Hi ha diversos softwares que s'utilitzen com a node en cada un dels participants de la xarxa, els principals amb una quota del 50% i 40% de participants respectivament són, Geth i Parity[68].

Una de les principals innovacions, és que utilitza la tecnologia blockchain per connectar, sincronitzar, emmagatzemar i validar valor de forma **descentralitzada** i **distribuïda** entre tots els participants de la xarxa per generar la seva pròpia governabilitat gràcies al

[66] M. ANTONOPOULOS, Andreas. 2018. *Mastering Ethereum: Building smart contracts and dapps*. Editorial O'Reilly.
[67] Capitalització dels principals token creats en la plataforma Ethereum. Per a més informació: Etherscan Tokens Tracer. https://etherscan.io/tokens [Consultat: 1 maig 2019]
[68] El programari Geth està creat amb llenguatge de programació Go, mentre que el Parity está generat amb Rust.

consens. Actualment funciona sobre el concepte de prova de treball utilitzant l'algorisme Ethash i està previst en un futur canviar la prova de treball per a la prova de participació.

En la plataforma existeixen dos tipus de comptes: els **comptes controlats pels usuaris**, els quals utilitzen sovint una aplicació de cartera que és externa a la plataforma d'Ethereum, i els **contractes**. Aquests últims, també anomenats contractes intel·ligents o smart contracts, són programes de codi executats en la Màquina Virtual d'Ethereum (EVM). Qualsevol aplicació descentralitzada que es desenvolupa en Ethereum, interactua amb els contractes intel·ligents, ja que són aquests els que tenen la lògica que es vol utilitzar en l'aplicació.

Per últim, cal destacar l'existència del sistema Turing-complet amb el que es basa (EVM) la qual és exclusiva en comparació a la resta de projectes de l'ecosistema blockchain. Aquesta màquina virtual és l'entorn en el qual s'executen els arxius bytecode, que són comandaments generats a partir dels contractes intel·ligents compilats, que es creen amb llenguatge de programació Solidity, entre d'altres. Per altra banda, la plataforma s'utilitza com a interfície amb l'usuari per fer més gràfic i dinàmic el seguiment i execució de les aplicacions programades.

El paper en blanc d'Ethereum[69] – o més popularment conegut com a whitepaper – estableix que el disseny del protocol d'Ethereum, ha d'intentar seguir els següents principis:

1. **Simplicitat**: Ha de ser tan simple com pràctic, però haurà de mantenir un alt nivell de complexitat per permetre la seva escalabilitat, internalitzar costos d'emmagatzematge, per a la seguretat, privadesa i transparència de les dades i dels participants. Tot això, implica mantenir una documentació clara, concisa i actualitzada al dia a dia. Qualsevol optimització del protocol que afegeixi complexitat en els seus processos, no hauria de ser inclosa, a no ser que aquesta optimització proveeixi d'un gran benefici per als seus participants i la mateixa plataforma.
2. **Universalitat**: Ethereum pretén ser una gran plataforma on qualsevol programador trobi l'entorn i les eines necessàries per desenvolupar el seu projecte.

[69] BUTERIN, Vitalik. *Whitepaper of Ethereum*. https://github.com/ethereum/wiki/wiki/White-Paper [Consultat: 17 abril 2019]

Per això, proporciona un llenguatge de programació complet de Turing[70] perquè qualsevol programador l'utilitzi per pal·liar les seves necessitats.

3. **Modularitat**: Les parts del protocol d'Ethereum han d'estar dissenyades per ser el més modular i separades possibles, amb l'objectiu de tenir un programa on qualsevol projecte pugui adaptar les seves necessitats modificant una part del protocol sense perdre la funcionalitat de la resta.
4. **Agilitat**: Tot i tenir un full de ruta compartit i establert, poden haver-hi modificacions d'alt nivell en aquest o en les proves computacionals. Si es descobreixen formes de millorar o potenciar per exemple la seguretat o l'escalabilitat del protocol, es duran a terme.
5. **No discriminació i no censura**: El protocol no pot prohibir o restringir l'ús que se l'hi dóna a la plataforma. Tots els mecanismes de regulació del protocol han de ser dissenyats per regular directament els perjudicis i no intentar oposar-se a aplicacions no desitjades.

3.2. Diferències entre Bitcoin i Ethereum

A causa del gran desconeixement que hi ha sobre Bitcoin i Ethereum, actualment Ethernet està ple de falses i/o incorrectes comparacions i definicions sobre Ethereum i Bitcoin. És per això, que és necessari aclarir i especificar les principals diferencies entre ambdós projectes.

Primerament, Bitcoin és segons l'especialista en criptomonedes Saifedean Ammous, "u*n sistema que ofereix una xarxa de pagament amb la seva pròpia moneda autòctona, i que utilitza un sofisticat mètode perquè els membres puguin verificar totes les transaccions sense haver de confiar amb cap component de la xarxa*"[71].

En declaracions de Vitalik Buterin[72], "*Bitcoin és com una calculadora, la qual fa molt bé la seva funció, però Ethereum és un smartphone, ja que ofereix als usuaris i desenvolupadors un marc més ampli de possibilitats amb la seva plataforma*".

[70] SELLIN, Evin. *What exactly is Turing Completeness?* https://medium.com/@evinsellin/what-exactly-is-turing-completeness-a08cc36b26e2 [Consultat: 17 abril 2019]
[71] AMMOUS, Saifedean. 2017. El patrón Bitcoin: La alternativa descentralizada de los bancos centrales. Editorial DEUSTO.
[72] "Think of the difference between something like a pocket calculator and a smartphone, where a pocket calculator does one thing, and it does one thing well. But really, people want to do all these other things. And if you have a smartphone, then you have a pocket calculator as an app, you have a music player as an

Un cop posat en coneixement ambdues definicions, podem determinar que són dos conceptes diferents pel que fa a funcionalitats.

Un dels aspectes més diferents entre ambdós projectes, és que Ethereum està suportat per l'organització EEA, la qual manté ordre i estabilitat en el projecte, mentre que Bitcoin es basa en el consens de la seva comunitat, fet que ha provocat múltiples bifurcacions[73] per falta de consens.

Pel que fa a les semblances, podem observar que utilitzen la tecnologia blockchain com a via per a descentralitzar el poder i distribuir la xarxa peer-to-peer de participants, sincronitzar les actualitzacions d'estat de la cadena de blocs i principalment resol el problema dels generals bizantins. També tenen semblances en la utilització de primitives criptogràfiques com ara signatures digitals i hash, i una moneda digital.

Pel que fa als **aspectes més tècnics** respecte a les **cadenes de blocs** que utilitzen ambdós projectes, les principals diferències són:

- La mida màxima del bloc en Ethereum està limitat segons el límit del gas utilitzat a l'hora d'executar un bloc[74], mentre que en Bitcoin està "fixat"[75] a 1MB per bloc.
- El temps de generació de dos blocs, varia segons el hashrate de la xarxa i la dificultat que per tant s'estipula. En Bitcoin, la mitjana és d'entre 10-20 minuts, mentre que en Ethereum és de 10-30 segons.

app, you have a web browser as an app, and pretty much everything else." Business Insider. *Vitalik Buterin on creating one of the world's largest cryptocurrencies.* https://www.youtube.com/watch?time_continue=87&v=fi0ORZR4A88 [Consultat: 17 abril 2019]

[73] GONZÁLEZ, David. *Estado actual de los Hardforks Bitcoin.* https://steemit.com/bitcoin/@ydavgonzalez/estado-actual-de-los-hardforks-bitcoin [Consultat: 19 abril 2019]

[74] No al nombre de transaccions i/o aplicacions llançades perquè s'executin, sinó a la despesa en gas que generen quan s'ha de crear el bloc. Més endavant, s'explica més àmpliament el gas i les seves característiques.

[75] Bitcoin està compost per diferents versions. Per exemple, Legacy (els que mantenen original la blockchain) i Segwit (un softfork). Els nodes que implementen Legacy comprovaran que cap bloc superi 1MB, i rebutjaran els que ho facin, però quan les transaccions dels nodes SegWit que ocupen 2MB, s'envien als nodes Legacy, s'extrauen dades que no són necessàries per fer vàlides les dades pels nodes Legacy. Per tant, en la cadena de blocs de Bitcoin sortirà la mida real (2MB), mentre que els nodes Legacy només tindran en el bloc les dades necessàries en 1MB. I per tant, ambdues cadenes de blocs seran vàlides i mantindran la integritat que es requereix. Per a més informació: CANELLIS, David. *Here's why Bitcoin's blockchain as blocs that go over the 1MB límit.* https://thenextweb.com/hardfork/2018/07/12/bitcoin-block-size/ [Consultat: 20 abril 2019]

- Ether és una moneda inflacionària[76], és a dir, no hi ha límit en la seva creació mentre que en Bitcoin el límit està en 21 milions de monedes. En cas que Ethereum passi a implementar la prova de participació, Ether tindrà un límit de monedes igual que Bitcoin[77].
- El sistema de recompensa de Bitcoin, segueix el patró de reducció de la recompensa, ja que cada 4 anys hi ha una reducció del 50% de la recompensa al miner[78], mentre que Ethereum amb la reducció de la recompensa en l'etapa Metropolis[79], manté la recompensa en 2 Ether + les comissions (0,05 Ether aproximadament) que paguen els desenvolupadors per introduir aplicacions a la plataforma Ethereum.

Tot i que no es pot mesurar la quantitat exacta de participants i seguidors d'ambdues xarxes, el nombre de desenvolupadors en l'ecosistema blockchain ha augmentat, i actualment la comunitat de desenvolupadors d'Ethereum és superior a la de Bitcoin, segons es desprèn un estudi realitzat per ElectricCapital[80].

[76] Fins que no s'implementi la prova de participació, hi ha un límit de 18 milions d'Ether nous a l'any, la qual s'espera que al pas del temps i l'augment de la dificultat provoqui una xarxa més lenta amb blocs més grans i amb menor recompenses. Aquest fet permetrà crear un equilibri entre la creació de nous Ether i la pèrdua d'Ether existents (per ús incorrecte, pèrdua de claus, la mort de cadenes, etc.). Per a més informació: ETHEREUM. *Ethereum is a global, open-source platform for decentralized applications.* https://ethereum.org/ [Consultat: 20 abril 2019]

[77] Si s'implementa la prova de participació, la creació de nous Ether s'elimina (ja que no hi ha recompensa), i per tant, passa a convertir-se una moneda amb un màxim de monedes com Bitcoin.

[78] HOLMES, Jamie. *The Halving:What Bitcoin's Block Reward Milestone Means.* https://btcmanager.com/the-halving-what-bitcoins-block-reward-milestone-means/ [Consultat: 20 abril 2019]

[79] EIP 1234: Notificació d'ajustament de recompensa de blocs i reducció de la bomba de dificultat. SCHOEDON, Afri. *Constantinople Difficulty Bomb Delay and Block Reward Adjustment.* https://eips.ethereum.org/EIPS/eip-1234 [Consultat: 20 abril 2019]

[80] SHEN, Maria. *The Dev Report of ELECTRIC CAPITAL*. https://static1.squarespace.com/static/5c745b19c2ff6174b1290e42/t/5c805a3ae4966b1ce3a2a937/1551915603922/The+Dev+Report.pdf [Consultat: 20 abril 2019]

Respecte al hashrate[81], és a dir, la quantitat de potència que utilitzen els nodes de la xarxa per realitzar una operació, la xarxa Bitcoin manté un hashrate de 49.076EH mentre que els nodes de la xarxa d'Ethereum utilitzen 153.578TH[82] i [83].

Pel que fa a les diferències de minar, l'opció més recomanada per minar Bitcoin és la d'utilitzar maquinari ASIC, el qual supera en hashrate tant a les CPU com a les GPU[84]. Pel que fa a la xarxa Ethereum, l'algorisme de la prova de treball, ethash, va ser basat per ser resistent i difícil de minar amb hardware ASIC[85], ja que aquest maquinari permet emmagatzemar la cadena de blocs en el núvol i per tant, és vist com una força de centralització de la xarxa. Per tant, la millor forma de minar Ether és amb GPU, tot i que també es pot utilitzar la CPU (es va descobrir que amb GPU s'obté major hashrate amb la mateixa despesa energètica)[86]. Ambdues opcions emmagatzemen la cadena de blocs en memòria, ja que és un requisit indispensable d'ethash.

Respecte al sistema d'emmagatzematge de les transaccions, ambdós utilitzen blockchain, però en aquest cas, Bitcoin utilitza la versió original del Merkle Tree, mentre que Ethereum utilitza el Merkle Patricia Tree[87].

Per últim, destacar que Ethereum és més escalable en comparació a Bitcoin, la qual cosa permet una major i més amplia diversitat dels projectes que es duen a terme, i que actualment, ambdues cadenes de blocs utilitzen la prova de treball per validar i crear blocs.

---

[81] Gràfica del hashrate de Bitcoin i Ethereum. Per a més informació: BitinfoCharts. *Bitcoin, Ethereum Hashrate Chart.* https://bitinfocharts.com/comparison/hashrate-btc-eth.html [Calculat: 20 abril 2019]

[82] 1 ExaHash equival a 1.000.000.000.000.000.000 Hash per segon (quantitat total de solucions obtingudes per segon en la xarxa) i 1 TeraHash equival a 1.000.000.000.000 Hash per segon. Coinguides. *HashPower Calculator – Convert Hash to kH/s to MH/s to GH/s to TH/s to PH/s.* https://coinguides.org/hashpower-converter-calculator/ [Consultat: 20 abril 2019]

[83] Tot i que en les xarxes es diu que Bitcoin és més insostenible, cal recordar que ambdós sistemes utilitzen, de moment, la prova de treball, i per tant, l'única diferència és que Bitcoin en aquest cas, disposa de molta més potència de hashrate en comparació a Ethereum.

[84] TUWINER, Jordan. *ASIC i Rigs de programes de mineria Bictoin*. https://www.buybitcoinworldwide.com/es/mineria/hardware/ [Consultat: 21 abril 2019]

[85] MOOS, Mitchell. *Vitalik Buterin: Ethash ASICs Not a Threat to Ethereum*. https://cryptoslate.com/vitalik-buterin-ethash-asics-ethereum/ [Consultat: 21 abril 2019]

[86] GAMALERO, Martin. *Las mejores GPU para minar rentablemente*. https://criptotario.com/las-mejores-gpu-para-minar#Por_que_usar_las_GPU_para_minar_y_no_los_CPU [Consultat: 21 abril 2019]

[87] KIM, Kiyun. *Modified Merkle Particia Trie*. https://medium.com/codechain/modified-merkle-patricia-trie-how-ethereum-saves-a-state-e6d7555078dd [Consultat: 22 abril 2019]

3.3. Evolució i Desenvolupament

Totes les grans innovacions provenen de solucionar problemes, i Ethereum va sorgir per resoldre'n alguns de Bitcoin. La idea va sorgir del jove programador Vilatik Buterin, el qual va adonar-se'n que si es volia desenvolupar programes, s'havien de realitzar grans canvis a causa de les grans limitacions que tenia el protocol Bitcoin com ara la limitació de transaccions i la mida d'emmagatzematge de dades entre d'altres.

Al veure el potencial de la criptografia per al desenvolupament d'aplicacions descentralitzades, va realitzar una proposta per afegir els canvis necessaris per millorar l'escalabilitat de Bitcoin. Com que no va rebre una resposta dels participants de la comunitat Bitcoin, Buterin es va centrar a crear una plataforma, independent de l'ecosistema Bitcoin. Aquesta plataforma tenia la finalitat de permetre als programadors desenvolupar aplicacions descentralitzades. A finals del 2013, Buterin va publicar el whitepaper d'Ethereum[88].

La proposta va ser presentada al públic el gener de 2014[89], en el marc de la conferència "North American Bitcoin Conference" a Miami[90], on Vitalik Buterin va presentar la nova plataforma juntament amb Mihai Alisie, Anthony Di lorio i Charles Hoskinson.

En paraules del Dr. Gavin Wood, "*La idea de fer servir una cadena de blocs d'ús general com Ethereum, és que un desenvolupador pugui programar la seva aplicació particular sense haver d'implementar els mecanismes subjacents de xarxes peer-to-peer, blockchains, algorismes de consens, etc. Ethereum és dissenyada per resumir aquests detalls i proporcionar un entorn de programació determinista i segur per a aplicacions de blockchain descentralitzades*"[91].

[88] MiEthereum. *Vitalik Buterin – Vida del joven genio creador de Ethereum.* https://www.miethereum.com/vitalik-buterin/ [Consultat: 17 abril 2019]
[89] CAWREY, Daniel. *Miami Bitcoin Conference Day2: Litecoin, New Coins and Regulatory Risks.* https://www.coindesk.com/miami-bitcoin-conference-day-2-litecoin-regulation [Consultat: 17 abril 2019]
[90] Btcmiami. *The North American Bitcoin Conference*. https://btcmiami.com/ [Consultat: 16 abril 2019]
[91] Ethereum.org. *DEVCON1: Ethereum for Dummies – Dr. Gavin Wood* https://www.youtube.com/watch?v=U_LK0t_qaPo [Consultat: 17 abril 2019]

Per al desenvolupament d'Ethereum, es va planejar un full de ruta separant les grans modificacions en 4 etapes diferents[92]. Tot seguit, es presentaran les modificacions realitzades seguint l'ordre cronològic dels esdeveniments en relació al bloc minat.

3.3.1. Fase Frontier

La primera etapa va des de la creació del primer bloc el 30 de juliol del 2015[93] fins al llançament al públic d'Ethereum el març del 2016, bloc número #1.149.999. Durant aquesta primera etapa, els programadors van començar a escriure contractes intel·ligents i a desenvolupar aplicacions descentralitzades per implementar en la xarxa Ethereum. També va ser una època on nous miners van començar a unir-se a la xarxa per ajudar en el procés de validació dels blocs, tot i que fins aleshores, era una xarxa privada i per tant era necessari el consentiment de la xarxa per accedir-hi.

Durant aquesta primera etapa, es va realitzar un hardfork en el bloc #200.000 anomenat Ice Age[94]. Aquesta modificació va permetre introduir la bomba de dificultat, la qual augmenta la dificultat a mesura que avança el temps[95]. L'objectiu d'aquesta modificació, és incentivar i pressionar als nodes de la xarxa a canviar quan sigui possible la prova de validació de blocs en la xarxa. Per altra banda, va ser una etapa de millores en seguretat de la cadena de blocs i de resoldre defectes de codi.

3.3.2. Fase Homestead

La segona etapa, va començar el 14 de març del 2016, quan es va dur a terme el primer llançament estable en la història d'Ethereum. Aquesta actualització de la xarxa va significar que la xarxa era classificada per als desenvolupadors com a "segura".

En aquesta etapa, la xarxa va patir en el bloc #1.192.000 un succés inesperat, el **The DAO**[96]. La presentació de la ICO més gran en la història de l'ecosistema blockchain, l'aplicació Decentralized Anonymous Organizations va recaptar 150 milions de dòlars.

---

[92] Coinmama. *History of Ethereum*. https://www.coinmama.com/guide/history-of-ethereum [Consultat: 16 abril 2019]
[93] Ethereum block 0 info. https://etherscan.io/block/0 [Consultat: 17 abril 2019]
[94] MADEIRA, Antonio. *What is the Ethereum Ice Age?* https://www.cryptocompare.com/coins/guides/what-is-the-ethereum-ice-age/ [Consultat: 18 abril 2019]
[95] Exemple del funcionament de la modificació implementada amb el hardfork Ice Age: JENTZSCH, Christoph. *New difficult algorithm.* https://gist.github.com/CJentzsch/c78768f9837afb8eef74 [Consultat: 18 abril 2019]
[96] En aquest cas, l'aplicació pretenia compartir béns com ara cotxes, apartaments (una versió basada en la tecnologia d'Airbnb). Per a més informació: THOMPSON, Collin. *The DAO of Ethereum.* https://medium.com/blockchain-review/the-dao-of-ethereum-e228b93afc79 [Consultat: 17 abril 2019]

Tot i això, es va detectar un defecte en el codi i va ser atacada posteriorment[97]. A l'hora de buscar una solució, una part de la xarxa Ethereum volia implementar un hardfork per retornar els diners als inversors de la DAO. Aquest fet va **dividir** a la comunitat, ja que va sorgir una nova cadena de blocs anomenada **Ethereum Classic**, per mantenir el principi d'immutabilitat dels registres , i la xarxa original d'**Ethereum**, la qual va tornar enrere en la cadena per eliminar el bloc on s'havia executat el robatori per tal de retornar els diners sostrets.

A part de la bifurcació de la cadena, seguint amb Ethereum, es van dur a terme dos hardforks aprovats per la majoria de la xarxa. El primer en el bloc #2.463.000 anomenat Tangerine Whistleen[98], i el segon en el bloc #2.675.000, anomenat Spurious Dragon[99]. Ambdós hardforks, van anar dirigits a augmentar la **protecció de la xarxa** davant els atacs de denegació de serveis (DoS) que patia de forma constant la xarxa.

Cal mencionar, que durant els principis del 2017, es va crear l'**Enterprise Ethereum Alliance** (EEA)[100], amb l'objectiu de servir de fòrum i de connexió amb grans empreses perquè aquestes entenguin i utilitzin la tecnologia Ethereum. S'espera que aquesta organització permeti l'entrada de milers de desenvolupadors que aprenguin Solidity, creïn estàndards, millorin la documentació d'Ethereum i despleguin recursos en l'ecosistema Ethereum.

3.3.3. Fase Metropolis

Aquesta és la tercera etapa en la qual es trobava immersa la xarxa Ethereum fins a l'actualització i modificació del full de ruta que s'ha fet aquest inici d'any, i estava separada inicialment en dues fases: Byzantium i Constantinople.

---

[97] Aquest defecte, tenia un error de "trucada recursiva" que permetia als usuaris del contracte intel·ligent retirar el doble d'Ether que havien invertit en el contracte. Tot i la declaració pública de la comunitat DAO assegurant que l'aplicació estava fora de perill, el juny del 2016 va ser atacada. L'atacant va explotar la vulnerabilitat i va retirar 50 milions de dòlars en Ether del contracte intel·ligent (aproximadament el 15% de tots els Ether en aquell moment) i els va drenar en un fill DAO sota el seu control. Posteriorment, la comunitat DAO va afirmar que l'atac era legal basant-se en el fet que els contractes intel·ligents s'autoaplicaven i eren autosuficients, i que per tant, no hi havia forma de recuperar els ether perduts. SIEGEL, David. *Understanding The DAO Attack.* https://www.coindesk.com/understanding-dao-hack-journalists [Consultat: 18 abril 2019]

[98] Notificació del hardfork Tangerine Whistleen. JAMESON, Hudson. *Upcoming Ethereum Hard Fork.* https://blog.ethereum.org/2016/10/18/faq-upcoming-ethereum-hard-fork/ [Consultat: 17 abril 2019]

[99] Notificació del hardfork Spurious Dragon. JAMESON, Hudson. *Hard Fork no.4: Spurious Dragon.* https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/ [Consultat: 17 abril 2019]

[100] Pàgina principal de l'organització. Enterprise Ethereum Alliance. https://entethalliance.org/ [Consultat: 16 abril 2019]

La fase Byzantium va ser implementada en el bloc #4.370.000 per augmentar la privacitat de la blockchain i afegir millores d'algunes funcions[101]. La fase es va centrar en la introducció de ZK-SNARKs, **retardar** la **bomba de dificultat** implementada durant l'etapa Frontier, introduir un **camp sobre l'estat** dels rebuts de les transaccions[102] i **modificacions** del funcionament dels **contractes intel·ligents** com ara la simplificació del llenguatge Solidity per promoure la seva utilització.

La segona fase, s'havia d'implementar durant l'any 2018, però després de diversos intents fallits, es va ajornar el llançament[103] i es va dividir el hardfork en dues noves modificacions, Constantinople i St. Petersburg[104]. Tot i que en el full de ruta s'havien especificat unes modificacions, algunes d'aquestes s'han ajornat i s'han afegit de noves per resoldre diversos errors trobats.

Principalment, Constantinople havia d'implementar tres hardforks de forma separada: Casper, un model híbrid entre la prova de treball i la prova de participació amb dipòsit de 1.000 ETH per participar, Abstraction, per augmentar el codi abstracte d'Ethereum per permetre als desenvolupadors prendre decisions específiques segons les necessitats de cada cas i Sharding, un conjunt de millores en escalabilitat[105].

Finalment, el 22 de febrer del 2019, en el bloc #7.280.000 es van implementar el nou Constantinople modificat i St. Petersburg. L'actualització d'aquests, va incloure entre d'altres[106], **millores de seguretat i escalabilitat** en els canals de pagament, un **nou retard**

[101] ETHEREUM TEAM. *Byzantium HF Announcement.* https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/ [Consultat: 17 abril 2019]
[102] Permet als clients verificar que una transacció ha estat satisfactòria sense la necessitat d'executar el codi. Si el valor del camp és 1 significa que la transacció no falla, i 0 si falla. EDGINGTON, Ben. *What is the exact meaning of a transaction's new receipt status field?* https://ethereum.stackexchange.com/questions/28889/what-is-the-exact-meaning-of-a-transactions-new-receipt-status-field?rq=1 [Consultat: 18 abril 2019]
[103] JAMESON, Hudson. *Security Alert: Ethereum Constantinople Postponement.* https://blog.ethereum.org/2019/01/15/security-alert-ethereum-constantinople-postponement/ [Consultat: 18 abril 2019]
[104] JAMESON, Hudson. *Ethereum Constantinople/St. Petersburg Upgrade Announcement.* https://blog.ethereum.org/2019/02/22/ethereum-constantinople-st-petersburg-upgrade-announcement/ [Consultat: 18 abril 2019]
[105] M. ANTONOPOULOS, Andreas. 2018. Mastering Ethereum: Building smart contracts and dapps. Editorial O'Reilly.
[106] FARIDI, Omar. *Everything You Need to Know for Ethereum's Hard Forks: Constantinople, St. Petersburg.* https://www.cryptoglobe.com/latest/2019/02/everything-you-need-to-know-for-ethereum-s-upcoming-constantinople-st-petersburg-upgrade/ [Consultat: 19 abril 2019]

en la bomba de dificultat, la **reducció de la recompensa fixa** a 2 ETH i la recompensa oncle en conseqüència i la **reducció de les despeses** de les transaccions.

3.3.4. Fase Ethereum 2.0

Amb el nou full de ruta[107], els objectius no han variat molt, i se centraran en Sharding, Casper i eWasm. Amb la combinació d'aquestes modificacions, s'espera que es resolgui el famós Trilema blockchain[108].

A falta de dates oficials, la implementació de Casper es farà durant el 2019-2021, i en comptes d'exigir un dipòsit de 1000 Ether per participar en la prova de validació com estava dictaminat inicialment, a partir d'ara, només es necessitaran 32 Ether, fet que permetrà augmentar la descentralització de la xarxa. Al mateix moment, i amb major prioritat per als desenvolupadors, s'implementarà Sharding.

3.4. La Moneda Ether i la Unitat Gas

La plataforma utilitza la moneda Ether, la qual com ja s'ha explicat anteriorment, servia originalment com a token per impulsar aplicacions en la plataforma i actualment com a criptomoneda per a l'intercanvi de béns i comerç entre altres criptomonedes. Tots els clients de la plataforma la utilitzen per realitzar pagaments a altres persones o a màquines per executar les operacions sol·licitades. En altres paraules, és l'incentiu que assegura que els desenvolupadors construeixen aplicacions de qualitat (com major pes té un projecte, més car és distribuir-lo per la xarxa de participants).

L'oferta inicial d'Ether es va decidir prèviament, en el moment de la venda el 2014 amb les següents dades:

- 60 milions d'Ether creats per als contribuents de la venda.

[107] GALVEZ, Johana. *Cambios en la hoja de ruta de Ethereum: ¿cuándo esperar los lanzamientos de Casper y Sharding?* https://ava.markets/forex/cambios-en-la-hoja-de-ruta-de-ethereum-cuando-esperar-los-lanzamientos-de-casper-y-sharding/ [Consultat: 18 abril 2019]

[108] Fins ara, s'ha demostrat que tecnològicament és impossible maximitzar simultàniament les tres característiques d'una blockchain. El problema inherent és que en augmentar la qualitat de qualsevol element, cal renunciar a alguns dels avantatges dels altres dos aspectes. OMETORUWA, Toju. *Solving the Blockchain Trilema: Decentralitzation, Security & Scalability.* https://www.coinbureau.com/analysis/solving-blockchain-trilemma/ [Consultat: 19 abril 2019]

- 12 milions d'Ether creats per als desenvolupadors, primers contribuents i la resta a la Fundació Ethereum[109].
- La recompensa per crear un bloc era de 5 Ether (cada 15 segons de mitjana) com a incentiu per als miners. Actualment la recompensa s'ha reduït a 2 Ether + una part de la comissió que paga tot desenvolupador que vol introduir el seu contracte o aplicació en un bloc perquè aquest quedi registrat en la cadena de blocs.
- La recompensa per crear un bloc orfe[110], és a dir, un bloc que finalment no és afegit a la cadena de blocs, era de 2-3 Ether depenen de les despeses generades. Actualment la recompensa s'ha reduït a màxim 1 Ether.

Per altra banda, l'emissió d'Ether està limitada a 18 milions per any (un 25% de l'oferta inicial), i s'utilitzen com a incentiu per als miners que creen blocs.

Amb la implementació de la prova de participació, el sistema de recompenses serà eliminat i es promourà un sistema de dipòsit on l'usuari que diposita Ether per poder participar en el procés de creació de blocs obté un rendiment gràcies a les comissions que paguen els desenvolupadors per introduir contractes i altres dades en la cadena de blocs.

Totes les transaccions que s'executen a l'EVM estan codificats mitjançant Solidity, on cada línia de codi d'aquest llenguatge, requereix una certa quantitat de gas per ser executat.

Taula 2: Comparació de subunitats d'Ether i Gas

1 Unitat	Unitats de Gas
Wei	0,000000001
Kwei	0,000001
Mwei	0,001
Gwei	1
Szabo	1.000
Finney	1.000.000
Ether	1.000.000.000

Font: Elaboració pròpia

Amb la finalitat d'evitar bucles infinits accidentals, hostils, o malbaratament computacional a causa del codi, Ethereum utilitza el Gas[111] per calcular el cost d'executar una transacció, és a dir, és la unitat que mesura la quantitat d'esforç computacional que es necessitarà per executar determinades operacions.

[109] CASTOR, Amy. *The Ethereum ICO: Where did all the tokens go?* https://www.theblockcrypto.com/2018/12/18/the-ethereum-ico-where-did-all-the-tokens-go/ [Consultat: 17 abril 2019]
[110] Sorgeix a causa del Problema dels Generals Bizantins
[111] El preu mitjà de gas és normalment 20 Gwei (0.00000002 ETH), però pot créixer en moments on hi ha una gran quantitat de transaccions a executar. MiEthereum. ETH Gas Station. https://www.ethgasstation.info/ [Consultat: 21 abril 2019]

Aquesta unitat s'utilitza per compensar la despesa de temps, infraestructura i energia dels nodes a l'hora de validar les transaccions.

Cada unitat de Gas, està mesurada en 1 Gwei.

Tot desenvolupador introdueix un gasprice i un gaslimit en cada transacció. Aquesta última mesura s'utilitza com a mecanisme de seguretat, ja que impedeix que tots els Ether d'un desenvolupador siguin consumits a causa d'un error del codi de la transacció o d'estimació. Si l'execució d'una transacció supera el gaslimit, el desenvolupador només perdrà el que hagi marcat com a màxim, i aquella transacció no serà finalment validada i tornarà a la llista d'espera[112].

Com més elevat sigui el gasprice que un desenvolupador paga de gas, més probabilitats tindrà de què més miners vulguin seleccionar la transacció per incorporar-la en el següent bloc, ja que contindrà una major comissió. Una de les normes del protocol, és que el preu mínim d'una unitat de Gas, és d'1 Gwei, que vindria a ser 1.000.000.000 de Wei.

Per altra banda, la xarxa de participants dictamina un gaslimit pels blocs, així que cap bloc pot superar aquest límit. Per tant, una transacció amb un gaslimit molt elevat, és possible que no s'executi, ja que un gaslimit molt elevat no implica que tot aquest sigui consumit.

3.5. Aplicacions Descentralitzades

Una de les principals innovacions que presenta la plataforma Ethereum juntament amb la tecnologia Blockchain, és la implementació d'aplicacions descentralitzades.

Una **aplicació descentralitzada** que s'implementa en una cadena de blocs, permet als usuaris relacionar-se entre ells i tancar acords. Aquest tipus d'aplicacions, permeten eliminar l'intermediari central, el qual gestiona el servei com és el cas de Facebook, on qualsevol missatge que s'envia per aquesta famosa aplicació, passa pels servidors centrals de la companyia abans d'arribar al seu destinatari.

[112] SALDANHA, Lucas. *Ethereum Explained: Gas, Payment and Mining*. http://pegasys.tech/ethereum-explained-gas-payment-and-mining/ [Consultat: 21 abril 2019]

L'únic intermediari que interactua en una aplicació descentralitzada són els nodes, els quals, verifiquen la integritat i veracitat del missatge seguint les normes establertes i acceptades per tota la comunitat de la xarxa.

Tota aplicació que vulgui ser classificada com a descentralitzada en un entorn d'una cadena de blocs, ha de seguir els següents requeriments[113]:

- L'aplicació ha de ser de codi obert, funcionar de forma autònoma i sense que cap entitat controli la majoria dels nodes.
- Les dades de l'aplicació i els registres de transaccions s'han d'emmagatzemar utilitzant la criptografia en una cadena de blocs descentralitzada i distribuïda.
- L'aplicació requereix un token o actiu digital per accedir a l'aplicació i recompensar amb incentius per les aportacions de valor.
- L'aplicació ha de generar tokens d'acord amb l'algorisme d'estàndard criptogràfic que actua com a prova de concepte per als nodes que validen i descentralitzen la xarxa.

En la plataforma Ethereum, podem trobar diferents tipus d'iniciatives d'aplicacions descentralitzades, des d'aplicacions de serveis de missatgeria i transferències de divises com e-chat[114] fins a La'Zooz[115], una alternativa descentralitzada de l'empresa Uber, la qual es basa en l'economia col·laborativa però amb un sistema centralitzat.

Així i tot, la iniciativa amb major potencial i probabilitat d'impacte tant econòmic com social, és la de connectar les aplicacions amb dispositius IoT, la qual cosa permetria que qualsevol aplicació que estigués incorporada en la plataforma d'Ethereum, pogués interactuar amb dades i/o aplicacions que s'han generat de forma externa a la plataforma. Tot i que ja han sorgit alguns projectes, com ara Elk[116], la qual és una iniciativa que està creant un xip que permet connectar aplicacions d'Ethereum amb l'exterior, la interacció i transmissió d'informació amb entorns externs, encara és limitada.

[113] What is a DApp? https://hackernoon.com/what-are-decentralized-applications-dapps-3b63b4d587fe/ [Consultat: 1 maig 2019]
[114] Primer servei de missatgeria descentralitzat i anònim. eChat. *Blockchain-based decentralized secure messenger and fastest-growing social network.* https://echat.io/ [Consultat: 1 maig 2019]
[115] Lazooz. *A value system designed for sustainability*. http://lazooz.org/ [Consultat: 27 abril 2019]
[116] Elk. *Start building blockchain-connected devices*. https://elk.cc/ [Consultat: 9 maig 2019]

Les aplicacions descentralitzades que s'implementen en Ethereum interactuen amb un conjunt de contractes intel·ligents. Aquests, porten la lògica de l'aplicació i s'executen de forma automàtica, eliminant qualsevol intermediari de l'equació, i fent que tota acció que es dugui a terme en l'aplicació provingui de la lògica dels contractes. Aquesta funció permet eliminar la possibilitat de qualsevol error humà o falta d'acord posterior, entre les parts participants en qualsevol acció de l'aplicació o d'una transacció.

És per això, que podem considerar que una aplicació descentralitzada està formada per, un conjunt de contractes intel·ligents els quals executen la lògica de les funcions de l'aplicació, un Front-End que actua com a interfície amb l'usuari, i un Back-End el qual s'encarrega de l'estructura general i la base de dades de l'aplicació, entre d'altres.

3.6. Contractes Intel·ligents

La primera vegada que es va utilitzar la terminologia de contracte intel·ligent, va ser en els anys 90, quan el criptògraf Nick Szabo els va descriure com "*un conjunt de promeses, especificades en format digital, inclosos els protocols en què les parts realitzen les altres promeses*".

Des d'aleshores, han sorgit una gran diversitat de definicions i d'opinions respecte als contractes intel·ligents. Com ara, l'expert en llei DAVID M. ALDERSTEIN, el qual els defineix com "*un acord consensuat entre almenys dos partits per obtenir un resultat comercial independent i automatitzat de la satisfacció o la no satisfacció, determinada objectivament a través del codi, d'una condició factual específica*"[117].

Altres autors com TUR FAÚNDEZ, defineixen els contractes intel·ligents com "*seqüències d'instruccions o indicacions destinades a ser utilitzades, directament o indirectament, en un sistema informàtic per realitzar una o diverses prestacions d'un contracte (per tant, programes d'ordinador), amb la particularitat de què, un cop activats, els actors en la firma del contracte deixen de tenir el control sobre el compliment, ja que es realitzarà per si mateix*"[118].

Totes les definicions tenen un aspecte en comú, cap d'elles esmenta la capacitat d'intel·ligència dels contractes, ja que com indica l'expert en matèria de dret Eduardo

[117] ADLERSTEIN, David M. *Are Smart contracts Smart?* https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract [Consultat: 23 abril 2019]
[118] TUR FÁUNDEZ, Carlos. 2018. Smart Contracts: Análisis jurídico. Reus Editorial.

García, els contractes intel·ligents no són intel·ligents perquè simplement són execucions automàtiques de codi prèviament establertes. L'únic moment en què podríem anomenar els contractes com a intel·ligents, seria en el moment en els que els contractes permetessin per si mateixos a partir de tècniques d'aprenentatge automàtic, millorar el seu codi i la seva execució segons les necessitats que es donessin a terme. Per altra banda, García també indica que no són exactament contractes legals, ja que abans de l'execució del contracte, hi ha un acord formal entre les parts participants[119].

Després d'analitzar les definicions presentades anteriorment, podem arribar a la conclusió de que els contractes intel·ligents són peces de codi que viuen en la cadena de blocs els quals executen ordres a partir d'una lògica compartida. Aquests, poden llegir i/o executar altres contractes, emmagatzemar dades d'una aplicació, prendre decisions a partir de la lògica del codi i funcionar com a compte de signatura múltiple[120].

Per altra banda, els contractes existiran i funcionaran sempre que la xarxa es mantingui activa. Només es pararan en cas que es quedin sense finançament transaccional o si en la lògica del codi estava programada l'opció d'autodestrucció en cas de complir certs criteris preestablerts.

La implementació de contractes intel·ligents permetrà reduir despeses legals, comissions i sobretot, els temps d'espera d'execució des del moment en què succeeix una acció fins al moment que s'executa la resposta a aquesta acció.

Com a aspecte curiós dels contractes intel·ligents, les funcions aleatòries, anomenades en anglès com a random, les quals generen nombres de forma aleatòria, no es poden utilitzar en els contractes intel·ligents perquè els nodes no poden verificar el seu origen.

3.7. Avantatges Ethereum

Gràcies al lideratge de l'organització anomenada Entrerprise Ethereum Alliance, liderada pel jove fundador Vitalik, ha aconseguit mantenir un **procés de desenvolupament molt ambiciós i organitzat** complint amb la majoria dels objectius establerts inicialment, els

[119] KEWLEY, Jonathan. *Smart Contracts - Legal Agreements for the Digital Age*. https://www.cliffordchance.com/briefings/2017/06/smart_contracts_-legalagreementsforth.html [Consultat: 26 abril 2019]

[120] Els fons d'aquest tipus de comptes només es gastaran quan un percentatge necessari de persones està d'acord. Per a més informació: HERTIG, Alyssa. *How do Ethereum Smart Contracts Work?* https://www.coindesk.com/information/ethereum-smart-contracts-work [Consultat: 28 abril 2019]

quals han permès potenciar i innovar la plataforma mantenint el suport de la xarxa en tot moment, amb la idea de desenvolupar aplicacions per descentralitzar el poder. Tot això, ha permès implementar **noves millores i actualitzacions** que no existien en els inicis del projecte, les quals no s'haurien pogut implementar sense una bona direcció la qual tingués el consens.

La **singularitat de la plataforma** en l'entorn de les criptomonedes i de la tecnologia blockchain, ha permès a Ethereum sorgir com a **base per a qualsevol classe de projecte**, creant una xarxa de centenars de projectes únics els quals molt probablement no tindrien ni finançament ni suport fora de la xarxa.

Com que tots els projectes creats fins ara s'han adherit a l'estàndard ERC-20, la xarxa gaudeix d'una **gran escalabilitat**, **estabilitat**, **diversitat** i **interacció entre projectes**. Aquest fet ha provocat una gran quantitat de diferents tokens i ha acabat reforçant el valor de la xarxa Ethereum com a un conjunt.

Gràcies al fet que Ethereum actua com a plataforma, ha permès la creació, el finançament i el posterior desenvolupament d'una **àmplia gamma d'aplicacions** les quals permeten descentralitzar el control i recuperar la privacitat de les dades. En conseqüència, ha estat possible agrupar una gran comunitat d'usuaris i desenvolupadors amb el propòsit de lluitar per defensar els drets dels ciutadans. Tot això, ha provocat que sigui la **comunitat més gran de programadors** en comparació a qualsevol altre projecte de l'entorn de les criptomonedes, inclòs al projecte de Bitcoin.

Tanmateix, la implementació dels contractes pot permetre, de cara a un futur no molt llunyà, **l'automatització de processos** que no aporten un gran valor afegit en les companyies, eliminant la possibilitat d'errors humans, la falta d'integritat de les dades i reduint despeses fins ara necessàries. La seva implementació, també permetrà **reduir els temps d'espera** en l'execució de les condicions d'un contracte, i **augmentar la flexibilitat** d'aquests en comparació als contractes legals actuals.

3.8. Inconvenients Ethereum

Tot i el gran potencial que té el projecte d'Ethereum, des de la seva creació han sorgit diversos inconvenients que han provocat canvis irreversibles en els principis i en els objectius per als quals es va crear aquesta idea.

Ethereum ha demostrat que **no és capaç de mantenir els principis intactes**, com el de la **immutabilitat dels registres** de la cadena de blocs, ja que durant el robatori conegut com The DAO, es va decidir retrocedir els registres per tal de recuperar els Ether robats eliminant les transaccions que havien fet els lladres durant el robatori. Tot això, està directament relacionat al fet que hi ha una **organització** (EEA) la qual té molt poder en la comunitat i que en gran mesura, **marca les pautes** de desenvolupament de la plataforma.

Pel que fa als contractes intel·ligents, ha quedat demostrat que només són tan segurs com ho és la qualitat del seu codi. Els canvis constants que es fan per pal·liar la **falta de programadors** amb coneixement suficient per desenvolupar amb el llenguatge Solidity, provoca que sigui **vital mantenir-se actiu** en la xarxa per estar al dia dels canvis. L'efecte d'aquesta innovació ha provocat que alguns contractes no s'implementin amb les noves millores, i això ha causat en alguns casos, la **baixa qualitat del codi**. Un altre aspecte negatiu dels contractes, és que de moment no és possible connectar-los amb esdeveniments i/o recursos externs de l'entorn d'Ethereum.

La gran evolució que està tenint la plataforma, ha provocat l'entrada de **nous usuaris desconeguts** amb **intencions malicioses** en les comunitats de desenvolupadors. Com que són els mateixos usuaris de forma individual, que acaben penjant millores i solucions a Internet dels problemes que van sorgint en les comunitats, succeeixen casos d'infeccions de programes maliciosos en nodes o robatoris de dades, a causa d'usuaris que han confiat i s'han baixat arxius contaminats.

Per últim, cal destacar la **gran volatilitat** que va impactar de forma molt negativa en tots els projectes de l'ecosistema de les criptomonedes, i en especial el d'Ethereum. El valor de l'Ether, va passar a ser la segona criptomoneda amb major capitalització en el mercat de les criptomonedes durant l'any 2017, augmentant més d'un 10.000% el seu valor, per després perdre els màxims dels 1.389 $ als 176 $ actuals, és a dir, una pèrdua del 87,7% del valor respecte al valor màxim obtingut el 15 de gener del 2017[121].

[121] Ethereum (ETH) price, charts, market cap and other metrics. https://coinmarketcap.com/currencies/ethereum/ [Consultat: 10 maig 2019]

4. APLICACIÓ PRÀCTICA D'UN SMART CONTRACT AMB ETHEREUM

4.1. Les Donacions a ONG's

Per tal de demostrar els coneixements obtinguts al llarg del projecte, i d'il·lustrar l'aplicació pràctica d'un contracte intel·ligent, s'aplicarà a un cas hipotètic concret: les donacions a ONG's.

Els objectius que es busquen assolir, són:

- Entendre tot el procés de creació i interacció amb el contracte.
- Identificar els principals avantatges i inconvenients d'implementar contractes intel·ligents.
- Identificar els principals problemes que sorgeixen de la gestió de les donacions.
- Fer més eficient el procés de donacions.
- Conèixer l'estat actual de maduresa del llenguatge Solidity.

1. *Qué pot aportar la implementació de contractes intel·ligents en les donacions a ONG's?*

Tal com destaca l'equip de tasques de finançament humanitari del Comitè permanent interinstitucional (IASC) en l'informe[122], la implementació dels contractes permetria reduir les gestions administratives, crear transparència en els ingressos i despeses, i eliminar les manipulacions polítiques dels Estats i grans corporacions a les quals estan sotmeses.

[122] "*Algunes de les restriccions identificades per l'estudi incloïen:* ***la programació inflexible dels pagaments en múltiples trams****;* ***retards en els pagaments****;* ***el requisit de retornar els saldos no gastats****;* ***finestres d'elegibilitat de despeses molt curtes****, especialment per als excedents pressupostaris assignats al final dels anys fiscals del donant; i una flexibilitat limitada per negociar extensions sense cap cost o redistribució de fons per adaptar-se a requisits humanitaris i circumstàncies operatives modificades."* Inter-Agency Standing Committee (IASC) Humanitarian Financing Task Team. Donor conditions and their implications for Humanitarian response. Article online: https://interagencystandingcommittee.org/system/files/20160416_donor_conditions_study_final_0.pdf [Consultat: 4 maig 2019]

2. *Però realment, quins són aquests beneficis?*

- Realitzar *n* donacions.
- Reduir el retard de la donació en arribar al fons de l'ONG[123].
- Reduir despeses generades de la gestió i administració d'aquestes organitzacions.
- Reduir les comissions de transferències internacionals en donacions.
- Permetre que cada individu pugui cancel·lar el contracte en qualsevol moment.
- Eliminar el poder burocràtic dels estats envers les ONG's com ara permisos i concessions

3. *Com es podrien implementar els contractes intel·ligents?*

Una opció seria la de crear una aplicació descentralitzada, en la plataforma d'Ethereum, la qual actués de plataforma perquè els usuaris poguessin realitzar donacions a les organitzacions que volguessin. Aquestes donacions es durien a terme a partir de la implementació dels contractes intel·ligents, els quals contenen la lògica del procés.

L'altra opció, la qual serà la que es durà a terme en aquest projecte, és la d'implementar el contracte mitjançant l'extensió a Firefox de Metamask[124] i el navegador Remix[125], per tal de crear, testar i interactuar amb el codi del contracte i connectar-nos amb les adreces de la xarxa d'Ethereum.

4. *Quins beneficis podria aportar per a qualsevol donant d'una ONG?*

- Enviar diners ràpidament.
- Veure el balanç de l'adreça.
- Traçabilitat de moviments.
- Total transparència per veure l'estat real dels comptes.
- Acabar de forma ràpida la relació.

5. *Com funcionaria el contracte?*

[123] Les transferències internacionals fora de SEPA, poden arribar a tardar entre 2 a 5 dies i generen altes comissions a l'hora de realitzar la transferència. Transferwise Team. *Transferencias internacionales con BBVA: Tarifas y Comisiones*. https://transferwise.com/es/blog/transferencia-internacional-bbva [Consultat: 17 maig 2019]
[124] Extensió dels navegadors d'Internet que permet crear i tenir accés a adreces i monedes de diferents cadenes de blocs. METAMASK. https://metamask.io/ [Consultat: 10 abril 2019]
[125] Remix Ethereum. https://remix.ethereum.org/ [Consultat: 7 abril 2019]

El contracte té l'adreça del receptor (ONG) fixa, per tant, qualsevol donant que vulgui enviar diners a l'ONG, només haurà de connectar la seva adreça amb la plataforma, per tal de tenir una adreça des d'on obtenir fons per a la transferència.

4.2. Procediment

És per tant, que per crear, testejar i poder desplegar el contracte en la blockchain d'Ethereum, s'utilitzarà Remix, el qual és un IDE pensat per crear i provar codi des del navegador d'Internet. Aquest navegador, permet editar codi font, eines d'automatització, depurar codi i desplegar contractes en blockchain a partir de l'extensió de Metamask.

L'objectiu d'utilitzar el navegador Remix, és el de comprovar línia per línia que no hi ha errors en el codi i en les execucions de les funcions i que permet infinits intents. Així i tot, només s'utiltiza per a crear codis simples, ja que a partir de certa complexitat del codi, el navegador comença a donar problemes de velocitat d'execució.

Un dels aspectes més importants d'aquest navegador, és que permet desplegar contractes tant en cadenes de blocs privades com públiques com ara la mateixa Ethereum.

4.3. Creació del Contracte

Com ja s'ha esmentat prèviament, el llenguatge de programació que s'utilitza per crear els contractes intel·ligents és Solidity. A continuació, es presenta el programa el qual és un arxiu en format .json[126], que conté el codi del contracte intel·ligent a implementar:

```
pragma solidity ^0.5.1;

contract EnviarEther {

address payable public addr = 0x453432A3C2e1B3B7Dd578EFDcbeaa2D9B12cC6Fb;
bool valid = false;

    constructor ( ) payable public{
    }

    function enviarEther( ) public payable {
    require(msg.value <= 0.1 ether);
    addr.transfer(msg.value);
    valid = true;
    }

    function veureEstatAddr( ) public view returns (uint256) {
```

[126] (Acrónim de JavaScript Object Notation): És un format de fitxer estàndard obert que utilitza text llegible per a humans per transmetre objectes de dades. Per més informació: Wikipedia. https://en.wikipedia.org/wiki/JSON [Consultat: 16 maig 2019]

```
    return address(addr).balance;
    }

    function eliminarDades ( ) public{
    require(valid!=false);
    selfdestruct(addr);
    }
}
```

Per a una millor comprensió del significat de cada una de les parts del codi presentat anteriorment, a continuació es dóna una explicació de cada una de les funcions i paraules clau que s'utilitzen.

Primerament, cal destacar que les paraules de color blau[127], són **paraules clau reservades** en el protocol del llenguatge de programació Solidity, les quals tenen una funció específica i una definició ja establerta en el protocol del llenguatge. Aquest fet, permet als desenvolupadors poder escriure codi de forma més ràpida, neta i senzilla, evitant així haver d'escriure centenars de línies de codi per a simples declaracions.

- *pragma solidity ^0.5.1;* És la declaració de la versió del compilador del llenguatge Solidity que s'hauria d'utilitzar per compilar el codi.
- *contract EnviarEther {}* Declaració del contracte amb el nom *EnviarEther*, el qual executarà el codi que està dins dels parèntesis.
    - *constructor ( ) payable public {}* Un ***constructor*** és una subrutina que només s'executa una vegada i que la seva funció és la d'inicialitzar un objecte d'una classe (en aquest cas, la classe *EnviarEther*). Tota execució del codi, passarà sempre, per defecte, a executar primerament les dades que estiguin en el constructor.
      En aquest cas, és un requeriment del protocol d'Ethereum que qualsevol contracte que vulgui realitzar una transferència de valor, haurà de portar la definició de ***payable***, la qual, significa que pot transmetre Ether a objectes externs al contracte. Per últim, gràcies a la funció ***public***, es permet crear el contracte des de fora d'aquest, a partir d'una transacció. Gràcies a aquesta funció, serem capaços de crear el contracte amb el navegador Remix en la blockchain.

[127] S'utilitzen diferents tipus de colors de blau en el codi, per permetre observar i poder entendre millor les diferents paraules i funcions clau que s'utilitzen en el contracte intel·ligent.

- *Address payable public addr = 0x4baB642a718738504871e4e9399C8F103aE0A23E*; Declaració de la variable *addr* amb la funció ***address***, ***public*** i ***payable*** de l'adreça on s'enviaran els Ether. La funció ***address***, s'utilitza per indicar a la màquina virtual (EVM en aquest cas), que una variable conté una adreça. En aquest cas, la variable *addr*, conté l'adreça 0x4baB642a718738504871e4e9399C8F103aE0A23E, la qual serà receptora dels Ether que s'enviin.

Pel que fa al codi, està format per tres funcions[128]: la funció *enviarEther( )*, la funció *veureEstatAddr( )* i la funció *eliminarDades( )*. A continuació s'explicarà de forma detallada el contingut de cada una d'aquestes funcions i la seva funcionalitat en el contracte:

- La funció *enviarEther( )* està declarada com a ***public***, ***payable*** ja que indica que aquesta funció envía Ether. Aquesta funció, conté tres línies de codi:
  - require(msg.value <= 0.1 ether); La paraula clau ***require***, indica que conté una condició. Aquesta, ha de retornar el valor true per tal que l'execució del codi continuï, en cas contrari, retornarà el valor false i provocarà que no s'executi la resta de la funció.
    La condició a complir, requereix que la quantitat a enviar ***msg.value***, que s'introdueix quan l'usuari indica la xifra a enviar, ha de ser inferior o igual a 0.1 Ether. Aquesta condició permet evitar que grans quantitats d'Ether s'enviï, per tal d'evitar que un error humà en la introducció de la xifra a enviar, provoqui la transferència d'una xifra més elevada a 0.1 Ether.
  - *addr.transfer(msg.value);* Indica que el contingut de la variable *addr*, la qual és una adreça, rebrà la transferència que s'indica amb la paraula clau *transfer*, d'Ether. Entre parèntesis, la paraula clau *msg.value* indica la quantitat d'Ether que s'enviarà un cop s'executi i s'accepti la funció

[128] Cada funció está separada, i això permet a l'usuari poder seleccionar la/les funcions a executar, i l'ordre d'execució d'aquestes. Per conèixer més a fons el procés, veure apartat **4.3. Compilació i Execució en Remix**

enviarEther(). La quantitat d'Ether a enviar la introdueix l'usuari (Vegeu *Il·lustració 6: Captura de pantalla del navegador Remix*).

- valid = true; Indica que s'assigna el valor true a la variable *valid*, que prèviament s'ha declarat en l'inici del contracte com a false.

- La funció *veureEstatAddr( )* està declarada com a ***public***, ***view***, la qual és una paraula clau que indica que no té cap efecte d'edició i modificació de variables o altres elements utilitzats en el codi, i ***returns***, la qual és una paraula clau que retorna un valor de format uint256, que és un valor numèric d'un màxim de 256 bits. Aquesta funció retorna el balanç d'Ether de l'adreça del receptor d'Ether del contracte.
  - *return address(addr).balance;* Indica que retorna el balanç d'Ether, de l'adreça que conté la variable *addr*.
- La funció *eliminarDades( )* està declarada com a ***public***. Aquesta funció elimina les dades que s'emmagatzemen en les variables indicades d'aquest contracte. Això permet indicar als usuaris de la xarxa[129] que el contracte, s'ha utilitzat i que està obsolet.
  - require(valid != false); Indica que si es compleix la condició que la variable *valid* és diferent de false, és a dir, que és true, es continuarà executant la funció. En aquest cas, la variable només serà true en el moment en què primer s'hagi executat la funció *enviarEther( )* i per tant, el propòsit del contracte s'hagi complert. A partir de la primera transferència d'Ether, la funció *eliminarDades( )* es podrà executar.
  - selfdestruct(addr); La paraula clau selfdestruct, elimina el contingut de la variable *addr*, que en aquest cas conté l'adreça d'on s'han d'enviar els Ether en aquest contracte.

    Un cop executada aquesta funció, qualsevol nova execució de la funció *enviarEther( )*, provocarà que els Ether a enviar, no s'enviïn a l'adreça que contenia la variable *addr* sinó que es quedaran en el balanç del contracte.

[129] Contracte creat en la xarxa Ropsten el qual ha quedat inutilitzat després d'executar la funció selfdestruct. L'última transferència d'Ether, s'ha quedat en el balanç del contracte ja que l'adreça que contenia la variable *addr* ha estat destruïda. Per a més informació: Ropsten Address. https://ropsten.etherscan.io/address/0x9ae9031306230bc4ac3caff77ab2b291225b9721 [Consultat: 17 maig 2019]

Actualment, els Ether que es queden en el balanç d'un contracte que ha executat la funció selfdestruct no es poden recuperar.

4.4. Compilació i Execució en Remix

El procés de compilació i execució del contracte s'ha fet amb el navegador Remix (Vegeu *Il·lustració 6: Captura de pantalla del navegador Remix*). Per al desplegament del contracte en aquest navegador, es necessita introduir les següents dades del quadre de comandament:

1. L'**entorn d'execució** que s'utilitza és el de Javascript VM, ja que és un entorn individual que proveeix d'infinites unitats d'Ether per a fer proves amb el codi. També reinicia la cadena de blocs des de zero cada vegada que es carrega la pàgina.
2. Un **compte** d'on s'agafen els Ether a enviar. En aquest entorn, el mateix navegador proporciona diversos comptes amb infinites unitats d'Ether falses.
3. Un **gas límit** que és el cost que el desenvolupador està disposat a pagar per introduir el contracte en la cadena de blocs. En aquest cas, la xifra estàndard i recomanada és de 3000000 wei.
4. Un **valor de la transferència**. En aquest cas, no cal introduir cap xifra perquè per incloure el contracte intel·ligent en la cadena de blocs no cal realitzar un pagament d'Ether.

Tot seguit, cal clicar en el botó de **desplegar** per introduir el contracte en la cadena. En aquest cas, en la pantalla inferior del navegador s'indica que el contracte s'ha creat i aporta algunes dades rellevants com ara el cost d'unitats de gas que ha suposat finalment o l'adreça del contracte.

Un pas que no es veu, ja que es realitza de forma interna, és que en realitat, el contingut de qualsevol transacció que es realitza en una blockchain, no està format pel codi que s'executa, sinó que està format per un conjunt d'arxius anomenats **bytecode**.

Aquests arxius són, comandaments simples predefinits (n'hi ha un per cada una de les accions que es poden dur a terme amb el codi), els quals són fàcils d'interpretar per la màquina virtual d'Ethereum (EVM).

Aquests comandaments es generen a partir del codi dels contractes, i són el contingut real de les transaccions que s'incorporen en cada un dels blocs de la cadena de blocs.

Un cop desplegat el contracte, es pot seleccionar qualsevol de les funcions que apareixen en pantalla. Cada funció és individual, i això permet a l'usuari poder seleccionar les funcions a executar. En aquest cas, la funció *enviarEther( )* és l'única que necessita que s'introdueixi una xifra en el camp de **valor de la transferència** per a la seva execució.

Per altra banda, cal recordar que la funció *eliminarDades( )* no es podrà executar fins que la funció *enviarEther( )* s'hagi executat com a mínim una vegada.

4.5. Implementació en Ropsten

Abans d'implementar el contracte en la cadena de blocs d'Ethereum, s'implementarà en la cadena de blocs privada Ropsten, la qual permetrà realitzar proves i evitar desplegar programes amb errors en la xarxa d'Ethereum.

Pel que fa a la xarxa Ropsten, també coneguda com a "testnet", és una xarxa de proves Ethereum preconfigurada amb la prova de concepte de treball (PoW). El principal propòsit de Ropsten Network, és que els desenvolupadors testin les seves aplicacions relacionades amb Ethereum. Per altra banda, els Ether d'aquesta xarxa no tenen cap valor real[130].

Aquesta implementació es realitzarà, a partir del mateix navegador utilitzat per crear el codi, mitjançant la connexió que habilita l'extensió del navegador Firefox amb Metamask.

El procés per crear i interactuar amb el contracte, és el mateix. Així i tot, es descriuran dos passos necessaris els quals no eren necessaris en el procés de l'apartat anterior.

Primerament, cal connectar l'extensió de Metamask amb el navegador Remix (Vegeu *Il·lustració 7: Captura de pantalla de l'avís de connexió amb Remix*) per tal de tenir accés al Compte 1. Aquest compte, el qual és des d'on enviarem Ether, té l'adreça: 0x223ECC659E59350ADcFf86c4c37168c40abB17F6.

[130] Es poden obtenir Ether de la xarxa Ropsten. Per a més informació: Faucet Ropsten. https://faucet.ropsten.be/ [Consultat: 19 maig 2019]

Tot seguit, per desplegar el contracte a la xarxa Ropsten s'haurà de confirmar la transacció en la xarxa. (Vegeu *Il·lustració 8: Captura de pantalla de la confirmació en la creació del contracte en Ropsten*)[131].

A partir d'aquí, l'usuari podrà interactuar amb el contracte[132] fins a quedar-se sense Ether per costejar les despeses de Gas. Accedint a l'adreça del Compte 1 en la xarxa Ropsten[133], es poden observar totes les transaccions realitzades des de la seva creació, mantenint total transparència i anonimat del propietari de l'adreça.

En l'adreça del contracte, en l'apartat de **transaccions internes** (Internal Txns), podem observar les transaccions que ha realitzat, de forma automàtica, la lògica del contracte. Aquest, ha enviat els Ether que l'hi hem enviat des del Compte 1, a l'adreça que conté la variable *addr*[134], que és (0x453432A3C2e1B3B7Dd578EFDcbeaa2D9B12cC6Fb).

L'única diferència amb el procés de creació del contracte anterior, és que estem connectant una wallet en la nostra propietat, la qual disposa d'Ether de la xarxa Ropsten, amb l'objectiu de comprovar que la lògica s'executa de forma correcta i de conèixer la despesa de gas (per saber la despesa que generarem en Ethereum) que es produeix en generar tant el contracte com les funcions del contracte.

4.6. Implementació en Ethereum

Per a la implementació del contracte en la mainnet, o més popularment coneguda com a Ethereum, hi ha diferents opcions. Des de és seguir amb el mateix procediment implementant-ho en Ethereum, fins a instal·lar el software dels protocols d'Ethereum per crear un node el qual executi la cadena de blocs sencera.

L'opció seleccionada, la qual és la que s'ha utilitzat per implementar el contracte intel·ligent en la blockchain d'Ethereum, és la que s'ha seguit en l'apartat anterior de la

[131] **Transacció on es crea el contracte en Ropsten**. Per a més informació: Ropsten Transaction. https://ropsten.etherscan.io/tx/0x363fd4a3b2cf34789d4c52c4f916b5b9f33d332946fa21537929eac447d62b3d [Consultat: 19 maig 2019]
[132] Adreça del **contracte** en la xarxa Ropsten. Per a més informació: Ropsten Address. https://ropsten.etherscan.io/address/0x85f7aaa7f72ef284b20a47bf4e062bc55a02cf82 [Consultat: 19 maig 2019]
[133] Adreça **des d'on s'han creat contractes** en la xarxa Ropsten. Per a més informació: Ropsten Address. https://ropsten.etherscan.io/address/0x223ecc659e59350adcff86c4c37168c40abb17f6 [Consultat: 19 maig 2019]
[134] Adreça de la xarxa Ropsten **on s'envien Ether**. Per a més informació: Ropsten Address. https://ropsten.etherscan.io/address/0x453432a3c2e1b3b7dd578efdcbeaa2d9b12cc6fb [Consultat: 21 maig 2019]

cadena de blocs de Ropsten, però en aquest cas, amb adreces de la xarxa Ethereum i amb Ether reals.

La creació del contracte s'ha realitzat en el bloc #7803558, i està registrada en el bloc com una transacció[135], ja que no executa cap funció interna de contractes. Si es busca l'adreça (0x223ECC659E59350ADcFf86c4c37168c40abB17F6) en la llista de 86 transaccions incorporades d'aquell bloc, es podrà observar com indica que s'ha creat un contracte.

Pel que fa a la primera interacció amb el contracte, la primera funció executada és la d' *enviarEther( )*, la qual està registrada en el bloc #7803620 com una transacció interna d'un contracte[136].

En la següent transacció realitzada, es va rebaixar de forma considerable el **gasprice** (amb valor d'1 Wei), amb l'objectiu de cancel·lar la transacció i observar-ne les conseqüències.

Com ja s'ha explicat anteriorment, quan el gasprice d'una transacció és molt baix, els miners tendeixen a excloure-la del següent bloc a minar de la cadena de blocs.

Mentre la transacció està en espera, el protocol proporciona l'opció de cancel·lar la transacció o augmentar el gasprice, per treure d'una forma o altra la transacció de la llista. En aquest cas, s'ha optat per cancel·lar la transacció.

Això ha provocat que hi hagi dues transaccions:

- La primera que executava un altre cop la funció d'*enviarEther( )*, la qual s'ha decidit finalment cancel·lar. En el seu registre, s'indica el hash de la segona transacció creada[137].

[135] Transacció de creació del contracte en la xarxa Ethereum. Per a més informació: Ethereum Transaction.
https://etherscan.io/tx/0x83d00d1e3a3b93d17e19c8caebfa0818d5068e252e734b5b9a87ff21fa056e5a
[Consultat: 21 maig 2019]
[136] Transacció d'execució de la funció *EnviarEther( )* registrada com a transacció interna d'un contracte. Per a més informació: Ethereum Transaction.
https://etherscan.io/tx/0x94b373d566eeba5d8f1f270a421feca30c7566c7435b01617e2c0c5f368a522e
[Consultat: 21 maig 2019]
[137] Transacció cancel·lada de la funció *enviarEther( )* d'Ether. Per a més informació: Ethereum Transaction:
https://etherscan.io/tx/0x5fa1c20a6ec7efb77e65e46a5c137af4f8e01272565f448304c1da1cea0738ba
[Consultat: 21 maig 2019]

- La segona, que retorna el valor que es pretenia enviar en la primera transacció a l'adreça des d'on s'han agafat els Ether[138].

Per últim, la transacció[139] que ha executat la funció d'*eliminarDades( )*, utilitzant la ja mencionada paraula clau selfdestruct, amb l'objectiu d'eliminar les dades de la variable *addr* per fer obsolet aquest contracte.

Cal destacar, que tot aquest procés ha quedat registrat, mantenint el principi d'immutabilitat de les dades, ja que com es pot observar en l'adreça d'origen, totes les accions dutes a terme, s'han registrat.

S'ha seleccionat aquesta opció, ja que és la més pràctica, senzilla i fàcil d'implementar quant a instal·lació de programari i metodologia per crear contractes en la xarxa.

Una altra opció molt utilitzada per la comunitat de desenvolupadors, implica instal·lar el software Truffle, el qual és un entorn de desenvolupament que permet major flexibilitat de cara a testar codi.

La gran diferència amb Remix, a part de les limitacions d'aquest, és que Truffle treballa en local, és a dir, sense necessitat de tenir accés a Internet, mentre . Tanmateix, el gran inconvenient d'aquesta opció, és que per instal·lar i configurar l'entorn, i desplegar el codi creat, es requereix fer-ho a través dels comandaments del sistema operatiu, és a dir, utilitzant el llenguatge màquina (cmd).

Com podem observar, no és necessari disposar d'un node de la xarxa per a desenvolupar i desplegar codi, ja que, el manteniment d'aquest, genera despeses no només de subministrament sinó també de devaluació del maquinari que s'utilitza.

[138] Transacció sorgida per retornar els Ether de la transacció cancel·lada a l'adreça que implementa l'acció. Per a més informació: Ethereum Transaction.
https://etherscan.io/tx/0x4539c6b320cf53f3514cd4cf61f5a4a88e1f94257c0b50b48337451c0acd1de1
[Consultat: 21 maig 2019]
[139] Transacció d'*eliminarDades( )* amb la funció d'executar selfdestruct. Per a més informació: Ethereum Transaction:
https://etherscan.io/tx/0x75c07a96957a7d20d45eb3cc4362497e751a3fd1576f2568a0e16c57ec3059dd
[Consultat: 21 maig 2019]

Disposar d'un full node d'Ethereum requereix actualment 238.83 GB d'espai en memòria[140] i la constant actualització i sincronització amb la resta de la xarxa la qual comporta un elevat consum energètic.

[140] BitinfoCharts. *Ethereum / Ether (ETH) Statistics, Price, Blocks Count, Difficulty, Hashrate and Value*. https://bitinfocharts.com/ethereum/ [Consultat: 22 maig 2019]

5. CONCLUSIÓ

Internet està donant a tothom l'oportunitat inigualable de construir el seu propi univers. És cert que en certa mesura ha facilitat eines i canals els quals atorguen llibertat de pensament i d'expressió. Malauradament també ha acabat lliurant a les grans corporacions i als governs, les eines més poderoses de vigilància, control i manipulació mai creats.

Cal emfatitzar, que un dels principals arguments per als contraris a una major adopció de les criptomonedes no és del tot cert. Ja que les criptomonedes són igual de virtuals i immaterials que els diners i les targetes de crèdit.

L'única diferència és que les divises tenen el suport de les entitats reguladores, és a dir, per als qui dictaminen les lleis, mentre que les criptomonedes sorgeixen d'un consens majoritari entre tots els seus participants.

El gran problema per a blockhain han estat les criptomonedes, en comptes de parlar de les virtuts i el valor afegit que pot aportar la seva implementació en els processos empresarials i fins i tot, en els processos públics per a la protecció de dades.

Les criptomonedes no acaben de tenir massa bona reputació, la cobdícia i l'especulació han generat una gran volatilitat del mercat. La mala reputació és força merescuda, només cal referir-nos a la dada sobre les ICO durant l'any 2018: més del 80% de les ICO han estat declarades estafes[141] o directament hagin tancat. Per tant, hi ha motius suficients per guanyar-se mala reputació. El problema és estendre aquesta una opinió negativa envers aquesta tecnologia i tots els projectes que l'estan implementant.

També s'ha de reconèixer que aquesta onada ha permès difondre i popularitzar el concepte, augmentant espectacularment els seguidors de la tecnologia, malgrat que ha hagi estat a canvi de banalitzar força la tecnologia de blockchain.

[141] FTREPORTER. *Satis Group: 80% Of ICOs Are Scams*. http://ftreporter.com/satis-group-80-of-icos-are-scams/ [Consultat: 15 abril 2019]

Actualment, tot just comença a generar-se una certa preocupació, encara molt minoritària, sobre la preservació de la nostra intimitat i una lluita social per controlar adequadament que es fa amb les nostres dades personals. L'aparició de la RGPD (Reglament General de Protecció de Dades), ha vingut a regular l'ús de les dades personals i això ha començat a alertar als ciutadans europeus sobre pràctiques, poc o gens ètiques, que una gran part important de la indústria digital ha practicat les darreres dècades.

Cal conscienciar més a les persones sobre la importància de les seves dades. Molts d'ells encara creuen que les seves dades tenen poc impacte econòmic. Una percepció individualista que cal canviar. Ja ha quedat demostrat que el valor agregat d'aquest conjunt de dades, pot generar (mala)influència política, guanyar unes eleccions i generar ingressos milionaris a empreses que ja estan sota sospita com Facebook o Google.

Les dades d'una persona tenen poc impacte, sí, però les dades de centenars de milers no. I és aquí, on la tecnologia blockchain pot arribar a oferir tot el seu potencial.

A partir d'eliminar la necessitat de confiar per a poder realitzar tota classe de transaccions, i amb la seguretat que les dades de les transaccions i dels usuaris, quedaran xifrades en un registre immutable on les úniques persones que podran accedir a les dades seran aquelles persones que hagin participat en el procés o que tinguin el permís d'aquests.

Cal deixar enrere el sentiment individualista humà, i començar a col·laborar de forma conjunta per tal de ser capaços de teixir una xarxa suficientment gran i potent, que permeti competir de tu a tu amb els sistemes econòmics tradicionals.

Per tant, la tecnologia blockchain permet connectar les persones i les seves dades, a partir d'un sistema de poder descentralitzat i de localització distribuïda, per tal d'evitar i reduir l'impacte de decisions polítiques i econòmiques que al cap i a la fi, acaba afectant el gran gruix de la població.

Amb la implementació de cadenes de blocs, es podria eliminar la figura del gestor de dades, la qual cosa pot permetre tornar a ser els propietaris reals de les dades que generem, incloure un incentiu substancial per a mantenir la xarxa activa i lliure de corrupció, i sobretot, mantenir les dades íntegres i originals, eliminant qualsevol classe d'amenaça sobre aquestes.

Pel que fa a l'estudi d'Ethereum, cal remarcar que ha estat essencial i un requeriment indispensable el fet d'estudiar a fons la tecnologia blockchain. Aquest, ha permès entendre com funciona i s'implementa en un entorn real, i com la tecnologia, permet als diferents usuaris interactuar entre ells i amb les dades que es gestionen.

A partir de l'anàlisi i l'estudi de les modificacions i funcionalitats d'Ethereum, ha estat possible entendre realment què és, en què es basa i els objectius pels quals s'ha desenvolupat i es dóna tanta importància a la plataforma. Tot això, ha permès comprendre el gran potencial de la plataforma d'Ethereum per a promoure i incentivar la creació de tota mena d'aplicacions descentralitzades, les quals poden arribar a competir amb les seves versions centralitzades del mercat.

Aquest estudi tanmateix, ha permès observar l'elevat grau de desconeixement en l'opinió pública respecte a les similituds i les grans diferències que hi ha amb Bitcoin i les altres principals criptomonedes, i també als propòsits per als quals es va fundar el projecte i la raó per la qual hi ha cada vegada més desenvolupadors treballant sota el paraigua d'Ethereum.

Cal remarcar que tot això es veu influenciat a partir dels articles en la xarxa, els quals la majoria d'aquests donen informació incorrecta o que poden induir a la confusió, explicant conceptes de forma incorrecta o suposant fets i funcionalitats inexistents.

Per últim i no menys important, la realització d'un contracte intel·ligent des del seu desenvolupament fins a la seva implementació en la cadena de blocs d'Ethereum, ha permès comprendre la dificultat de cada un dels passos que s'han de donar i per altra banda, ha permès ampliar el coneixement i la visió sobre el gran potencial de les aplicacions descentralitzades.

Un cop el full de ruta d'Ethereum s'hagi complert de forma exitosa, incloent-hi la implementació de l'esperada prova de participació, s'obrirà un nou horitzó amb un gran potencial per començar a produir aplicacions descentralitzades reduint l'empremta ecològica.

Ara per ara, cal observar com es desenvolupa l'última fase del full de ruta d'Ethereum, i veure si es poden millorar els aspectes d'escalabilitat i d'emmagatzemament de dades en la tecnologia blockchain.

6. ACRÒNIMS

Aplicació descentralitzada: És una aplicació que s'executa en una xarxa d'ordinadors P2P en lloc d'un únic ordinador. Són un tipus de programari dissenyat per existir a Internet d'una manera que no sigui controlada per cap entitat.

Application-Specific Integrated Circuit (ASIC): és un microxip dissenyat per a una aplicació i una funció específica. Capaç de superar tant en velocitat com en hashrate a altres elements com ara CPU o GPU.

Atac del 51%: Aquest atac es dóna quan més de la meitat de la potència d'una xarxa està sota el control d'una única entitat. Aquesta entitat pot emetre transaccions conflictives per malmetre la xarxa, o tenir almenys la intenció de fer-ho.

Atac de denegació de servei (DoS): És un atac a un sistema de computadors o xarxa que causa que un servei o recurs sigui inaccessible als usuaris legítims. Normalment provoca la pèrdua de la connectivitat de la xarxa pel consum de la transferència d'informació (ample de banda) de la xarxa de la víctima.

Bitcoin: És la primera moneda digital o criptomoneda, de codi obert i totalment descentralitzada. Fa servir una xarxa global P2P sense la necessitat de tenir intermediaris o un emissor centralitzat.

Bloc orfe: És un bloc vàlid que no forma part de la cadena de blocs principal. Solen ocórrer naturalment quan dos miners produeixen blocs gairebé al mateix moment o poden ser causats per atacants amb suficient hashrate que tracten de revertir una transacció. Serà recompensat però el seu bloc no formarà part de la cadena de blocs.

Blockchain o cadena de blocs: És un gran llibre de dades compartit amb una xarxa, on cada entrada o transacció es pot incloure al bloc de forma permanent. Serveix com a registre històric de totes les transaccions que van ocórrer alguna vegada.

Bomba de dificultat: És un algorisme que introdueix de forma exponencial la dificultat de validar minar i validar blocs d'una cadena de blocs. S'ha utilitzat com a concepte en la xarxa Ethereum per motivar la transició a la prova de participació.

Bytecode: Arxiu binari format per un conjunt de comandaments simples, els quals contenen el codi generat a partir de la compilació d'un contracte intel·ligent escrit amb llenguatge Solidity. Tots els nodes executen aquest arxiu.

Clúster: Conjunt d'ordinadors que s'uneixen per mitjà de xarxes d'interconnexió, per obtenir un sistema coordinat capaç de processar una càrrega els quals es comporten com si fossin una única computadora.

Captcha: Un captcha t'ajuda a protegir-te del spam i del desxifrat de contrasenyes demanant-te que completis una simple prova que demostri que ets humà i no un ordinador que intenta accedir a un compte protegida amb contrasenya.

Codi Obert: és un terme que indica que un producte inclou permís per utilitzar el seu codi font, dissenyar documents o contingut.

Compte de signatura múltiple: És un contracte intel·ligent que permet a un grup de persones posseir l'adreça Ethereum col·lectivament i executar transaccions amb ell. Per a més informació, visitar https://github.com/ethereum/EIPs/issues/763.

CPU: És la Unitat Central de Processament la qual interpreta les instruccions d'un programa informàtic mitjançant la realització de les operacions bàsiques. Aquesta unitat, sempre intenta executar diferents tasques de la forma més ràpida possible.

Criptomoneda: És una divisa digital la qual s'utilitza per a l'intercanvi de béns i comerç.

DAO: És una organització que opera de forma descentralitzada i sense una estructura jeràrquica, la qual es gestiona de forma automàtica a partir de la lògica que incorporen els contractes intel·ligents que executa la EVM en el cas que estigui en la xarxa d'Ethereum. Els usuaris poden adquirir participacions d'aquesta i interactuar amb ella.

Enterprise Ethereum Alliance (EEA): És una organització sense ànim de lucre que promou Ethereum a grans corporacions i les connecta amb experts en matèria amb l'objectiu de promoure la seva utilització i implementació.

ERC20: Estàndard que descriu les funcions i events que qualsevol token ha de seguir per poder crear-se en la plataforma d'Ethereum. Aquesta estàndard, permet desenvolupar

tokens de forma fàcil i ràpida, ja que proveeix tota l'estructura per a la seva creació i distribució.

ETH: Símbol del ticker per a la criptomoneda d'Ether. Un símbol de ticker és una abreviatura única que s'utilitza per identificar una moneda o un valor negociable.

Ethash: L'algorisme que s'utilitza en la prova de treball d'Ethereum 1.0. Per a més informació, visitar https://github.com/ethereum/wiki/wiki/Ethash.

Ether: En un principi, tenia la funció de token d'Ethereum ja que permetia finançar el projecte i només tenia valor en l'ecosistema d'Ethereum, però amb l'evolució del projecte, Ether ha acabat sorgint com a criptomoneda. Actualment, és una criptomoneda ja que permet l'intercanvi i el comerç de valor fora de la plataforma, i un token, ja que permet cobrir les despeses de gas i finançar projectes interns de la plataforma. El seu símbol és Ξ, el caràcter Xi en majúscules Grec.

Ethereum: És una plataforma descentralitzada i distribuïda de codi obert, que utilitza la tecnologia blockchain com a sistema d'emmagatzematge i xifratge de dades, la qual permet el desenvolupament i desplegament de programes.

Ethereum Improvement Proposal (EIP): Document que proveeix d'informació a la comunitat d'Ethereum on es descriu una proposta i els processos que s'han d'implementar per dur-la a terme.

Ethereum Virtual Machine (EVM): És la màquina virtual d'Ethereum, i és responsable d'executar els arxius bytecode i de proveir codi predefinit per facilitar la creació d'aplicacions als usuaris. Tots els nodes l'executen creant així la xarxa Ethereum.

Ethereum Flavored WebAssembly (eWasm): És la millora de l'EVM que s'espera implementar en el nou full de ruta presentat un cop acabada l'etapa Metropolis. S'espera que permeti implementar nous llenguatges de programació, i millores pel que fa a l'escalabilitat en les transaccions i flexibilitat de la plataforma.

Fork: Bifurcació en el desenvolupament de software, fa referència a l'esdeveniment d'un projecte independent que es desprèn del projecte original de software a causa de diferencies incompatibles o irreconciliables entre els membres de la comunitat.

Funció de hash: És un algorisme matemàtic que transforma qualsevol bloc arbitrari de dades en una nova serie de caràcters amb una llargada màxima.

Gas: Combustible virtual utilitzat a Ethereum per executar contractes intel·ligents. El EVM utilitza un mecanisme de comptabilitat per mesurar el consum de gasos i limitar el consum de recursos informàtics.

GasLimit: El màxim de gas que el desenvolupador que envia la transacció està disposat a gastar perquè s'executi la transacció.

GasPrice: El valor que el desenvolupador que envia la transacció està disposat a pagar per cada unitat de gas que s'utilitzi per executar la transacció.

Geth: És un programa que serveix de node per a la cadena de blocs Ethereum, i mitjançant la qual un usuari pot minar Ether i crear programari que funcioni amb l'EVM. Per a més informació, visitar https://github.com/ethereum/go-ethereum/wiki/Geth.

GPU: Unitat de processament de gràfics (GPU) és un circuit electrònic especialitzat dissenyat per manipular i modificar ràpidament la memòria per al processament de vídeo o de problemes matemàtics, de forma repetitiva. Disposen de moltes ALU (Unitat d'Aritmètica Lògica), per la qual cosa es pot prendre una gran quantitat de problemes matemàtics computacionals a diferència de CPU.

Hash: És un algorisme matemàtic, que aplicat sobre un conjunt de dades, genera una seqüència expressada en numeració hexadecimal, utilitza setze dígits que són els números del 0 al 9 i les primeres sis lletres de l'alfabet llatí (de la a a la f).

Hashrate: És la unitat de mesura de la quantitat de potència de càlcul que consumeix una xarxa per tal que pugui funcionar contínuament.

Initial Coin Offering (ICO): És un instrument de finançament utilitzat en l'ecosistema de les criptomonedes, i té la mateixa funció que una Initial Public Offering (IPO), és a dir, la venta de participacions de l'empresa o projecte a canvi de finançament.

Integrated Development Environment (IDE): És una aplicació de programari que proporciona instal·lacions integrals als programadors informàtics per al desenvolupament de programari, com ara una interfície gràfica multiplataforma d'una interfície similar a un navegador simplificat (com ara Chrome o Firefox).

Merkle Patricia Tree: És una combinació d'arbres de Patricia i Merkle implementada en el sistema d'emmagatzematge d'Ethereum. És una formació piramidal de hash en la que cada hash és el resultat d'aplicar una funció de hash sobre els hash inferiors. Per a més informació, visitar https://github.com/ethereum/wiki/wiki/Patricia-Tree#main-specification-merkle-patricia-trie.

Metadades: És informació que descriu el contingut d'un archiu o objecte.

Metamask: És una extensió que fa la funció de pont, ja que permet conectar qualsevol aplicació i/o pàgina web distribuïda amb el navegador d'Internet. En aquest cas, permet executar aplicacions descentralitzades en la plataforma d'Ethereum sense la necessitat d'executar un node d'Ethereum complet. Per a més informació, visitar https://metamask.io/.

Minar blocs: Acció de crear un bloc de la blockchain. La CPU de l'ordinador valida les transaccions i executa els algorismes i operacions matemàtiques necessaries que generaran els hash que es requereixen per crear un bloc.

Miner: Crea els blocs de la cadena a partir de la repetició d'operacions. Un cop obté el hash correcte, ho comunica als altres nodes per a que ho verifiquin.

Minning pols : Agrupacions de nodes de diferents miners que s'uneixen en una xarxa determinada per compartir i ampliar el seu hashrate o poder de processament, agilitzant així la seva capacitat per resoldre un bloc.

Node: Software que conté la EVM amb les normes establertes del protocol i la cadena de blocs de la xarxa, i que s'encarrega de validar blocs i transaccions, i d'actualitzar la cadena de blocs.

Parity: Programari dissenyat com a porta d'entrada a la xarxa Ethereum, la qual disposa d'una interfície entre el web i la plataforma. L'objectiu és ser el client Ethereum més ràpid, més lleuger i més segur. Per a més informació, visitar https://wiki.parity.io/Parity-Ethereum.

Remix: És un IDE basat en un navegador que funciona com a compilador de codi obert que permet als usuaris construir contractes Ethereum amb el llenguatge Solidity i depurar

les transaccions. Escrit en JavaScript, Remix suporta tant l'ús en el navegador com a nivell local. Per a més informació, visitar https://github.com/ethereum/remix-ide.

RLPx Transport: És un protocol de transport basat en TCP que s'utilitza per a la comunicació entre els nodes d'Ethereum. El protocol conté missatges xifrats pertanyents a una o més "capacitats" que es negocien durant l'establiment de la connexió. Per a més informació, visitar https://github.com/ethereum/devp2p/blob/master/rlpx.md.

Ropsten: És una xarxa de proves privada que s'utilitza essencialment com a entorn de prova abans d'introduir el codi a la xarxa principal d'Ethereum. A diferència de la xarxa principal, escriure a la xarxa de prova és gratuïta.

SHA-256: Funció hash criptogràfica que pren una entrada de mida aleatòria i produeix una sortida de mida fixa. S'utilitza en moltes criptomonedes, en especial Bitcoin.

Smart contracts: O contractes intel·ligents, són programes codificats i dissenyats per facilitar de forma segura i transparent, l'intercanvi d'un recurs o l'execució d'un esdeveniment sense la necessitat d'un intermediari. Aquests contractes s'estableixen a partir d'una lògica que ha de complir unes condicions predefinides.

Solidity: Llenguatge de programació d'alt nivel i orientat a objectes amb el que es creen contractes intel·ligents. Per a més informació: https://solidity.readthedocs.io/en/v0.5.8/.

Token: És una representació o símbol de qualsevol actiu que es susceptible al seu comerç, i que té valor en determinats llocs o cirsumstàncies. Un clar exemple, és una fitxa d'un casino.

Trilema blockchain: Problema expressat per primera vegada per Vitalik Buterin, en el que qualsevol cadena de blocs només pot centrar-se en dues de les tres característiques: Seguretat, descentralització i/o escalabilitat. Una cadena de blocs ideal seria la qual pogués maximitzar totes tres característiques.

Turing-complet: Sistema que permet que un ordinador pugui arribar a programar-se per realizar qualsevol tipus d'operació.

Wallet: La cartera executa i marca amb una firma tota transacció que realitza el seu propietari, i guarda té totes les adreces alfanumèriques i les claus d'on estan les situades

les monedes en una cadena de blocs. No guarda el valor d'una transacció, ja que aquesta està dipositada en la cadena de blocs.

Wei: La denominació més petita d'Ether. 10^{18} wei = 1 Ether.

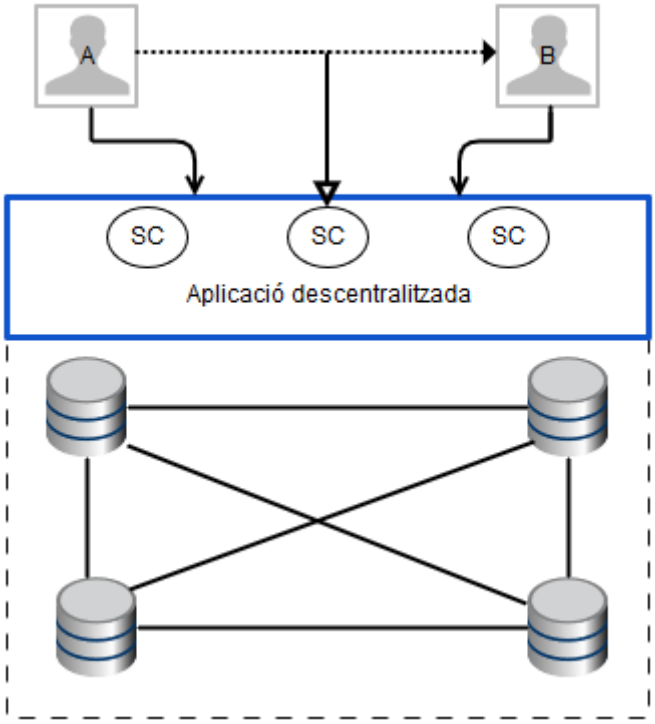
Whitepaper: Un document blanc és un document en forma de guía, amb la funció d'intentar explicar a tots els usuaris com resoldre un problema o ajudarlos a entendre un tema en concret.

Xarxa P2P: O xarxa Peer-to-Peer, és una sèrie de nodes que es comporten alhora com a clients i com a servidors dels altres nodes de la xarxa, la qual divideix tasques o càrregues de treball entre iguals. Els iguals són igualment privilegiats i són equipotents en l'aplicació.

ZK-SNARKS: Protocol de coneixement zero introduït per la criptomoneda ZCash. Aquesta prova permet validar el contingut de la informació sense revelar-ne el seu contingut.

7. ANNEX

Il·lustració 1: Esquema gràfic de la relació entre Blockchain, Ethereum i els contractes intel·ligents



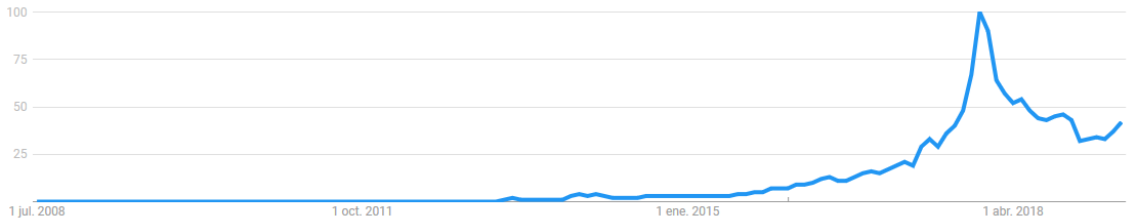
Font: Elaboració pròpia utilitzant el software de gliffy.com

Cada aplicacació descentralitzada, conté *n* contractes intel·ligents (SC), i cada contracte, conté una lògica específica, com per exemple *enviar diners a una persona*. Com quan l'usuari A realitza una transacció a l'usuari B.

Cada node de la xarxa d'Ethereum està connectat amb la resta, i manté sincronitzada la Blockchain d'Ethereum, la qual manté totes les aplicacions descentralitzades creades en la plataforma d'Ethereum.

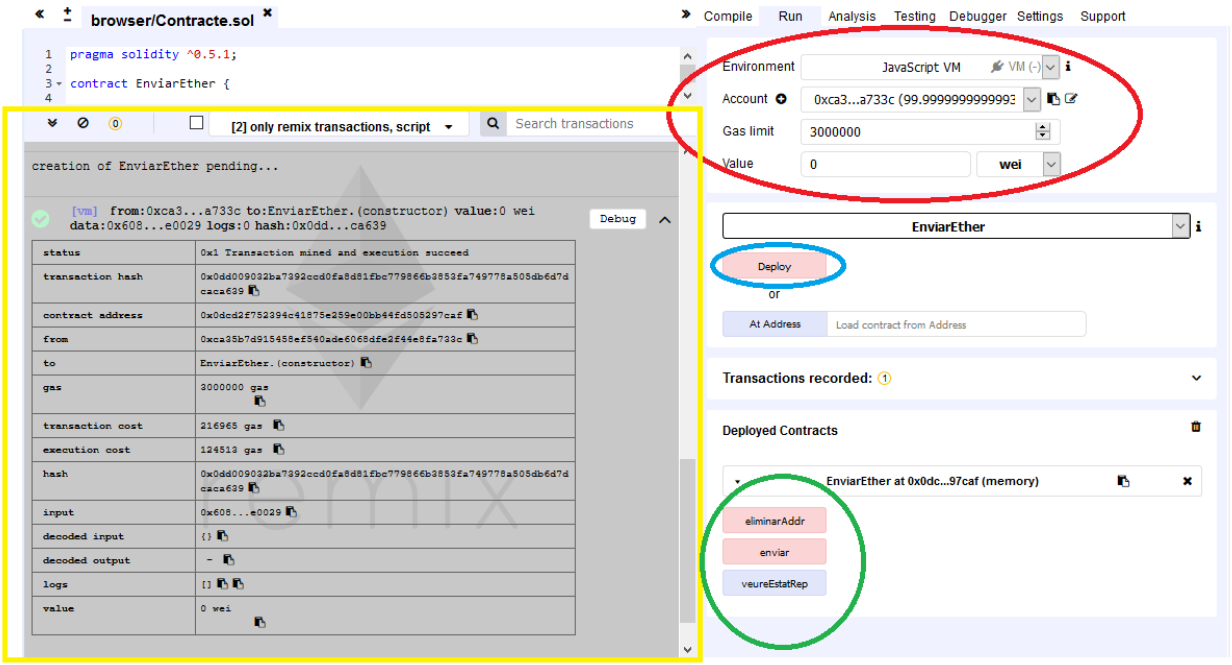
A mesura que es realitzen noves transaccions, aquestes es van incorporant en els blocs de la blockchain que suporta aquella xarxa.

Il·lustració 2: Tendència de cerca de la paraula Blockchain en Google



Font: Elaboració a partir dels filtres i dades disponibles en Google Trends

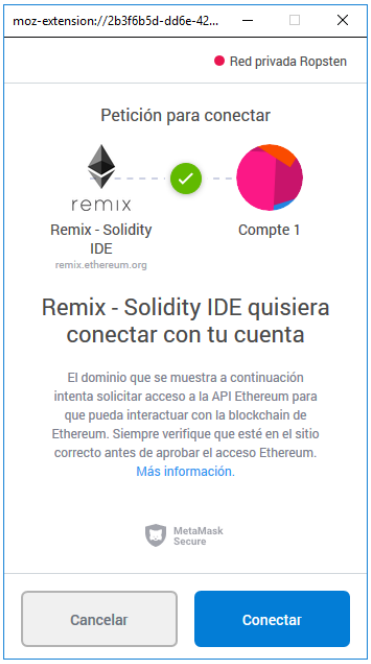
Il·lustració 6: Captura de pantalla del Navegador Remix



Font: Captura pantalla del navegador Remix

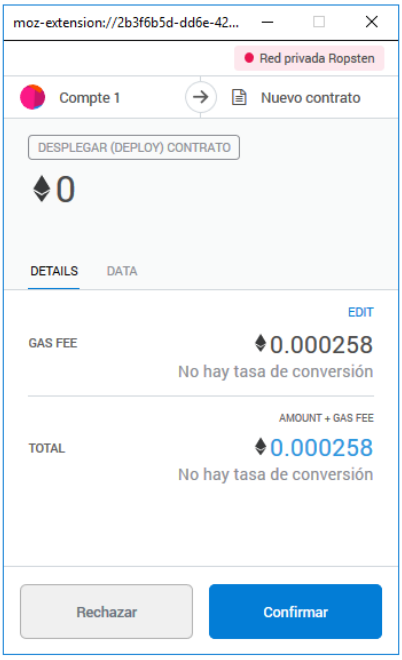
- **Color vermell**: el quadre de comandament (amb l'entorn, compte des d'on s'envien Ether, el gas límit i el valor de la transferència/msg.value)
- **Color blau**: botó per desplegar el contracte
- **Color verd**: Funcions a seleccionar del contracte
- **Color groc**: Informe amb dades rellevants del procés de creació del contracte

Il·lustració 7: Captura de pantalla de l'avís de connexió amb Remix



Font: Captura pantalla del navegador Remix

Il·lustració 8: Captura de pantalla de confirmació en la creació del contracte en Ropsten



Font: Captura pantalla del navegador Remix

8. BIBLIOGRAFIA

TAPSCOTT, Don; TAPSCOTT, Alex. 2017. *La revolución blockchain:* Editorial DEUSTO.

PREUKSCHAT, Alex. 2017. *Blockchain: la revolución industrial de internet*. Editorial Gestión 2000.

- PREUKSCHAT, Alex; NÚÑEZ, Jaime. 2017. *Blockchain: la revolución industrial de internet*. Editorial Gestión 2000. Criptografía y consenso aplicado a la blockchain: 203-220.

M. ANTONOPOULOS, Andreas. 2014. *Mastering Bitcoin*. Editorial O'Reilly.

AMMOUS, Saifedean. 2017. *El patrón Bitcoin: La alternativa descentralizada de los bancos centrales*. Editorial DEUSTO.

TUR FÁUNDEZ, Carlos. 2018. *Smart Contracts: Análisis jurídico*. Reus Editorial.

M. ANTONOPOULOS, Andreas. 2018. *Mastering Ethereum: Building smart contracts and dapps*. Editorial O'Reilly.

8.1. Recursos Electrònics

Delton Rhodes. A Complete History of Bitcoin (2008 – 2019 Timeline). https://blockexplorer.com/news/bitcoin-history-timeline/ [Consultat: 26 gener 2019]

The Ethereum node explorer. https://www.ethernodes.org/network/1 [Consultat: 27 gener 2019]

Global Bitcoin Nodes Distribution. https://bitnodes.earn.com/ [Consultat: 27 gener 2019]

HIGGINSON, Matt. *Blockchain explained: What it is and isn't, and why it matters*. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-explained-what-it-is-and-isnt-and-why-it-matters [Consultat: 28 febrer 2019]

Google Trends. https://trends.google.com/trends/explore?date=2015-01-01%202019-05-26&q=blockchain [Consultat: 26 maig 2019]

IBM Blockchain - Enterprise Blockchain Solutions & Services https://www.ibm.com/blockchain [Consultat: 2 febrer 2019]

Crypto51. https://www.crypto51.app/ [Consultat: 2 febrer 2019]

CryptoCribs. https://www.cryptocribs.com/ [Consultat: 23 maig 2019]

ERASMUS. *A Peer-to-Peer Electronic Rental System*. https://www.cryptocribs.com/images/whitepaper.pdf [Consultat: 23 maig 2019]

IBM Food Trust. https://www.ibm.com/es-es/blockchain/solutions/food-trust [Consultat: 23 maig 2019]

David Galvin. *IBM and Walmart: Blockchain for Food Safety*. https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf [Consultat: 23 maig 2019]

ALCÁNTARA, Jose. *Red distribuida*. https://www.versvs.net/pedia/red-distribuida/ [Consultat: 2 març 2019]

DINKINS, David. *Bitcoin es descentralizado pero no distribuido, y ese hecho probablemente contribuyó a la guerra civil de Bitcoin*. https://es.cointelegraph.com/news/bitcoin-is-decentralized-but-not-distributed-and-that-fact-likely-contributed-to-bitcoins-civil-war. PORT, Torp. *Centralized vs decentralized vs distributed networks + Blockchain.* https://medium.com/@torp_port/centralized-vs-decentralized-vs-distributed-networks-blockchain-f895416dc22 [Consultat: 16 març 2019]

POENITZSCH, Julia. *What's the difference between decentralized and distributed?* https://medium.com/nakamo-to/whats-the-difference-between-decentralized-and-distributed-1b8de5e7f5a4 [Consultat: 10 abril 2019]

ROCA, Luis. *Seguridad Informática: Criptografía*. http://minubeinformatica.com/cursos/seguridad-informatica/criptografia/ [Consultat: 30 març 2019]

MEJIA, Jose Luis. ¿A dónde van los cargos por transacción de Bitcoin? https://steemit.com/spanish/@joseluismejia/a-donde-van-los-cargos-por-transaccion-de-bitcoin [Consultat: 3 abril 2019]

BOLAÑOS, Juan Francisco. *Blockchain y la Prueba de Trabajo – PoW –.* https://steemit.com/cryptocurrency/@juanfb/blockchain-y-la-prueba-de-trabajo-pow [Consultat: 31 març 2019]

BUTERIN, Vitalik. *Proof of Stake FAQ.* https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ [Consultat: 31 març 2019]

BOLAÑOS, Juan Francisco. *Blockchain y la Prueba de Participación (PoS).* https://www.academiablockchain.com/2018/05/17/blockchain-y-la-prueba-de-participacion-pos/ [Consultat: 31 març 2019]

DHANANI, Shanif. *Ethereum's Proof-of-Stake May Be A Profitable Venture For Current Holders.* https://medium.com/@shanif/ethereums-proof-of-stake-may-be-a-profitable-venture-for-current-holders-183024263151 [Consultat: 20 abril 2019]

MALDONADO, Jose. *¿Qué es la prueba de Autoridad (POA)?* https://www.criptotendencias.com/base-de-conocimiento/que-es-la-prueba-de-autoridad-poa/ [Consultat: 31 març 2019]

OLMO, Lara. *10 grandes frases de Warren Buffet para los negocios (y la vida).* https://www.estrategiaynegocios.net/empresasymanagement/1113606-330/10-grandes-frases-de-warren-buffett-para-los-negocios-y-la-vida [Consultat: 31 març 2019]

LEUSSINK, Klaas. *Hard and Soft forks.* https://cryptographics.info/cryptographics/blockchain/hard-soft-forks/ [Consultat: 31 març 2019]

Blockchain Explorer. https://www.blockchain.com/es/explorer [Consultat: 2 abril 2019]

BOTJES, Edzo. *Pulling the Blockchain apart. The transaction life-cycle* https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3 [Consultat: 1 abril 2019]

RAY, James. *Dagger Hashimoto.* https://github.com/ethereum/wiki/wiki/Dagger-Hashimoto [Consultat: 21 abril 2019]

SOTO, Marvin G. *El problema de los Generales Bizantinos (PGB).* https://medium.com/@marvin.soto/el-problema-de-los-generales-bizantinos-pgb-e0cb8c4279c2 [Consultat: 20 abril 2019]

GARCÍA, Isra. *Blockchain: descentralización y disrupción como nunca antes en la historia.* http://www.expansion.com/blogs/economia-disruptiva/2018/01/15/blockchain-descentralizacion-y.html [Consultat: 13 abril 2019]

https://arewedecentralizedyet.com/ [Consultat: 16 abril 2019]

MERLO, Irene. *¿Cuánto tarda una transferencia internacional en hacerse efectiva?* https://www.helpmycash.com/blog/cuanto-tarda-una-transferencia-internacional-hacerse-efectiva/ [Consultat: 13 abril 2019]

Bit2Me Academy. *Cómo saber la comisión de una transacción Bitcoin.* https://academy.bit2me.com/como-saber-la-comision-de-una-transaccion-bitcoin/ [Consultat: 13 abril 2019]

FERNÁNDEZ, Froilan. *Las criptomonedas retan al sistema bancario tradicional.* https://www.criptonoticias.com/opinion/criptomonedas-retan-sistema-bancario-tradicional/ [Consultat: 13 abril 2019]

GAMALERO, Martin. *Blockchain eliminará desperdicios en la industria de la logística.* https://criptotario.com/blockchain-eliminara-desperdicios-la-industria-la-logistica [Consultat: 13 abril 2019]

Legality of bitcoin by country or territory explained. http://everything.explained.today/Legality_of_bitcoin_by_country_or_territory/ [Consultat: 14 abril 2019].

CASADO, Nicomedes. *Medidas y Regulaciones que vienen en camino para las criptomonedas*. https://www.criptomano.com/medidas-y-regulaciones-que-vienen-en-camino-para-las-criptomonedas/ [Consultat: 14 abril 2019].

Digiconomist. *Bitcoin Energy Consumption Index*. https://digiconomist.net/bitcoin-energy-consumption [Consultat: 6 abril 2019]

SALAZAR, Jonathan. *Una sola transacción de Bitcoin utiliza la misma cantidad de energía que una casa en tres semanas.* https://tekzup.com/una-sola-transaccion-de-bitcoin-utiliza-la-misma-cantidad-de-energia-que-una-casa-en-tres-semanas/ [Consultat: 6 abril 2019]

WALL, Jeremy. *Bitcoin Cash Hard Fork Aftermath: BCHABC and BCHSV Continue to Battle It Out*. https://www.investinblockchain.com/bitcoin-cash-hard-fork-aftermath/ [Consultat: 7 abril 2019]

GAS, Dani. *Una quinta parte de Bitcoin está perdido, el suministro real de BTC es muy bajo.* http://infocoin.net/2018/07/07/una-quinta-parte-de-bitcoin-esta-perdido-el-suministro-real-de-btc-es-muy-bajo/ [Consultat: 6 abril 2019]

CASTRO, Luis. *¿Qué es escalabilidad?* https://www.aboutespanol.com/que-es-escalabilidad-157635 [Consultat: 7 abril 2019]

YAKUBOWSKI, Max. *Europa da pasos serios hacia adopción de blockchain*. https://es.cointelegraph.com/news/europe-takes-serious-steps-towards-blockchain-adoption [Consultat: 15 abril 2019]

CARMELO, José. *¿Existe regulación de blockchain en la Unión Europea?* http://www.notariallopis.es/blog/i/1424/73/existe-regulacion-de-blockchain-en-la-union-europea [Consultat: 15 abril 2019]

LEONARD, Andreu. *The Blockchain is a remainder of the Internet's Failure.* https://onezero.medium.com/the-blockchain-is-a-reminder-of-the-internets-failure-b16c58d70413 [Consultat: 15 abril 2019]

IGLESIAS, Andreina. *La computación cuántica podría hacer vulnerable a la Blockchain.* https://bitcoin.es/actualidad/la-computacion-cuantica-podria-hacer-vulnerable-a-la-blockchain/ [Consultat: 11 abril 2019]

GHEORGHIU, Vlad; GORBUNOV, Sergey; MOSCA, Michele; MUNSON, Bill. *Quantum-Proofing the blockchain*.

https://www.evolutionq.com/assets/mosca_quantum-proofing-the-blockchain_blockchain-research-institute.pdf [Consultat: 11 abril 2019]

VILLATORO, Francisco R. *El ruido cuántico contra el futuro de la computación cuántica*. https://francis.naukas.com/2016/11/29/el-futuro-de-la-computacion-cuantica/ [Consultat: 11 abril 2019]

PIRES, Tiago. *TIPS, the new European payment system.* https://technologist.eu/tips-the-european-instant-payment-settlement/ [Consultat: 15 abril 2019]

CALLEJA, Carlos. *Hashgraph, la nueva Blockchain? Explicación y razonamientos*. https://steemit.com/hashgraph/@kallejo/hashgraph-la-nueva-blockchain-explicacion-y-razonamientos [Consultat: 16 abril 2019]

GONZÁLEZ, Manuel. *Encriptación modulable, ¿la alternativa al "blockchain"?* https://retina.elpais.com/retina/2018/11/29/innovacion/1543493308_805539.html [Consultat: 15 abril 2019]

Etherscan Tokens Tracer. https://etherscan.io/tokens [Consultat: 1 maig 2019]

BUTERIN, Vitalik. *Whitepaper of Ethereum*. https://github.com/ethereum/wiki/wiki/White-Paper [Consultat: 17 abril 2019]

SELLIN, Evin. *What exactly is Turing Completeness?* https://medium.com/@evinsellin/what-exactly-is-turing-completeness-a08cc36b26e2 [Consultat: 17 abril 2019]

Business Insider. *Vitalik Buterin on creating one of the world's largest cryptocurrencies.* https://www.youtube.com/watch?time_continue=87&v=fi0ORZR4A88 [Consultat: 17 abril 2019]

GONZÁLEZ, David. *Estado actual de los Hardforks Bitcoin.* https://steemit.com/bitcoin/@ydavgonzalez/estado-actual-de-los-hardforks-bitcoin [Consultat: 19 abril 2019]

CANELLIS, David. *Here's why Bitcoin's blockchain as blocs that go over the 1MB límit.* https://thenextweb.com/hardfork/2018/07/12/bitcoin-block-size/ [Consultat: 20 abril 2019]

ETHEREUM. *Ethereum is a global, open-source platform for decentralized applications.* https://ethereum.org/ [Consultat: 20 abril 2019]

HOLMES, Jamie. *The Halving:What Bitcoin's Block Reward Milestone Means.* https://btcmanager.com/the-halving-what-bitcoins-block-reward-milestone-means/ [Consultat: 20 abril 2019]

SCHOEDON, Afri. *Constantinople Difficulty Bomb Delay and Block Reward Adjustment.* https://eips.ethereum.org/EIPS/eip-1234 [Consultat: 20 abril 2019]

SHEN, Maria. *The Dev Report of ELECTRIC CAPITAL*. https://static1.squarespace.com/static/5c745b19c2ff6174b1290e42/t/5c805a3ae4966b1ce3a2a937/1551915603922/The+Dev+Report.pdf [Consultat: 20 abril 2019]

BitinfoCharts. *Bitcoin, Ethereum Hashrate Chart*. https://bitinfocharts.com/comparison/hashrate-btc-eth.html [Calculat: 20 abril 2019]

Coinguides. *HashPower Calculator – Convert Hash to kH/s to MH/s to GH/s to TH/s to PH/s.* https://coinguides.org/hashpower-converter-calculator/ [Consultat: 20 abril 2019]

TUWINER, Jordan. *ASIC i Rigs de programes de mineria Bictoin.* https://www.buybitcoinworldwide.com/es/mineria/hardware/ [Consultat: 21 abril 2019]

MOOS, Mitchell. *Vitalik Buterin: Ethash ASICs Not a Threat to Ethereum.* https://cryptoslate.com/vitalik-buterin-ethash-asics-ethereum/ [Consultat: 21 abril 2019]

GAMALERO, Martin. *Las mejores GPU para minar rentablemente.* https://criptotario.com/las-mejores-gpu-para-minar#Por_que_usar_las_GPU_para_minar_y_no_los_CPU [Consultat: 21 abril 2019]

KIM, Kiyun. *Modified Merkle Particia Trie.* https://medium.com/codechain/modified-merkle-patricia-trie-how-ethereum-saves-a-state-e6d7555078dd [Consultat: 22 abril 2019]

MiEthereum. *Vitalik Buterin – Vida del joven genio creador de Ethereum.* https://www.miethereum.com/vitalik-buterin/ [Consultat: 17 abril 2019]

CAWREY, Daniel. *Miami Bitcoin Conference Day2: Litecoin, New Coins and Regulatory Risks.* https://www.coindesk.com/miami-bitcoin-conference-day-2-litecoin-regulation [Consultat: 17 abril 2019]

Btcmiami. *The North American Bitcoin Conference*. https://btcmiami.com/ [Consultat: 16 abril 2019]

Ethereum.org. *DEVCON1: Ethereum for Dummies – Dr. Gavin Wood.* https://www.youtube.com/watch?v=U_LK0t_qaPo [Consultat: 17 abril 2019]

Coinmama. *History of Ethereum*. https://www.coinmama.com/guide/history-of-ethereum [Consultat: 16 abril 2019]

Ethereum block 0 info. https://etherscan.io/block/0 [Consultat: 17 abril 2019]

MADEIRA, Antonio. *What is the Ethereum Ice Age?* https://www.cryptocompare.com/coins/guides/what-is-the-ethereum-ice-age/ [Consultat: 18 abril 2019]

JENTZSCH, Christoph. *New difficult algorithm.* https://gist.github.com/CJentzsch/c78768f9837afb8eef74 [Consultat: 18 abril 2019]

THOMPSON, Collin. *The DAO of Ethereum.* https://medium.com/blockchain-review/the-dao-of-ethereum-e228b93afc79 [Consultat: 17 abril 2019]

SIEGEL, David. *Understanding The DAO Attack.* https://www.coindesk.com/understanding-dao-hack-journalists [Consultat: 18 abril 2019]

JAMESON, Hudson. *Upcoming Ethereum Hard Fork.* https://blog.ethereum.org/2016/10/18/faq-upcoming-ethereum-hard-fork/ [Consultat: 17 abril 2019]

JAMESON, Hudson. *Hard Fork no.4: Spurious Dragon.* https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/ [Consultat: 17 abril 2019]

Enterprise Ethereum Alliance. https://entethalliance.org/ [Consultat: 16 abril 2019]

ETHEREUM TEAM. *Byzantium HF Announcement.* https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/ [Consultat: 17 abril 2019]

EDGINGTON, Ben. *What is the exact meaning of a transaction's new receipt status field?* https://ethereum.stackexchange.com/questions/28889/what-is-the-exact-meaning-of-a-transactions-new-receipt-status-field?rq=1 [Consultat: 18 abril 2019]

JAMESON, Hudson. *Security Alert: Ethereum Constantinople Postponement.* https://blog.ethereum.org/2019/01/15/security-alert-ethereum-constantinople-postponement/ [Consultat: 18 abril 2019]

JAMESON, Hudson. *Ethereum Constantinople/St. Petersburg Upgrade Announcement.* https://blog.ethereum.org/2019/02/22/ethereum-constantinople-st-petersburg-upgrade-announcement/ [Consultat: 18 abril 2019]

FARIDI, Omar. *Everything You Need to Know for Ethereum's Hard Forks: Constantinople, St. Petersburg.* https://www.cryptoglobe.com/latest/2019/02/everything-you-need-to-know-for-ethereum-s-upcoming-constantinople-st-petersburg-upgrade/ [Consultat: 19 abril 2019]

GALVEZ, Johana. *Cambios en la hoja de ruta de Ethereum: ¿cuándo esperar los lanzamientos de Casper y Sharding?* https://ava.markets/forex/cambios-en-la-hoja-de-ruta-de-ethereum-cuando-esperar-los-lanzamientos-de-casper-y-sharding/ [Consultat: 18 abril 2019]

OMETORUWA, Toju. *Solving the Blockchain Trilema: Decentralitzation, Security & Scalability.* https://www.coinbureau.com/analysis/solving-blockchain-trilemma/ [Consultat: 19 abril 2019]

CASTOR, Amy. *The Ethereum ICO: Where did all the tokens go?* https://www.theblockcrypto.com/2018/12/18/the-ethereum-ico-where-did-all-the-tokens-go/ [Consultat: 17 abril 2019]

ETH Gas Station. https://www.ethgasstation.info/ [Consultat: 21 abril 2019]

SALDANHA, Lucas. *Ethereum Explained: Gas, Payment and Mining*. http://pegasys.tech/ethereum-explained-gas-payment-and-mining/ [Consultat: 21 abril 2019]

What is a DApp? https://hackernoon.com/what-are-decentralized-applications-dapps-3b63b4d587fe/ [Consultat: 1 maig 2019]

eChat. *Blockchain-based decentralized secure messenger and fastest-growing social network.* https://echat.io/ [Consultat: 1 maig 2019]

Lazooz. *A value system designed for sustainability*. http://lazooz.org/ [Consultat: 27 abril 2019]

Elk. *Start building blockchain-connected devices*. https://elk.cc/ [Consultat: 9 maig 2019]

ADLERSTEIN, David M. *Are Smart contracts Smart?* https://www.coindesk.com/when-is-a-smart-contract-actually-a-contract [Consultat: 23 abril 2019]

KEWLEY, Jonathan. *Smart Contracts - Legal Agreements for the Digital Age*. https://www.cliffordchance.com/briefings/2017/06/smart_contracts_-legalagreementsforth.html [Consultat: 26 abril 2019]

HERTIG, Alyssa. *How do Ethereum Smart Contracts Work?* https://www.coindesk.com/information/ethereum-smart-contracts-work [Consultat: 28 abril 2019]

Ethereum (ETH) price, charts, market cap and other metrics. https://coinmarketcap.com/currencies/ethereum/ [Consultat: 10 maig 2019]

Inter-Agency Standing Committee (IASC) Humanitarian Financing Task Team. Donor conditions and their implications for Humanitarian response. Article online: https://interagencystandingcommittee.org/system/files/20160416_donor_conditions_study_final_0.pdf [Consultat: 4 maig 2019]

Transferwise Team. *Transferencias internacionales con BBVA: Tarifas y Comisiones.* https://transferwise.com/es/blog/transferencia-internacional-bbva [Consultat: 17 maig 2019]

Metamask. https://metamask.io/ [Consultat: 10 abril 2019]

Remix Ethereum. https://remix.ethereum.org/ [Consultat: 7 abril 2019]

Wikipedia. https://en.wikipedia.org/wiki/JSON [Consultat: 16 maig 2019]

Faucet Ropsten. https://faucet.ropsten.be/ [Consultat: 19 maig 2019]

Ropsten Address. https://ropsten.etherscan.io/address/0x9ae9031306230bc4ac3caff77ab2b291225b9721 [Consultat: 17 maig 2019]

Ropsten Transaction. https://ropsten.etherscan.io/tx/0x363fd4a3b2cf34789d4c52c4f916b5b9f33d332946fa21537929eac447d62b3d [Consultat: 19 maig 2019]

Ropsten Address. https://ropsten.etherscan.io/address/0x85f7aaa7f72ef284b20a47bf4e062bc55a02cf82 [Consultat: 19 maig 2019]

Ropsten Address. https://ropsten.etherscan.io/address/0x223ecc659e59350adcff86c4c37168c40abb17f6 [Consultat: 19 maig 2019]

Ropsten Address. https://ropsten.etherscan.io/address/0x453432a3c2e1b3b7dd578efdcbeaa2d9b12cc6fb [Consultat: 21 maig 2019]

Ethereum Transaction. https://etherscan.io/tx/0x83d00d1e3a3b93d17e19c8caebfa0818d5068e252e734b5b9a87ff21fa056e5a [Consultat: 21 maig 2019]

Ethereum Transaction. https://etherscan.io/tx/0x94b373d566eeba5d8f1f270a421feca30c7566c7435b01617e2c0c5f368a522e [Consultat: 21 maig 2019]

Ethereum Transaction. https://etherscan.io/tx/0x5fa1c20a6ec7efb77e65e46a5c137af4f8e01272565f448304c1da1cea0738ba [Consultat: 21 maig 2019]

Ethereum Transaction. https://etherscan.io/tx/0x4539c6b320cf53f3514cd4cf61f5a4a88e1f94257c0b50b48337451c0acd1de1 [Consultat: 21 maig 2019]

Ethereum Transaction. https://etherscan.io/tx/0x75c07a96957a7d20d45eb3cc4362497e751a3fd1576f2568a0e16c57ec3059dd [Consultat: 21 maig 2019]

BitinfoCharts. *Ethereum / Ether (ETH) Statistics, Price, Blocks Count, Difficulty, Hashrate and Value.* https://bitinfocharts.com/ethereum/ [Consultat: 22 maig 2019]

FTREPORTER. *Satis Group: 80% Of ICOs Are Scams*. http://ftreporter.com/satis-group-80-of-icos-are-scams/ [Consultat: 15 abril 2019]