Universitat Politècnica de Catalunya

Facultat d'Informàtica de Barcelona

Sistema de reputació a Internet sobre una blockchain

Treball de Fi de Grau

Autora: Yaiza Cano Duarte
Director: Pere Barlet Ros
Especialitat: Computació

---

22 de Juny del 2021

Índex

Capítol 1

Context

En aquest capítol s'explica el format en el qual es realitza aquest estudi, també es descriu el problema a resoldre, s'esmenten els possibles actors implicats als que beneficiaria el seu desenvolupament, s'argumenta tota una justificació respecte al seu cas d'ús i es reporta una possible proposta de resolució.

1.1 Introducció

Aquest projecte es realitza en modalitat A, és a dir, íntegrament a la universitat. Jo, l'autora d'aquest estudi, sóc de l'especialitat de Computació i aquest projecte és tot un repte per mi atès que es tracten molts temes que disten del que he estudiat fins ara. Ara bé, l'objectiu principal és completar el desenvolupament d'una aplicació web que mostri la reputació associada a un domini donat, segons el servei de votacions implementat a una *blockchain* amb *smart contracts*.

1.2 Formulació del problema

Avui dia, les pàgines web estan plenes d'elements que fan que l'experiència de l'usuari no sigui del tot satisfactòria, ja sigui l'ús reiterat d'anuncis intrusius, com ara pop-ups o banners, o temps llargs de descàrrega, tot afecta a la percepció de fiabilitat d'un domini. En aquest estudi, però, ens volem centrar en les amenaces que, dia rere dia, exploten les vulnerabilitats dels usuaris.

Entre els diferents agents[1] que conformen les amenaces web en destaquen: els **no humans**, inclouen codis maliciosos, desastres naturals, fallada de la

xarxa, fallada de la tecnologia i riscos físics; els **humans de forma intencionada**, inclouen tant personal intern com extern i estan basats en intencions malicioses; els **humans per accident**, similar als anteriors però basats en errors humans; els **humans per negligència**, similars als anteriors però basats en comportaments negligents o descurança de seguretat.

Els agents acabats d'esmentar exploten vulnerabilitats no només dels usuaris, sinó també de les diferents organitzacions que poden provocar que diversa informació sensible sigui revelada, la interrupció de l'ús del sistema informàtic, l'apoderament de nivells d'accés privilegiat, entre d'altres.
Tots aquests resultats poden comportar a danys severs a la reputació dels dominis, la interrupció dels seus serveis i diversos tipus de robatoris.

Actualment, existeixen serveis tant de pagament com gratuïts, els quals informen sobre la reputació d'una pàgina web o una adreça IP. A l'article de Lenny Zeltser[2] podem trobar tot un seguit d'eines gratuïtes que ens indiquen els llocs webs potencialment perillosos de deferents maneres. Aquests serveis, però, són centralitzats i hermetitzats en el referent a qui pot contribuir. Aquest fet fa que usuaris normals o investigadors independents no puguin participar directament en aquesta branca de la ciberseguretat a menys que pertanyin a una organització amb reputació suficient o que ja tingui implementat aquest servei de forma interna.

L'esperança d'entreveure aquest món augmenta dràsticament amb l'aparició de la tecnologia *blockchain*, la qual impulsa el desenvolupament de nous tipus d'aplicacions i serveis que fins ara no eren possibles o que requerien d'algun intermediari per poder ser utilitzades. La seva principal característica i que s'utilitza en aquest projecte és la possibilitat d'emmagatzemar dades de manera distribuïda i sense restriccions.

Així doncs, en definitiva, aquest projecte es basa en crear un xarxa distribuïda sense restriccions que computarà les reputacions dels diferents dominis i a la que tothom hi tindrà accés i hi podrà col·laborar.

1.3 Actors implicats

El desenvolupament d'aquest projecte beneficia tant a usuaris normals com a empreses que monitoritzen de manera freqüent els seus dominis i analitzen mètriques web[3] com ara la quantitat d'usuaris que visiten la web durant un temps específic, el temps que està de mitja un usuari a una pàgina en

concret, el percentatge d'usuaris que reboten, entre d'altres. A continuació parlaré més en profunditat d'ambdós grups.

En quant als usuaris normals en distingirem als investigadors i als professionals del camp de la ciberseguretat que estan al dia amb els avanços d'amenaces web i ajuden a mantenir actualitzades les diferents bases de dades de reputacions d'adreces IP. Aquests, analitzen sovint arxius i mostres de softwares maliciosos per poder crear indicadors de compromís[1] i compartir informes sobre els riscos i solucions que ells mateixos han descobert amb la resta del món.
També tindrem en compte en aquesta categoria als usuaris de casa, aquells que no tenen o tenen pocs coneixements sobre la ciberseguretat i els possibles atacs web que existeixen i que volen saber si les pàgines que visiten amb regularitat són tan segures com semblen a primera vista.

En quant a les empreses, les quals depenen molt de l'opinió dels seus usuaris i clients, en destacarem els equips de màrqueting[4], els quals són els encarregats d'analitzar les dades i desenvolupar estratègies per tal d'assolir els diferents objectius de l'empresa, definir campanyes que creen i milloren la imatge de l'empresa, entre d'altres. A més a més, tindrem en compte, tot i que en menor mesura, els SOCs[5], centres d'operacions de seguretat que ofereix un servei de monitoratge i anàlisi continuat a la seguretat a la xarxa i a Internet d'una organització; els grups d'administradors de sistemes i els grups d'investigació a les universitats que treballen amb projectes relacionats.

1.4 Justificació

Aquest projecte es centra en determinar, de forma fiable i ràpida, la reputació d'un domini segons l'opinió dels usuaris que el freqüenten. Creiem que aquest projecte és necessari degut a que, com ja s'ha explicat a la *Formulació del Problema* 1.2, existeixen serveis que proporciona aquest tipus de servei però són molt hermètics i centralitzats. Volem aportar un sistema on tothom pugui contribuir i vegin els efectes de les seves opinions al moment. El fet de recollir només l'opinió subjectiva dels usuaris es deu a que volem que més gent hi pugui participar, tan activament al votar o proposar dominis al sistema, com passivament al només consultar les reputacions computades.

Així doncs, els motius principals pels que es du a terme aquest projecte

[1] fragments de dades de la informàtica forense que identifiquen activitats potencialment malicioses en un sistema o una xarxa

són els usuaris normals; són aquelles persones que cada dia visiten moltes pàgines web, compren en botigues *online* o es comuniquen a través de les xarxes socials. Aquestes persones van deixant parts d'informació privada i sensible a totes i cadascuna d'elles sense cap tipus de preocupació o inquietud sobre què es va amb elles. Alguns d'aquests dominis poden, fins i tot, infectar-te l'ordinador de diferents formes, com ja s'ha mencionat breument a la *Formulació del Problema* 1.2, existeixen varis tipus d'amenaces web que afecten cada dia a diverses empreses.

Per tant, per una part, es vol conscienciar la gent dels possibles perills que s'amaguen cada dia a les pàgines web fent ús d'un sistema de reputació visual i consensuat mentre que, per una altra part es vol posar a prova la nova tecnologia *blockchain* creant una plataforma única on poder trobar tota la informació unificada sobre les reputacions dels dominis. La idea que es té en ment per fer aquesta plataforma fàcilment accessible a la gent que només vol consultar la informació, és mitjançant el desenvolupament d'un *plugin* pels diferents navegadors el qual indiqui la reputació de les pàgines web a les que s'accedeixen; però aquesta implementació és feina per un altre treball de recerca.

Un cop explicades les característiques conceptuals del projecte, passaré a comentar breument els trets tècnics:

- El *back end*[1] es vol crear des de 0 i es vol que sigui mínim; que la seva única feina sigui connectar la *blockchain* amb el *front end*.
- Referent a la tecnologia *blockchain*, es vol utilitzar una xarxa *blockchain* i es volen dissenyar *smart contracts* que controlin i gestionin tot el sistema.
- El *front end*[2] es vol implementar distribuït utilitzant IPFS[6] (de l'anglès, *InterPlanetary File System*), és un software de codi obert que permet l'emmagatzematge i compartiment de fitxers de forma distribuïda.

Informació més detallada sobre els conceptes teòrics i la implementació tècnica es pot trobar a mesura que s'avança en la lectura d'aquest informe.

[1] capa de d'accés a dades
[2] capa de presentació

1.5 Proposta de solució

En aquesta secció explicaré els conceptes en els que es basa el meu projecte amb més detall, així com la implementació que es vol dur a terme.

Una *blockchain*[7], també coneguda com DLT (de l'anglès, Distributed Ledger Technology), és un tipus especial de base de dades distribuïda. Les dades són emmagatzemades en blocs connectats un darrere l'altre formant una cadena. Cada bloc conté informació del bloc anterior un cop passada per funcions de *hash*[3]. De manera que totes les dades es troben replicades en forma de cadenes de blocs a tots els nodes[4] que conformen la xarxa *peer-to-peer*[5] d'una *blockchain*. Aquestes característiques fan que la xarxa pertanyi simultàniament a tothom i, per tant, que sigui resistent a les modificacions de dades. També, és evident que la descentralització dóna l'avantatge que si algú vol deixar la xarxa, és a dir, esborrar el seu node, la resta d'usuaris poden seguir oferint accés a la informació i compartir dades.
Existeixen *blockchain* de públiques i de privades (aquestes últimes utilitzades principalment en configuracions empresarials). Per la part de desenvolupament d'aquest projecte es proposa la utilització d'una *blockchain* pública, mentre que per la part teòrica final es proposa la implementació d'una *sidechain*[8], cadena de blocs alternativa, amb una programació i característiques completament diferents als blocs de la de la xarxa "mare"però que és compatible amb aquesta i es poden comunicar i complementar majors sense problemes.

Els *smart contracts*[9] són programes deterministes[6] que, donada una condició, executen una tasca en particular. Són utilitzats a les *blockchains* com a protocols de confiança per verificar negociacions d'un contracte. Amb l'aparició d'aquesta aplicació, desapareix la necessitat d'intermediaris i, com a conseqüència, es redueixen significativament els costos operacionals.

Trobareu més informació sobre aquestes tecnologies al capítol *Tecnologia Blockchain* 9 més endavant.

En un primer moment es vol realitzar aquest project sobre la *blockchain* d'Ethereum: EVM (de l'anglès, Ethereum Virtual Machine), degut a les avantat-

[3]donada una entrada de tamany variable i unes fórmules matemàtiques, proporcionen una sortida de tamany fixe
[4]màquines connectades a la xarxa
[5]grup de dispositius que emmagatzemen i comparteixen fitxers conjuntament
[6]algorismes predictius segons l'entrada

ges que proporciona que estigui desvinculada completament de la màquina amfitriona i a que sigui la més utilitzada per implementar aquest tipus d'aplicacions distribuïdes; però també es vol realitzar un estudi actualitzat sobre les diferents *blockchains* on es podria dur a terme el desenvolupament.
En quant al llenguatge en el qual s'escriuen els *smart contracts*, utilitzarem Solidity en cas d'escollir finalment la EVM; un llenguatge nou i senzill creat específicament per redactar *smart contracts* i que és el més utilitzat en aquesta *blockchain*.

En quant a com està implementat el *back end*, en aquest projecte es vol deixar que la part dominant de la plataforma sigui la *blockchain* i els *smarts contracts*, de manera que el *back end* serà mínim; la intenció és que faci les funcions de comunicació entre el *front end* i la *blockchain*.
En quant a com està implementat el *front end*, en aquest projecte es vol fer distribuït mitjançant el software mencionat anteriorment, IPFS.

Finalment i com a resum, per totes les raons donades fins ara al llarg d'aquest informe, es vol desenvolupar un nou servei de reputació de dominis basat en l'opinió tant professional com personal dels usuaris, implementat amb la nova tecnologia *blockchain*, que sigui realment obert a la consulta i col·laboració de tothom, que no estigui sotmès al control de cap empresa o entitat i que tingui la seguretat de que no es perdran les dades gràcies a la seva distribució de la xarxa.

Capítol 2

Projectes relacionats

Abans de determinar com es faria aquest projecte, es van investigar exemples d'altres projectes que implementessin un sistema de reputació utilitzant la tecnologia *blockchain*. Alguns d'aquells projectes, els que semblaven més interessants i els que van aportar algun tipus de decisió o proposta de solució, els comentarem breument en aquest capítol per a que els lectors es puguin fer una idea del nostre tren de pensaments fins a arribar a la solució definitiva.

2.1 Projecte #1

El primer projecte que volem comentar és *Rep on the block : A next generation reputation system based on the blockchain*, per *Richard Dennis* i *Gareth Owen* [10]; el qual tracta sobre un nou sistema de reputació per utilitzar als *E-Commerce*[1].

Aquest estudi proposa un nou sistema de reputació basat en la tecnologia *blockchain*. L'objectiu principal és definir una cadena de blocs completament nova la qual redueixi la càrrega i la inflació de la *blockchain* actual de Bitcoin mitjançant l'emmagatzematge de la reputació de les transaccions completades. La *blockchain* que proposen té dues finalitats: suportar atacs documentats prèviament a sistemes de reputació i proporcionar un sistema de reputació generalitzat que es pugui implementar a qualsevol xarxa. Per resoldre aquests problemes o inconvenients, proposen quantificar les reputacions eliminant l'opinió humana de la transacció. El seu sistema emmagatzema la reputació en una única dimensió on cada usuari deixarà un "1"per indicar que la transacció ha estat satisfactòria i un "0"altrament. El seu sistema classifica com a transacció positiva aquelles que l'usuari ha rebut el fitxer

[1]comerç electrònic

que ha sol·licitat.

D'aquest projecte s'ha incorporat la forma de votació, la qual, com s'explica al capítol de *Models* 10, les votacions es guarden amb un "1"si el domini és fiable i amb un -1"altrament. A més a més, gràcies a aquest projecte s'ha decidit que el sistema de reputació es vol fer bidireccional amb un rang de [-100, 100] i que es volia tenir en compte el criteri personal de l'usuari, a més a més del professional.

2.2 Projecte #2

El segon projecte que volem comentar és *IoT Public Fog Nodes Reputation System: A Decentralized Solution Using Ethereum Blockchain*[11]; el qual tracta sobre com aprofitar de forma més eficient el *foge computing* dels IoT (de l'anglès, *Internet of Things*.
La computació FOB és una arquitectura creada per mediar entre els servidors al núvol i els clients per tal de donar suport als dispositius IoTs. Aquests dispositius solen tenir una potència de càlcul força feble, un emmagatzematge mínim i unes capacitats de xarxa limitades. Els *fog nodes* ofereixen una font externa de potència de processament i d'espai d'emmagatzematge addicional.

Per tant, els dispositius d'IoTs han d'establir un nivell de confiança als *fog nodes* que utilitzen. Aquest projecte defineix una arquitectura que proporciona als dispositius els mitjans necessaris per escollir els nodes disponibles més adequats per cada dispositiu i acció. Així doncs, el sistema consisteix en els *fog nodes* a avaluar, els clients dels dispositius d'IoT que avaluen aquests nodes i la xarxa d'Ethereum i els contractes intel·ligents que regeixen la comunicació i la interacció entre nodes i dispositius connectats.

D'aquest projecte s'ha incorporat els factors que es tenen en les puntuació, els quals són la credibilitat dels votants i la reputació assignada als nodes. Com s'explica al capítol de *Models* 10, tenim en compte aquests dos factors també els quals hem adaptat a les nostres dades i hem creat el nostre propi algoritme que els computa.

2.3 Projecte #3

El tercer projecte a comentar és, en realitat, un treball de fi de màster anomenat *Towards a Decentralized Publication System: A Proposal Using Blockc-*

hain and P2P Technologies per *Viktor Jacynycz García* [12]; el qual tracta sobre la reputació aplicada a la investigació científica i els índexs d'impacte de les seves publicacions.

Aquest estudi proposa una blockchain a *Ethereum* on els investigadors puguin publicar els seus estudis i on els usuaris facin les funcions de revisors atorgant reconeixement a aquelles que considerin. A més a més, també es computa un sistema de reputació a aquest revisors, els quals poden aconseguir reconeixement que, de manera tradicional a les revistes científiques i les conferències normals, el procés de revisió es fa, en la majoria de casos, de forma completament anònima. D'aquesta manera es pretén fomentar revisions bones i entregades a temps i dissuadir a aquells revisors que no estiguin disposats a formar part d'un sistema honest, mitigant, en la major manera possible, el frau en les revisions i la rivalitat a la investigació.

D'aquest projecte s'ha incorporat el sistema de reputació dels usuaris, en el nostre cas dels votants el qual anava a ser ensenyat inicialment per pantalla a les adreces corresponents per evitar el frau tal com ho fa el projecte acabat d'esmentar però, al final s'ha decidit afegir com a terme per computar la credibilitat explicada al capítol de *Models* 10.

Capítol 3

Abast

En aquest capítol es defineixen els objectius que es volen assolir amb el desenvolupament d'aquest treball, així com els requeriments, tant funcionals com no funcionals, la metodologia a seguir i les eines de seguiment a emprar.

3.1 Objectius

L'objectiu principal d'aquest projecte és completar el desenvolupament d'un sistema de reputació de dominis a una *blockchain* amb *smart contracts*.

A més a més, també es vol incorporar un sistema de fiabilitat als votants, és a dir, als usuaris que participen activament aportant la seva opinió al sistema, de manera que afecti a les reputacions dels dominis als que voten.

Així doncs, desglossant els objectius una mica ens queden que els sub-objectius son:

- Emmagatzemar els dominis a la *blockchain*.
- Gestionar els vots dels usuaris als diferents dominis.
- Computar i associar una reputació a cada domini.
- Cercar els diferents dominis disponibles a la plataforma.
- Contribuir a la col·lecció de dominis del servei.
- Computar i associar un nivell de fiabilitat als votants.

3.2 Requeriments

3.2.1 Requeriments funcionals

Tot i que els requisits principals d'aquest projecte es defineixen a la secció 3.1, aquests es poden definir en dos punts:

- Mutabilitat i publicitat. Tant les empreses com els usuaris normals poden afegir i consultar dominis a la plataforma. Això permet eliminar el problema d'hermeticitat mencionat a la secció 1.2 d'aquest projecte.
- Accessibilitat a una base de dades que indica les reputacions de dominis donats segons el criteri dels usuaris dels quals també es té en compte la fiabilitat de les seves aportacions. Això permet eliminar l'inconvenient d'haver de visitar varies bases de dades o pàgines web, així com el procés d'informar-se en profunditat en ciberseguretat per part dels usuaris no professionals, com ja s'ha comentant a la secció 1.4 d'aquest projecte.

3.2.2 Requeriments no funcionals

Gràcies a la tecnologia *blockchain*, obtenim els següents requeriments no funcionals:

- Replicació de dades. Si un node de la xarxa falla, el servei no queda inhabilitat. Elimina el problema de centralitat mencionat a la secció 1.4.
- Restriccions a l'hora de fer *mala praxis*[1]. *Blockchain* compta amb les mesures de seguretat preventives per evitar el mal ús tant de la plataforma com de la informació que hi conté.

3.3 Obstacles i riscos

Com he mencionat a la secció 1.1 d'aquest projecte, sóc de l'especialitat de Computació, això fa evident que el meu coneixement sobre les xarxes és força bàsic i sobre la ciberseguretat és pràcticament nul. A més a més, la tecnologia *blockchain* és relativament recent i encara s'estan explorant les possibilitats que ofereix.

Un altre aspecte a tenir en compte i que és molt important és que estem

[1]terme que s'utilitza per referir-se a la responsabilitat professional pels actes realitzats amb negligència

vivint una pandèmia provocada pel virus *COVID-19*; aquest situació genera grans problemes a l'hora de reunir-me amb el meu equip, no només pel fet de que la presencialitat de les reunions ha quedat descartada, sinó que entre d'altres entrebancs, el fet de que algú es posi realment malalt pot afectar a la continuïtat del projecte.

Per últim, un cas poc probable però que també s'ha de tenir en compte és la completa desconnexió de la xarxa *blockchain* escollida, la qual impediria el desenvolupament i el funcionament de la plataforma.

Capítol 4

Metodologia

En aquest capítol es detalla la metodologia utilitzada per la realització d'aquest projecte, així com les mesures de validació i les eines de seguiment emprades per verificar l'assoliment dels objectius mencionats a la secció 3.1.

4.1 Metodologia i Validació

Degut a la modalitat del meu projecte esmentada a la secció 1.1, aquest estudi es realitza en relativament poc temps, per tant s'opta per emprar mètodes àgils [13], en concret Scrum [14].
Les avantatges d'aquesta metodologia són l'adaptabilitat i la flexibilitat que ofereix envers els diferents problemes o canvis que es puguin ocasionar al llarg del desenvolupament del projecte i, a més a més, permet maximitzar la productivitat alhora que optimitzar el temps.

En quant a la validació, aquesta es durà a terme a les reunions setmanals on es revisen els objectius que s'han assolit cada setmana i les modificacions necessàries sobre la planificació pertanyent a les setmanes restants del projecte.

4.2 Eines de seguiment

L'eina principal de seguiment del desenvolupament del projecte serà GitHub; el qual proporciona un servei d'emmagatzematge de codi i permet el control absolut sobre les diverses versions que es van realitzant.

Durant la realització del projecte es desplegaran diversos *smart contracts* a

la *blockchain* de proves els quals es podran consultar i analitzar en qualsevol moment.

Capítol 5

Planificació Temporal

El desenvolupament d'aquest projecte comença a finals de Febrer del 2021 amb la iniciació de l'assignatura de GEP i abasta fins el torn de lectura a finals de juny del mateix any.

5.1 Consideracions

Com ja s'ha mencionat anteriorment, aquest projecte es realitza íntegrament al centre universitari en modalitat A i, degut a la situació de pandèmia que estem vivint, és important destacar que les reunions setmanals amb l'equip es poden veure notablement afectades. A més a més, pels continguts donats a la meva especialitat, mai abans havia utilitzat o estudiat res relacionat amb les tecnologies que s'utilitzen en aquest projecte, fet que repercuteix en la duració de les tasques d'investigació i implementació que s'expliquen a continuació.

5.2 Planificació de les tasques

La duració d'aquest estudi s'ha estimat en, com a mínim, unes 450 hores les quals s'assignen a les tasques obtingudes de desglossar els objectius ja explicats a la secció 3.1, a més de les que es poden extreure del referent a la gestió del projecte en sí.
Aquestes tasques estan assignades en diferents *sprints*[1] els quals duen associats un *sprint planning*[2] just abans de començar l'*sprint* corresponent i un

[1] breu període de temps on un equip treballa per completar una quantitat de treball determinada

[2] l'equip decideix quin treball es farà durant l'sprint i com es farà

sprint review[3] just després d'acabar-lo.

5.2.1 Canvis respecte la planificació inicial

S'ha decidit afegir aquest apartat extra a la planificació ja que s'ha vist necessari comentar i comparar els canvis que han sorgit respecte al tema d'aquest projecte tenint en compte els objectius, les tasques originals i les que s'han acabat realitzant.

A continuació es descriuen les tasques que es van proposar en un primer moment juntament amb les seves assignacions temporals. A més a més, a cada apartat es comenta què s'ha modificat i què s'ha substituït específicament.

Per una mica de context, aquest estudi anava a ser inicialment una millora del treball de fi de grau del meu company Pau Risa Subirats, *Sistema de reputación en Internet basado en la tecnología blockchain*[15]. Conforme va anar avançant la investigació i es van anar incorporant canvis, es va arribar a la conclusió que aquest projecte tenia suficient identitat pròpia per no haver de plantejar-se com a continuació d'un altre. Tot i així és important mencionar-lo donat que molts canvis a la planificació han estat derivats d'aquest fet.

Finalment, tot i que s'utilitzen les mateixes tecnologies que al TFG del meu company, els elements que es guarden a la blockchain i com es gestionen ha canviat radicalment.
Per tant, part de la investigació que es va fer en un principi ha estat aprofitada correctament, però també s'ha hagut d'invertir temps extra en investigar els elements que han canviat. En quant a la planificació general, aquest projecte s'estima que s'ha endarrerit prop d'un mes i mig.

5.2.2 Descripció de les tasques

A continuació es descriuen en detall les tasques que estructuren els objectius. Una versió general i resumida de les estimacions de les tasques per *sprints* es pot visualitzar a la taula 5.5.

Gestió del projecte

Aquí s'inclouen les tasques del projecte que tenen relació amb la seva gestió i documentació: reunions d'equip, contextualització, abast, metodologia,

[3] l'equip demostra quina feina ha realitzat durant l'sprint

planificació temporal, estimació de pressupost, informe de sostenibilitat, avaluació de qualitat i redacció final.
És evident que aquesta tasca estarà present durant tota la realització del projecte ja que és dependent del treball que es realitza a cada *sprint* i s'estima de durarà unes 168h en total.

A continuació es mostren les hores dividides en les diferents subtasques igual que al diagrama de gantt 5.1, però a la taula resum hi apareixen totes recollides sota el nom de *gestió del projecte* per evitar fatigar al lector amb massa informació diferent junta.

Tasca	**Data Inici**	**Data Fi**	**Hores**
Contextualització	*06/04/2021	*14/04/2021	8h
Abast	23/02/2021	03/03/2021	6h
Metodologia	23/02/2021	03/03/2021	4h
Planificació	*15/04/2021	*20/04/2021	16h
Estimació de pressupost	09/03/2021	15/03/2021	6h
Informe de sostenibilitat	09/03/2021	15/03/2021	6h
Avaluació de qualitat	16/04/2021	18/06/2021	32h
Reunions d'equip	26/02/2021	18/06/2021	40h
Redacció Final	23/02/2021	21/06/2021	50h

Taula 5.1: Tasques de la gestió del projecte

El canvi de continguts del projecte ha afectat en major mesura a les tasques de *Contextualització*, ja que s'ha tornat a redactar la formulació del problema, a adaptar els actors implicats, a completar la justificació i a formular una proposta de resolució diferent; i de *Planificació*, ja que algunes de les tasques han canviat, s'han descartat i s'han proposat de noves, les quals han afectat a les assignacions temporals originals.

Per tant, la tasca de *Contextualització* es va refer sencera des a les dates que apareix a la taula 5.1, però les dates originals eren: 23/02/2021

- 03/03/2021. De igual manera, les dates originals de *Planificació* eren: 04/03/2021 - 08/03/2021.

Investigació de Blockchain

S'inclou la investigació del funcionament general de la tecnologia *blockchain* així com el funcionament en baix nivell de la *blockchain* específica escollida per implementar el sistema de reputació.
Aquesta tasca és independent, es realitza principalment a l'inici del projecte i s'estima que durarà unes 40h.

Aquesta tasca no s'ha vist afectada pel canvi de continguts del projecte degut a que s'ha continuat utilitzant aquesta tecnologia.

Investigació d'Smart Contracts

S'inclou la investigació sobre la implementació i funcionament d'*smart contracts* així com del llenguatge en el qual s'escriuen i de la cerca d'entorns de desenvolupament que facilitin la seva redacció i depuració.
Aquesta tasca és parcialment dependent a la *blockchain* escollida 5.2.2, es realitza tant a l'inici com durant el desenvolupament del projecte i s'estima que durarà unes 24h.

Aquesta tasca no s'ha vist afectada pel canvi de continguts del projecte degut a que s'ha continuat utilitzant aquesta tecnologia.

Investigació sobre NodeJS

Aquesta tasca inclou la investigació de com implementar un *back end* amb *NodeJS*[16], juntament amb els *frameworks* i paquets necessaris per comunicar el *front end* amb la *blockchain*, com ara *Express*[17] i *axios*[18].

Aquesta tasca és independent, es realitza a l'inici del projecte i s'estima que durarà unes 24h.

Aquesta tasca no s'ha vist afectada pel canvi de continguts del projecte degut a que s'ha continuat utilitzant aquesta tecnologia.

Investigació d'IPFS

S'inclou la investigació sobre la implementació d'un *front end* distribuït utilitzant aquesta eina de sistema de fitxers.

Aquesta tasca és independent, es realitza quan s'està prop de finalitzar la implementació del *back end* i s'estima que durarà unes 32h.

Aquesta tasca no s'ha vist afectada pel canvi de continguts del projecte degut a que s'ha continuat utilitzant aquesta tecnologia.

Desenvolupament de la Blockchain

Inclou el desplegament d'un node d'una xarxa *blockchain* local i del desenvolupament, desplegament i interacció d'*smart contracts* necessaris.
Aquesta tasca és dependent de les tasques: *Investigació de Blockchain* i *Investigació d'Smart Contracts* 5.2.2 i s'estima que durarà unes 120h.

Aquesta tasca es pot dividir en les següents subtasques:

Tasca	**Data Inici**	**Data Fi**	**Hores**
Desplegar xarxa Blockchain local	29/03/2021	29/03/2021	2h
Redactar Smart Contracts	29/03/2021	09/04/2021	36h
Interactuar amb Smart Contracts	09/04/2021	27/04/2021	50h

Taula 5.2: Tasques del desenvolupament de la Blockchain

Aquesta tasca s'ha vist afectada pel canvi de continguts del projecte ja que la redacció dels *smart contracts* s'ha hagut de modificar.

Desenvolupament del Back End

Inclou la instal·lació dels *frameworks* necessaris, a més a més de les respectives utilitzacions per desplegar el *back end* i comunicar el *front end* amb la *blockchain*.
Aquesta tasca és depenent de la tasca de *Desenvolupament de la Blockchain* i s'estima que durarà unes 80h.

Aquesta tasca es pot dividir en les següents subtasques:

Tasca	Data Inici	Data Fi	Hores
Desplegar Back End bàsic	28/04/2021	28/04/2021	2h
Connectar Back End amb Blockchain	28/04/2021	07/05/2021	32h
Connectar Back End amb Front End	08/05/2021	14/05/2021	18h

Taula 5.3: Tasques del desenvolupament de la Blockchain

Aquesta tasca no s'ha vist afectada pel canvi de continguts del projecte degut a que s'ha continuat utilitzant aquesta tecnologia.

Desenvolupament del Front End

S'inclou la implementació d'un *front end* que mostri el que s'emmagatzema a la *blockchain*. Aquesta tasca és dependent de les tasques de *Desenvolupament de la Blockchain*, *Desenvolupament del Back End* i *Investigació d'IPFS* 5.2.2 i s'estima que durarà unes 160h.

Aquesta tasca es pot dividir en les següents subtasques:

Tasca	Data Inici	Data Fi	Hores
Desplegar Front End bàsic	17/05/2021	17/05/2021	4h
Mostrar llistat dominis + info	18/05/2021	27/05/2021	32h
Mostrar llistat adreces votants + info	28/05/2021	02/06/2021	16h
Funcionalitat afegir dominis	03/06/2021	07/06/2021	12h
Funcionalitat votar dominis	08/06/2021	14/06/2021	20h
Funcionalitat cercar als llistats	15/06/2021	15/06/2021	4h

Taula 5.4: Tasques del desenvolupament de la Blockchain

Aquesta tasca s'ha vist afectada pel canvi de continguts del projecte ja que les dades que tracta la *blockchain* ja no són les mateixes així com tampoc ho és la forma de mostrar-les.

Testeig

S'inclou el testeig del servei sencer així com diferents probes de qualitat. Es reserven unes hores per si cal realitzar canvis o millores.
Aquesta tasca és dependent de les tasques de *Desenvolupament de la Blockchain*, *Desenvolupament del Back End* i *Desenvolupament del Front End* 5.2.2 i s'estima que durarà unes 40h.

Preparació de la lectura

S'inclou la defensa del projecte amb l'ajuda de la creació d'una presentació visual.
Aquesta tasca és dependent a la tasca *Testeig* 5.2.2 i s'estima que durarà 40h.

Tasca	**Secció**	**Data Inici**	**Data Final**	**Hores**
Gestió del projecte	5.2.2	23/02/2021	21/06/2021	168h[4]
Investigació Blockchain	5.2.2	08/03/2021	12/03/2021	40h
Investigació Smart Contracts	5.2.2	15/03/2021	17/03/2021	24h
Investigació de NodeJS	5.2.2	18/03/2021	22/03/2021	24h
Investigació d'IPFS	5.2.2	23/03/2021	26/04/2021	32h
Desenvolupament de la Blockchain	5.2.2	29/03/2021	27/04/2021	88h[5]
Desenvolupament del Back End	5.2.2	28/04/2021	14/05/2021	52h[6]
Desenvolupament del Front End	5.2.2	17/05/2021	15/06/2021	88h[7]
Testeig	5.2.2	16/06/2021	22/06/2021	40h
Preparació torn de lectura	5.2.2	23/06/2021	29/06/2021	40h

Taula 5.5: Taula resum d'estimacions de tasques per sprints

[4]Les hores desglossades en subtasques es poden veure a la taula 5.1
[5]Les hores desglossades en subtasques es poden veure a la taula 5.2
[6]Les hores desglossades en subtasques es poden veure a la taula 5.3
[7]Les hores desglossades en subtasques es poden veure a la taula 5.4

5.3 Recursos

Els recursos necessaris per dur a terme aquest projecte els diferenciarem en dos tipus:

Entre els *recursos humans* en destaquem 4: l'estudiant, el qual és el principal realitzador d'aquest projecte, el ponent i doctorand els quals orienten a l'estudiant i l'ajuden amb el seu coneixement profund sobre el tema; i el tutor, el qual ajuda a que la documentació on es descriu tot el desenvolupament del projecte estigui ordenat i sigui fàcil de llegir i entendre.

Entre els *recursos materials* en destaquen un equip informàtic i totes aquelles eines software que ajuden a la gestió i documentació del projecte.

En quant al desenvolupament d'*smart contracts*, en destaquen els relacionats amb la instal·lació d'un entorn amb una xarxa de *blockchain* local, els *IDEs*[8] que facin més fàcil el procés de redacció i interaccio amb els *smart contracts* i altres softwares relatius.
En quant a la implementació del *back end*, en destaquen aquelles relacionats amb el desplegament del *back end* i la comunicació amb el *front end* i la *blockchain*.
En quant a la implementació del *front end*, en destaca el software IPFS i els IDEs que facilitin el procés de programació de la pàgina web.

5.4 Diagrama de Gantt

El diagrama de Gantt es pot trobar a les figures 5.1 i 5.2, ambdues en format horitzontal. S'ha considerat que cada dia es treballen 8h excepte a les tasques de desenvolupament a les quals es treballa 4h i que els dies marcats com a festius al calendari de la facultat són no lectius.

[8] un entorn integrat de desenvolupament

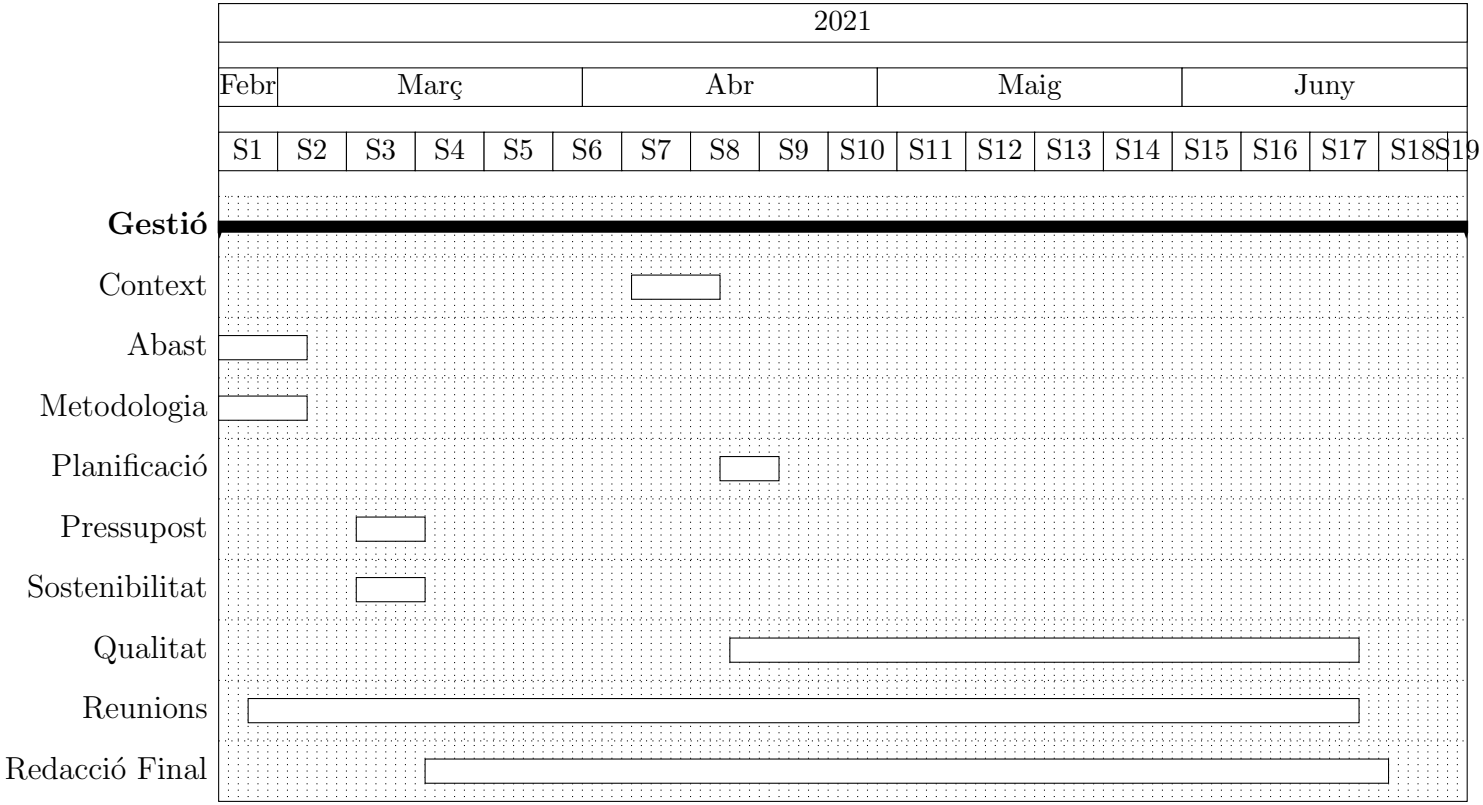

Figura 5.1: Diagrama de Gantt: Gestió del projecte

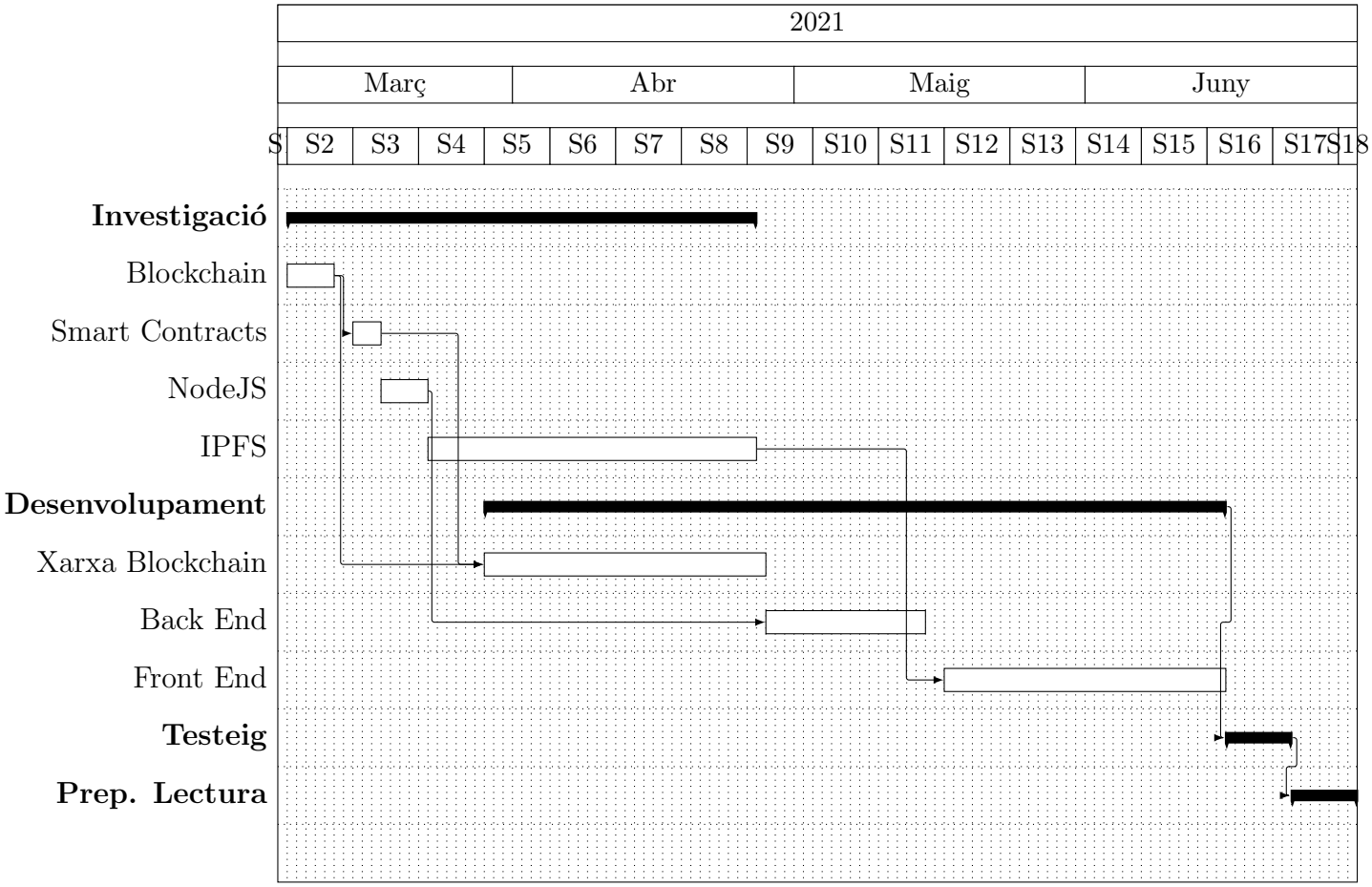

Figura 5.2: Diagrama de Gantt: Investigació i Desenvolupament

5.5 Gestió de riscos

A continuació es tracten els diferents riscos que s'han esmentat al llarg d'aquest informe, a més a més, aquell que sorgeix d'una planificació poc acurada.

En quant a la situació de pandèmia que estem vivint, el risc d'endarrerir la realització del projecte és real. La dificultat de poder reunir-me amb els meus orientadors pot afectar notablement a la planificació. Per altra banda, al ser l'única persona responsable del desenvolupament de la plataforma, puc dedicar el temps dels dies no lectius si calgués per tal de no provocar canvis grans a la planificació.

En quant a la completa desconnexió de la xarxa *blockchain* escollida, el risc és realment baix. Tot i així, donat el moment, es pot crear una *blockchain* local que perpetués el servei i, com a la *blockchain* original, també es podrien continuar utilitzant *smart contracts*. Finalment i, si es desitgés, es podria distribuir aquesta cadena com a una *sidechain*[8] de la xarxa escollida de manera que es pogués accedir de forma global.

En quant a tenir una planificació incorrecta, el risc és mitjà. Durant un projecte poden aparèixer molts inconvenients que afecten al seu desenvolupament. En cas que aquesta situació succeeixi, a l'informe final s'explicaran els motius pels quals el projecte s'ha desviat de la planificació inicial i es redactaran com s'haurien desenvolupat aquelles tasques que no s'han pogut realitzar, els possibles problemes que hi podrien haver sorgit i com s'haurien abordat.

Capítol 6

Pressupost

En aquest capítol s'explica com està distribuït el pressupost acordat per dur a terme aquest projecte, així com un pla de contingència en cas que apareguin desviacions.

En distingirem 4 costos: humans, de hardware, de software i generals. A la taula 6.6 es pot veure la distribució resumida del pressupost per cada secció mencionada.

Per calcular les amortitzacions dels pressupostos que ho requereixen s'ha fet servir la formula següent:

$$Amortització = \frac{Valor\ inicial - Valor\ residual}{Temps\ de\ vida\ útil\ esperat} \tag{6.1}$$

6.1 Despeses humanes

Aquest projecte està desenvolupat íntegrament per una sola persona amb l'orientació i guia del director i el doctorant.

A continuació es mostra una taula amb els diferents rols que adopta aquesta persona al llarg del desenvolupament del projecte, juntament amb les tasques que realitza, les hores respectives i el sou pertanyent.

Rol	**Tasques**	**Hores**	**Sou (€/h)**	**Total (€)**
Gestor de projecte	5.2.2 5.2.2	208	51 [19]	10.608

continua a la següent pàgina

Tècnic blockchain	5.2.2 5.2.2 5.2.2 5.2.2 5.2.2	304	13 [20]	3.952
Desenvolupador web	5.2.2 5.2.2	184	20 [21]	3.680
Tester	5.2.2	40	16 [22]	640
Total	5.2.2	736	-	18.880

Taula 6.1: Pressupost humà

6.2 Despeses de software

Durant el desenvolupament d'aquest projecte s'utilitzen diversos serveis a les tasques relatives al desenvolupament. Tots ells són softwares lliures[1] o gratuïts però, per si de cas, s'ha destinat una part del pressupost a aquesta secció explicada a l'apartat de control gestió de riscos 6.5.

Servei	**Temps útil**	**Total (€)**	**Amortització (€)**
Github	Infinit	0	N/A
Hardhat	Infinit	0	N/A
MetaMask	Infinit	0	N/A
Remix	Infinit	0	N/A
SublimeText	Infinit	0	N/A
IPFS	Infinit	0	N/A

Taula 6.2: Pressupost software

[1] programari que pot ser usat, estudiat i modificat sense restriccions

6.3 Despeses de hardware

Totes les tasques del desenvolupament d'aquest projecte es duen a terme al meu ordinador personal de sobretaula que està muntat per peces. Tenint en compte això, el temps útil va variant segons les peces que el componen, les quals es poden anar reemplaçant independentment. Tot i així, s'ha decidit estimar una vida útil de 6 anys i s'ha pres com a 0 el valor residual ja que aquest mateix ordinador pot ser utilitzat per fer altres projectes, o mantenir l'actual, en un futur.

Hardware	**Temps útil**	**Total (€)**	**Amortització (€)**
PC sobretaula	6 anys	1.400	$233,\widehat{33}$

Taula 6.3: Pressupost hardware

6.4 Despeses generals

Degut a que el desenvolupament d'aquest projecte es realitza al meu habitacle en comptes de a la universitat o a una empresa, tindrem en compte els costos personals per calcular les despeses d'electricitat, d'Internet i d'aigua.

Recurs	**Temps (mesos)**	**Preu (€)**	**Total (€)**
Electricitat	4	150/2mesos	300
Internet	4	40	160
Aigua	4	30	120
Total	4	-	580

Taula 6.4: Pressupost general

6.5 Control de gestió

Aquest projecte té una sèrie de riscos que ja s'han mencionat anteriorment 5.5 i que podrien provocar variacions en els pressupostos contemplats. Per tant, a continuació s'expliquen les mesures que es poden prendre en cas de necessitat per mitigar aquestes desviacions.

El primer obstacle i risc clar a considerar és la inexperiència del desenvolupador, és a dir, la meva. És un risc real i és, alhora, el recurs que té una despesa més gran. Aquest, juntament amb la situació de pandèmia que estem vivint, poden afectar greument a la *deadline*, i això, afecta directament als pressupostos computats. La possibilitat d'haver d'allargar el desenvolupament del projecte fins al torn de lectura a l'octubre pot costar fins a uns altres 4 mesos. Tot i així, el fet de que es necessités el doble del temps estimat per acabar aquest projecte és força inversemblant, per tant, es reservarà un 20% de les despeses humanes ja computades 6.1 per poder proporcionar un temps de gràcia en cas que sigui necessari.

Amb la distribució de pressupost, apareixen nous riscos que també s'han de contemplar.

En quant al software, en un primer moment es pretén utilitzar software lliure com s'ha explicat a la secció 6.2. Tot i així, es reservarà un 5% de les despeses humanes en cas que es necessiti llogar algun tipus de servei o llicència pel desenvolupament del projecte.
En quant al hardware, cap la possibilitat de que qualsevol de les peces que conformen el meu ordinador s'espatlli i s'hagi de reemplaçar. El risc és relativament baix degut a que aquest ordinador es va muntar fa aproximadament 3 anys, és a dir, ara es troba a la meitat de la seva vida útil estimada a 6.3. Tot i així es destinarà un 5% de les despeses humanes.

Incident	**Risc (%)**	**Preu (€)**
Inexperiència + Deadline	50	3.776
Recursos software	15	944
Recursos hardware	20	944
Total	-	5.664

continua a la següent pàgina

Taula 6.5: Pressupost per riscos

6.6 Despeses totals

A continuació es mostren de manera resumida totes les despeses computades fins ara.

Despeses	**Total (€)**
Humanes	18.880
Software	0
Hardware	1.400
Generals	580
Contingència	5.664
Total	26.524

Taula 6.6: Pressupost total

Capítol 7

Sostenibilitat

El terme *sostenibilitat* sembla conegut per tothom. És una paraula comú que qualsevol persona pot identificar, però que poques reflexionen realment sobre les implicacions del grau de sostenibilitat d'un projecte.

Reconec que fins i tot jo mateixa vaig cometre un error, que crec que està força estès a la comunitat d'enginyers, quan vaig començar a redactar aquesta part de l'informe. Sota la meva opinió personal, crec que tot enginyer, almenys aquells que estan prop d'acabar la carrera o que just l'han acabada, tenen la predisposició a *justificar* els impactes de negatius que tenen el projectes als quals hi participen, però només una minoria pensa en com *mitigar* aquests impactes, en com trobar desenvolupaments alternatius, en com comptectar amb empreses que proporcionin serveis més sostenibles tot i que repercuteixi al pressupost. Molts pensen, que els impactes en les diferents dimensions de la sostenibilitat són fixes, un dany col·lateral que han de justificar el millor possible per a que el cap de departament doni el vist i plau al projecte i puguin començar amb el desenvolupament.

Si observem les notícies, sempre hi ha alguna secció on es parla de com ens estem carregant el planeta, de com el recursos que estem gastant són limitats, de com ens estem apropant cada dia que passa al punt de no retorn, si no l'hem passat ja. Però no veig iniciatives a solucions, veig gent queixant-se, em veig a mi mateixa dubtant a l'hora de separar escombraries als diferents contenidors. No veig iniciatives a les escoles, no veig iniciatives a les universitats, no veig iniciatives a les empreses. I no estic parlant només de campanyes d'actuació i conscienciació, sinó de campanyes d'informació.

M'he adonat, gràcies a aquesta secció, que els meus coneixements sobre la sostenibilitat són, francament, quasi inexistents i, sincerament, no sabria ni

per on començar a informar-me. Tot projecte té una fase inicial de recerca, la qual és completament indispensable i des de la qual es partirà el seu desenvolupament. Bé, no podem esperar que la humanitat s'involucri activament en la reducció dels diferents impactes relacionats amb la sostenibilitat si no els proporcionem primer el temps i els recursos necessaris per a que s'informin. Sinó, el que obtenim és un projecte a mig fer, amb necessitat d'un manteniment constant i amb opcions a millores molt escurçades, exactament com tenim ara el nostre estimat planeta.

7.1 Impacte ambiental

El gran impacte ambiental que té aquest projecte és innegable. El manteniment de les *blockchain* avui dia continua necessitant molta quantitat d'energia, tot i que s'estima que en els pròxims anys, aquesta energia necessària vagi disminuint i, fins i tot, acabi sent menor inclús que la de servidors centralitzats.

Les *blockchains* que treballen amb PoW (de l'anglès, *Proof of Work*) consumeixen més que les que treballen en PoS (de l'anglès, *Proof of Stake*) degut a la complexitat del problema matemàtic que afronten; aquests termes s'explicaran en detall més endavant en aquest informe. Així que s'espera que moltes *blockchains* migrin de protocol en un futur proper.

7.2 Impacte econòmic

L'impacte econòmic d'aquest projecte està detallat i justificat al capítol 6. Inicialment pot semblar que per la curta durada del desenvolupament, el cost és elevat i, probablement no valgui la pena, però si desglossem les diverses despeses veurem que la majoria són humanes.

A més a més, degut a la branca en la que es desenvolupa aquest projecte, la ciberseguretat, la seva vida útil és molt llarga, i, al estar implementada de forma distribuïda, l'amortització està assegurada.

7.3 Impacte social

L'impacte social d'aquest projecte està detallat al capítol1 i, realment és el motiu principal pel qual es vol dur a terme. Es vol solucionar el problema de l'accés restringit que existeix avui dia a les reputacions de les pàgines web.

En definitiva, aquest projecte ajudarà a tothom qui vulgui col·laborar en l'emmagatzematge i computació de reputacions, sense restriccions de dominis i de manera gratuïta. Volem impulsar la cooperació de tota la comunitat de la ciberseguretat per crear i mantenir un front comú contra els ciberatacs alhora que eduquem la població més desconnectada d'aquest món o, almenys, els intentem protegir.

Capítol 8

Problemes i inconvenients

Durant l'avanç d'aquest projecte ens hem trobat amb varis problemes i inconvenients que han modificat la planificació i la el procés de desenvolupament d'aquest projecte.

Principalment, la pandèmia ha fet que els professors tinguin més feina de forma remota i els hi sigui més difícil coordinar-se. Aquesta situació no afecta només als professors, sinó que als alumnes com jo, els quals han fet les últimes assignatures juntament amb el TFG, dificulta el poder reunir-se tant amb altres companys com amb professors.
Aquest projecte no ha sortit impune d'això, les reunions s'han anat establint cada dues setmanes en comptes de cada una. Això juntament amb el fet que no es tenia del tot clar des d'un principi com es volia enfocar el projecte i que cap dels integrants de l'equip tenia una coneixement gaire ample sobre les tecnologies utilitzades, la planificació ha estat, malauradament, molt poc acurada.

Els problemes i inconvenients han provocat que haguem de rescindir de desenvolupar un *front end* distribuït amb IPFS explicada a la tasca 5.2.2. La plataforma s'ha implementat finalment utilitzant el *framework* de React[23] i de manera centralitzada.

Capítol 9

Tecnologia Blockchain

En aquest capítol s'expliquen en profunditat els conceptes que s'han anat mencionat al *Context* 1 d'aquest informe i es detalla com s'ha fet el desenvolupament del projecte.

Abans de començar, però, volem comentar els beneficis d'utilitzar aquesta tecnologia per desenvolupar el nostre sistema i no qualsevol altra que també implementés un sistema d'emmagatzematge distribuït com ara IPFS[6]:

- Robustesa: el mètode d'emmagatzematge en forma de blocs (s'explica més en detall en la següent secció) sincronitzats entre ells de forma cronològica, fa que sigui impossible que un individu controli la informació que s'hi guarda, fent així que la *blockchain* sigui altament segura.
- Xarxa descentralitzada: la informació emmagatzemada és emesa per tota la xarxa al mateix temps fent que no hi hagi cap autoritat central com passa als sistemes més tradicionals.
- Immutabilitat: un cop un bloc és segellat criptogràficament o afegit a la cadena principal, és impossible esborrar-lo o editar-lo.
- Transparència: els usuaris poden verificar i seguir en tot moment tant les seves transaccions com totes les altres transaccions que s'han fet a la *blockchain*.

Per aquest motius volem oferir un sistema de reputació de dominis transparent però segur. Fet que mitjançant mètodes més tradicionals i centralitzats podríem patir d'atacs i de no transparència, mentre que utilitzant altres mètodes distribuïts gratuïts podríem patir de frau a les votacions i no volem que els usuaris pensin que estem modificant els resultats ni volem que els seus vots siguin no conscienciats. Volem representar l'opinió honesta dels usuaris que utilitzen Internet diàriament.

9.1 Blockchain

Com ja s'ha mencionat a la secció de *Proposta de Resolució* 1.5, una *blockchain*[24] és una estructura de dades on la informació es troba emmagatzemada en forma de *blocs* els quals estan connectats entre ells per mitjà de la criptografia. Les principals característiques per les que aquesta tecnologia s'està expandint tan ràpidament són que, un cop s'ha determinat com s'afegeixen dades al sistema i aquestes han estat emmagatzemades, són impossibles de modificar o eliminar de forma virtual.

Els blocs mencionats estan construïts mitjançant, no només la informació pertanyent a les dades noves, sinó també informació en forma de *hash* del bloc que s'ha construït anteriorment, de manera que queden vinculats. Si ens imaginem la replicació infinita d'aquest procés, podem veure similituds amb una *cadena* (*"blockchain"*, en anglès), d'aquí el nom d'aquesta manera metodologia d'emmagatzemar dades.

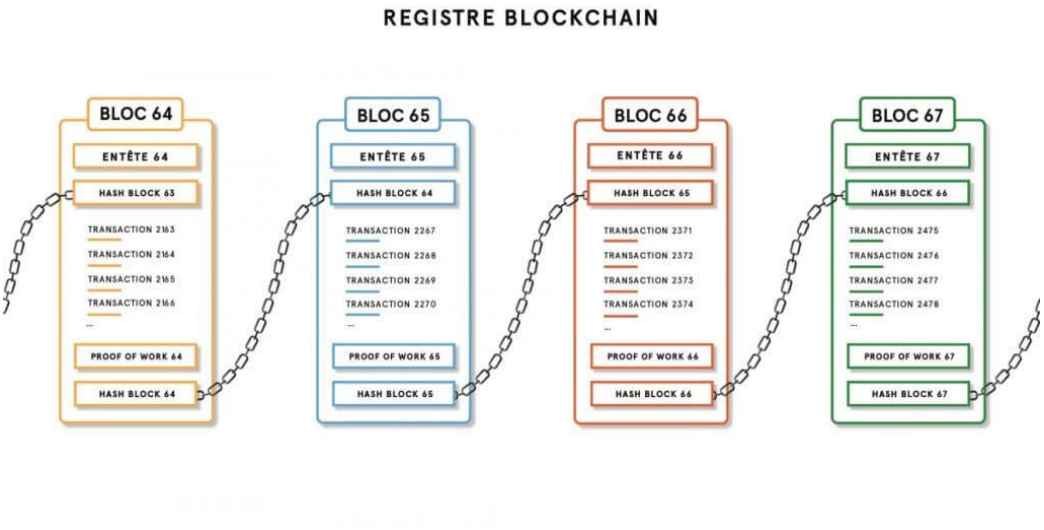

Figura 9.1: *Font extreta de [25].* Representació visual dels blocs a una blockchain

Un cop explicada l'estructura bàsica de *blockchain*, no sembla un concepte tan interessant i innovador, però la veritat és que els usuaris d'aquesta tecnologia no es queden per la forma d'emmagatzemar les dades, sinó per l'ecosistema que representa. Aquesta tecnologia[26] és compartida, immutable i no es troba sota el control de ningú. Cap actor no té la potestat suficient com

per editar els *inputs* mentre es salta les normes establerta anteriorment (en parlarem més en detall d'això quan arribem als *smarts contracts*). Mirant-ho des d'un altre punt de vista, podríem entendre que tothom té possessió de la xarxa de manera simultània i que tots es regeixen sota un algoritme de consens. D'aquest mecanisme en parlarem més en detall en la *blockchain* escollida.

Per últim, queda parlar dels *nodes*, aquests són, senzillament, els dispositius encarregats de validar les transaccions de cada bloc, mantenir còpies precises de la informació que hi ha emmagatzemada a la xarxa i compartir-la amb la resta d'unitats del sistema.

9.2 Ethereum

Ethereum[27] és una plataforma *open source*[1] descentralitzada a on es poden programar *smart contracts*. A diferència d'altres plataformes similars, Ethereum és programable, és a dir, permet que desenvolupadors arreu del món puguin utilitzar-la per crear tot tipus d'aplicacions descentralitzades (*dapps*) les quals obtenen els beneficis tant de la criptomoneda com de la tecnologia *blockchain*.

La criptomoneda nativa d'Ethereum es diu Ether. El seu propòsit principal consisteix en permetre l'existència d'un mercat per la computació. Aquest mercat, proporciona al seu torn un incentiu econòmic pels agents que verifiquen i/o executen sol·licituds de transaccions i proporcionen recursos computacionals a la xarxa.

Ethereum es regeix per l'algorisme de consens anomenat PoW (de l'anglès, *Proof of Work*. PoW[28] és un protocol que requereix que els agents que volen afegir nous blocs a la cadena resolguin un problema computacional d'una determinada dificultat i que requereix d'una potència computacional específica. Al resoldre aquest problema, queda validat el bloc de transaccions i l'agent en qüestió és recompensat amb Ethers.
Aquest procés és conegut al món de les criptomonedes com *minar* i els agents que el duen a terme són denominats *miners*.

Abans de comentar què entén Ethereum com a transacció, hem de poder distingir els dos tipus de contes que contempla: *externally owned*, és a dir,

[1] de codi obert

controlada per qualsevol que tingui possessió de les claus privades; i de contracte, és a dir, un *smart contract* que ja ha estat desplegat a la xarxa. Ambdós tipus poden rebre, mantenir i enviar Ethers i *tokens*[2] i poden interactuar amb *smart contracts* un cop desplegats.
Les principals diferències, a part dels costos que comporta crear les comptes (les *externally owned* són gratis mentre que les de contractes valen diners degut a que utilitzen emmagatzematge de la xarxa), tenen relació amb com interactuen amb les transaccions: les *externally owned* poden iniciar transaccions, mentre que les de contractes només poden enviar transaccions en resposta a rebre una transacció; les transaccions entre dues comptes *externally owned* només poden ser de transferència de Ethers mentre que les transaccions entre un compte *externally owned* i un de contractes pot executar codi, el qual pot dur a diferents accions, des de transferir *tokens* fins desplegar nous contractes.

Per últim, Ethereum entén com a transacció totes aquelles accions que són iniciades per un compte *externally owned*, no d'un de contracte. Aquestes requereixen d'una *fee* (quota, de l'anglès) anomenada *gas* i han de ser minades per ser vàlides. Aquest *gas* varia depenent de la dificultat computacional del problema a resoldre i és la recompensa que obtenen els miners de la xarxa.

S'ha decidit utilitzar Ethereum per implementar aquest projecte degut a que és la més estesa en aquest camp i, per tant, de la que més informació relacionada i exemples d'altres projectes hi trobarem. D'aquesta manera, s'intenta reduir el risc de la inexperiència del desenvolupador esmentada a la secció 5.5.

9.2.1 Hardhat

Hardhat[29] és un entorn de desenvolupament per compilar, desplegar, testejar i debugar softwares d'Ethereum. Aquest entorn consta de 3 parts principals: una xarxa local d'Ethereum que permet córrer l'EVM, el desenvolupament d'*scripts* que permeten diverses funcionalitat com ara desplegar *smart contracts* a la xarxa de proves i, per últim, el desenvolupament de testos que permeten validar el bon funcionament de les funcions dels *smart contracts*.
En definitiva, Hardhat és un software útil a l'hora d'aprendre com funciona la tecnologia *blockchain* i els *smart contracts* sense necessitat d'anar directament a una xarxa de test d'una plataforma definitiva.

[2]altres tipus de monedes virtuals o criptomonedes

9.2.2 Metamask

MetaMask[30] és una extensió de navegadors que fa les funcions d'una *wallet* (çartera", en angès) de criptomonedes que connecta a la *blockchain* d'Ethreum. Aquest *software* permet als usuaris connectar amb les *dapps* d'Ethereum sense haver de descarregar tot l'ecosistema de la *blockchain*. Degut a aquesta característica, és una de les *wallets* més populars entre les carteres que accedeixen a *DEX* (de l'anglès, *descentralized exchanges*, plataformes *gaming*, pàgines de jocs d'atzar i altre tipus d'aplicacions.

A més a més, utilitzarem Metamask[31] per connectar *Remix*9.3.1 i la nostra *blockchain* local amb *Hardhat*. Només ens caldrà importar les comptes que genera aquest darrer entorn. També es poden desplegar els *smart contracts* a les diferents xarxes de proves d'Ethereum mitjançant *Metamask*, així com a la *mainnet*.
En aquest projecte s'ha utilitzat la *testnet* de Kovan[32] per fer els testos.

9.3 Smart Contract

Els *smart contracts* són, a l'àmbit de les criptomonedes, programes que s'executen a una *blockchain* i que actuen com a acords digitals que obliguen als usuaris a seguir una sèrie de regles específiques. Aquestes instruccions estan predefinides a un codi que és replicat i executat per tots els nodes de la xarxa.

Com ja s'ha explicat anteriorment, Ethereum identifica els *smart contracts* com un tipus de compte. Això vol dir que tenen un *balance* propi, és a dir, una quantitat de *tokens* i poden enviar transaccions a la xarxa. Aquestes comptes no estan controlades per cap usuari sino que estan desplegades a la xarxa i s'executen com estan programades. Les comptes d'usuari poden interaccionar amb elles mitjançant transaccions que executen funcions predefinides als *smart contracts*. Aquests poden definir regles, com un contracte normal i aplicar-les automàticament mitjançant codi.

Qualsevol usuari pot programar *smart contracts*, els únics prerequisits són: desenvolupar en els llenguatges acceptats per la xarxa i tenir Ethers suficients al compte de l'usuari, això és degut a que desplegar un *smart contract* compta com una transacció i, les transaccions tenen *fees* associades que s'han de pagar, com ja s'ha mencionat anteriorment.
En aquest projecte s'utilitzat *Solidty* per programar els diversos *smart contracts*.

La composició dels *smart contracts* és molt escalable degut a que es poden utilitzar com APIs (de l'anglès, *Application Programming Interface*). Aquest fet permet que es puguin cridar funcions d'altres contractes dins del teu contracte i, inclús, és possible desplegar altres contractes. Ambdues funcionalitats les veurem en acció a la secció dels models implementats.

Evidentment i, com tota tecnologia, els contractes intel·ligents tenen limitacions. Entre les principals en destaquem que no poden rebre informació de l'exterior, és a dir, no es poden enviar peticions HTTP. Aquesta decisió es va prendre durant el seu disseny degut a que es va considerar que el fet d'obtenir informació sobre el món exterior podria posar en perill el protocol de consens, el qual és realment important per la seguretat i la descentralització del sistema.

En relatiu al procés de desenvolupament, quan volem programar *smart contract* hem de tenir clars que: totes les dades que guarden a un *smart contract* prenen el nom d'*estat* i que tot canvi referent a l'estat d'un *smart contract* costa diners, donat que estàs modificant l'espai d'emmagatzematge de la xarxa.

9.3.1 Remix

Remix[33] és un IDE (de l'anglès, *Integrated Development Environment* que permet el desenvolupament, desplegament i administració d'*smart contracts* per Ethereum. A més a més, ofereix interaccions amb *smart contracts* de manera molt visual i, degut a la inexperiència del desenvolupador, s'ha decidit fer ús d'aquest software tot i que no aporta cap funcionalitat que no es pugui realitzar amb l'entorn Hardhat.

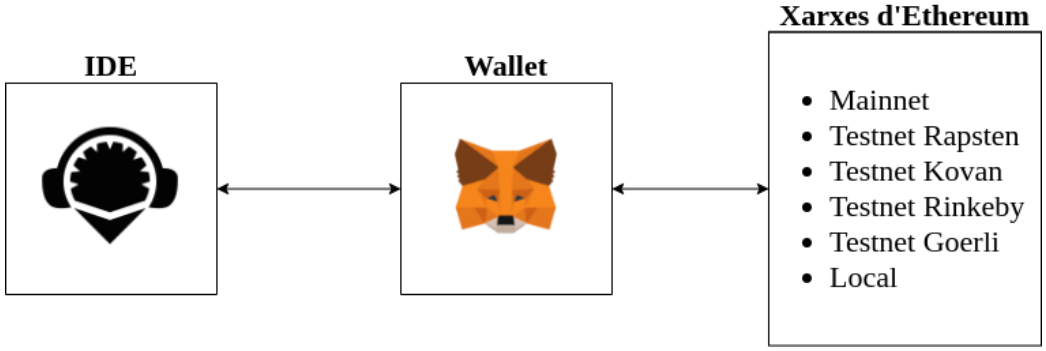

Figura 9.2: *Elaboració pròpia.* Estructura comunicació amb la xarxa

Capítol 10

Models

Entrant en més detall que a la *Proposta de resolució* 1.5, en aquesta capítol s'expliquen quins i com són els models que s'han implementat i quina metodologia s'ha seguit per realitzar els testos necessaris.

Inicialment es vol afrontar el problema explicat a la secció 1.2 amb un sistema de reputacions de dominis amb les següents funcionalitats:

- *Qualsevol usuari pot afegir un domini al sistema.
- *Qualsevol usuari pot votar, tant positivament com negativament, un domini que ja estigui afegit al sistema.
- Qualsevol usuari pot veure el llistat de dominis al sistema, juntament amb la seva reputació i amb la fiabilitat dels votants que l'han votada.
- Qualsevol usuari pot veure el llistat de votants que han votat mai al sistema, juntament amb el llistat de dominis que han votat.

La fiabilitat dels dominis es computa com la mitja de les fiabilitats dels votants que l'han votat. Aquestes es computen al *backend* i té en compte 2 factors: la credibilitat dels votants, la qual es valora tenint en compte la quantitat de dominis que s'han votat respecte un valor màxim de dominis que s'ha predefinit; i la reputació dels votants, la qual té en compte que el vot individual de cada votant coincideixi amb la reputació general del domini.
La reputació dels dominis es computa tenint en compte la suma dels valors de les votacions i el número total de votacions.

Les funcionalitat marcades amb un (*) són les que modifiquen l'estat del/s *smart contract/s*, és a dir, són les que costen diners. Així doncs, s'han implementat models diferents segons sobre quin tipus d'usuari recau el cost econòmic d'aquestes interaccions.

10.1 Model #1

Aquest model s'ha implementat seguint el procediment més comunament usat per aplicacions distribuïdes que s'han creat anteriorment a aquest projecte. Consisteix en un únic *smart contract* el qual emmagatzema una llista de dominis i una llista de votants. Així doncs, al següent fragment de codi podem veure l'estat d'aquest contracte intel·ligent.

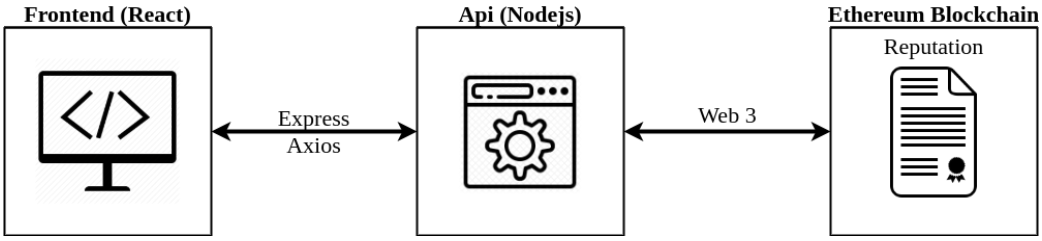

Figura 10.1: *Elaboració pròpia.* Estructura del Model #1

```
contract Reputation {
    struct Voter {
        address addr;           // person ho has voted
        string[] urlsVoted;     // urls voted by that person
        int[] votes;            // votes recorded
    }

    struct URL {
        string name;            // doains's name
        int256 reputation;      // raw reputation
        uint256 votes;          // number of votes received
    }

    URL[] urlList;              // llistat de dominis
    Voter[] voters;             // llistat de votants


    constructor() {
        console.log("Welcome to URL reputation system");
    }

    ...
}
```

De les funcionalitats implementades, en destaquen aquelles que modifiquen l'estat del contracte: les funcions d'afegir un nou domini al sistema i

de votar un domini que ja estigui emmagatzemat a la *blockchain*. Al següent fragment de codi es mostren les funcions descrites.

```
contract Reputation {
    ...

    //afegim el nou domini a la llista de dominis
    function addURL (string memory _url) public {
        //comprova que la URL introduida no es trobi ja
    emmagatzemada al sistema
        checkURL(_url);
        urlList.push(URL({
            name: _url,
            reputation: 0,
            votes: 0
        }));
    }

    //actualitzem la quantitat de vots i lestat de la
    reputacio en cru, tambe es guarda el valor del vot
    function vote (string memory _url, bool _vote) public {
        //comprova que la URL que es vol votar esta afegida
    al sistema i retorna la seva posicio al llistat de domini
        uint i = getURL(_url);
        //retorna la posicio del votant al llistat de votants
        uint v = getVoterIndex(_url);
        urlList[i].votes++;
        if (_vote) {
            urlList[i].reputation++;
            voters[v].votes.push(-1);
        }
        else {
            urlList[i].reputation--;
            voters[v].votes.push(-1);
        }
    }

    ...
}
```

Com podem veure, guardem el vot del votant per poder calcular, al *backend*, la fiabilitat de les reputacions del domini, com ja s'ha mencionat abans.

El pes econòmic principal d'aquest model recau sobre el votant. Tot i que és cert que desplegar l'*smart contract* recau sobre nosaltres (l'equip del projecte), es contempla com un cost que forma par del desenvolupament del

projecte. De cara a l'usuari interessat en contribuir, creiem que els costos (el de votar i el d'introduir dominis), pot fer que disminueixi notablement l'al·licient de formar part del sistema.

Per plasmar-ho de forma numèrica[34] i tenint en compte que a la mainnet d'*Ethereum* el preu del gas està actualment a 22 Gwei[27], desplegar aquest *smart contract* té un cost d'uns 0.031614 Ethers ≈ $80,80. Afegir un nou domini a la xarxa té un cost variable depenent de la llargada del domini (la quantitat de bytes que s'emmagatzemen a la xarxa). Agafant com a referència alguns dominis de la bibliografia, el cost d'afegir urls estaria entre els $3,89 i els $7,64. Per últim, votar un domini té un cost aproximat d'uns $11,39.

Clarament, els costos no són tan baixos com per a que els usuaris que no tenen interès per la ciberseguretat o en tenen poc, contribueixin activament i, tot i que és molt important el fet de que la gent que participaria al sistema sigui gent honesta i realment interessada en el projecte, també som conscients de que necessitem una gran activitat per part dels usuaris per a que el sistema sigui confiable i utilitzat.
D'aquest 'inconvenient' o, més aviat, canvi de filosofia, sorgeix el model #2.

Evidentment, aquest *smart contract* té funcions que retornen l'estat del contracte sense modificar-lo. Aquestes funcions son del tipus *view* i són gratuïtes de cridar. Al tros de codi següent es mostren alguns exemples.

```
1  contract Reputation {
2      ...
3
4      //retorna la llista de dominis emmagatzemada al contracte
5      function getURLList() public view returns (URL[] memory)
       {
6          return urlList;
7      }
8
9      //retorna la llista de votants emmagatzemada al contracte
10     function getVotersList() public view returns (Voter[]
       memory) {
11         return voters;
12     }
13
14     ...
15 }
```

A nivell de programació, m'agradaria comentar la utilitzat dels *events* de Solidity amb un exemple aplicat a aquest *smart contract*. Tot i que en aquest projecte no s'utilitzen, aquesta funcionalitat és comunament utilitzada per mostrar els *logs* de les interaccions amb els *smart contracts on chain*. Aquesta és la forma d'accedir a les dades de la *chain* en temps real, sense necessitat de passar per un *front end* que no saps si ha pogut estar manipulat.

```
contract Reputation {

    event newURL(string indexed _url);
    event votePositive(string indexed _url, address indexed
    _voter);
    event voteNegative(string indexed _url, address indexed
    _voter);

    ...


    function addURL (string memory _url) public {
        ...
        emit newURL(_url);
    }

    function vote (string memory _url, bool _vote) public {
        ...
        if (_vote) {
            ....
            emit votePositive(_url, msg.sender);
        }
        else {
            ...
            emit voteNegative(_url, msg.sender);
        }
    }

    ...
}
```

```
//arrow function al backend que sent els events
const listenEvents = async() => {
    await myContract.getPastEvents('newURL', {
            fromBlock: 0,
            toBlock: 'latest'
        })
        .then(function(events) {
```

```
8               console.log(events)
9           });
10      await myContract.getPastEvents('votePositive', {
11              fromBlock: 0,
12              toBlock: 'latest'
13          })
14          .then(function(events) {
15              console.log(events)
16          });
17      await myContract.getPastEvents('voteNegative', {
18              fromBlock: 0,
19              toBlock: 'latest'
20          })
21          .then(function(events) {
22              console.log(events)
23          });
24  }
```

A la següent figura es mostra l'*output* que es pot esperar dels *events* a l'afegir una url i al votar-la positivament. Amb aquesta informació, al ser completament pública ja que està connectada amb els canvis a la *blockchain*, qualsevol persona pot decidir muntar una api que mostri, per exemple, tots els moviments que s'han anat fent a la xarxa.

Figura 10.2: *Elaboració pròpia.* Exemples d'output dels events

A continuació es mostren alguns exemples visuals del *front end* d'aquest model.

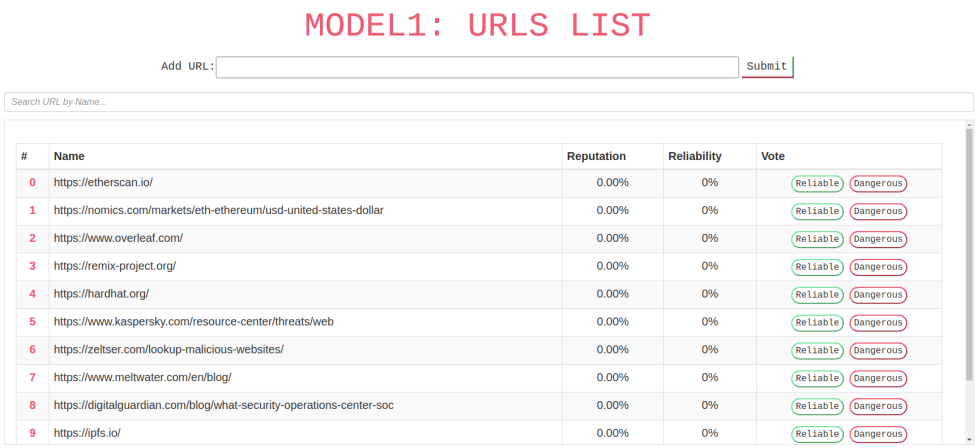

Figura 10.3: *Elaboració pròpia.* Front end Model #1

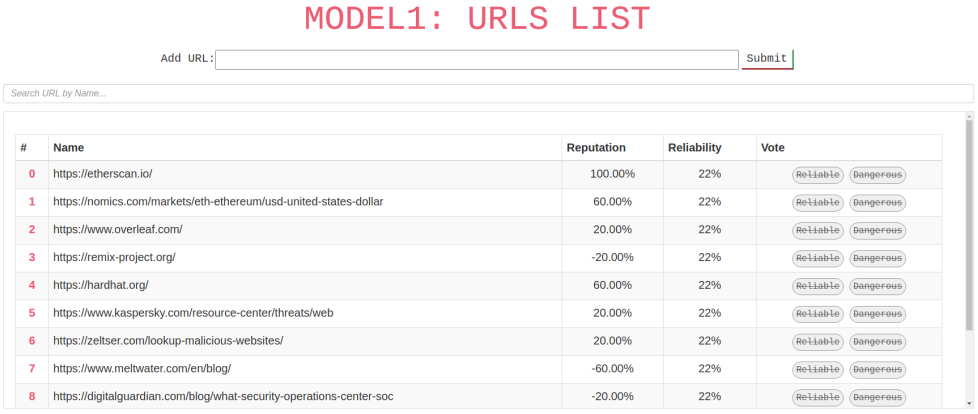

Figura 10.4: *Elaboració pròpia.* Front end del Model #1

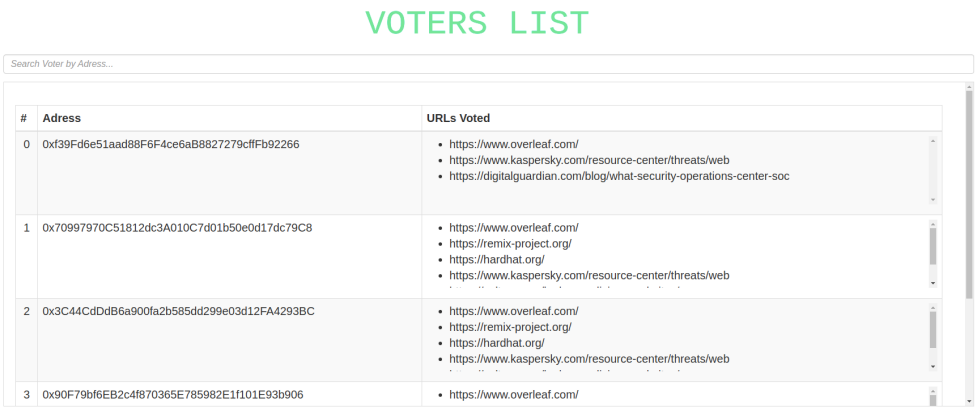

Figura 10.5: *Elaboració pròpia.* Front end del Model #1

10.2 Model #2

Aquest model segueix una filosofia que dista una mica de la relativa a plataformes distribuïdes com Ethereum ja que la intenció principal arribat a aquest punt és que la major part del cost monetari recaigui sobre els amos dels dominis, els quals són els que més profit poden arribar a treure d'aquesta aplicació. Conforme va anant avançant la investigació, vam comprendre que aquesta implementació tenia un forat de seguretat molt gran que s'explica més endavant en aquest apartat.

En aquest model s'implementen 2 *smarts contracts*. El primer és un contracte que guarda l'estat d'un únic domini mentre que el segon és l'administrador de totes les instàncies que es despleguen del primer contracte.

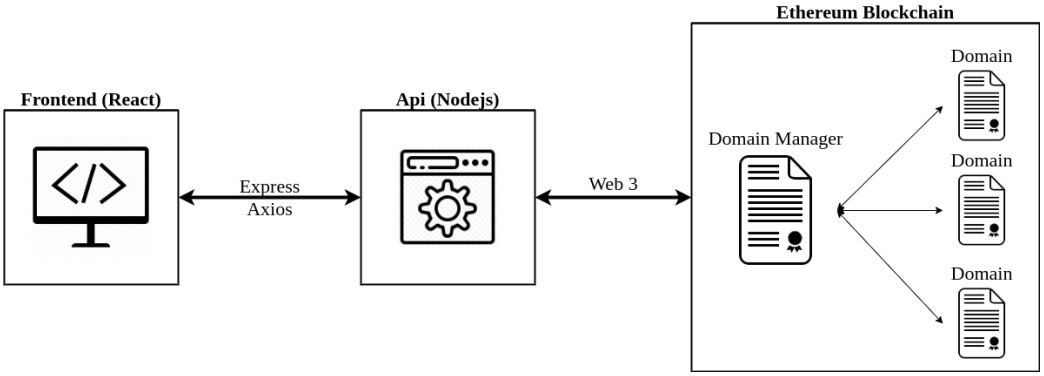

Figura 10.6: *Elaboració pròpia.* Estructura del Model #2

Aquesta diferenciació és degut a com s'han enfocat els costos els quals volem que els amos dels dominis fossin els que despleguessin els seus *smart contracts* a través de l'administrador, corrent així amb els castos de desplegament (tenint en compte que el preu del gas està a 22 Gwei[35], desplegar una instància del primer contracte costa[34] entre uns 0.008933 ETH ≈ $21,77 i uns 0.01039ETH ≈ $25,32, agafant com a referències les urls de la bibliografia). Desplegar l'*smart contract* administrador corre a carreg nostre de igual manera que desplegar el model #1; aquest, però, té un cost molt més elevat 0.062673 ETH ≈[34] $152,75.

```
1  contract Domain {
2      address owner;                // propietari del domini
3      string domain;                // domains name
4      int256 reputation;            // raw reputation
5      uint256 votes;                // votes received
6
7      constructor(address _owner, string memory _domain) {
8          owner = _owner;
9          domain = _domain;
10         reputation = 0;
11         votes = 0;
12     }
13
14     ...
15 }
16
17 contract DomainManager {
18     struct Voter {
19         address addr;             // person ho has voted
20         string[] urlsVoted;       // urls voted by a person
21         int[] votes;              // votes recorded
22     }
23
24     mapping(string => Domain) reputations;  // diccionari amb
       el nom dun domini i ladreca de lsmart contract Domain que
       sha desplegat
25     Voter[] voters;                    // llistat de votants
26     string[] domains;                  // llistat dels noms
      dels dominis
27
28     ---
29
30     constructor() {
31         console.log("Welcome to URL reputation system model
      #2");
32     }
33
```

```
34      // desplega una instancia de lsmart contract Domain i
        guarda la seva adreca a larray reputations
35      function createDomain(string memory _domain) public
        DomainAlreadyExists(_domain) {
36          reputations[_domain] = new Domain(msg.sender, _domain
        );
37          domains.push(_domain);
38      }
39
40  }
```

A més a més, tampoc es vol que els usuaris assumeixin els costos de les votacions, per aconseguir això s'ha implementat que els amos dels dominis puguin enviar Ethers als seus *smart contracts* amb la intenció de que, cada cop que es rebi un vot, el contracte retorna el cost d'aquesta transacció a l'usuari. En el cas de que un contracte no tingui diners suficients per dur a terme aquesta funció, no es proporcionarà informació sobre la reputació del domini que representa; d'aquesta manera es pretén que els amos dels dominis mantinguin els contractes amb diners i evitar fraus de deixar d'invertir diners un cop s'ha arribat a un nivell de reputació alt.

Els costos de les transaccions per votar varien seguint el mateix comportament que al model #1. En aquests els costos estan entre els $8.5 i els $11.5. Aquest cost no és el final ja que, com hem mencionat, el contracte intel·ligent retorna un valor aproximat del cost, aquest retorn està al voltant dels $9.5, així que realment les transaccions estan costant $1 - $2.

```
1
2   contract Domain {
3       ...
4
5       //actualitza quantitat de vots i lestat de la reputacio
        en cru, a mes retorna el cost aproximat de la trasaccio
6       function vote(bool _vote, uint _initGas, address payable
        _address) public {
7           votes++;
8           if (_vote)
9               reputation++;
10          else
11              reputation--;
12
13          uint transGas = (_initGas - gasleft())*22;
14          require(address(this).balance > transGas+(8887*22), "
        Not balance enough");
```

```
15          _address.transfer(transGas);
16      }
17
18      ...
19  }
20
21  contract DomainManager {
22      ...
23
24      //els owners envien diners als smarts contracts que
        poseeixen
25      function sendMoney(string memory _domain) public payable
        DomainDoesNotExists(_domain) NotOwner(_domain){
26              bool sent = address(reputations[_domain]).send(
        msg.value);
27              require(sent, "Failed to send Ether");
28          }
29
30      //guarda el votant i el tipus de vot a un domain i crida
        la funcio propia del domain per computar el vot
31      function vote (string memory _domain, bool _vote) public
        DomainDoesNotExists(_domain) OwnerCantVote(_domain) {
32          uint initGas = gasleft();
33          uint v = getVoterIndex(_domain);
34          if (_vote) {
35              voters[v].votes.push(1);
36          }
37          else {
38              voters[v].votes.push(-1);
39          }
40          reputations[_domain].vote(_vote, initGas, msg.sender)
        ;
41
42      }
43
44      ...
45  }
```

Aquest model, però, té 2 problemes principals:
El primer i més important a nivell conceptual és que el projecte hauria de ser suficientment conegut i utilitzat per a que els amos dels dominis decideixin contribuir al sistema. Tot i que és cert que poden obtenir informació sobre l'opinió dels seus usuaris a través d'aquesta plataforma a més a més de l'opinió respecte a altres pàgines web, la veritat és que seria una despesa considerable i aquest tipus d'informació es pot acabar obtenint per altres medis de forma més eficient i efectiva.

El segon i més important a nivell tècnic és que existeix un gran forat en la seguretat. Sabent que et retornen la gran majoria de la inversió al votar, pot fer que patim atacs de bots o frau de vots.

Aquest model també compta amb funcions *view* com l'anterior, a continuació es mostren uns exemples.

```
contract Domain {
    ...

    // retorna la reputacio en cru emmagatzemada
    function getReputation() public view returns (int256) {
        return reputation;
    }

    // retorna lamo del domini
    function getOwner() public view returns (address) {
        return owner;
    }

    ...
}

contract DomainManager {
    ...

    // retorna la reputacio en cru dun Domain
    function getDomainReputation(string memory _domain)
    public view DomainDoesNotExists(_domain) returns (int256)
    {
        return reputations[_domain].getReputation();
    }


    // retorna lamo dun Domain
    function getDomainOwner(string memory _domain) public
    view DomainDoesNotExists(_domain) returns (address) {
        return reputations[_domain].getOwner();
    }

    ...
}
```

A nivell de programació, m'agradaria comentar la utilitat dels *modifiers* de Solidity degut a que apareixen a les funcions acabades de mostrar. Aquests,

contenen requeriments que s'han de complir per a que les instruccions dins de les funcions s'executin.

```
contract DomainManager {
    ...

    //el domini donat te associat una adreca de contracte
    intelligent de Domini
    modifier DomainDoesNotExists(string memory _domain) {
        require(keccak256(abi.encodePacked(reputations[_domain
    ])) != keccak256(abi.encodePacked(address(0))),
         "The Domain does not exists in our db.");
         _;
    }

    //lamo del domini te funcions que nomes pot executar ell
    modifier NotOwner(string memory _domain) {
        require(reputations[_domain].getOwner() == msg.sender,
     "You are not the owner of this domain");
        _;
    }

    //lamo no pot votar el seu propi domini
    modifier OwnerCantVote(string memory _domain) {
         require(reputations[_domain].getOwner() != msg.sender
    , "You are the owner of this domain, you can not vote");
         _;
    }

    ...
}
```

Per últim i com al model anterior, seguidament es mostren alguns exemples visuals del *front end* d'aquest model. La taula de votants no canvia entre models, es pot trobar aquí 10.5.

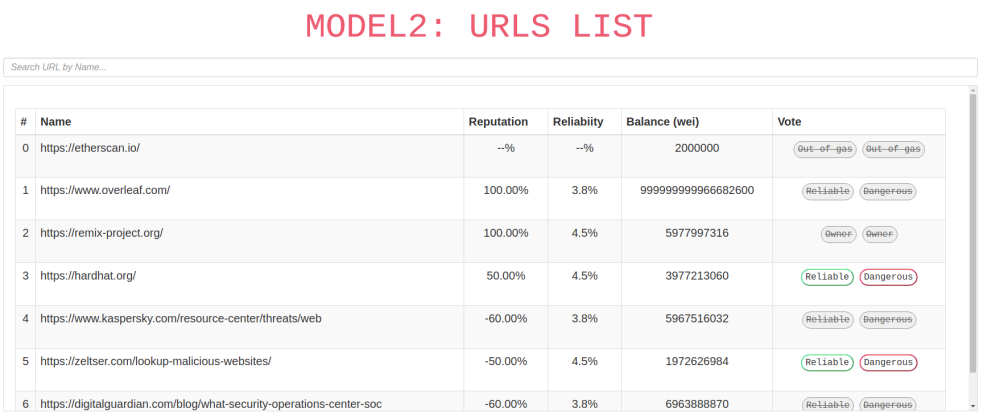

Figura 10.7: *Elaboració pròpia.* Front end Model #2

10.3 Testos

Els testos en aquest projecte s'han fet manualment, gràcies a la facilitat d'interacció visual amb els *smart contracts* que proporciona l'eina Remix mencionada a la seva secció 9.3.1.
Per cada funcionalitat que s'ha implementat, s'ha comprovat el seu bon funcionament executant-la des de varies contes i, s'ha revisat que els casos que haurien de llançar una excepció, efectivament ho fan.

A continuació adjunto imatges de l'*smart contract* del primer model desplegat des del Remix i la seva interacció a l'afegir la url https://academy.binance.com/en/articles/what-are-smart-contracts i votar-la.

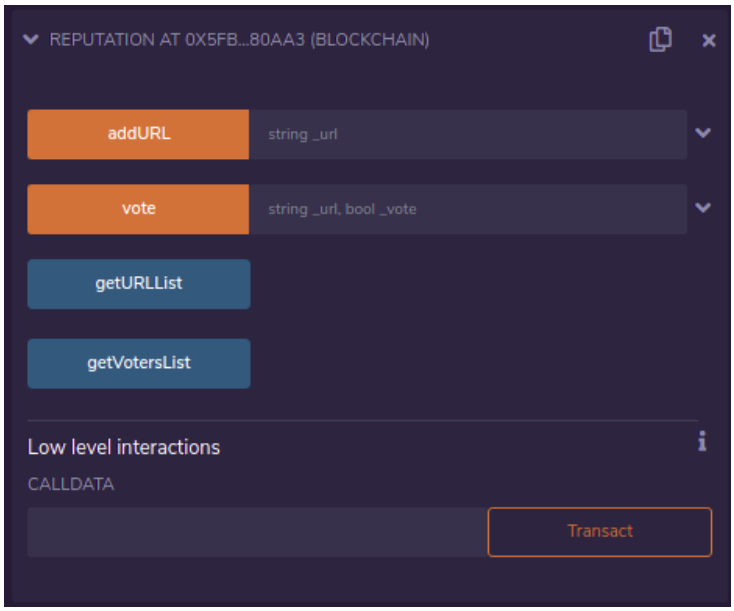

Figura 10.8: *Elaboració pròpia.* Desplegament de l'*smart contract* Reputation

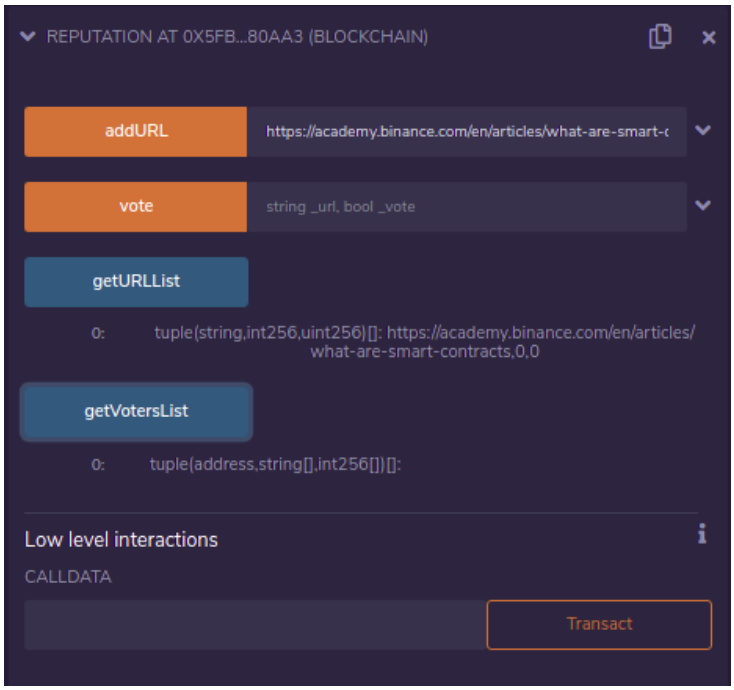

Figura 10.9: *Elaboració pròpia.* Funcionalitat d'afegir urls a Reputation

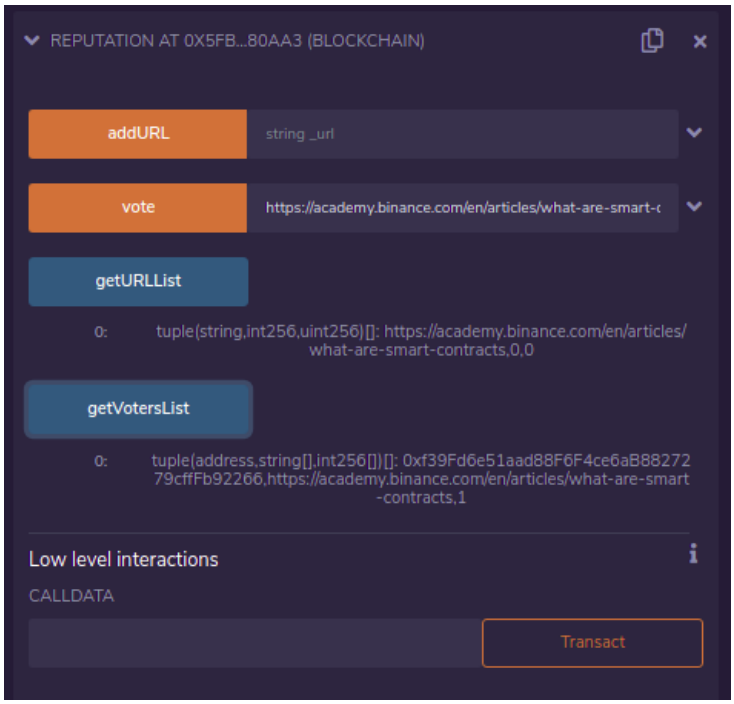

Figura 10.10: *Elaboració pròpia.* Funcionalitat de votar urls a Reputation

En quant al segon model on tenim 2 *smart contracts* i un és cridat des de l'altre. Per visualitzar i interactuar amb les instàncies del segon contracte, utilitzem una altra funcionalitat de Remix. Primer de tot desplegueem el contracte administrador.

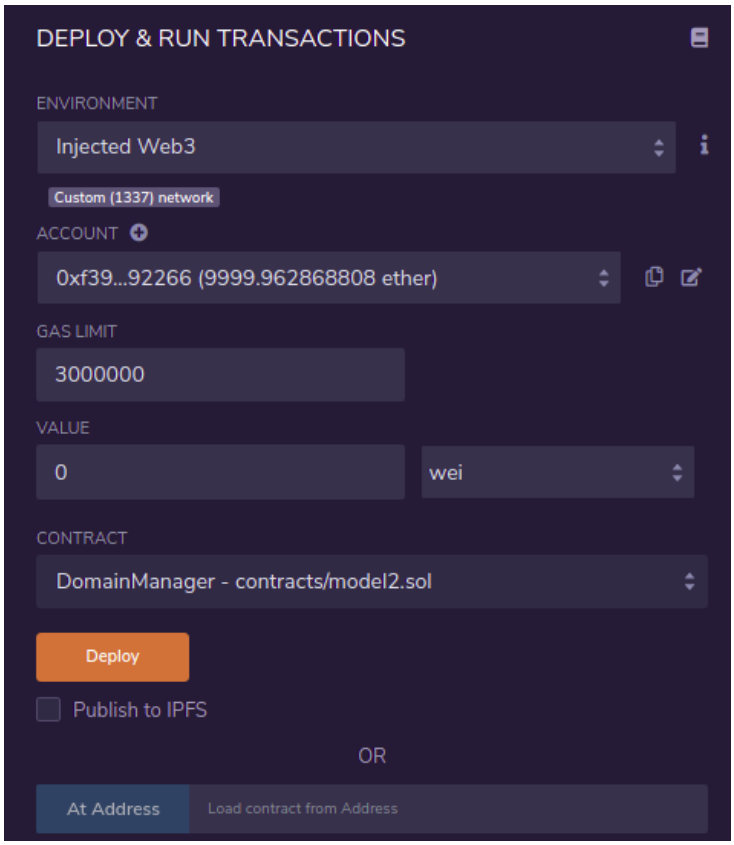

Figura 10.11: *Elaboració pròpia.* Desplegament de l'*smart contract* DomainManager

Seguidament afegirem el mateix domini que al model #1 i obtindrem l'adreça del contracte que s'ha desplegat.

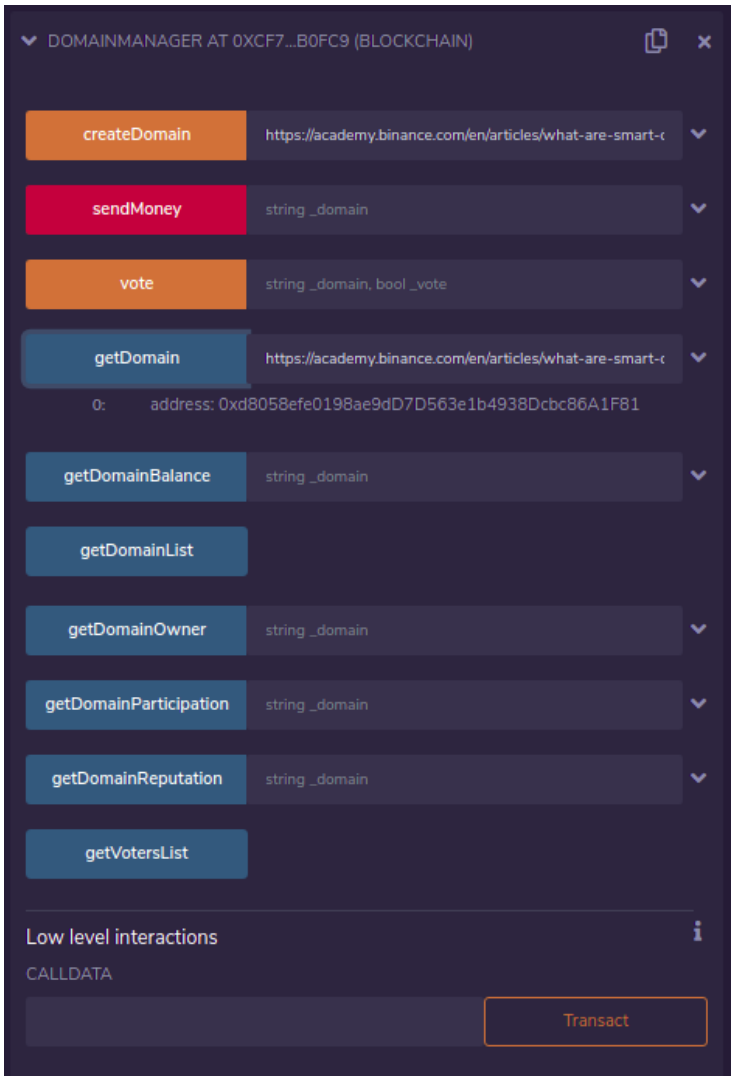

Figura 10.12: *Elaboració pròpia.* Funcionalitat d'afegir urls a DomainManager

Per obtenir la visualització de l'*smart contract* ja desplegat utilitzarem la funcionalitat *address* de Remix. S'ha de parar atenció a que tinguem el contracte correctament sel·leccionat, si comparem la següent imatge amb la figura 10.11, el valor del camp *contract* és diferent.

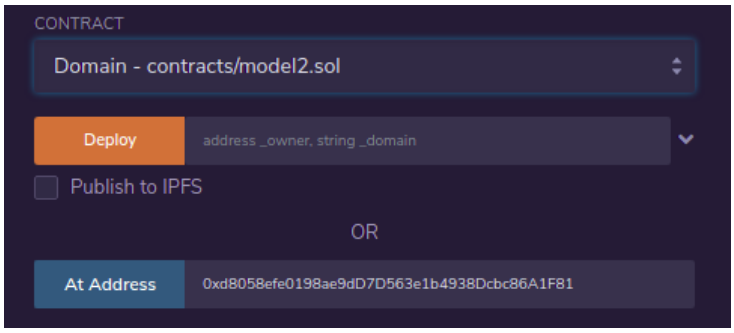

Figura 10.13: *Elaboració pròpia.* Aconseguir visualització d'un sc ja desplegat

Per últim comprovem que tenim l'*smart contract* de forma visual com l'administrador.

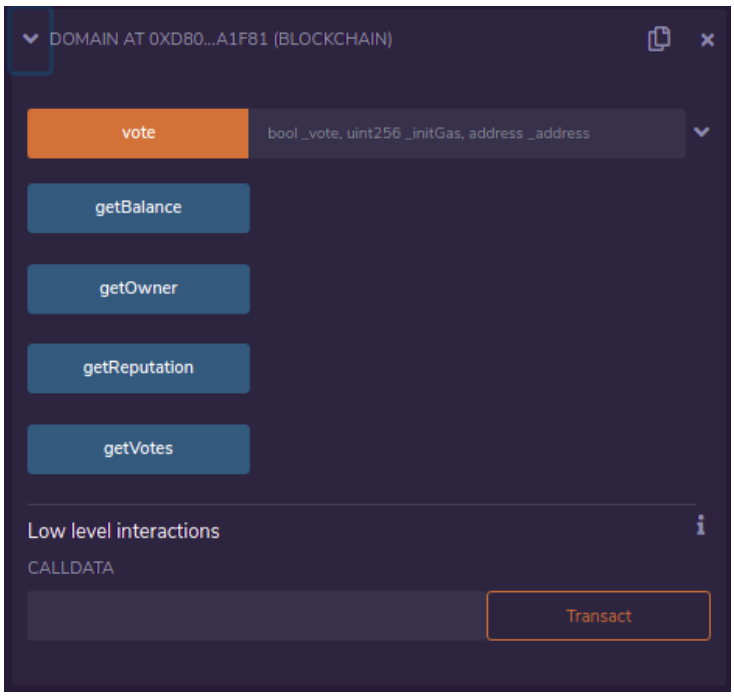

Figura 10.14: *Elaboració pròpia.* Visualització d'una instància de Domain

Explicat així pot semblar un caos, però durant el procés de desenvolupament dels contractes, aquestes visualitzacions han estat realment útil per algú sense experiència en aquest àmbit.

Capítol 11

Conclusions

En aquest capítol es raonaran les reflexions que s'han extret de la implementació d'ambdós models, així com les conclusions generals del projecte.

11.1 Reflexions dels models

Durant el desenvolupament dels models s'ha entès que el fet de pagar taxes a plataformes distribuïdes com Ethereum, minimitza els riscs de frau i d'atacs de bots i que, a més, aquest tipus d'entorns funcionen en part per aquesta característica. Tot i així s'ha decidit investigar solucions alternatives per tractar de minimitzar els problemes o inconvenients que s'han observat.

11.1.1 Model #1

S'ha arribat a la conclusió que seria útil i els usuaris l'utilitzarien si el cost de les transaccions no fos tan elevat. Així que proposem un migració o un desplegament del sistema a altres plataformes com ara la xarxa de BSC[36] (de l'anglès, *Binance Smart Chain*) o esperar a l'actualització d'Ethereum 2.0 on s'introduirà la *Beacon Chain*[37], la qual pretén, a manera de resum, canviar el protocol de *POW* mencionat a la secció 9.2 a *POS* (de l'anglès, *Proof of Stake*[38]. Aquest mecanisme canvia els nodes *miners* del protocol anterior per nodes *validadors*; aquells nodes que vulguin ser considerats aptes per validar, hauran de tenir emmagatzemats un cert nombre d'Ethers per poder ser escollits. Juntament amb això, segueixen un seguit millores:

- Millor eficiència energètica: no cal tanta energia per minar blocks.
- Els requisits per participar són més baixos: al disminuir l'energia necessària per minar, no cal tenir un hardware d'elit.

- Té millor resistència a la centralització: al poder minar amb hardwares més assequibles, hi ha més probabilitats de que hi hagin més nodes a la xarxa.

- Fragmentació de la blockchain en *shard chains*[39]: mitjançant aquest tipus de cadena, es redueix la congestió a la xarxa i s'incrementen les transaccions per segon. És un factor molt important que millorarà notablement l'escalabilitat de la xarxa d'Ethereum.

Degut a tots els canvis, també baixaran significativament els costos de les quotes i el model #1 podria arribar a ser utilitzat per tothom ja que no suposaria un gran problema pagar uns quants cèntims per votar o afegir dominis.

Una altra solució possible seria fer ús de *sidechains* o *layers 2*.
Les *sidechains*[8] són cadenes de blocs alternatives que permeten millorar les condicions d'una *blockchain* ja existent. Aquesta conté programacions i característiques diferents a la *blockchain* original però es completament compatible amb aquesta, d'aquesta manera, pot fluir la comunicació i poden complementar les seves capacitats. Un exemple de *sidechain* on es podria aplicar aquest model i tenir èxit pot ser *Matic*, ara coneguda com a *Polygon*[40] o també es podria mirar d'implementar una *sidechain* amb un protocol de consens totalment des de 0 que minimitzés el problema de les *fees*.

També existeix la possibilitat d'utilitzar un *layer 2*. D'aquestes n'hi ha varis tipus però només explicarem les *optimistic rollups*. *Layer 2*[41] és un terme col·lectiu per designar solucions que ajuden a escalar les aplicacions gestionant transaccions fora de la *mainnet*[1] d'Ethereum mentre que mantenen tot els beneficis d'aquesta. El temps de validació de transaccions depèn de com de congestionada està la xarxa i això pot afectar a l'experiència de l'usuari en determinades aplicacions ja que conforme més ocupada estigui la xarxa, més puja el preu del gas; per aquest motiu Ethereum és tan cara. Les *rollups* són solucions que realitzen validacions de transaccions fora de la xarxa principal d'Ethereum mantenint la seva seguretat. Aquesta solució és útil no només per reduir les *fees*, oferir més possibilitats de participació i incrementar el rendiment d'execució de transaccions.
Els *optimistic rollups*[41] actuen en paral·lel amb la *mainnet* d'Ethereum com a *layer 2*. Amb aquesta tecnologia, les transaccions s'escriuen a la *mainnet* com *calldata*, optimitzant així encara més el cost del gas que amb altres tipus de *layer 2*. La computació és lenta i cara a Ethereum, *optimistic rollups* poden oferir fins un 100x de millores en l'escalabilitat depenent de les

[1] xarxa principal

transaccions. Aquest número augmentarà encara més amb la incorporació de les *shard chains* que s'acaben de mencionar quan s'ha explicat l'actualització d'Ethereum 2.0. Un exemple d'*optimistic rollup* conegut i que ens podria servir és Optimism[42].

11.1.2 Model #2

Els problemes giren en torn a que el càlcul del cost de transacció. En aquest projecte s'han estudiat dues maneres: fer-lo de forma externa des del *backend* o fer-lo de forma interna des del mateix *smart contract*.

El primer mètode té el problema que des del *backend* s'hauria de cridar una funció del contracte, passant-li com a paràmetre la quantitat d'Ethers que s'han de retornar. Aquesta funció, per ser accessible des de la API ha de ser pública i, per tant, en cas de tenir algun forat de seguretat des del *frontend*, poden canviar el valor de retorn pot causar grans pèrdues als amos dels dominis i donar mala reputació a la nostra plataforma. A més a més, al estar amagada aquesta funcionalitat en comptes de pública a la *blockchain*, pot fer que els usuaris la vegin amb desconfiança.

El segon mètode té el problema que el càlcul del cost de la transacció no és exacte i, tampoc seria aplicable al món real. El càlcul aproximat s'obté de mirar quant *gas* restant queda de l'inicial assignat al principi de la funció i al final d'aquesta, aquest gas que s'utilitza, s'ha de multiplicar pel preu actual de gas per saber el cost en Ethers. Si recordem a la secció 9.3 es comenta que els *smart contracts* no poden contactar amb l'exterior, això fa impossible el fet d'aconseguir el preu del gas a cada moment.
Per fer les proves en aquest projecte s'ha *hardcodejat* aquest valor segons anava canviant ja que hem cregut que és l'opció menys dolenta però volem deixar clar que aquesta implementació, tot i ser transparent per la resta de funcions, no és viable al món real. Haver de canviar manualment el valor del gas cada minut fa que, cada cop haguem de desplegar l'*smart contract*, com no tenim cap mecanisme per accedir a la informació emmagatzemada al contracte anterior i connectar-la amb l'actual, no podríem mostrar un *frontend* consistent tal i com està tot plantejat actualment.

En definitiva, aquest model no segueix la filosofia de plataformes com Ethereum i hauria de ser implementat en un altre sistema distribuït que assegurés la fiabilitat de les dades i alhora fos gratuït o el cost recaigués d'una manera segura sobre els beneficiaris finals.

11.2 Conclusions del projecte

En aquest projecte s'ha après no només a utilitzar les noves tecnologies esmentades, sinó també a *fer* un projecte abans de *començar-lo*. Al principi pensava que no seria tan important, que fer una planificació quan el projecte només el desenvolupava una persona només seria una pèrdua de temps; però gràcies a aquesta planificació inicial, no ha condit el pànic quan, per varis motius, ens vam endarrerir tant en el desenvolupament. També s'ha après que a vegades és necessari rescindir d'uns objectius per poder entregar un treball ben fet i no un a mitges i que prendre decisions importants moltes vegades és complicat.

La part tècnica ha estat tota una aventura, investigar una tecnologia tan recent i que encara s'està expandint ha estat una de les coses més interessants que he estudiat des que vaig començar la carrera i tinc un parell d'anècdotes bones per explicar.
En el referent a la plataforma d'Ethereum i la tecnologia blockchain, he d'agrair de tot cor a les persones que em van recomanar Remix i Hardhat ja que ha fet l'aprenentatge molt més ràpid i fàcil que si l'hagués fet directament amb la terminal i el Visual Studio Code. A més a més, i aquí he de pecar de mala praxis, quan vaig instal·lar *Hardhat*, vaig deixar tota la configuració per defecte, entre ella, el mnemotècnic que actua com a clau privada de les comptes que proporciona. Així doncs, quan vaig provar de desplegar els contractes a la *testnet* de Kovan, em van desaparèixer els 2 ETH que donen cada 24h per a que duguis a terme les proves necessàries. Podria dir que em sorprèn que hi hagi gent amb bots que roben diners de *wallets* a una xarxa de proves, els quals no tenen valor real a la *mainnet*, però estaria mentint. Ha estat una anècdota graciosa i un bon recordatori de que, no totes les instal·lacions són *siguiente, siguiente, siguiente, aceptar*.
Una altra anècdota interessant és que no em vaig adonar, fins molt al final, que les reputacions no sortien fraccionades (inicialment es volia que la reputació dels dominis es computés directament a l'*smaart contract* i no al *backend*), això és degut a que en Solidity només es poden representar números enters.

En el referent tant al *frontend* com al *backend*, aquest projecte m'ha donat l'oportunitat de treballar amb JavaScript per primer cop i, sincerament, venint de 4 anys programant en llenguatges fortament tipats, no ha estat fàcil acostumar-se. De fet, la majoria de problemes que he tingut han estat pels tipus de variables, els quals es podrien haver solucionat molt fàcilment amb la instal·lació del software de TypeScript, però vaig decidir que, mentre em

quedés paciència, volia intentar programar en JS com s'havia pensat des de l'inici. En quant al *frontend*, pensava que seria com jugar al *pinta y colorea*, però el realitzar aquest projecte m'ha fet adonar-me de que aquesta part de la informàtica és tota una ciència en la que m'agradaria poder invertir més temps en aprendre en un futur proper.

D'aquest projecte em quedo amb l'interès que m'ha nascut de saber com evoluciona el món de les xarxes de criptomonedes, el qual vull continuar seguir informant-me freqüentment i amb llibreries de NodeJS que m'han servit per connectar el *backend* amb el *frontend*, que segur que puc reutilitzar en altres projectes.
Per últim m'agradaria mencionar com la filosofia d'entorns com Ethereum també han contribuït a construir la meva manera de pensar, veure sistemes fets de gent que tenen el mateix poder, regir-se per diferents protocols i regles de consens de manera efectiva, crec que és un gran avanç cap a les societats del futur i veig que es pràcticament imparable. Projectes nous com ara Polkadot[43] el qual desafia el món hermètic d'aquestes xarxes amb una promesa d'intercomunicació entre elles em fan posar els pèls de punta i pensar que el *futur* és *ara*.

Bibliografia

[1] AO Kaspersky Lab. What are web threats? [en línia]. Disponible a: https://www.kaspersky.com/resource-center/threats/web, 2021. [Consulta: 27.03.2021].

[2] Lenny Zeltser. Free online tools for looking up potentially malicious websites [en línia]. Disponible a: https://zeltser.com/lookup-malicious-websites/, 2021. [Consulta: 27.03.2021].

[3] Álvaro Ovejas. Analítica web: Las 7 herramientas y 9 métricas más importantes [en línia]. Disponible a: https://leadmotiv.com/blog/analitica-web-y-sus-metricas/#Metricas_de_analitica_web_mas_importantes, 2021. [Consulta: 27.03.2021].

[4] John Boitnott. 6 essential roles of the modern marketing team [en línia]. Disponible a: https://www.meltwater.com/en/blog/6-essential-roles-of-the-modern-marketing-team, 2020. [Consulta: 27.03.2021].

[5] Juliana De Groot. Data protection 101: What is a security operations center (soc)? [en línia]. Disponible a: https://digitalguardian.com/blog/what-security-operations-center-soc, 2020. [Consulta: 27.03.2021].

[6] IPFS. Ipfs powers the distributed web [en línia]. Disponible a: https://ipfs.io/, 2021. [Consulta: 27.03.2021].

[7] Binance Academy. What is blockchain technology? the ultimate guide [en línia]. Disponible a: https://academy.binance.com/en/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners#who-invented-blockchain-technology, 2021. [Consulta: 28.03.2021].

[8] Bit2me Academy. ¿qué es una cadena lateral o sidechain? [en línia]. Disponible a: https://academy.bit2me.com/que-es-cadena-lateral-sidechain/, 2021. [Consulta: 28.03.2021].

[9] Binance Academy. What are smart contracts? [en línia]. Disponible a: https://academy.binance.com/en/articles/what-are-smart-contracts, 2021. [Consulta: 28.02.2021].

[10] Richard Dennis and Gareth Owen. Rep on the block: A next generation reputation system based on the blockchain. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 131–138, 2015.

[11] Mazin Debe, Khaled Salah, Muhammad Habib Ur Rehman, and Davor Svetinovic. Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain. *IEEE Access*, 7:178082–178093, 2019.

[12] Viktor Jacynycz García. Towards a decentralized publication system: A proposal using blockchain and p2p technologies. Master's thesis, Universidad Complutense de Madrid. Disponible a: https://eprints.ucm.es/id/eprint/49793/, 2017/2018.

[13] Wikipedia contributors. Agile software development [en línia]. Disponible a: https://en.wikipedia.org/wiki/Agile_software_development, 2021. [Consulta: 27.02.2021].

[14] Claire Drumond. Scrum: learn how to scrum with the best of 'em [en línia]. Disponible a: https://www.atlassian.com/agile/scrum, 2021. [Consulta: 27.02.2021].

[15] Pau Risa Subirats. *Sistema de reputación en Internet basado en la tecnología blockchain [en línia]*. Treball final de grau, UPC, Facultat d'Informàtica de Barcelona. Departament de Tecnologies de la Informació. 2020. Disponible a: https://upcommons.upc.edu/handle/2117/335490. [Consulta: 27.03.2021].

[16] OpenJS Foundation. Node.js® is a javascript runtime built on chrome's v8 javascript engine. [en línia]. Disponible a: https://nodejs.org/en/, 2021. [Consulta: 27.02.2021].

[17] OpenJS Foundation. Espress: Fast, unopinionated, minimalist web framework for node.js. [en línia]. Disponible a: https://expressjs.com/, 2021. [Consulta: 27.02.2021].

[18] NPM. Axios: Promise based http client for the browser and node.js. [en línia]. Disponible a: https://www.npmjs.com/package/axios, 2021. [Consulta: 27.02.2021].

[19] PayScale. Average project manager, information technology (it) salary in spain [en línia]. Disponible a: https://www.payscale.com/research/ES/Job=Project_Manager%2C_Information_Technology_(IT)/Salary, 2021. [Consulta: 20.03.2021].

[20] Infoempleo. La profesión [en línia]. Disponible a: https://www.infoempleo.com/guias-informes/empleo-it-mujeres/perfiles/experta-blockchain.html, 2020. [Consulta: 13.03.2021].

[21] PayScale. Average front end developer / engineer salary in spain [en línia]. Disponible a: https://www.payscale.com/research/ES/Job=Front_End_Developer_%2F_Engineer/Salary, 2021. [Consulta: 20.03.2021].

[22] PayScale. Average test engineer salary in spain [en línia]. Disponible a: https://www.payscale.com/research/ES/Job=Test_Engineer/Salary, 2021. [Consulta: 20.03.2021].

[23] Facebook Inc. React: Una biblioteca de javascript para construir interfaces de usuario[en línia]. Disponible a: https://es.reactjs.org/, 2021. [Consulta: 10.05.2021].

[24] Wikipedia Contributors. Blockchain[en línia]. Disponible a: https://en.wikipedia.org/wiki/Blockchain, 2021. [Consulta: 28.03.2021].

[25] Coin 24. Comment fonctionne la blockchain? [en línia]. Disponible a: https://coin24.fr/dictionnaire/blockchain/, 2021. [Consulta: 01.06.2021].

[26] IBM. What is blockchain technology? [en línia]. Disponible a: https://www.ibm.com/topics/what-is-blockchain, 2021. [Consulta: 28.03.2021].

[27] Sam Richards. Intro to ethereum [en línia]. Disponible a: https://ethereum.org/en/developers/docs/intro-to-ethereum/, 2021. [Consulta: 18.03.2021].

[28] Bhavish Yalamanchi. Proof-of-work (pow) [en línia]. Disponible a: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/, 2021. [Consulta: 18.03.2021].

[29] Hardhat. Ethereum development environment for professionals [en línia]. Disponible a: https://hardhat.org/, 2021. [Consulta: 23.03.2021].

[30] Werner Vermaak. What is metamask? [en línia]. Disponible a: https://metamask.io/, 2021. [Consulta: 10.05.2021].

[31] MetaMask. A crypto wallet & gateway to blockchain apps [en línia]. Disponible a: https://metamask.io/, 2021. [Consulta: 10.05.2021].

[32] Kovan. Kovan testnet: The fast and reliable ethereum test chain [en línia]. Disponible a: https://kovan-testnet.github.io/website/, 2021. [Consulta: 10.05.2021].

[33] Remix. Deploy & run transactions in the blockchain [en línia]. Disponible a: https://remix-project.org/, 2021. [Consulta: 23.03.2021].

[34] Nomics. 1 ethereum to united states dollar [en línia]. Disponible a: https://nomics.com/markets/eth-ethereum/usd-united-states-dollar, 2021. [Consulta: 15.05.2021].

[35] Etherscan. The ethereum blockchain explorer [en línia]. Disponible a: https://etherscan.io/, 2021. [Consulta: 15.05.2021].

[36] Binance Academy. Una introducción a binance smart chain (bsc) [en línia]. Disponible a: https://academy.binance.com/es/articles/an-introduction-to-binance-smart-chain-bsc, 2021. [Consulta: 15.05.2021].

[37] Ethereum. The beacon chain [en línia]. Disponible a: https://ethereum.org/en/eth2/beacon-chain/, 2021. [Consulta: 19.05.2021].

[38] Ozora Ogino. Proof-of-stake (pos) [en línia]. Disponible a: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/, 2021. [Consulta: 19.05.2021].

[39] Ethereum. Shard chains [en línia]. Disponible a: https://ethereum.org/en/eth2/shard-chains/, 2021. [Consulta: 01.06.2021].

[40] Polygon. Ethereum's internet of blockchains [en línia]. Disponible a: https://polygon.technology/, 2021. [Consulta: 01.06.2021].

[41] Paul Wackerow. Layer 2 rollups [en línia]. Disponible a: https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/#:~:text=Optimistic%20rollups%20sit%20in%20parallel,or%20%22notarise%22%20the%20transaction, 2021. [Consulta: 01.06.2021].

[42] Optimism. The new scalability stack for ethereum [en línia]. Disponible a: https://optimism.io/, 2021. [Consulta: 01.06.2021].

[43] Polkadot. Polkadot is live [en línia]. Disponible a: https://polkadot.network/, 2021. [Consulta: 16.06.2021].