



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona



FACULTAT D'INFORMÀTICA DE BARCELONA
(FIB)

UNIVERSITAT POLITÈCNICA DE CATALUNYA (UPC)

GRAU EN ENGINYERIA INFORMÀTICA (GEI)

CURS 2021-2022

DIRECTOR: CARLES FARRÉ TOST

Web3 Ethereum Application: Plataforma de micromecenatge

Treball de fi de grau

Arnau Garcia Rodríguez

18 de juny de 2022

Your assumptions are your
windows on the world. Scrub
them off every once in a while,
or the light won't come in.

Isaac Asimov

Agraïments

Vull agrair al meu tutor del treball de fi de grau, Carles Farré, per la seva orientació i ajut a l'hora d'escollir quin projecte dur a terme. També vull remarcar la importància de tot el coneixement rebut a la facultat, que m'ha ajudat a iniciar la meva carrera professional i a saber a què em vull dedicar. Molts dels conceptes apresos durant aquests anys al grau d'enginyeria informàtica han sigut indispensables a l'hora de desenvolupar el projecte i elaborar aquesta memòria.

També vull agrair-li a tots els meus companys a la universitat, que m'han donat suport i s'han interessat en l'estat del projecte.

Finalment, vull agrair especialment a totes aquelles persones properes, tant amics com família, per prestar-se a ajudar-me en qualsevol situació i fer-me costat. També vull donar les gràcies a un bon amic meu, Marcos Pérez Shan, que s'ha prestat a dissenyar el logotip de la pàgina web.

Resum

La idea de la web3, juntament amb la tecnologia de la cadena de blocs, s'està fent lloc a la indústria de la informàtica i és cada cop té més rellevància en la societat. Tanmateix, gran part de la població sap que són les criptomonedes o almenys n'ha sentit a parlar; aquestes s'estan utilitzant per fer transaccions i sembla que en un futur no molt llunyà formaran part de les nostres vides quotidianes.

Aquest projecte pretén profunditzar en el desenvolupament d'aplicacions descentralitzades, construint així una pàgina web de micromecenatge que interaccioni amb contractes intel·ligents desplegats a la xarxa Polygon, una cadena de blocs basada en Ethereum. La web oferirà un servei de creació de campanyes de recaptació de fons per projectes i es duran a terme ICOs (*Initial Coin Offerings*). Totes les transaccions es faran mitjançant MATIC, la criptomoneda nativa de la xarxa Polygon. A més, hi haurà funcionalitats addicionals com una secció de comentaris per cadascuna de les campanyes, una barra de cerca, campanyes preferides, configuració de l'usuari, etc.

Resumen

La idea de la web3, junto a la tecnología de la cadena de bloques, se está haciendo sitio la industria de la informática y es cada vez tiene más relevancia en la sociedad. Además, gran parte de la población sabe que son las criptomonedas o al menos ha oído hablar de ellas; estas se están utilizando para hacer transacciones y parece que en un futuro no muy lejano podrían formar parte de nuestras vidas cotidianas.

Este proyecto pretende profundizar en el desarrollo de aplicaciones descentralizadas, construyendo así una página web de micromecenazgo que interaccione con contratos inteligentes desplegados en la red Polygon, una cadena de bloques basada en Ethereum. La web ofrecerá un servicio de creación de campañas de recaptación de financiamiento para proyectos y se llevarán a cabo ICOs (*Initial Coin Offerings*). Todas las transacciones se harán mediante MATIC, la criptomoneda nativa de la red Polygon. Además, habrá funcionalidades adicionales como por ejemplo una sección de comentarios para cada campaña, una barra de búsqueda, las campañas favoritas del usuario, configuración de l'usuari, etc.

Abstract

Web3, along with blockchain technology, is fighting for a place in the IT industry and is gaining importance in today's society. Furthermore, most people know what cryptocurrencies are or have heard of them. These, are being used to send transactions, and it seems they could be part of our day-to-day life in a near future.

This project intends to dig deeper into the development of decentralized applications (dapps), building a crowdfunding web page which interacts with smart contracts deployed on Polygon network, an Ethereum-based blockchain. The web page will offer a funding campaign creation service and will be a platform where ICOs (*Initial Coin Offerings*) can take place. Every transaction will be done with MATIC, the native cryptocurrency of the Polygon Network. Furthermore, there will be more functionalities such as a comment section for every campaign, a search bar, favourite campaigns, user configuration, etc.

Índex

1	Introducció	7
1.1	Contextualització	7
1.2	Termes i conceptes	7
1.3	Descripció del problema i justificació del treball	8
1.4	Actors implicats	9
2	Estat de l'art	10
2.1	Web3	10
2.2	Micromecenatge	12
2.3	ICO	13
3	Abast del projecte	15
3.1	Objectius	15
3.2	Requisits funcionals	15
3.2.1	Diagrama de casos d'ús	15
3.2.2	Descripció <i>brief style</i>	16
3.3	Requisits no funcionals	18
3.4	Riscos	21
4	Metodologia de treball	22
5	Planificació inicial	24
5.1	Descripció de les tasques	24
5.2	Dependències	27
5.3	Taula resum	27

5.4	Gantt	30
6	Gestió del risc: Plans alternatius i obstacles	31
7	Pressupost	32
7.1	Estimació dels costos	32
7.1.1	CPA	33
7.1.2	CG	33
7.1.3	Contingències	34
7.1.4	Imprevistos	34
7.2	Control de gestió	34
8	Sostenibilitat i compromís social	35
8.1	Autoavaluació	35
8.2	Anàlisi de sostenibilitat	36
9	Descripció funcional	38
9.1	Navegabilitat	38
9.2	Vistes	38
9.2.1	Connectar el moneder	39
9.2.2	Pantalla principal	39
9.2.3	Pantalla ICOs	40
9.2.4	Campanyes preferides	41
9.2.5	Campanyes de l'usuari	41
9.2.6	Pantalla About	42
9.2.7	Buscar campanyes	42
9.2.8	Començar campanya	43

9.2.9	Configurar usuari	44
9.2.10	Informació d'una campanya	46
9.2.11	Respostes a un comentari	47
9.2.12	Pantalla d'informació d'una ICO	48
10	Disseny	51
10.1	Arquitectura	51
10.2	Model de dades	52
10.3	Patrons de disseny	53
11	Implementació	55
11.1	Llenguatges	55
11.2	Tecnologies	55
12	Identificació de lleis i regulacions	69
12.1	Llicències	69
12.2	Condicions d'ús Netlify	70
12.3	Condicions de servei de Polygon	70
12.4	Normativa del TFG a la FIB-UPC	71
13	Planificació revisada i canvis	72
13.1	Canvis respecte a l'objectiu inicial	72
13.2	Descripció final de les tasques	73
13.3	Taula resum actualitzada	74
13.4	Gantt resultant	78
13.5	Desviacions en el pressupost	78

14 Integració de coneixements	81
15 Conclusions	83
15.1 Competències tècniques	83
15.2 Valoració personal	86
15.3 Futur del projecte	87
Annexos	88
Referències	90

Índex de figures

1	Diagrama de casos d'ús. Elaboració pròpia	16
2	Resum tasques de gestió. Elaboració pròpia	28
3	Resum tasques eines TIC. Elaboració pròpia	28
4	Resum tasques de programació. Elaboració pròpia	29
5	Gantt de la planificació inicial del projecte. Elaboració pròpia	30
6	Pressupost dividit en partides. Elaboració pròpia	32
7	Barra de navegació. Elaboració pròpia	38
8	Vista per connectar el moneder. Elaboració pròpia	39
9	Pantalla principal de l'aplicació. Elaboració pròpia	40
10	ICOs disponibles. Elaboració pròpia	40
11	Campanyes favorites. Elaboració pròpia	41
12	Campanyes de l'usuari. Elaboració pròpia	42
13	Buscar una campanya. Elaboració pròpia	43
14	Botó per crear una campanya. Elaboració pròpia	43
15	Formulari per crear una campanya. Elaboració pròpia	44
16	Configurar usuari. Elaboració pròpia	45
17	Veure adreça del compte. Elaboració pròpia	45
18	Pàgina d'informació d'una campanya. Elaboració pròpia	46
19	MATIC enviat correctament. Elaboració pròpia	47
20	Secció de comentaris. Elaboració pròpia	47
21	Respostes a un comentari. Elaboració pròpia	48
22	Pantalla d'informació d'una ICO. Elaboració pròpia	49
23	IVO al moneder de l'usuari. Elaboració pròpia	50

24	Pantalla d'informació d'una ICO per l'usuari propietari. Elaboració pròpia	50
25	Arquitectura de l'aplicació. Elaboració pròpia	51
26	Model de dades. Elaboració pròpia	53
27	Remix IDE. Elaboració pròpia	56
28	Resultat de l'execució dels tests als contractes intel·ligents. Elaboració pròpia	59
29	Metamask. Elaboració pròpia	60
30	Petició per firmar la transacció. Elaboració pròpia	62
31	Tokens obtinguts amb la compra. Elaboració pròpia	62
32	Creació instància IPFS. Elaboració pròpia	67
33	Resum de tasques d'eines tic actualitzades	75
34	Resum de tasques de programació actualitzades (1)	76
35	Resum de tasques de programació actualitzades (2)	77
36	Gantt de la planificació resultant del projecte. Elaboració pròpia	78
37	Pressupost final dividit en partides (1). Elaboració pròpia	79
38	Pressupost final dividit en partides (2). Elaboració pròpia	80

1 Introducció

1.1 Contextualització

El projecte serà desenvolupat com a treball de fi de grau (TFG) del grau d'enginyeria informàtica, impartit per la Facultat d'Informàtica de Barcelona. L'objectiu és posar en pràctica coneixements adquirits durant el grau, tant de desenvolupament de software com de gestió de projectes. El projecte consistirà en la construcció d'una plataforma de micromecenatge a una cadena de blocs de l'ecosistema Ethereum.

1.2 Termes i conceptes

És imprescindible definir un conjunt de conceptes relacionats amb el tema perquè qualsevol lector pugui entendre'ls i assumir-los abans de començar la lectura d'aquest estudi:

- **Cadena de blocs:** Una cadena de blocs, de l'anglès *blockchain*, és una base de dades distribuïda dissenyada perquè resulti gairebé impossible alterar les dades un cop ha sigut introduïda. Això és degut al fet que cadascun d'aquests blocs està enllaçat i encriptat per protegir la seguretat i privacitat de les transaccions [1].
- **Ethereum:** Plataforma que assumeix la tecnologia de la cadena de blocs i permet als desenvolupadors crear software descentralitzat a través del qual es poden gestionar transaccions i automatitzar alguns processos. Això és possible gràcies als contractes intel·ligents o *smart contracts*, que ens permeten eliminar la figura de l'intermediari i l'esforç dels processos manuals [2, 3].
- **Sidechain d'Ethereum:** Cadena de blocs alterna que busca millorar les prestacions de la xarxa principal d'Ethereum, treballant de forma paral·lela a la cadena principal i podent interactuar amb aquesta. [4]. D'una banda, és una tecnologia molt establerta i té completa compatibilitat amb qualsevol eina típica d'Ethereum, ja que està basada en EVM (*Ethereum Virtual Machine*). També ens permet desplegar els contractes de forma més econòmica, ja que té una escala molt més gran que la cadena de blocs principal. D'altra banda, és menys descentralitzada que la xarxa principal d'Ethereum.

Un exemple de *sidechain* d'Ethereum és Polygon Network, que és la xarxa que utilitzarem per desplegar els contractes intel·ligents.

- **Contractes intel·ligents:** També coneguts com a *smart contracts*, són contractes desplegats en cadenes de blocs en forma de script que són capaços d'executar-se i fer-se complir de forma automàtica, sense intermediaris ni mediadors. En el cas d'Ethereum, estan escrits en el llenguatge Solidity.

En aquests es poden definir estructures de dades, mètodes, interfícies, etc. També poden estendre altres contractes com els estàndards ERC20 per crear tokens o ERC721 per crear NFTs. Els contractes es poden comunicar entre si mitjançant l'adreça on es troben desplegats.

Els contractes es caracteritzen per ser transparents, descentralitzats i immutables gràcies a ser de codi obert i a la tecnologia de la cadena de blocs[5].

- **Aplicació descentralitzada:** També coneguda com a *dapp*, és una aplicació que es troba a la cadena de blocs. Aquestes no requereixen una autoritat central per controlar o restringir les operacions, sinó que funcionen mitjançant els contractes intel·ligents. [6].
- **Crowdfunding:** En català micromecenatge, és una forma d'inversió col·lectiva per internet per donar suport a un treball o un projecte dut a terme per un grup de persones o organització. Els projectes finançats solen estar relacionats amb l'ajuda humanitària, periodisme, art, campanyes electorals o empreses emergents [7].

1.3 Descripció del problema i justificació del treball

Com és ben conegut, en els darrers anys hi ha hagut un creixement exponencial de la tecnologia, i ha comportat la seva democratització. Cada cop més gent té accés als coneixements i a les eines informàtiques necessàries per a dur a terme projectes tecnològics. D'altra banda, aquests projectes no depenen d'un gran capital per començar.

En segona instància, les empreses més importants del món es mouen en l'àmbit tecnològic i atrauen molts emprenedors a fundar noves startups o empreses emergents. Alguns exemples d'aquestes empreses punteres són Apple Inc., Microsoft Corporation, Amazon, Alphabet Inc. (Google), Tencent...

Segons un estudi de D&B, a Espanya hi ha un total de 22.771 startups, és a dir, un 5% del total d'empreses creades entre 2015 -2020 [8].

Tots aquests projectes i empreses emergents necessiten algun tipus de finançament. Les opcions tradicionals, com bancs o prestadors, apliquen interessos molt alts. Les plataformes de micromecenatge tradicionals, com

Kickstarter o Indiegogo, apliquen comissions de 5% i 9% respectivament [9]. És necessària una plataforma que es mostri oberta a tots aquests projectes i que permeti una gran comunicació entre les persones que porten la campanya de finançament i els usuaris interessats en el projecte.

Per altra banda, l'interès per la tecnologia blockchain ha crescut exponencialment els darrers anys i cada cop sembla més probable que el web3 [10] serà la nova iteració de la World Wide Web. Aquest fet comportarà un augment del nombre d'aplicacions descentralitzades i guanyarà importància l'economia basada en cripto actius.

Per aquest motiu, he cregut oportú dur a terme una aplicació descentralitzada a la cadena de blocs d'Ethereum, que permeti que aquests projectes es duïn a terme sense intermediaris, finançar-se sense pagar excessius impostos i dipositar el capital a un moneder digital.

1.4 Actors implicats

Les parts implicades o stakeholders són totes aquelles persones o organitzacions que es relacionen amb les activitats i decisions d'un projecte. És indispensable estudiar aquestes parts interessades i s'han de tenir en compte per a la planificació estratègica de qualsevol projecte.

- **Autor TFG:** L'autor del TFG, Arnau Garcia Rodríguez, serà l'encarregat de dur a terme el projecte, és a dir: documentar, gestionar, implementar i desplegar. És la part més interessada, ja que depèn de la compleció del projecte per aprovar l'assignatura de treball de fi de grau i part del seu futur professional depèn d'aquest.
- **Director TFG:** El director d'aquest TFG, Carles Farré Tost, estarà encarregat d'assessorar en el desenvolupament de les competències tècniques i transversals, fer seguiment del treball i avaluar les fites que li corresponguin.
- **Competència:** Bancs, prestadors i webs de micromecenatge ja existents. Aquestes últimes tindran un nou competidor, per la qual cosa s'hauran d'esforçar més per destacar per sobre de la competència.
- **Startups:** Empreses emergents que busquin una font de finançament no tradicional i que estiguin interessats a rebre-la en forma de cripto actius.
- **Usuaris:** Tots aquells usuaris de la web3 que estiguin interessats a finançar o invertir en projectes tecnològics mitjançant criptomonedes.

2 Estat de l'art

En aquest apartat es parlarà de l'estat actual d'alguns conceptes com: Web3, Crowdfunding, ICO. Es profunditzarà en cadascun, definint-lo de forma més estesa que a l'apartat 1.2 Termes, comentant aspectes importants que ajudaran al lector a comprendre l'objectiu final del projecte.

2.1 Web3

Web3 és el nom que alguns tecnòlegs li han donat a un nou tipus de servei a internet basat en la tecnologia de cadena de blocs esmentada anteriorment. Es pensa que podria ser una nova iteració de la *world wide web*, en la que s'incorpora el concepte de descentralització, que contrasta amb la web 2.0 actual, on la majoria de la informació i el contingut estan guardats de forma centralitzada en servidors d'un conjunt de companyies anomenat *Big Tech*. Aquestes són Google, Amazon, Facebook, Apple i Microsoft.

El concepte va néixer el 2014 pel fundador de Polkadot, Gavin Wood, referint-se a un sistema en línia descentralitzat en una cadena de blocs. Cal diferenciar-la de la web 3.0 o web semàntica, que és un concepte existent des del 1999 i parla de fer internet interpretable per les màquines.

Per tant, el terme es fa servir des de fa gairebé una dècada, però no ha sigut fins al creixement d'algunes criptomonedes com el Bitcoin o l'Ether que s'ha posat de moda. Packy McCormick, un inversionista que ha ajudat molt al creixement i a la popularització de la web3, la va definir com: «un internet que és propietat dels desenvolupadors i els usuaris, coordinada per tokens».

L'apogeu d'aquests serveis s'ha vist reflectit en la quantitat de capital, talent i energia que s'està invertint en les empreses emergents de cripto. El 2021, les empreses de capital de risc van invertir més de vint-i-set mil milions de dòlars en projectes relacionats amb les criptomonedes, i gran part d'aquests projectes estaven relacionats amb el web3. [10]

Característiques

- **Descentralitzada:** El control i la presa de decisions és responsabilitat d'una xarxa distribuïda, en contraposició amb una xarxa centralitzada.

- **Oberta:** *Open source* construït per comunitats obertes de desenvolupadors. Totes les transaccions són públiques i es poden veure a algunes webs com <https://etherscan.io/>.
- **Permissionless:** Cap part implicada necessita autorització de governs. Tampoc calen contrasenyes per interaccionar amb les cadenes de blocs, ja que l'únic necessari és tenir connectat un moneder virtual.

Avantatges i inconvenients

Alguns experts argumenten que la web3 ens portarà més seguretat de les dades, escalabilitat, transparència i privacitat per als usuaris. També podrà combatre la influència i el control de les grans multinacionals i corporacions esmentades en el paràgraf anterior.

Tot i això, la descentralització també té alguns desavantatges que cal mencionar.

Com els usuaris som els propietaris de tota la informació, hi ha la possibilitat que hi hagi persones que s'aprofitin d'aquesta llibertat per fer mal. Per exemple, com que no hi ha normes o regulacions d'una plataforma centralitzada, serà més fàcil compartir informació de forma maliciosa o desinformació sense cap mena de càstig.

Alguns escèptics creuen que la web3 no té sentit des d'una perspectiva tècnica. Diuen que les cadenes de blocs són significativament més lentes i amb menys capacitat que les bases de dades estàndard. Per aconseguir que els serveis de la web3 funcionin tan bé, els crítics sostenen que s'haurien de construir serveis centralitzats sobre aquests, cosa que anul·laria tot el propòsit.

Malgrat el potencial d'aquesta tecnologia per evitar la centralització de la informació i tornar el poder als usuaris, també han sorgit crítiques que diuen que el web3 està basat en nocions idealistes. De la mateixa manera, grans empreses com Meta i Microsoft han començat a invertir en aquest sector, i han provocat que hi hagi preocupació del fet que el futur de la web3 continuï sent com un “jardí emmurallat” [11], és a dir, un entorn on es controla a quins continguts i serveis pot accedir un determinat usuari.

Aplicacions

Segurament, avui en dia l'aplicació més popular de la web3 es troba en l'esfera de les criptomonedes i els NFT (*Non-fungible token*). Així i tot, la utilitat d'aquesta tecnologia pot anar molt més enllà.

Ja podem trobar apps descentralitzades, també anomenades *dapps*, enfocades en finances, art, col·leccionables, *gaming*, casino, micromecenatge, xarxes socials, etc.

Per exemple, en el cas de l'art, els artistes poden evitar pagar als intermediaris que es troben en els mètodes tradicionals. En el cas dels videojocs, els usuaris poden guanyar diners en forma de criptomonedes mentre juguen. Un exemple és Axie Infinity, un videojoc que utilitza NFTs i criptomonedes basades en Ethereum per recompensar als jugadors amb diners reals per assolir objectius dins del joc.

De forma similar, no podem parlar del web3 i no mencionar els famosos metaversos. Aquest concepte ha guanyat molta importància els darrers mesos, gràcies a la inversió en aquest sector de grans companyies com Meta (Facebook). Cada cop hi ha més interès en ells, i moltes companyies grans estan intentant tenir la seva parcel·la en el desenvolupament d'aquests.

Es tracta de mons digitals immersius en què els usuaris poden interactuar entre ells. Alguns defensors del web3 creuen que és una part essencial dels metaversos, ja que permetrien la creació de mons descentralitzats que no es regirien per un únic conjunt de normes dictat per una multinacional.

2.2 Micromecenatge

També conegut *crowdfunding*, és la cooperació d'un conjunt de persones, normalment per internet, on es dona confiança a un projecte i s'inverteixen diners per a donar-li suport, sobretot a l'inici. Ja s'ha fet una petita definició del concepte a la introducció d'aquesta memòria.

Aquest mètode té els seus inicis el 1997, quan un grup d'americans va subvencionar la gira de Marillion pels Estats Units a través d'una campanya a internet promoguda pels mateixos fans que va recaptar 60000 dòlars. Un altre exemple de les primeres aplicacions del *crowdfunding* va ser l'any 2004, a la indústria del cinema. Els productors Guillaume Colboc i Benjamin Pommeraud van iniciar una campanya per internet per finançar la seva pel·lícula *Demain la Veille*, i van arribar a reunir uns 50000 dòlars.

També parlarem del projecte *Star Citizen*. Es tracta d'un videojoc multijugador a l'espai de simulació de combats. Va ser anunciat l'any 2012, quan va reunir a Kickstarter uns 2M de dòlars. Avui en dia se'l coneix per ser el videojoc que més ha recaptat amb aquest mètode i un dels projectes amb més finançament fins ara, havent reunit uns 400M de dòlars el dia 21 de novembre de 2021. [12]

El funcionament és molt simple. Sol ser un sistema basat en donacions, en el que sol haver-hi recompenses econòmiques (en el cas que es puguin generar beneficis o participacions en l'empresa) o simbòliques, per atraure els mecenes. Normalment, aquestes recompenses no monetàries són en forma d'agraïment o recompensant els mecenes amb el producte que has pogut crear gràcies als seus donatius. [7]

2.3 ICO

Un ICO (*Initial Coin Offering*) és l'equivalent en la indústria de les criptomonedes a una IPO (*Initial Public Offering*). Solen ser companyies que volen recaptar fons per crear un nou servei, i llancen al mercat un nombre limitat de tokens.

Les persones interessades inverteixen diners per rebre tokens creats per aquesta companyia, amb l'esperança que pugin de preu i puguin revendre-les. [13]

La majoria de les ICOS no estan regulades, per la qual cosa els inversors han de ser cautelosos a l'hora d'invertir en segons quins projectes.

Normalment, aquests projectes tenen un *whitepaper*, que sol ser una pàgina web dedicada a aquell token i al projecte en si. Solen explicar en què consisteix el projecte, quina quantitat de finançament necessiten recaptar, quin tipus de pagament s'accepten i quant de temps durarà la campanya. Els inversors poden participar i comprar tokens amb algunes criptomonedes conegudes com BTC o ETH. A canvi, reben aquests nous tokens creats per la companyia, de la mateixa manera en què es ven estoc en una IPO.

Estructura de les ICO

Les organitzacions poden escollir d'entre tres tipus d'estructura per una ICO:

- **Supply i preu estàtic:** La companyia especifica un objectiu de recaptació, per la qual cosa cadascun dels tokens té un preu fixat, i la

quantitat de *supply* està fixada.

- ***Supply* estàtic i preu dinàmic:** Això vol dir que la quantitat de finançament recaptat fins al moment determina el preu per cada token.
- ***Supply* dinàmic i preu estàtic:** Depenent de la quantitat de finançament recaptat fins al moment determina el *supply* de tokens que s'ofereix.

Avantatges i inconvenients

Els serveis en línia han provocat que sigui molt fàcil generar nous tokens, fet que provoca que les companyies considerin més fàcilment iniciar una ICO. Els creadors de la ICO generen els tokens, els reben, i els venen. Com que aquesta activitat no està regulada per autoritats financeres, els fons perduts per frau o per incompetència pot ser que mai siguin recuperats.

Els inversors busquen comprar aquests tokens perquè en un futur apugi el seu preu, i així puguin vendre'ls traient un benefici. Tot i això, no està clara la legalitat de les criptomonedes en un futur. L'any 2017, el banc popular de la Xina va vetar les ICO, al·legant que eren contra productives a l'estabilitat econòmica i financera. L'any 2021, el govern Xinès va il·legalitzar la mineria de criptomonedes i l'ús d'aquestes per fer transaccions.

3 Abast del projecte

En aquest apartat s'identifiquen quins són els objectius d'aquest projecte, totes les funcionalitats que estaran disponibles pels usuaris i les característiques de funcionament o 'requisits no funcionals' de la plataforma.

3.1 Objectius

L'objectiu general d'aquest treball de final de grau és el desenvolupament d'una aplicació web descentralitzada de micromecenatge per a empreses emergents, desplegada a la cadena de blocs d'Ethereum. Mitjançant els contractes intel·ligents, es poden definir algunes fites per anar finançant els projectes a mesura que es van complint, amb el fi d'evitar frau. També evitaríem les comissions que es queden moltes plataformes de micromecenatge actuals, i serien substituïdes per les taxes per mantenir la cadena de blocs de Polygon, que són molt menors a les comissions esmentades. Alguns projectes podrien finançar-se mitjançant les ICO (*Initial Coin Offering*), i així tindrien més oportunitat de trobar inversors.

3.2 Requisits funcionals

Els requisits funcionals són totes les funcionalitats que un sistema ha de complir i cal descriure'n el comportament de forma clara i concisa. Aquestes han sigut representades mitjançant casos d'ús, és a dir, interaccions entre l'usuari i el sistema per algun objectiu en concret.

3.2.1 Diagrama de casos d'ús

La interacció dels actors amb els casos d'ús, i la pròpia relació entre aquests, ha sigut definida mitjançant un diagrama de casos d'ús UML (Figura 1).

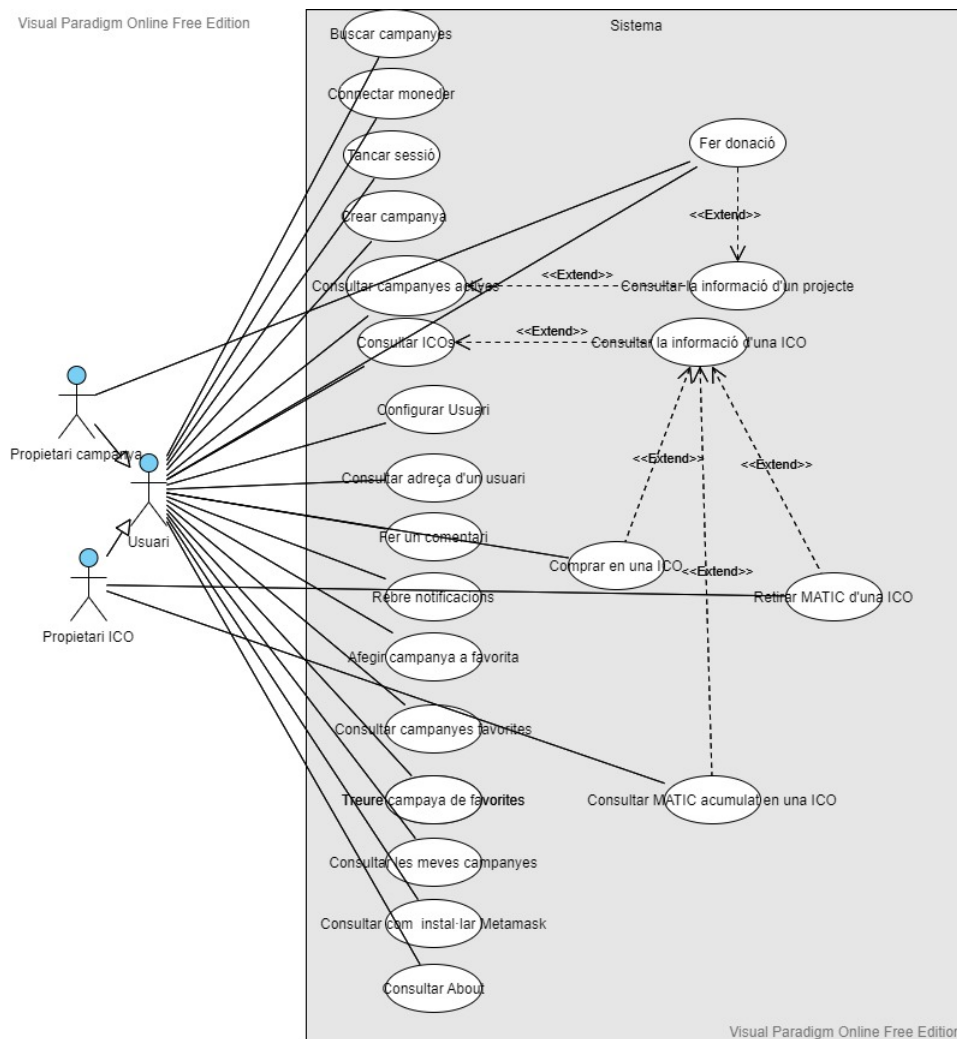


Figura 1: Diagrama de casos d'ús. Elaboració pròpia

3.2.2 Descripció *brief style*

A continuació, definirem els casos d'ús seguint el patró *brief style*:

UC01 - Connectar moneder: L'usuari connecta el seu moneder Metamask mitjançant un botó. Un cop connectat se li presentarà la pàgina principal de l'aplicació, i a la barra de navegació trobarà la seva adreça de moneder, o per contrapartida, el seu nom d'usuari si existeix.

UC02 - Tancar sessió: L'usuari tanca sessió mitjançant una icona a la barra de navegació. Les dades de l'usuari son esborrades de l'emmagat-

zematge de la sessió del negador.

UC03 - Crear campanya: L'usuari pot crear una nova campanya de finançament introduint les dades necessàries en un formulari.

UC04 - Consultar la informació d'un projecte: L'usuari pot accedir a una pantalla on pot trobar tota la informació de les campanyes.

UC05 - Fer una donació: L'usuari pot donar MATIC a una campanya de finançament, introduint la quantitat desitjada en un camp de text a la pantalla d'informació del projecte.

UC06 - Consultar campanyes actives: L'usuari pot accedir a la pàgina principal on trobarà totes les campanyes actives que encara no hagi arribat a l'objectiu de finançament.

UC07 - Consultar ICOs: L'usuari pot accedir a una pàgina on trobarà totes les ICOs disponibles.

UC08 - Consultar la informació d'una ICO: L'usuari pot accedir a una pantalla on pot trobar tota la informació de la ICO. També trobarà l'adreça del contracte, per si vol importar-se els tokens comprats al Meta-mask.

UC09 - Comprar en una ICO: L'usuari pot comprar criptomonedes en una ICO. Escriu la quantitat de monedes que vol comprar i li apareix la quantitat en MATIC que li costarà. Clica a comprar i se li transferiran les monedes al seu moneder. El MATIC gastat quedarà guardat a l'adreça del contracte.

UC10 - Consultar MATIC acumulat en una ICO: L'usuari propietari de la ICO podrà consultar quant MATIC i ha acumulat al contracte.

UC11 - Retirar MATIC d'una ICO: L'usuari propietari de la ICO podrà retirar el total de MATIC gastat pels altres usuaris.

UC12 - Buscar campanyes: L'usuari pot buscar campanyes escrivint en una barra de cerca. Apareixeran totes aquelles campanyes en què el títol inclogui la/es paraula/es buscada/es.

UC13 - Consultar *About*: L'usuari pot accedir a una pàgina on s'explica qui és l'autor i en quin context s'ha elaborat el projecte.

UC14 - Configurar usuari: L'usuari pot canviar-se el nom d'usuari i el color en què aquest apareixerà.

UC15 - Consulta adreça d'un usuari: L'usuari podrà clicar sobre el nom d'un usuari i apareixerà un text amb l'adreça de l'usuari en qüestió.

UC16 - Fer un comentari: L'usuari podrà escriure comentaris a la pàgina de la campanya i d'una ICO. També podrà respondre a altres comentaris.

UC17 - Rebre notificacions: L'usuari rebrà notificacions quan algú li respongui a algun comentari, quan una de les seves campanyes arribi a l'objectiu de finançament o quan algun usuari comenti en alguna d'aquestes.

UC18 - Afegir campanya a favorita: L'usuari podrà afegir les campanyes a la llista de favorites.

UC19 - Treure campanya de favorites: L'usuari podrà treure una campanya a la llista de favorites.

UC20 - Consultar campanyes favorites: L'usuari podrà consultar la llista de les seves campanyes favorites.

UC21 - Consultar les meves campanyes: L'usuari podrà consultar la llista de campanyes iniciades per ell.

UC22 - Consultar com instal·lar Metamask: L'usuari es trobarà un text on se li indicarà com instal·lar el *plug-in* de Metamask i com afegir-hi la xarxa de Polygon.

UC23 - Consultar respostes a comentaris: L'usuari podrà veure les respostes a un determinat comentari.

UC24 - Clicar a les notificacions: L'usuari podrà clicar a les notificacions de forma que se'l redirigirà a la pantalla corresponent.

UC25 - Canviar de compte: L'usuari podrà canviar de compte a Metamask i l'aplicació es recarregarà amb la informació d'usuari del compte actual.

3.3 Requisits no funcionals

Els requisits no funcionals defineixen quines propietats ha de complir el sistema. A continuació, els trobareu llistats seguint la plantilla d'especificació de requisits de Volere (setzena edició) [14].

10. Look and Feel Requirements

- *10a. Appearance Requirements:* L'aplicació ha de complir amb les expectatives de l'autor del projecte i ha de complir amb els estàndards actuals de dissenys de pàgines web.
- *10b. Style Requirements:* L'aplicació ha de tenir un estil propi i reconeixible pels usuaris. És important que el consumidor vegi el producte de forma positiva, donat que molts cops l'aparença del producte és qui determina si el projecte és un èxit o no.

11. Usability and Humanity Requirements

- *11a. Ease of Use Requirements :* L'aplicació ha de ser fàcil d'utilitzar per als potencials usuaris. S'ha de tenir en compte l'habilitat dels usuaris esperats i la complexitat del seu funcionament.
- *11c. Learning Requirements:* Els usuaris han de saber fer servir l'aplicació de forma intuïtiva.
- *11d. Understandability and Politeness Requirements:* L'aplicació utilitzarà vocabulari comprensible per a qualsevol tipus de persona. També s'empraran botons en forma d'icones fàcils de distingir i amb un comportament previsible.
- *11e. Accessibility Requirements:* Qualsevol usuari ha de poder accedir a l'aplicació. Per aquelles persones no familiaritzades amb els moneders *crypto*, se subministraran enllaços amb informació a la pantalla per connectar el moneder.

12. Performance Requirements

- *12a. Speed and Latency Requirements:* L'aplicació ha de respondre de forma ràpida i fluida a les interaccions amb l'usuari. La velocitat de processament de les transaccions no hauria de suposar una mala experiència per a l'usuari, tot i que en algun moment la xarxa de Polygon pot patir saturació.
- *12b. Safety-Critical Requirements:* L'aplicació no causarà cap mal ni al dispositiu on es troba el navegador ni a l'usuari.
- *12c. Precision or Accuracy Requirements:* L'aplicació permet l'ús de decimals en totes les transaccions monetàries.
- *12d. Reliability and Availability Requirements:* L'aplicació ha d'estar disponible sempre a partir de la seva posada en producció.

- *12h. Longevity Requirements:* Aquesta aplicació hauria de mantenir-se operativa amb el nombre màxim de pressupost per un mínim de 4 anys.

13. Operational and Environmental Requirements

- *13a. Expected Physical Environment:* L'aplicació s'ha de poder utilitzar en qualsevol tipus d'ordinador sota qualsevol situació d'entorn.
- *13b. Requirements for Interfacing with Adjacent Systems:* L'aplicació ha de poder interaccionar amb la cadena de blocs MATIC a partir de les interfícies binàries (ABI) dels contractes intel·ligents i de Metamask, que fa de proveïdor de web3.
- *13d. Release Requirements :* L'aplicació s'anirà actualitzant a mesura que els usuaris demanin més funcionalitats. El desplegament de l'aplicació es farà de forma automàtica al servidor, per la qual cosa els usuaris podran veure els canvis en entrar a la web.

14. Maintainability and Support Requirements

- *14b. Supportability Requirements:* Els usuaris han de poder posar-se en contacte amb l'autor de l'aplicació per demanar suport. Aquest, els hauria de respondre en el termini màxim d'una setmana.
- *14c. Adaptability Requirements:* Eventualment, l'aplicació estarà disponible pel telèfon mòbil.

15. Security Requirements

- *15a. Access Requirements:* Tots els usuaris poden veure tota la informació: transaccions, adreces, informació, etc
- *15b. Integrity Requirements:* L'aplicació impedeix que l'usuari introdueixi dades errònies com donar 0 MATIC a una campanya. També canvia les dades de l'usuari quan aquest decideix canviar de compte al moneder. Si l'usuari decideix canviar de xarxa, es tanca la sessió i se'l redirigeix a la pàgina on es connecta el moneder, mostrant un missatge de xarxa errònia.

16. Cultural Requirements

- *16a. Cultural Requirements:* L'aplicació no ha de ser ofensiva envers cap col·lectiu.

17. Legal Requirements

- *17a. Compliance Requirements:* L'aplicació ha de complir totes les lleis relacionades amb el sistema construït.

3.4 Riscos

És important conèixer els riscos del nostre projecte amb antelació, ja que ens permetrà ser conscients de quins són els factors que poden afectar negativament al projecte i minimitzar-los.

- **Estafes:** Qualsevol projecte relacionat amb la recaptació de finançament sol ser una font d'estafes, i és un dels punts més crítics del nostre projecte.

Hem d'intentar que els projectes siguin tan fiables com sigui possible i publicitar aquells que siguin més prometedors i que portin més feina darrera.

- **Volatilitat de les criptomonedes:** El segon gran risc és la volatilitat del valor de les criptomonedes. Aquest fet podria provocar que algunes startups que necessitessin una base sòlida de capital no s'interessessin a finançar-se a la nostra plataforma, ja que el valor del Matic podria variar molt en un període de temps curt.

- **Desconfiança en la tecnologia:** En tercer lloc, està la creixent desconfiança de la societat en les criptomonedes. A mesura que les criptomonedes i la tecnologia blockchain s'ha anat fent un lloc en el món, més detractors i crítics han aparegut. En alguns països com la Xina, Marroc o Algèria, s'ha restringit o prohibit qualsevol transacció amb criptomonedes, mentre que a la majoria de països del món encara no està regulat. [15].

Això és degut a molts factors, com la necessitat dels governs i entitats financeres per regular els diners i l'economia o l'aparició d'alguns criptoactius sense cap mena de projecte real que els recolzi[16].

4 Metodologia de treball

S'han fet servir tot un seguit d'eines especialitzades en el desenvolupament àgil de software que han ajudat a portar un bon control de l'estat del projecte i a compartir el treball realitzat amb el director del projecte.

Documentació

La memòria final del projecte s'ha elaborat en LaTeX a Overleaf, que és un editor de textos en línia per escriure documents científics. Aquesta eina ha ajudat a estructurar el document de forma senzilla, a crear una bona bibliografia i citar els diferents recursos consultats. Altres documents més simples, per les entregues de l'assignatura GEP, han sigut redactades amb Google Docs.

Seguiment

Respecte al seguiment amb el director del projecte, s'han fet reunions cada quinze dies per a assegurar que el projecte estava avançant adequadament i per parlar de possibles millores de tot allò que ja s'havia fet. L'autor ha utilitzat aquestes reunions per fer consultes al director respecte les fites i documents a entregar del projecte.

Desenvolupament

El codi s'ha desenvolupat de forma local i s'ha anat actualitzant a un repositori remot de GitHub, mitjançant la tecnologia de control de versions Git. Per cada nova tasca, s'ha creat una nova branca a partir de la principal amb el nom de la tasca i quan s'ha implementat i testejat s'ha fusionat a la branca principal. Aquest sistema ha sigut útil quan l'autor ha treballat en dues tasques diferents al mateix temps, ja que s'ha estalviat errors deguts a altres tasques que no estaven tancades i no s'havien acabat d'implementar.

Gestió de les tasques

Pel que fa a la gestió de les tasques i del temps emprat, s'ha utilitzat Jira amb la plantilla SCRUM. Hi havia un backlog on es van afegir totes les tasques que s'havien de fer durant el projecte i que es van estimar en

hores per a poder planificar el projecte correctament. També, s'hi han anat afegint aquelles que han anat sorgint o en les que l'autor no havia pensat. Com s'ha esmentat s'ha seguit el mètode SCRUM, per tant, s'ha desenvolupat el projecte mitjançant esprints, que han sigut de dues setmanes. En començar cada esprint s'afegien algunes tasques a la columna To Do seguint la planificació inicial i s'intentaven tancar totes en aquelles dues setmanes. Durant la implementació de les tasques s'han anat indicant les hores dedicades a cadascuna, de manera que la suma d'hores de totes les tasques havia de correspondre de forma aproximada a les hores que havia pensat dedicar a un esprint.

Les tasques han passat pels estats: To Do \rightarrow Doing \rightarrow Implemented \rightarrow Closed. Han passat de To Do a Doing quan començava a implementar-les; de Doing a Implemented quan s'acabaven d'implementar i l'autor les pujava al repositori remot; finalment passaven a Closed quan la branca corresponent a la tasca era fusionada amb la branca principal. En el cas que l'autor trobés un *bug*, s'ha creat una nova tasca per arreglar-lo i se li donava més o menys prioritats depenent de la gravetat del problema.

5 Planificació inicial

En aquest apartat es descriuen totes les tasques a realitzar durant el projecte. Seguidament, s'estimaran i trobareu un diagrama de Gantt amb la planificació temporal dividida en esprints. Finalment, s'avaluaran els possibles riscos a l'hora d'implementar el projecte i possibles solucions o plans alternatius a aquests problemes. Abans de començar, s'indiquen un seguit de dades globals que permetran ser més precisos i realistes en la planificació:

- Data d'inici: 21/02/2022
- Data de finalització: 20/06/2022
- Durada en hores: 540 h de feina disponibles
- Data prevista per a la lectura del TFG: 27 juny - 1 juliol
- Hores diàries: 6 h (30 h setmanals)

Aquest apartat mostra la planificació inicial, és a dir, es descriuen les tasques i la planificació que l'autor havia ideat **inicialment**. Aquestes, han pogut variar durant el projecte, per la qual cosa s'especificaran les modificacions de qualsevol dels següents subapartats a l'apartat 13 (Planificació revisada).

5.1 Descripció de les tasques

S'enumeren les tasques a realitzar dividides en grups i a continuació s'indicaran les dependències temporals entre elles. Finalment, trobareu una taula de resum de totes les tasques.

Tasques de gestió del projecte

T1. Reunions amb el director de TFG: Reunir-se amb el director del TFG cada 15 dies per comprovar que el projecte va en bon camí i per discutir els objectius al següent esprint. Estimació: 10 h

T2. Documentació memòria final: Anar escrivint la memòria final en LaTeX a mesura que vaig avançant amb el projecte. Estimació: 100 h.

T3. Abast: Definició de l'abast del projecte en el context del seu estudi. Entrega el dia 1 de març. Estimació: 25 h

T4. Planificació temporal: Planificació temporal per a l'execució total del TFG. Entrega 7 de març. Estimació: 15 h

T5. Pressupost i sostenibilitat: Autoavaluació sostenibilitat del projecte. Entrega 14 de març. Estimació: 10 h

T6. Integració del document final: Document final amb la síntesi del projecte. Entrega 21 de març. Estimació 15 h

Tasques de gestió eines TIC

T7. Creació Jira: Creació del projecte a Jira. També cal afegir totes les tasques definides en el document de Planificació temporal al *backlog*. Estimació: 5 h

T8. Creació repositori GitHub: Creació del repositori de GitHub i incloure-hi la llicència que cregui més adequada. Estimació: 5 h.

T9. Inicialització projecte: Creació d'un projecte de React i Hardhat i actualització GitHub. Estimació: 10 h.

T10. Desplegament de l'aplicació: Desplegament de la pàgina web feta amb JavaScript i Solidity. Estimació: 20 h.

T11. Desplegament dels *smart contracts*: Desplegament dels contractes intel·ligents a Polygon. Estimació: 20 h. El cost de desplegament dels *smart contracts* a Polygon pot ser molt variable. Serà al voltant dels 0.3 €.

Tasques de programació

T12. Transferència d'Ether: Com a usuari vull poder fer una transferència de MATIC a una adreça determinada per a així poder finançar un projecte vinculat a aquesta.

En el cas dels projectes amb ICO caldrà que l'usuari rebi les criptomonedes oferides pel projecte al seu moneder. Estimació: 35 h.

T13. Sign up i sign in: Com a usuari vull poder iniciar sessió mitjançant Metamask per a així poder veure els projectes que m'interessen i

llegir les notificacions. Estimació: 30 h.

T14. Creació pantalla principal: Com a usuari vull veure una pantalla principal on apareguin les campanyes més exitoses i les notificacions de l'usuari. També apareixeran les meves notificacions i podré accedir a altres pantalles, com a la de configuració. Estimació: 40 h.

T15. Pantalla de configuració: Com a usuari vull tenir una pantalla de configuració del meu perfil on pugui canviar el meu nom d'usuari i el color. Estimació: 30 h.

T16. Cercador de projectes: Com a usuari vull un cercador a la pàgina principal on pugui escriure paraules i apareguin projectes que incloquin aquella/es paraula/es. Estimació: 20 h.

T17. Informació d'un projecte: Com a usuari vull una pantalla per cada projecte on pugui veure una descripció detallada i diferents enllaços i recursos que hagi penjat l'usuari promotor de la campanya. Hi haurà una secció amb el finançament necessari, on es mostrarà quin percentatge d'aquest es porta recaptat fins al moment. Estimació: 20 h.

T18. Donar MATIC: Com a usuari vull un camp a la pantalla d'informació del projecte on indicar quina quantitat de MATIC vull donar i un botó per confirmar-ho. Estimació: 30 h.

T19. Comentar un projecte: Com a usuari vull una secció de comentaris a cada projecte per a poder preguntar dubtes o interactuar amb altres usuaris. Estimació: 30 h.

T20. Iniciar campanya: Com a usuari vull poder començar una campanya per recaptar fons per un projecte. Apareixerà un formulari amb camps com: nom del projecte, descripció amb un mínim de paraules, data de finalització de la campanya, referències (enllaços) a altres webs, fotografies i vídeos que hauran d'estar penjats a YouTube. Es podrà demanar finançament amb ICO (*Initial Coin Offering*) o sense. En el primer cas caldrà indicar quin volum de criptomonedes poses a la venda i el valor de cadascuna i en segon caldrà indicar la xifra a recaptar. Estimació: 30 h.

T21. Donar Like a un projecte: Com a usuari vull donar Like a un projecte per a a que el projecte s'afegeixi a la llista dels que m'interessen. També vull poder treure el Like. Estimació: 25 h.

T22. Rebre notificacions: Com a usuari vull rebre notificacions quan hi hagi informació actualitzada d'un projecte que m'interessi i quan em responguin a un comentari. Estimació: 30 h.

5.2 Dependències

$T3 \rightarrow T4 \rightarrow T5 \rightarrow T6; T4 \rightarrow T7; T8 \rightarrow T9; T9 \rightarrow T12; T9 \rightarrow T13; T13 \rightarrow T14; T13 \rightarrow T15; T14 \rightarrow T16; T20 \rightarrow T17; T17 \rightarrow T18; T17 \rightarrow T19; T14 \rightarrow T20; T17 \rightarrow T21; T21 \rightarrow T22; T19 \rightarrow T22; T11 \rightarrow T10.$

A més a més, la tasca T11 (desplegar els contractes intel·ligents) no es pot fer fins a acabar totes les tasques d'implementació.

5.3 Taula resum

En aquest apartat trobareu tres taules de resum [Figures 2,3 i 4] de totes les tasques definides anteriorment.

Per a estimar el cost calcularem el cost de personal per activitat. L'únic perfil que treballa en totes les tasques serà un programador, que segons la mitjana espanyola guanya un 15 €/hora brut [17]. Afegint la seguretat social, cal multiplicar-ho per 1,3, o sigui, 19,5 €/hora. Això ho he multiplicat per les hores de cada tasca per saber el cost estimat de cadascuna.

En el cas de la tasca de desplegament dels *smart contracts*, s'ha sumat al cost de personal la taxa per efectuar aquest desplegament a la *sidechain* de Polygon, que rondaria els 0,3 € [18].

El temps estimat per a dur a terme el projecte és de 560 hores. Tenint en compte que s'han sobreestimat moltes tasques, és molt probable que el temps emprat sigui menor.

Codi	Nom	Estimació (h)	Dependències	Recursos (€)
T1	Reunions amb el director de TFG	10	-	195
T2	Documentació memòria final	100	-	1950
T3	Abast	25	-	487,5
T4	Planificació temporal	15	T3	292,5
T5	Pressupost i sostenibilitat	15	T4	292,5
T6	Integració del document final	15	T5	292,5

Figura 2: Resum tasques de gestió. Elaboració pròpia

T7	Creació Jira	5	T4	97,5
T8	Creació repositori GitHub	5	-	97,5
T9	Inicialització projecte	10	T8	195
T10	Desplegament de la pàgina web	20	T11	390
T11	Desplegament dels smart contracts	20	Totes les de programació	390,3

Figura 3: Resum tasques eines TIC. Elaboració pròpia

T12	Transferència de Matic	35	T9	682,5
T13	Signup i sign in	30	T9	585
T14	Creació pantalla principal	40	T13	780
T15	Pantalla de configuració	30	T13	585
T16	Cercador de projectes	20	T14	390
T17	Pantalla d'informació d'un projecte	20	T20	390
T18	Donar Matic	30	T17	585
T19	Comentar un projecte	30	T17	585
T20	Iniciar campanya	30	T14	585
T21	Donar Like a un projecte	25	T17	487,5
T22	Rebre notificacions	30	T21, T19	585

Figura 4: Resum tasques de programació. Elaboració pròpia

5.4 Gantt

A continuació trobareu un diagrama de Gantt on s'han plasmat quines tasques es duran a terme cadascuna de les setmanes i esprints en les quals es treballarà en el projecte [Figura 5]. Com es pot observar, la segona setmana de cada esprint s'haurà de treballar de forma paral·lela en alguna tasca de programació i de documentació. A part, s'han de fer la reunió de seguiment amb el tutor del TFG.

S'ha intentat equilibrar la càrrega de treball. Al principi del projecte, es pot observar que es treballarà en més tasques. Això és degut al fet que són tasques de documentació per a l'assignatura de GEP i d'inicialització dels entorns i eines que s'utilitzaran per al desenvolupament del projecte. Aquestes, a priori, haurien de portar una càrrega de treball menor a les tasques de programació. Al final del projecte, s'ha intentat tenir menys càrrega de tasques de programació, ja que seran les setmanes on més es treballarà en la redacció de la memòria del projecte.

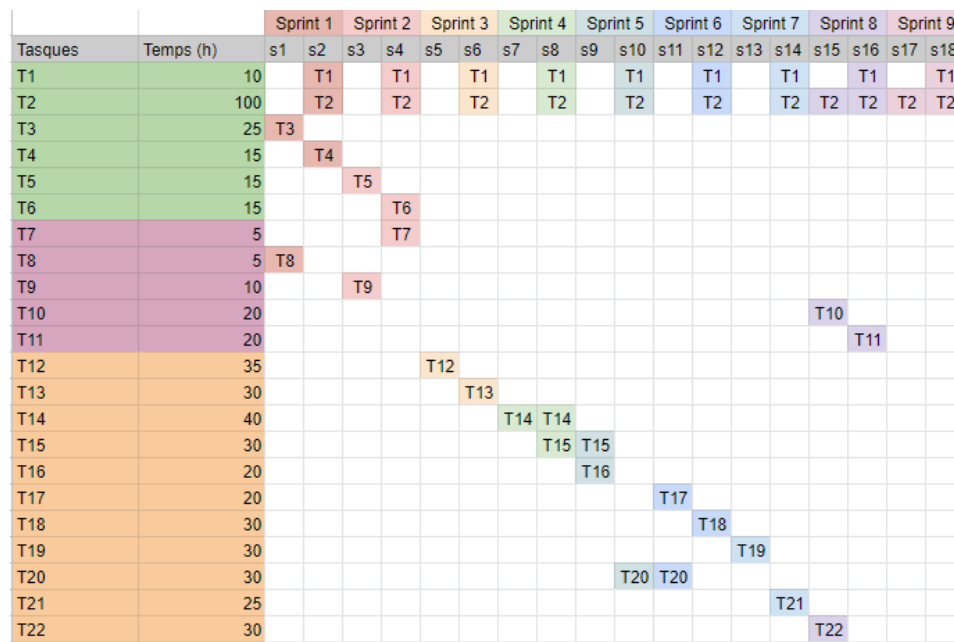


Figura 5: Gantt de la planificació inicial del projecte. Elaboració pròpia

6 Gestió del risc: Plans alternatius i obstacles

Un dels grans obstacles que amb els que em puc trobar al llarg del projecte és la meua poca experiència com a desenvolupador d'aplicacions descentralitzades. És molt probable que més d'un cop no sàpiga com implementar alguna funcionalitat en Solidity.

En el cas que em trobi amb aquest problema, crearé una nova tasca de recerca d'informació sobre aquest tema. Ja tinc guardades algunes pàgines web i alguns cursos especialitzats en cadena de blocs que em poden ajudar en aquesta situació. A més, he sobreestimat algunes tasques a causa de la poca experiència que tinc amb aquestes tecnologies.

Com mostra el diagrama de Gantt [Figura 2], als dos últims sprints no tinc gaire feina de programació i la càrrega de treball és més baixa, per la qual cosa es podria allargar una mica la implementació del projecte i acabar el projecte en el termini indicat. Els recursos addicionals necessaris serien els costos de consum d'energia del meu ordinador.

Un altre risc és la volatilitat del preu del Matic, que en ser una criptomoneda pot variar dràsticament. Aquesta moneda la necessitaré per desplegar els meus contractes a la cadena de blocs de Polygon. De moment, el preu de desplegament no sol ser major dels 0,40 € en moments pic per un contracte de mida mitjana.

En el cas que aquest preu s'elevi dràsticament, com passa en la xarxa principal d'Ethereum, em plantejaré desplegar els contractes a alguna altra xarxa, i sumaria hores a l'estimació de la tasca T11. També podria ser que no s'acabés alguna funcionalitat completament o de la manera desitjada. En aquest cas no existiria el risc del preu del MATIC i simplement es desplegarien els contractes a una xarxa de test, donat que el sistema encara no es posaria en producció.

7 Pressupost

7.1 Estimació dels costos

S'ha dividit el pressupost en quatre partides: costos de personal per activitat (CPA), costos genèrics (CG), contingències i imprevistos.

A continuació trobareu una taula amb el pressupost (Figura 6) i en els següents apartats es justificaran els resultats obtinguts en cadascuna d'aquestes partides.

Activitat	Import (€)	Observacions
T1	195	
T2	1950	
T3	487,5	
T4	292,5	
T5	292,5	
T6	292,5	
T7	97,5	
T8	97,5	
T9	195	
T10	390	
T11	390	
T12	682,5	
T13	585	
T14	780	
T15	585	
T16	390	
T17	390	
T18	585	
T19	585	
T20	585	
T21	487,5	
T22	585	Activitats que estan al diagrama de Gantt
Total CPA	10920	
Cost Genèric 1: Total costes d'electricitat	61,6	
Cost Genèric 2: Amortització ordinador	86€	Amortització fixada en un 26%.
Cost Genèric 3: Desplacament dels smart contracts	0,3	
Total CG	147,9	
Contingència	1660,2	Fixat un nivell de contingència del 15%. (Total CPA + Total CG) *15%
Imprevist 1: Prolongació activitats per desconeixement de la tecnologia (Cost=4.4 , risc = 10%	78,4	
Total imprevistos	78,4	
Total	12806,5	

Figura 6: Pressupost dividit en partides. Elaboració pròpia

7.1.1 CPA

L'únic perfil que treballa en totes les tasques serà un programador, que segons la mitjana espanyola guanya un 15 €/hora brut [17]. Afegint la seguretat social, cal multiplicar-ho per 1,3, o sigui, 19,5 €/hora. Això ho he multiplicat per les hores de cada tasca i ho he sumat.

7.1.2 CG

La partida de costos genèrics l'he dividit en costos energètics, amortització i desplegament dels contractes.

Cost energètic

Per a calcular el cost energètic, s'ha multiplicat el preu del kWh (0,4 €/kw aprox.) pel consum d'energia d'un ordinador cada hora (0,275 kWh) [19]. Per tant, 1 hora de treball a l'ordinador costaria uns $0,4 \text{ €/kw} * 0,275 \text{ kWh} = 0,11 \text{ €}$ l'hora. S'ha multiplicat per les hores de totes les tasques i s'ha sumat.

Amortització

Pel que fa a l'amortització s'ha buscat quina és l'amortització d'un ordinador (26%) [20] i s'ha multiplicat pels 800 € que va costar l'ordinador. Això són 208 € a l'any, però com el projecte durarà 4 mesos, s'ha dividit $208 / 4 = 86 \text{ €}$ d'amortitzacions.

Desplegament contractes

El desplegament dels contractes surt de buscar la quantitat de gas que es fa servir per desplegar un contracte mitjà a Polygon (3,85 M) i multiplicar-ho per la taxa mitjana per gas (50 Gwei = 0,05 MATIC) [18]. El resultat és 0,1925 MATIC, que en el moment del càlcul equival a 0,27 cèntims. Per arrodonir-ho, s'ha indicat 0,3 €.

7.1.3 Contingències

Pel que fa a les contingències podria variar fins a un 15%, per la qual cosa s'ha sumat el total del CPA i del CG i s'ha multiplicat per 0,15.

7.1.4 Imprevistos

Pel que fa a l'únic imprevist que s'ha tingut en compte, és que s'hagi de dedicar més hores a alguna tasca pel fet que l'autor no estigui acostumat a la tecnologia, o per l'aparició de *bugs* inesperats. Per això, s'ha pensat que pot ser que l'autor li dediqui unes 40 hores més al projecte. El cost d'això serien $40 * 0,11 \text{ €} + 40 * 19,5 \text{ €} = 784 \text{ €}$. En aplicar-li les probabilitats que passi, que podrien ser d'un 10%, queda en uns 78,4 €.

7.2 Control de gestió

El pressupost anterior permetrà comparar-ho amb el que realment s'ha gastat a cada tasca. En finalitzar el projecte es calcularà el desviament per cada concepte de cost i activitat, seguint l'esquema de la taula de pressuposts:

1. Costos directes per les activitats del Gantt
2. Costos indirectes
3. Contingències i imprevistos
4. Costos totals

8 Sostenibilitat i compromís social

8.1 Autoavaluació

Els meus coneixements teòrics sobre sostenibilitat són amplis en els tres camps: social, econòmic i ambiental. A la societat actual cada cop es tenen més en compte els aspectes socials i ambientals, i per això rebem formació des de petits. Tot i això, a la pràctica, només sé gestionar l'economia d'un projecte i això pot comportar problemes de caràcter social i ambiental.

Soc conscient de quines són les grans problemàtiques ambientals i de les seves causes i conseqüències, però no sé aplicar mètriques per mesurar la petjada ambiental d'un projecte ni quins indicadors seguir. A més a més, en els projectes que he fet fins ara no he tingut gaire en compte aquestes problemàtiques.

D'altra banda, sí que soc molt més conscient de l'impacte social dels meus projectes i sempre intento tenir en compte la justícia social i la salut a l'hora de dur-los a terme. De la mateixa manera que en l'aspecte ambiental, no conec eines ni mètriques per mesurar aquest impacte.

Pel que fa a l'àmbit econòmic d'un projecte, sí que he rebut més formació en aquest àmbit i sí que sé fer servir eines per estudiar la viabilitat econòmica com l'anàlisi d'externalitats, l'anàlisi de la competència, el DAFO, pla de negoci, etc.

Respecte a la gestió de recursos, tinc experiència i conec les eines per planificar projectes tenint en compte els recursos humans i econòmics, però no materials.

En conclusió, són conscient de la gravetat de la petjada ecològica i ambiental de la informàtica i de quins són els motius. No obstant això, no conec les eines per mesurar aquest impacte i seria clau rebre formació i mentalitzar-nos de la importància que poden tenir les nostres decisions pel futur del medi ambient. El mateix succeeix amb l'impacte social, el qual tinc en compte quan començo un projecte, però no sé com comprovar que compleix les meves expectatives socials un cop està en producció. Pel que fa a l'economia d'un projecte tinc un bon coneixement i puc gestionar-la correctament.

8.2 Anàlisi de sostenibilitat

En aquest apartat farem un anàlisi de la sostenibilitat del projecte en les tres dimensions esmentades, en format pregunta i resposta.

Dimensió ambiental

Projecte posat en producció: Has estimat l'impacte ambiental que tindrà la realització del projecte? T'has plantejat minimitzar l'impacte reutilitzant recursos?

El projecte no impactarà directament de forma negativa al medi ambient. Tot i això, sí que utilitzaré la tecnologia *blockchain*, que depèn d'ordinadors amb potència de càlcul en constant funcionament. Això està provocant un gran consum elèctric i un augment en la producció de microxips, que acaba resultant en contaminació i residus perjudicials per al planeta.

Pel que fa a la reutilització de recursos, l'únic recurs material serà el meu ordinador personal, que serà el mateix amb què faré el projecte.

Vida útil: Com es resol actualment el problema que vols abordar? En què millorarà ambientalment la teva solució a les existents?

Actualment, les empreses emergents es financen mitjançant prestadors convencionals, com bancs o estats, i també a través de plataformes de micromecenatge convencionals. La meua solució trasllada aquest últim cas a la cadena de blocs i el finançament es farà a través de la criptomoneda MATIC.

Ambientalment, no hi haurà cap millora. De fet, és possible que la tecnologia de la cadena de blocs consumeixi més energia que la web tradicional, que només necessita electricitat pels servidors.

Dimensió econòmica

Projecte posat en producció: Has estimat el cost de la realització del projecte?

Sí. He estimat que el cost serà de 12728,54.

Vida útil: Com es resol actualment el problema que vols abordar? En què millorarà econòmicament la teva solució a les existents?

tents?

La meva solució millorarà les existents perquè reduiré les taxes que s'han de pagar per les transaccions. Moltes plataformes convencionals es queden una part dels diners finançats a la seva plataforma, en la meva aplicació només caldrà pagar les taxes de gas per poder fer la transacció a la cadena de blocs de Polygon, i solen ser de molt pocs cèntims.

Dimensió social

Projecte posat en producció: Què creus que t'aporta a nivell personal la realització d'aquest projecte?

La meva solució millorarà les existents perquè reduiré les taxes que s'han de pagar per les transaccions. Moltes plataformes convencionals es queden una part dels diners finançats a la seva plataforma, en la meva aplicació només caldrà pagar les taxes de gas per poder fer la transacció a la cadena de blocs de Polygon, i solen ser de molt pocs cèntims.

Vida útil: Com es resol actualment el problema que vols abordar? En què millorarà socialment (qualitat de vida) la teva solució sobre les existents? Existeix una necessitat real de projecte?

La meva solució millorarà les existents pel que fa a la privacitat. Cap entitat ni organisme sabrà quants diners has recaptat, mentre que si s'opera de la forma convencional, els bancs i els estats saben perfectament quants diners has obtingut.

9 Descripció funcional

En aquest apartat es mostraran les diferents parts de l'aplicació web, en les que es poden dur a terme cadascun dels casos d'ús definits a l'apartat 3.2 d'aquest document. Primer es parlarà de la navegabilitat i després de les vistes.

9.1 Navegabilitat

Per a dur a terme la barra de navegació he utilitzat una llibreria anomenada "styled-components", que permet utilitzar CSS pur per estilitzar els components. Un cop connectat el moneder, se li mostra a l'usuari la barra de navegació juntament amb la pantalla principal de l'aplicació. Es pot accedir a les següents vistes:

- Pantalla principal (UC06 - Consultar campanyes actives)
- Pantalla de les ICOs (UC07 - Consultar ICOs)
- Pantalla de campanyes preferides (UC20 - Consultar campanyes favorites)
- Campanyes de l'usuari (UC21 - Consultar les meves campanyes)
- About (UC13 - Consultar About)

També hi ha un camp de text per buscar campanyes pel títol (UC12 - Buscar campanyes), l'adreça de l'usuari connectat (UC15 - Consulta adreça d'un usuari), un botó per tancar sessió (UC02 - Tancar sessió) i un altre per configurar l'usuari (UC14 - Configurar usuari) (Figura 7).

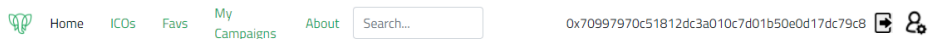


Figura 7: Barra de navegació. Elaboració pròpia

9.2 Vistes

En aquest apartat s'anirà explicant cadascuna de les vistes de l'aplicació. Cadascuna correspon al seu propi component de React i cadascuna gestiona el seu propi estat.

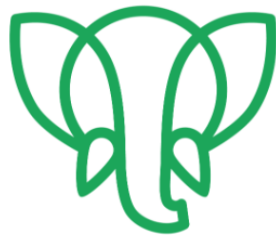
9.2.1 Connectar el moneder

En aquesta vista (Figura 8) es pot veure una capsa informativa on s'indica a l'usuari com instal·lar Metamask i afegir-hi la xarxa de Polygon.

A sota, hi ha un botó per connectar el compte de Metamask de l'usuari a l'aplicació.

Welcome to Ivory Fund!
The place for funding new projects or creating your own campaign!

Sign in and join our community!



If you have not installed the Metamask plugin yet, install it [here](#). To add Polygon Network follow this [documentation](#).

[Connect Metamask Wallet](#)

Figura 8: Vista per connectar el moneder. Elaboració pròpia

9.2.2 Pantalla principal

La pantalla principal de la web mostra les campanyes actives en una graella de tres columnes. Per cada campanya es pot veure una imatge, el títol, la descripció, la recaptació i un botó per veure més informació (Figura 9). En el cas que no hi hagi campanyes obertes, apareix el text *"No open campaigns"*.

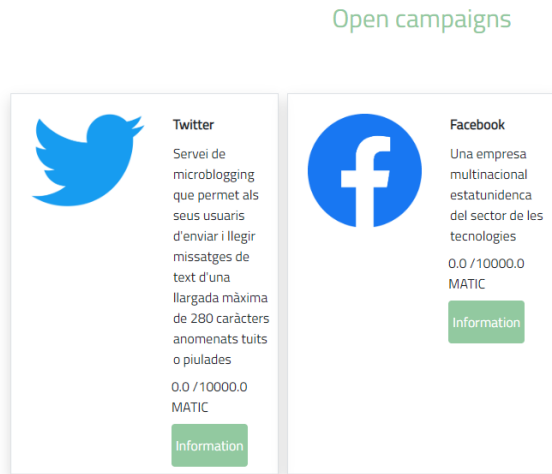


Figura 9: Pantalla principal de l'aplicació. Elaboració pròpia

9.2.3 Pantalla ICOs

La pantalla de les ICO mostra totes aquelles que s'han desplegat (cada ICO correspon a un contracte intel·ligent). Mostra el nom del token que es ven, l'estoc de tokens que queda per vendre i un botó per veure més informació (Figura 10).

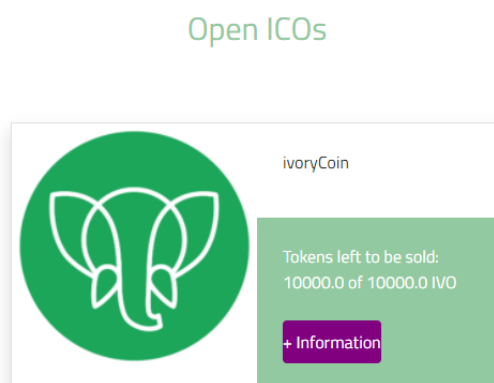


Figura 10: ICOs disponibles. Elaboració pròpia

9.2.4 Campanyes preferides

A la vista de campanyes preferides apareixen aquelles que l'usuari ha marcat com a preferides. Aquestes es mostren de la mateixa forma que a la pantalla principal (Figura 11). En cas que l'usuari no en tingui cap, apareix el text *Üser doesn't have any favourite campaigns*".

Favourite campaigns

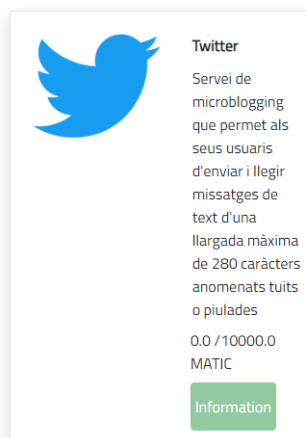


Figura 11: Campanyes favorites. Elaboració pròpia

9.2.5 Campanyes de l'usuari

A la pantalla de les campanyes de l'usuari apareixen totes les que aquest ha creat. També mostren el mateix que a la pantalla principal (Figura 12). En cas que l'usuari no n'hagi creat cap, apareix el text: *Üser has not started any campaign*".

My own campaigns



Figura 12: Campanyes de l'usuari. Elaboració pròpia

9.2.6 Pantalla About

A la pantalla *About*, s'explica breument en quin context s'ha desenvolupat el projecte i qui és l'autor. El text diu: *"Over a year ago, I became interested in blockchain technology and all the possible services it could offer. As a computer science student, I thought it would be a great idea to explore a little more and create a decentralized application on the Ethereum blockchain for my final thesis: IvoryFund"*.

9.2.7 Buscar campanyes

L'usuari té l'opció de buscar campanyes pel títol. Si escriu alguna paraula a la barra de cerca i prem "Enter", se li mostren totes les campanyes el títol de les quals inclou aquella paraula. També apareix un text amb el nombre de coincidències (Figura 13).

Results matching the word Facebook: 1



Figura 13: Buscar una campanya. Elaboració pròpia

9.2.8 Començar campanya

Per iniciar una campanya, l'usuari té disponible un botó a l'esquerra de la pantalla (Figura 14). Quan hi clica, se'l redirigeix a una pantalla on es troba un formulari amb els camps: títol, descripció curta, informació, URL, objectiu de finançament i pot carregar una imatge local. Quan ha omplert tots els camps i ha posat un URL correcte, pot clicar al botó "Start" de la part inferior i haurà creat una campanya (Figura 15).

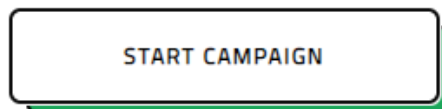


Figura 14: Botó per crear una campanya. Elaboració pròpia

Start Campaign

*Title

*Short description

*Information

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam et pulvinar tellus, ac cursus orci. Duis sit amet arcu non orci efficitur efficitur. Sed erat nunc, rhoncus eu dapibus ut, tempus id diam. Cras scelerisque nibh id lacinia semper. Donec velit magna, tempus at ipsum eget, efficitur ultrices sem. Fusce tincidunt, purus nec mollis ornare, ante lectus ultricies nisi, eget maximus magna mi scelerisque lectus. Nunc finibus accumsan tortor sed consequat. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Vivamus pellentesque metus sit amet lacus malesuada, at egestas orci commodo.

*URL

*Funds Requested (MATIC)

Image

Seleccionar archivo

Start

Figura 15: Formulari per crear una campanya. Elaboració pròpia

9.2.9 Configurar usuari

L'usuari també té l'opció de posar-se un nom i un color. A la pantalla per configurar l'usuari, hi ha un formulari amb un camp de text i un botó i un camp de text per canviar de color. Si l'usuari decideix escriure el codi hexadecimal del color, aquest s'actualitza al botó i viceversa.

Si l'usuari clica el botó, apareix un "SketchPicker", importat de la llibreria 'react-color'. En aquest, es pot escollir el color mitjançant la paleta, el camp de text pel codi hexadecimal o els camps per introduir el codi RGBA (Figura 16).

Un cop configurat, el compte ja tindrà un nom d'usuari. En cas de voler veure l'adreça d'aquell compte, només cal posicionar el cursor a sobre del nom i apareix un text amb l'adreça.

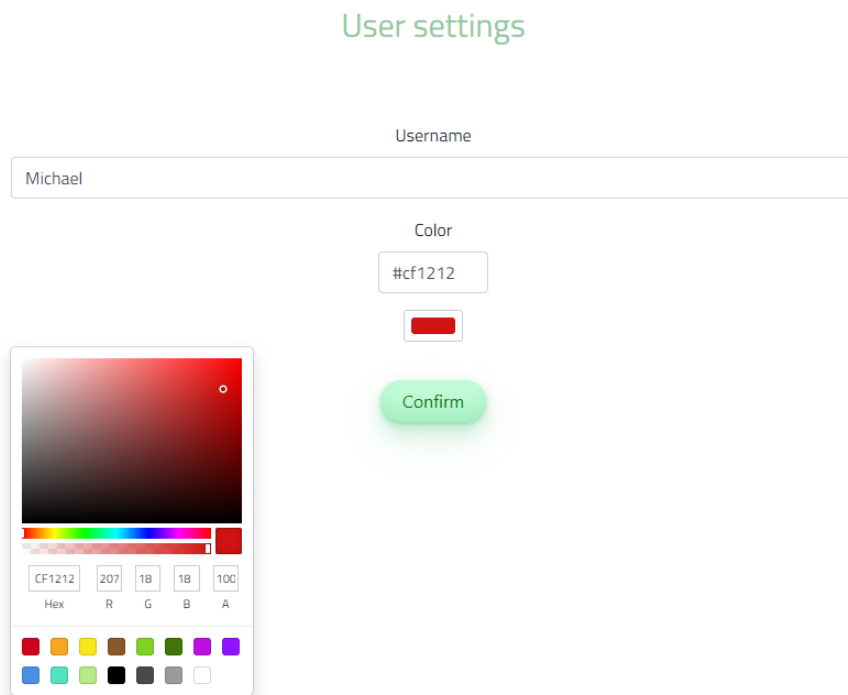


Figura 16: Configurar usuari. Elaboració pròpia

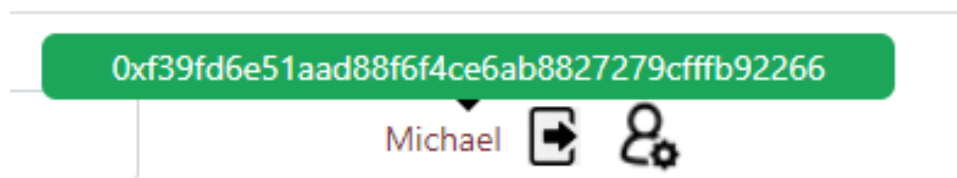


Figura 17: Veure adreça del compte. Elaboració pròpia

9.2.10 Informació d'una campanya

A la pantalla d'informació d'una campanya l'usuari pot trobar el títol, una petita descripció, un paràgraf d'informació, les URLs, l'adreça de l'usuari creador de la campanya, la quantitat de finançament obtingut, un camp de text i un botó per fer donacions i un botó amb forma d'estrella per afegir-la o treure-la de favorits. També pot trobar la secció de comentaris a la part inferior



Figura 18: Pàgina d'informació d'una campanya. Elaboració pròpia

Quan un usuari, que no sigui el propietari de la campanya, dona MATIC a una campanya, s'actualitza la pantalla i apareix el finançament acumulat i s'omple la barra de finançament obtingut (Figura 19).

A la part inferior de la vista hi ha una secció de comentaris. Primer hi ha un camp de text, on l'usuari pot escriure el seu comentari i clicar al botó "Comment". Un cop executada la transacció, aquest comentari apareix a la part inferior juntament amb els altres (Figura 20). Els comentaris consten d'un nom d'usuari, del qual es pot consultar l'adreça de la mateixa forma que a la Figura 17, i d'un missatge.

A cada comentari hi ha dos botons: *reply* i *thread* (on s'indica la quantitat de respostes al comentari entre parèntesis). El primer botó obre un



Figura 19: MATIC enviat correctament. Elaboració pròpia

desplegable on es pot escriure una resposta al comentari i enviar-la. El segon, permet anar a una nova vista amb totes les respostes a aquell comentari.

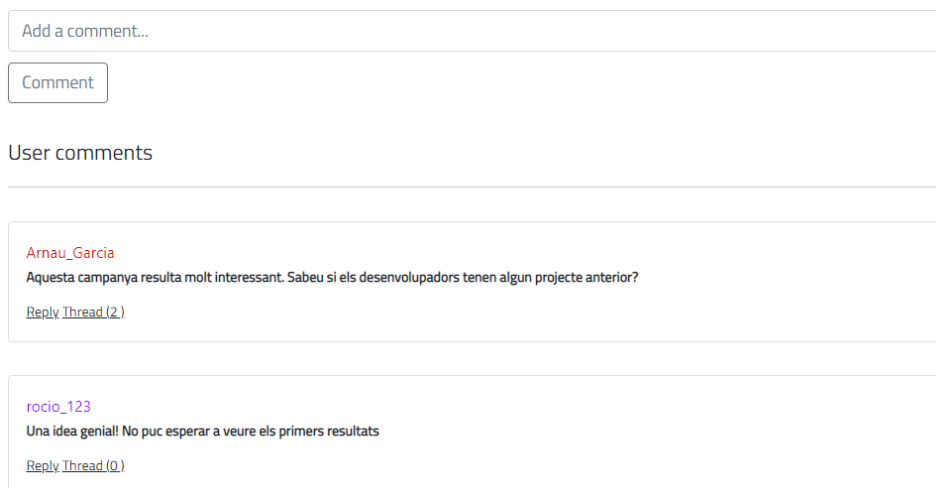


Figura 20: Secció de comentaris. Elaboració pròpia

9.2.11 Respostes a un comentari

Aquesta vista és una de les més senzilles. Quan l'usuari hi accedeix, pot veure totes les respostes a un comentari. Aquestes, es presenten de la mateixa forma que a la pantalla d'informació del projecte, i també permeten respondre a les respostes i accedir al *thread* (fil de respostes) de cadascuna.

Answers

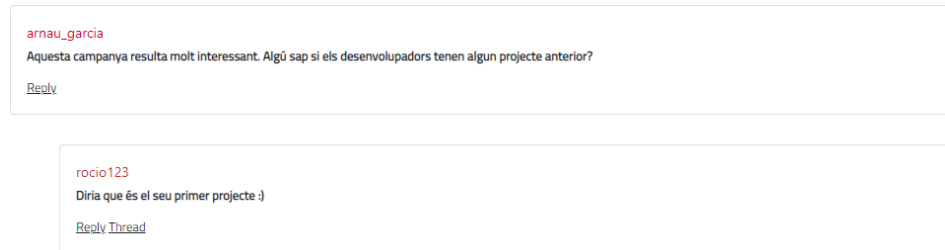


Figura 21: Respostes a un comentari. Elaboració pròpia

9.2.12 Pantalla d'informació d'una ICO

En aquesta vista l'usuari troba informació detallada de la ICO i una secció de comentaris, de la mateixa forma que en les campanyes. La diferència principal és que l'objectiu de la ICO es vendre els seus tokens a canvi de MATIC.

Els usuaris que vulguin participar en la ICO, caldrà que especifiquin al camp de text (Figura 22) quant tokens volen comprar. Al costat els apareix quant MATIC els costarà la transacció, i quan vulguin acceptar-ho clicaran al botó "Buy tokens". Un cop executada la transacció apareixerà un toast amb la frase "Successfully bought!".

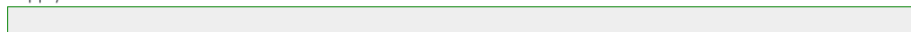


IvoryICO

Crowdfunding platform based on ethereum

= 10 MATIC [Buy tokens](#)

Supply left: 10000.0 of 10000.0 IVO



Information

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam ut aliquet justo. Suspendisse dapibus convallis ipsum, ut imperdiet augue varius venenatis. Sed pharetra tellus quis mattis congue. Fusce et nibh tellus. Integer molestie vulputate sapien, vitae tempus turpis suscipit ullamcorper. Nullam euismod, urna a vehicula placerat, est felis hendrerit quam, eu malesuada risus nunc ut libero. Donec congue velit eu felis euismod, eu mollis diam ultricies. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Sed vulputate fermentum leo, ac bibendum augue aliquet id. Fusce sagittis enim sit amet diam vulputate vulputate. Donec ultricies sapien nisl. Proin ultrices suscipit congue. Sit amet condimentum nunc porttitor id. Ut venenatis con eu nibh dignissim cursus. Donec vel tellus sit amet mauris auctor

Figura 22: Pantalla d'informació d'una ICO. Elaboració pròpia

En cas que els usuaris que han comprat aquests tokens els vulguin visualitzar al seu moneder per assegurar-se que són seus, només caldrà que importin el token a Metamask utilitzant l'adreça del contracte facilitada en la pantalla d'informació de la ICO. A la Figura 23, es pot veure com han arribat la quantitat exacta d'IVO que l'usuari havia comprat a canvi de 10 MATIC.

S'ha explicat la vista de l'usuari no propietari de la ICO, però encara queda veure quines peculiaritats es troba l'usuari designat com a propietari a l'hora de desplegar el contracte.

Aquest, en entrar a la pantalla, es trobarà un camp de text i un botó que diu "Withdraw MATIC". Al costat, hi ha una capsula d'informació amb el MATIC acumulat al contracte. En executar l'operació, el propietari rep el MATIC que estava acumulat al contracte al seu moneder i s'actualitza la pantalla, restant el MATIC que el propietari ha extret.

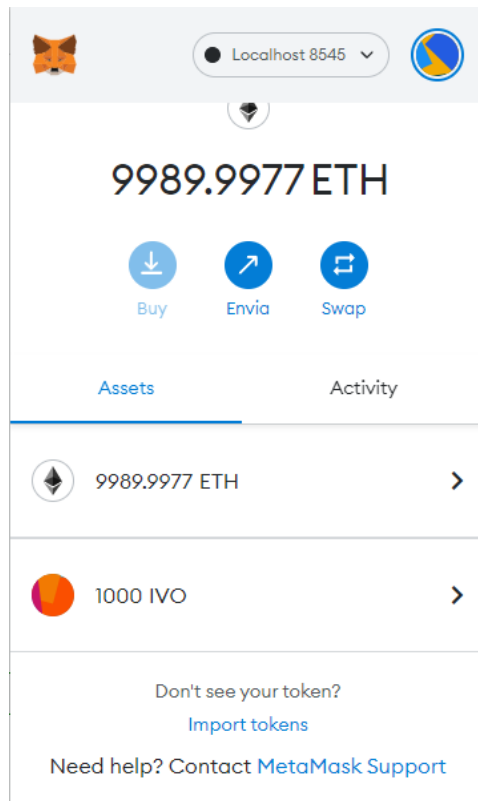


Figura 23: IVO al moneder de l'usuari. Elaboració pròpia

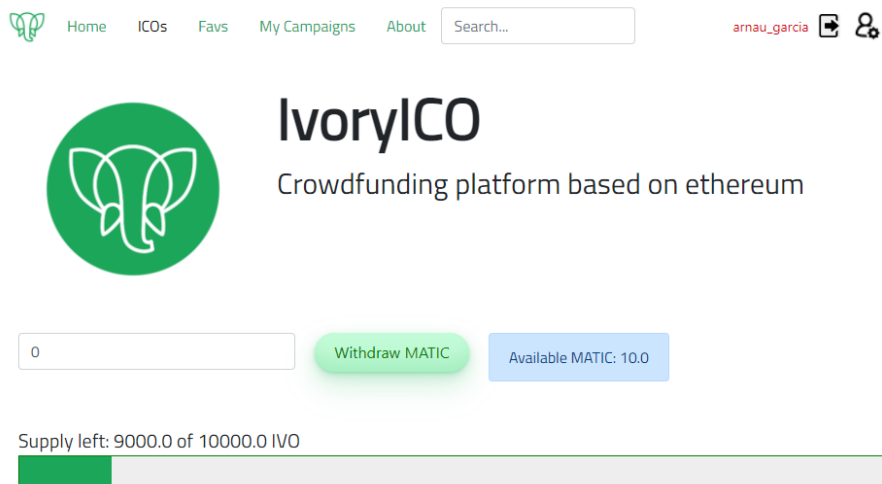


Figura 24: Pantalla d'informació d'una ICO per l'usuari propietari. Elaboració pròpia

10 Disseny

10.1 Arquitectura

L'aplicació té una arquitectura bastant diferent de les aplicacions web convencionals. Normalment, aquestes consistirien en un client *front-end* connectat a un servidor *back-end*. Finalment, les peticions al servidor manipularien les dades de la base de dades.

En les aplicacions descentralitzades l'arquitectura és més complexa i menys coneguda, per la qual cosa és important explicar cadascuna de les parts. Per facilitar la comprensió del lector, s'ha representat l'arquitectura mitjançant un esquema (Figura 25) on apareixen representades cadascuna de les parts i a continuació s'han explicat en detall.

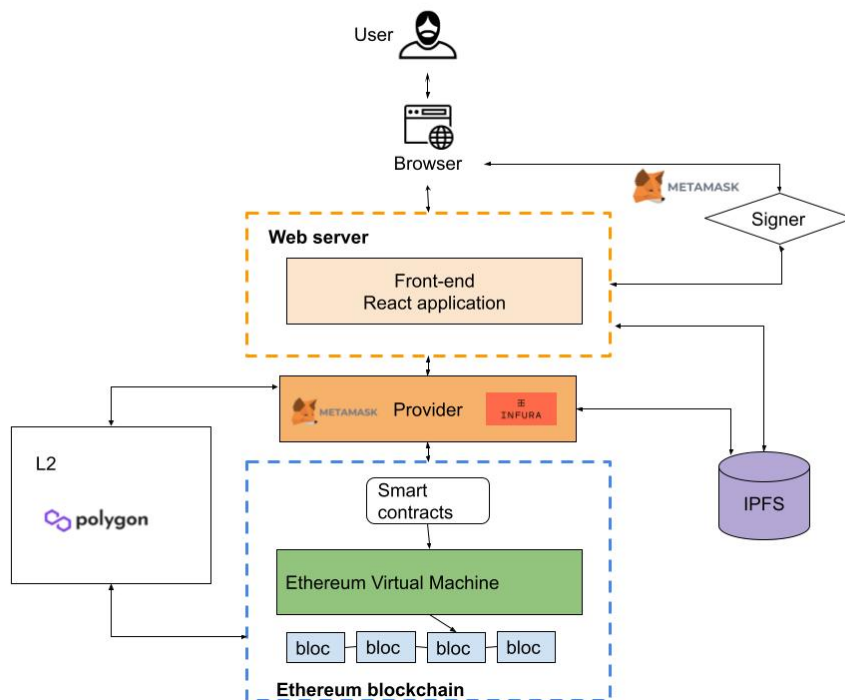


Figura 25: Arquitectura de l'aplicació. Elaboració pròpia

A l'esquema, es pot visualitzar un servidor web convencional, representat com "Web server". En aquest, es troba desplegat un client JavaScript que està connectat al **Signer**, el qual permetrà a l'usuari rebutjar o acceptar les transaccions. En el cas de l'aplicació d'aquest projecte, el client JavaScript

es troba desplegat en un servidor de Netlify i per entrar a la web ha de connectar el moneder de Metamask, que farà de Signer.

També veiem com està connectat a un **Provider**, el qual també serà Metamask. Aquest, és capaç de connectar la nostra aplicació amb qualsevol cadena de blocs basada en Ethereum. En aquest cas, s'utilitza la xarxa **Polygon**, que és una *sidechain* d'Ethereum, per raons d'escalabilitat i reducció en les taxes de les transaccions, la qual també veiem representada a la figura sota el tag L2. L2 (Layer 2) és un terme utilitzat per descriure un conjunt de solucions d'escalabilitat d'Ethereum, és a dir, les *sidechains*.

Al servidor **IPFS** és on es guarden les imatges de les campanyes. Més endavant s'explicarà què és IPFS, que de forma resumida, es tracta d'un protocol per emmagatzemar i compartir fitxers de forma descentralitzada. Els nodes en una xarxa IPFS formen un sistema d'arxius distribuïts. L'aplicació web hi accedeix mitjançant un node d'Infura.

10.2 Model de dades

Un model de dades és un tipus de llenguatge orientat a parlar d'una base de dades, i permet descriure l'estructura de les dades i la forma en què es relacionen. També, permet descriure quins atributs es troben en cadascuna de les classes en què es divideixen les dades i quines operacions es poden utilitzar per manipular-les.

UML, és el llenguatge de modelatge pels sistemes de *software* més conegut i utilitzat en l'actualitat. En el cas del projecte s'ha utilitzat mitjançant una llibreria anomenada sol2uml, que transforma els contractes intel·ligents en un diagrama UML (Figura 26). El resultat és una mica diferent del que es pot trobar en una base de dades, donat que al projecte no hi ha "classes" de dades. Es treballa amb contractes, que poden contenir estructures de dades, les quals sí que són més semblants a les típiques classes del desenvolupament de software convencional.

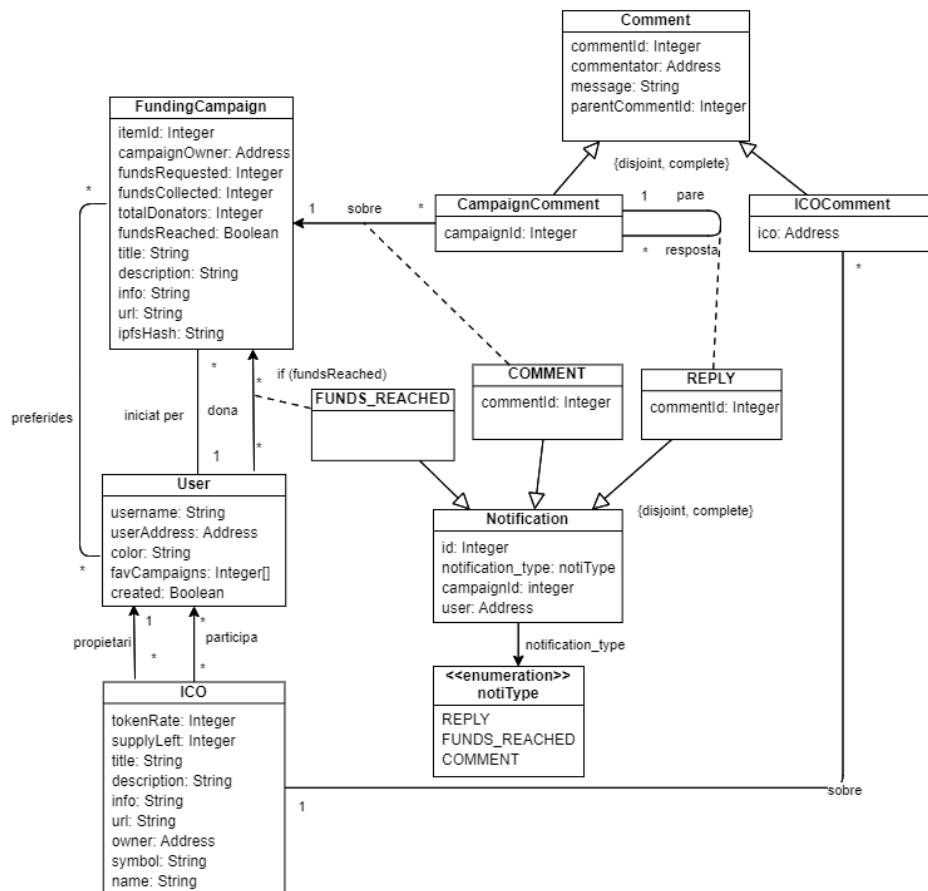


Figura 26: Model de dades. Elaboració pròpia

10.3 Patrons de disseny

A continuació es parlara dels patrons de disseny per al desenvolupament de Software i pel desenvolupament de components amb React.

MVC

El patró Model-Vista-Controlador és un patró comú en el disseny i l'arquitectura de software per implementar interfícies d'usuari, dades i lògica de control. Aquesta separació de conceptes permet una millor divisió del treball. Podem descriure les tres parts de la següent forma:

1. Model: Fa referència a les classes i les seves respectives dades. A les aplicacions web convencionals, fa referència a la base de dades.
2. Vista: S'encarrega del disseny i la presentació de la pàgina web.
3. Controlador: Fa d'intermediari entre el model i la vista, gestionant el flux d'informació. En altres paraules, provoca una transformació de les dades al model per la interacció de l'usuari amb la interfície d'usuari.

En el cas de les aplicacions descentralitzades, que és el cas que ens ocupa, hi ha algunes diferències molt remarcables que fan que s'hagi d'interpretar aquest patró des d'una nova perspectiva donat que ja no s'està treballant amb la típica l'arquitectura basada en un client i un servidor.

El Model, ja no és una base de dades. En aquest cas, correspon a les estructures de dades descrites en Solidity als contractes intel·ligents desplegats a la cadena de blocs, que són els encarregats de guardar la informació i les dades.

D'altra banda, el Controlador és bàsicament l'encarregat d'actualitzar els models, per la qual cosa correspondria als mètodes definits als contractes intel·ligents. El que és el mateix, el Controlador són els mètodes de la interfície ABI, resultat de la compilació dels contractes.

Finalment, la Vista continua sent el mateix que en les webs tradicionals. És a dir, un *front-end* HTML, CSS i JavaScript, que en el cas del projecte utilitza la llibreria ethers.js per fer crides als mètodes del controlador.

Patró *Hook*

L'API per utilitzar aquests *Hooks* va ser introduïda a React 16.8 i va revolucionar la forma de construir els components. Aquests permeten als components funcionals accedir de forma simple a algunes característiques de React com l'estat, les propietats, el cicle de vida, etc.

Aquest patró és molt útil pel fet que els components amb molt codi eren molt difícils d'interpretar i de mantenir, ja que es necessitava un mètode per cada etapa del cicle de vida. fent que apareguessin moltes inconsistències.

En aquest projecte s'han fet servir dos mètodes de la llibreria de react: `useState` i `useEffect`. El primer ens permet declarar i actualitzar l'estat dels components funcionals; el segon permet executar una funció després que la pàgina es renderitzi.

11 Implementació

En aquest apartat parlarem de tots els llenguatges de programació i les tecnologies emprades durant el projecte. Per cadascuna d'elles, explicarem què són i com han sigut integrades.

11.1 Llenguatges

- **JSX**: És una extensió de la llibreria ReactJS que permet la representació de components amb una sintaxi molt semblant a l'HTML.
- **CSS**: És un llenguatge de disseny gràfic per definir l'aparença d'un document estructurat. Normalment, s'utilitza per establir el disseny visual d'una interfície d'usuari per una pàgina web escrita en HTML.
- **Solidity**: És un llenguatge de programació orientat a objectes per escriure contractes intel·ligents. S'utilitza en diverses plataformes *blockchain*, però la més comuna és Ethereum.
- **JSON**: És un estàndard basat en text creat per a l'intercanvi d'informació entre sistemes, llegible per humans. A l'aplicació s'utilitza per a guardar informació de l'usuari *session storage* del navegador.

11.2 Tecnologies

En aquest apartat es parla d'algunes tecnologies emprades en el desenvolupament de la web. Moltes llibreries han sigut excloses d'aquest apartat, donat que són d'ús comú i no aportaria gaire al treball descriure-les.

S'ha profunditzat en aquelles més desconegudes, utilitzades en el món crypto i web3, com poden ser Remix IDE, ethers.js i Metamask. L'objectiu és que el lector entengui perquè serveixen, com funcionen i com les he integrat en el projecte.

Entorns de desenvolupament integrats

He utilitzat dos entorns de desenvolupament, que m'han servit per construir l'aplicació de forma més còmoda i ràpida: Remix IDE i Atom.

Remix IDE

Remix és un entorn de desenvolupament especialitzat en la creació de contractes intel·ligents a Ethereum. Et permet desenvolupar-los mitjançant un editor de textos, compilar-los i desplegar-los en una cadena de blocs local.

Una de les funcionalitats més interessants és una interfície d'usuari per executar les transaccions del contracte que l'usuari ha desplegat prèviament. A l'esquerra de la imatge (Figura 27) podem veure els botons per executar les transaccions. En algunes hi ha un camp de text al costat del botó, que correspon als arguments de la funció.

Si la transacció s'ha executat correctament, apareix una icona en forma de tick a la consola, seguit d'informació del cost en gas, del codi de la transacció i de les adreces del contracte i del compte des del qual s'ha executat.

En cas d'error, apareix una icona en forma indicant quina és la causa de l'error. Normalment, aquesta situació es dona quan s'incompleix un dels requisits definits a la funció del contracte intel·ligent.

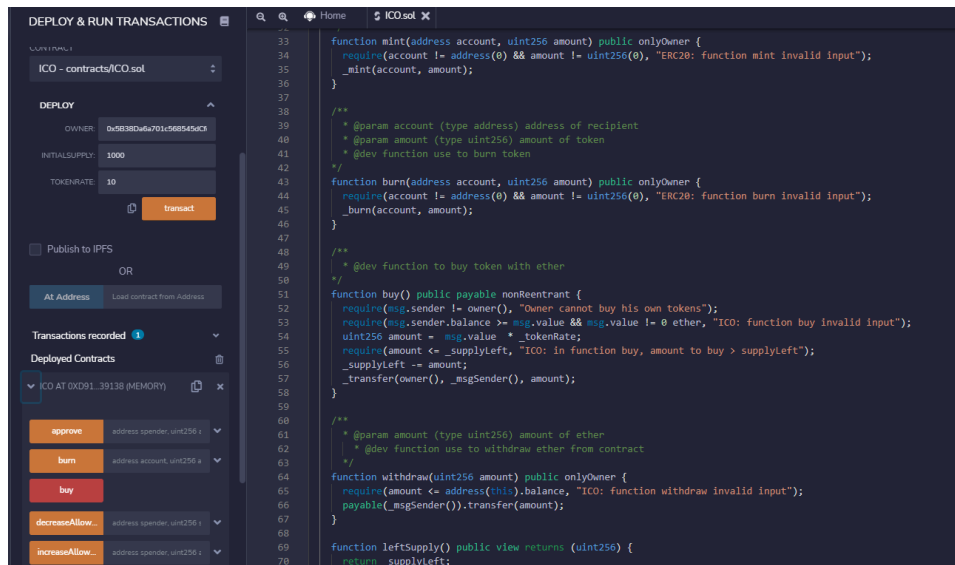


Figura 27: Remix IDE. Elaboració pròpia

Atom

Atom és un entorn de desenvolupament de codi obert amb suport de múltiples plug-in escrits en Node.js i amb control de versions de Git integrat. Aquesta última característica ha sigut molt útil a l'hora de pujar el codi

al repositori remot. Podia veure quins canvis havia fet en cadascun dels documents abans de fer els *commits* i pujar-los a GitHub.

M'he trobat amb característiques interessants com l'autocompleció de codi, que m'ajudava a escriure el codi més ràpidament. També permet dividir la seva interfície en diversos panells per a poder comparar codi i editar alhora múltiples fitxers.

M'ha resultat molt útil per elaborar el client amb React, ja que és una IDE molt senzilla i flexible que m'ha facilitat la construcció de l'aplicació.

Xarxa Polygon

És una xarxa situada a L2 (*Layer 2*) l'objectiu de la qual és incrementar l'escalabilitat de la xarxa d'Ethereum i reduir els costos de transacció. Aquesta característica és molt interessant pel projecte, donat que fer transaccions a la xarxa principal d'Ethereum resulta massa car, i un dels objectius principals de l'aplicació era reduir les taxes que es paguen en altres webs de micromecenatge que utilitzen diners tradicionals.

El 2017, la xarxa de test de la plataforma va fer-se pública sota el nom de Matic Network. Posteriorment, passaria a anomenar-se Polygon, però el nom del token natiu que s'utilitza a la xarxa va mantenir-se amb el nom de MATIC.

La quantitat total de tokens MATIC és de 10 mil milions. S'utilitza per pagar taxes de transacció i liquidacions entre membres de l'ecosistema Polygon. Per la qual cosa, aprofitarem aquest token per a fer les donacions i participar en les ICOs que ofereix l'aplicació, producte d'aquest projecte [21].

Hardhat

És un entorn de desenvolupament d'Ethereum dissenyat per al desenvolupament full-stack. Aquest ens permet desplegar els nostres contractes, executar tests, depurar codi, etc.

Un cop instal·lat hardhat mitjançant el gestor de paquets npm, cal inicialitzar l'entorn amb la comanda:

```
npx hardhat
```

Aquesta ens crearà:

- **hardhat.config.js:** Fitxer amb tota la configuració necessària (ruta als contractes intel·ligents compilats, versió de Solidity, URL del node de la xarxa de MATIC, codi identificador de la cadena de blocs en local...).
- **scripts:** Conté un fitxer per desplegar els contractes intel·ligents d'exemple quan l'executem.
- **test:** Conté un fitxer d'exemple per fer tests.
- **contracts:** Conté un fitxer amb un contracte intel·ligent d'Ethereum d'exemple.

Un cop afegits els nostres contractes intel·ligents a la carpeta corresponent, cal compilar-los amb la comanda.

```
npx hardhat compile
```

Això ens generarà un fitxer.json que contindrà un ABI (una interfície binària) amb la que podrem interaccionar des del nostre client amb la cadena de blocs.

Necessitarem iniciar el nostre node local per a poder desplegar els contractes i poder provar la nostra aplicació. Per a fer-ho cal executar la comanda:

```
npx hardhat node
```

Això ens generarà 20 comptes amb 10.000 ETH de test a cadascuna, que ens resultaran realment útils a l'hora de provar la nostra aplicació i fer tests.

Per a desplegar la nostra aplicació, només caldrà executar la següent comanda indicant-li a quina xarxa volem fer-ho (per ara a la xarxa de tests local).

```
npx hardhat run scripts/deploy.js --network localhost
```

Un cop escrits tots els tests a la carpeta del projecte corresponent, només cal executar la comanda:


```
npx hardhat test
```

Seguidament, apareixen els resultats de l'execució de cadascun dels tests unitaris als contractes intel·ligents (Figura 28):

```
PS C:\Users\arnau\OneDrive\Documents\TFG\crowdfunding-dapp> npx hardhat test
  ✓ Should fetch campaigns that include a word (185ms)
  ✓ Should create a campaign and fetch created ones (133ms)
  ✓ Should comment a campaign, reply it, and get both comments (240ms)

ICO
  ✓ Should buy all tokens and final balance should be 0 (84ms)
  ✓ Should withdraw the ether another user used to buy tokens (488ms)
  ✓ Should fetch all contract attributes (114ms)
  ✓ Should fetch ether balance of the contract address

User
  ✓ Should configure a user and get the current user (62ms)
  ✓ Should get user with no username and no color
  ✓ Should get number of users
  ✓ Should add fav campaign and check that it is successfully added to the list (84ms)
  ✓ Should remove fav campaign and check that it is successfully removed from the list (77ms)
  ✓ Should create a notification for replying (61ms)
  ✓ Should create a notification for reaching funding goal (57ms)
  ✓ Should create a notification for commenting (56ms)

17 passing (7s)
```

Figura 28: Resultat de l'execució dels tests als contractes intel·ligents. Elaboració pròpia

Metamask

És un *software* que he utilitzat en forma d'extensió per al navegador Google Chrome. Es tracta d'un moneder de criptomonedes molt utilitzat en el món del web3 i s'utilitza per a interactuar amb les aplicacions descentralitzades. Permet guardar Ether i qualsevol token que segueixi l'estàndard ERC-20 i fer transaccions d'una d'aquestes criptomonedes a qualsevol adreça d'Ethereum.

Si obrim l'extensió i iniciem sessió, tenim una pestanya per veure els nostres tokens (Figura 29) i una altra per veure les transaccions. A la part superior, podem canviar de xarxa i afegir la nostra cadena de blocs local per a interactuar amb els contractes intel·ligents que haurem desplegat en aquesta mateixa xarxa.

En desplegar els nostres contractes a la xarxa de Polyogn al final del projecte, també podrem afegir-la a l'extensió.

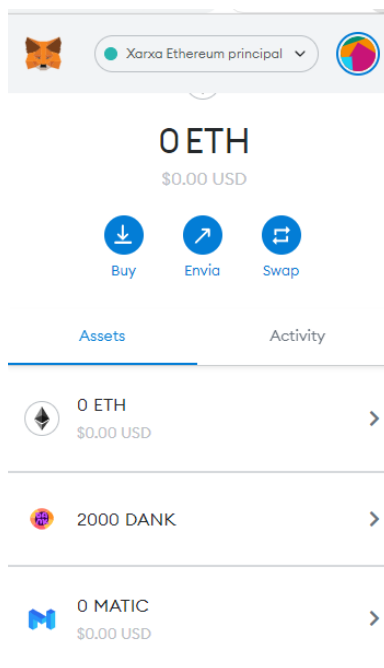


Figura 29: Metamask. Elaboració pròpia

D'altra banda, també ens dona eines i ens facilita el procés de desenvolupament de la nostra aplicació descentralitzada. Metamask injecta una API global a `window.ethereum`. Aquesta API ens permet demanar els comptes Ethereum de l'usuari, llegir dades de la cadena de blocs a la que estigui connectada i que l'usuari pugui signar les transaccions.

A continuació trobareu un llistat de totes les trucades diferents que he fet des del client a l'API de Metamask.

Amb el següent tros de codi podem obtenir els comptes connectats a Metamask:

```
window.ethereum.request({method: "eth_requestAccounts"})
```

Amb aquesta podem obtenir el codi identificador de la xarxa a la qual l'usuari està connectat:

```
window.ethereum.chainId
```

Podem executar funcions quan passi algun esdeveniment, com per exemple que l'usuari canviï de compte o de xarxa:

```

window.ethereum.on('accountsChanged', function () {
  setEventListener=true;
  logout()
})

window.ethereum.on('chainChanged', function () {
  setEventListener=true;
  logout()
})

```

A més, he utilitzat Metamask com a proveïdor de web3 al client JavaScript.

```
const provider = new ethers.providers.Web3Provider(window.ethereum)
```

A les aplicacions descentralitzades, l'usuari ha de signar la transacció quan s'està modificant alguna dada de la cadena de blocs, i ha de pagar una petita taxa que varia depenent de la saturació de la xarxa. Metamask mostrarà a l'usuari la transacció amb la taxa a pagar (també anomenat gas), i l'usuari podrà cancel·lar-la o acceptar-la. A la imatge de l'exemple (Figura 30), l'usuari vol comprar uns tokens d'un ICO i li costarà 80 Ether més els costos de la taxa.

Finalment, si l'usuari vol veure que els tokens comprats li han arribat correctament, només cal que l'importi a la pestanya d'*assets* especificant l'adreça del contracte (Figura 31).

Ethers.js

Es tracta d'una llibreria que s'utilitza per interactuar amb la cadena de blocs d'Ethereum i el seu ecosistema. Algunes de les característiques més destacables són que ens permet connectar-nos a la cadena de blocs mitjançant diversos tipus de nodes (el projecte utilitza un proporcionat per Metamask), que té llicència MIT pel que és totalment open-source i l'existència d'una comunitat activa.

Aquesta llibreria utilitza tres classes que és important definir:

1. **Provider:** És una classe que proporciona una abstracció per connectar-se a la xarxa d'Ethereum. Proporciona dret de lectura de la cadena de blocs i el seu estatus.

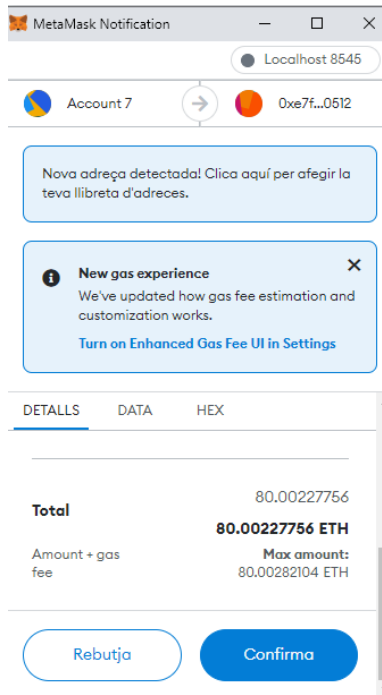


Figura 30: Petició per firmar la transacció. Elaboració pròpia

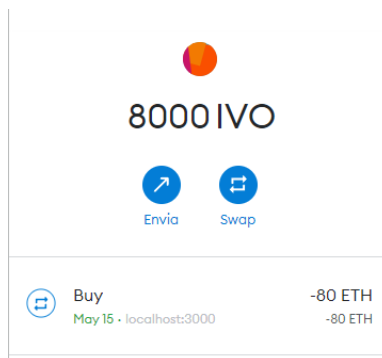


Figura 31: Tokens obtinguts amb la compra. Elaboració pròpia

2. **Signer:** És una classe que té accés a una clau privada, amb la qual es poden signar missatges i transaccions per autoritzar a la xarxa carregar Ether a nom del teu compte per dur a terme transaccions.
3. **Contract:** És una abstracció que representa una connexió a un contracte específic de la xarxa d'Ethereum, perquè les aplicacions puguin utilitzar-ho com un objecte normal JavaScript.

He emprat Ethers.js per a dur a terme totes les consultes i transaccions a la cadena de blocs. A continuació es mostra un petit exemple del codi del projecte on es poden veure les tres classes definides al paràgraf anterior:

```
async function donateico(donation) {
  if(typeof window.ethereum !== 'undefined'){
    const provider = new ethers.providers.Web3Provider(window.ethereum);
    const signer = provider.getSigner()
    const contract = new ethers.Contract(ivyICOAddress,ICO.abi, signer)
    try {
      const value = parseInt(donation) / ico.rate
      const transaction = await contract.buy({value:
        ethers.utils.parseUnits(value.toString(),'ether')})
      await transaction.wait()
      successBuyToast()
      await loadICO()
    }
    catch (err){
      console.log("Error: " , err)
      failedBuyToast()
    }
  }
  else console.log("Ethereum window undefined")
}
```

Es tracta de la funció per comprar o participar en una *Initial Coin Offering*. Es pot observar com es crea el Provider mitjançant `window.ethereum`, un proveïdor de web3 estàndard injectat per Metamask.

El Signer també s'extrau de Metamask, ja que aquest guarda la clau privada amb la que es podrà signar la transacció.

També es pot veure la instanciació del contracte, mitjançant la seva adreça, la interfície binària i el Signer.

Un cop instanciat el contracte, s'executa la funció *buy* passant com a paràmetre un valor de donació convertit a BigNumber amb 18 zeros darrere del nombre introduït. És a dir:

```
parseUnits("1.0", "ether");  
// { BigNumber: "1000000000000000000" }
```

Això és degut al fet que als smart contracts s'opera amb wei, i 1 ether representa 10^{18} wei.

Openzeppelin Contracts

Openzeppelin és una empresa que proporciona productes de seguretat per construir, automatitzar i operar aplicacions descentralitzades. Un dels seus productes és **Openzeppelin Contracts**.

Es tracta d'una llibreria per la construcció de contractes intel·ligents segurs. Aquesta inclou implementacions dels estàndards ERC més utilitzats, com ERC20 (*fungible token*) i ERC721 (*Non-fungible token*), control d'accés basat en rols i la creació de components Solidity reusables [22].

A continuació, trobareu llistats tots els contractes utilitzats d'aquesta llibreria en els smart contracts del projecte:

- **ERC20:** Aquest contracte permet crear nous tokens ERC20, indicant-li un subministrament inicial arbitrari. En el projecte s'utilitza per crear els contractes de les ICOs, donat que s'ha de generar un nou token que serà posteriorment venut.
- **ReentrancyGuard:** Mòdul que permet prevenir la reentrada de trucades a una funció. Heretar d'aquest mòdul permet utilitzar el modificador "nonReentrant" a les funcions, evitant així les trucades reentrants i un possible problema de seguretat greu.
- **Ownable:** Contracte que s'hereda per dur a terme control d'accés d'algunes funcions mitjançant el modificador "onlyOwner". Hi ha un compte que és el "propietari" del contracte, el qual pot renunciar o transferir la seva propietat.
- **Counters:** Contracte que s'utilitza per obtenir un comptador que només pot ser incrementat o disminuït. Resulta útil per a la generació de codis d'identificació i per comptar algun tipus d'activitat al contracte.

Repositori de Git

Un repositori de codi és un lloc on s'emmagatzema i es distribueix el codi d'una aplicació. Això, es troba a un servidor segur que utilitza algun sistema de control de versions, en el nostre cas, **Git**.

Un repositori permet poder treballar en paral·lel a una o més persones en una mateixa aplicació, de manera que no es donin mai per vàlides versions que entren en conflicte entre si.

També, ens permet accedir a l'historial de canvis. Això permet portar un bon control de cada versió i corregir canvis.

Un dels sistemes de control més utilitzats és **Git**, que és el que he fet servir jo en aquest projecte. Git és *software* lliure i és compatible amb la pàgina web GitHub. També hi ha un plug-in per a Atom (la IDE que he utilitzat per a dur a terme la pàgina web), que m'ha facilitat dur a terme els *commits* i a pujar-los al repositori remot amb l'ajut d'una interfície gràfica.

React.js

React és una llibreria JavaScript de codi obert per crear interfícies d'usuari. Està mantingut per Facebook i per la comunitat de codi obert. És declaratiu i basat en components que gestionen el seu propi estat, que combinats, poden construir interfícies d'usuari més complexes.

Característiques

React utilitza **JSX**, una sintaxi semblant a HTML. Utilitzar-lo és una experiència similar a l'HTML, però fa el codi més llegible.

També manté un **virtual DOM** propi (Model d'Objectes del Document), en comptes de confiar exclusivament en el del navegador. Això permet veure quines parts del DOM han canviat comparant la versió nova amb la que hi ha emmagatzemada al DOM i utilitzar el resultat per determinar com actualitzar eficientment el DOM del navegador.

Els components tenen un **estat**. Es defineix com una representació d'ell mateix en un moment concret.

Existeixen **dues** maneres d'escriure els components. Una és mitjançant funcions i l'altre mitjançant classes. Com diu el seu propi nom, el component funcional és una funció escrita en

JavaScript que retorna JSX. Un component en forma de classe és una classe JavaScript que amplia la classe `React.Component`. Els dos també tenen una forma diferent de representar l'estat.

Actualment, es recomana treballar amb els components funcionals perquè acabes escrivint menys codi i són més fàcils de llegir i depurar. A més, et permeten utilitzar els Hooks (com `useState()`), que simplifiquen els components, l'arquitectura, la jerarquia i la reutilització de codi.

A continuació podeu veure un exemple de la declaració d'ambdós tipus de components a la meua aplicació:

```
class AccountSettings extends React.Component {
  constructor(props) {
    super(props)
    this.state = {
      username: '',
      color: '#000000',
      redirect: false,
      showPicker: false,
    }
    this.configUser = this.configUser.bind(this);
  }
  ...
  render() {...}
};

const Campaign = () => {
  const [campaign, setCampaign] = useState([])
  const [fundsPercentage, setFundsPercentage] = useState(0)
  const [donation, setDonation] = useState("0")
  ...
  return (...);
};
```

Chai.js

Chai.js és una llibreria d'assertions que es pot fer servir a qualsevol marc de treball JavaScript. Ofereix diverses interfícies: *assert*, *expect* i *should*, que permet al desenvolupador escollir l'estil que li resulti més còmode i llegible. En el cas del projecte, s'ha fet servir la interfície *expect*. Chai se sol utilitzar

en mètodes TDD (*Test Driven Development*), on s'escriu primer el test i després s'implementa la funcionalitat fins que el test passa, tot i que en aquest treball no s'ha seguit aquest mètode.

S'ha emprat per a dur a terme tests unitaris sobre els contractes intel·ligents, és a dir, tests que consisteixen a posar a prova cadascun dels mètodes definits als contractes i veure que funcionen de forma independent a la resta del projecte.

IPFS

IPFS (Sistema d'arxius interplanetari) és una xarxa dissenyada per crear un mètode p2p (*peer-to-peer*) per emmagatzemar i compartir hipermèdia en un sistema d'arxius distribuït.

Es pot accedir al sistema d'arxius de formes molt senzilles, per exemple, per HTTP. En qualsevol moment es pot posar un arxiu local a disposició del món sencer. Aquests s'identifiquen per un *hash*, que és fàcil d'emmagatzemar.

En el nostre cas, hem emprat aquesta tecnologia per a pujar al sistema d'arxius distribuït IPFS les fotografies de cadascuna de les campanyes. Els usuaris, en començar-ne una, pugen una fotografia que tinguin en local. Seguidament, es puja a aquesta xarxa i ens retornen el codi hash, que l'emmagatzemem a la cadena de blocs per després poder carregar la fotografia.

Com podem observar a la Figura 32, hem utilitzat la llibreria 'ipfs-api', que és una llibreria client per a IPFS HTTP API, implementada en JavaScript. Hem creat la instància utilitzant un node remot d'Infura.

```
const IPFS = require('ipfs-api')
const ipfs = new IPFS({host: 'ipfs.infura.io', port: 5001, protocol: 'https'});

export default ipfs;
```

Figura 32: Creació instància IPFS. Elaboració pròpia

En el formulari per iniciar una campanya, hi ha un botó per afegir una imatge que l'usuari tingui en local. Quan es fa clic, s'executa el mètode que carrega el fitxer i el guarda a l'estat del component com a dades binàries. Quan es clica al botó d'Enviar el formulari, s'afegeix el fitxer a IPFS mitjançant la instància creada prèviament. Ens retorna un hash, que el passem com a argument quan fem la transacció per crear la campanya al *smart contract*.

Un cop tenim el hash de les imatges a la cadena de blocs, només caldrà buscar el hash mitjançant una trucada al contracte intel·ligent i renderitzar-les a les parts de l'aplicació web que s'escaigui. A continuació, podem veure com s'injecta el hash de la imatge a l'URL de la imatge:

```
<img src={'https://ipfs.io/ipfs/${campaign.ipfsHash}'}  
      alt="Campaign" />
```

12 Identificació de lleis i regulacions

És indispensable ser coneixedors de les lleis i regulacions existents relacionades en la construcció d'aquest projecte, ja que poden influir en el desenvolupament i el resultat final d'aquest. Revisarem les llicències i normatives de les tecnologies utilitzades i la normativa del treball de fi de grau de la Facultat d'Informàtica de Barcelona.

12.1 Llicències

El projecte s'ha construït a base de tecnologies amb llicències de codi obert, seguint el principi de transparència, un dels pilars fonamentals del web3. A continuació, trobareu la llista de tecnologies (llibreries, eines, etc.) emprades seguides de les seves respectives llicències:

- react: MIT License
- ethers.js: MIT License
- react-license: MIT License
- hardhat: MIT License
- react-router: MIT License
- react-router-dom: MIT License
- react-color: MIT License
- reactcss: MIT License
- styled-components: MIT License
- react-hooks-global-state: MIT License
- react-dom: MIT License
- ipfs-api: MIT License
- @openzeppelin/contracts: MIT License
- bootstrap: MIT License
- atom: MIT License
- Remix IDE: N/D

- Metamask: Llicència propietària de codi obert
- Git: GPLv2

la llicència MIT és una popular llicència permissiva que només obliga a preservar el copyright i l'avís de drets d'autor. El codi i derivats poden ser utilitzats per motius comercials, modificats i distribuïts sota terminis totalment diferents i sense el codi font [23].

La llicència GPLv2 (*GNU General Public License version 2.0*) és similar a l'anterior, amb la diferència que el codi ha d'estar disponible en cadascuna de les distribucions. Aquesta llicència és una de les recomanades pel projecte GNU, que pertany al moviment *Free Software* impulsat per Richard Stallman i la seva organització *Free Software Foundation*. Per a més informació podeu consultar el web <https://www.fsf.org/>.

12.2 Condicions d'ús Netlify

Tots els serveis, programes i solucions oferides per Netlify estan governats per unes condicions d'ús [24]. A continuació resumirem alguns dels punts més relacionats amb el nostre projecte:

- **Elegibilitat i edat:** el servei no pot estar dirigit a menors de tretze anys. Cada usuari és responsable de les accions que es produeixin en el seu compte.
- **El teu contingut:** El servei web no oferirà contingut de naturalesa il·legal, programes piratejats ni contingut que pugui incitar a la violència o a l'odi.
- **Ús acceptable:** No es farà servir el servei per a fer *spam*, ni com a proxy obert. Tampoc es podrà suplantar la identitat de cap persona. No es pot fer servir únicament com a servidor d'emmagatzematge.
- **Netlify *etiquette*:** No es mostraran ni hi haurà cap mena d'enllaç a continguts que es puguin considerar censurables.

12.3 Condicions de servei de Polygon

El projecte ha de complir les polítiques de servei definides per Polygon [25]. En aquestes es tracten 19 punts, dels quals s'han extret les idees principals i s'han resumit a continuació:

- Els usuaris són responsables de les interaccions entre ells i de quina informació comparteixen.
- Es prohibeixen accions que puguin afectar materialment o negativament l'experiència d'altres usuaris.
- Es prohibeixen actes maliciosos com suplantació d'identitat, missatges d'incitació a l'odi o introduir programes maliciosos a la xarxa.
- Polygon es reserva el dret a restringir l'accés a qualsevol usuari de la xarxa.

12.4 Normativa del TFG a la FIB-UPC

Es tracta d'un document que recull la normativa del treball de fi de grau i informació rellevant. En aquest, s'hi defineix el nombre de crèdits, les diferents modalitats (UPC, empresa, mobilitat, empresa a l'estranger), com inscriure's i matricular-se a l'assignatura, l'itinerari, el mètode d'avaluació i la propietat intel·lectual del projecte, entre altres aspectes [26].

Per a poder cursar l'assignatura amb èxit i presentar el treball de fi de grau, cal seguir les pautes dictaminades en aquest document, que recull tota la informació necessària.

13 Planificació revisada i canvis

En aquesta secció es descriuran les modificacions en la planificació que s'han produït durant el desenvolupament del projecte. Algunes tasques s'han avançat i altres s'han endarrerit. També s'han afegit alguns casos d'ús durant el projecte i han aparegut alguns *bugs*, fet que ha implicat la creació de noves tasques.

L'addició d'aquestes funcionalitats ha sigut possible gràcies al fet que ha costat menys temps del previst implementar les tasques planificades inicialment. És per això que trobareu el temps i el cost d'algunes tasques modificades.

També hi ha hagut alguna variació respecte als objectius i el cicle de vida del projecte.

13.1 Canvis respecte a l'objectiu inicial

Els canvi més important respecte la idea inicial del projecte ha estat relacionat amb la funcionalitat de les ICOs. Aquesta és una de les tasques més complicades, ja que s'hi havien d'aplicar diversos coneixements respecte als smart contracts i els estàndards per crear tokens ERC20 (tokens ethereum).

La idea principal era que l'usuari pogués iniciar una ICO a partir d'un formulari, de la mateixa manera que s'ha fet amb les campanyes de finançament. La problemàtica es troba en el fet que es vol crear un token diferent per cada ICO i cal un contracte intel·ligent per cada tipus de token, ja que cadascuna ha de tenir una adreça única. Aquest problema em va fer replantejar quina era la millor alternativa.

De moment, les ICOs es duen a terme de forma manual. S'ha creat un exemple d'ICO pel projecte *ivoryFund* amb un token amb símbol *IVO*. La idea és continuar investigant i intentar crear aquestes ICOs (contractes intel·ligents) de forma automàtica. Per això, en el moment de presentar el projecte encara no s'ha posat l'aplicació en producció, ja que encara cal polir aquesta funcionalitat.

És per això que he desplegat els contractes a una xarxa de test de Polygon anomenada Mumbai, en la que no ha costat diners desplegar-los i puc aplicar-hi tots els canvis que cregui necessaris.

Això també ha impactat de forma molt lleugera, quasi nul·la, en el pressupost del projecte, ja que m'he estalviat els costos de desplegament dels

contractes.

13.2 Descripció final de les tasques

A continuació es descriuen les tasques afegides durant el projecte i finalment trobareu una taula resum de totes les tasques, incloent-hi aquestes últimes.

Tasques de programació

T20. Iniciar campanya (*Modificada*): Com a usuari vull poder començar una campanya per recaptar fons per un projecte. Apareixerà un formulari amb camps com: nom del projecte, descripció curta, informació, referències (enllaços) a altres webs, etc.

T22. Rebre notificacions (*Modificada*): Com a usuari vull rebre notificacions quan s'arribi a l'objectiu de recaptació a una de les meves campanyes o quan m'escriguin un comentari. Estimació: 20 h.

T23. Pantalla *About Me*: Com a usuari vull poder consultar la pàgina d'informació de la web.

T24. Tancar sessió: Com a usuari vull poder tancar sessió.

T25. Pàgina de les ICO: Com a usuari vull una pàgina on veure totes les ICO disponibles

T26. Pantalla de campanyes creades Com a usuari vull veure la llista de les meves campanyes.

T27. Pantalla de campanyes preferides: Com a usuari vull veure la llista de les meves campanyes preferides.

T28. Pantalla de respostes a un comentari Com a usuari vull poder veure les respostes a un determinat comentari.

T29. Tests als contractes intel·ligents: Realització de tests unitaris a cadascun dels contractes intel·ligents emprats en l'aplicació.

T30. Consultar MATIC acumulat a una ICO: Com a usuari propietari d'una ICO vull poder consultar quan MATIC hi ha acumulat al contracte intel·ligent per poder extreure'l.

Solucionar bugs

T31. Nom d'usuari i color no s'actualitzen en canviar de comte: L'usuari pot tenir diverses comptes connectades a l'aplicació. Quan aquest canviava a un altre compte, quedaven guardats el nom d'usuari i el color del compte anterior.

T32. Enllaços a webs externes incorrectes: L'usuari podia crear una campanya amb un URL incorrecte. S'ha fet que la URL segueixi un patró perquè l'usuari sigui redirigit correctament en cas de clicar-hi.

13.3 Taula resum actualitzada

En aquest apartat trobareu una taula actualitzada de les tasques de programació, de les eines TIC i de les tasques de solució de *bugs*.

Pel que fa a la tasca de desplegament dels contractes intel·ligents, s'han restat els 0,3 € que es van afegir perquè s'ha acabat desplegant a una xarxa de test, on no costa diners reals desplegar-los.

El temps total resultant és de 547 hores. Per tant, s'ha reduït el temps total en 13 hores, tal com s'havia previst des de l'inici.

T7	Creació Jira	5	T4	97,5
T8	Creació repositori GitHub	5	-	97,5
T9	Inicialització projecte	10	T8	195
T10	Desplegament de la pàgina web	20	T11	390
T11	Desplegament dels smart contracts	20	Totes les de programació	390

Figura 33: Resum de tasques d'eines tic actualitzades

T12	Transferència de Matic	35	T9	682,5
T13	Signup i sign in	30	T9	585
T14	Creació pantalla principal	40	T13	780
T15	Pantalla de configuració	15	T13	292,5
T16	Cercador de projectes	20	T14	390
T17	Pantalla d'informació d'un projecte	20	T20	390
T18	Donar Matic	30	T17	585
T19	Comentar un projecte	15	T17	292,5
T20	Iniciar campanya	20	T14	390
T21	Donar Like a un projecte	15	T17	292,5
T22	Rebre notificacions	20	T21, T19	390
T23	Pantalla About Me	3	-	58,5
T24	Tancar sessió	1	T13	19,5
T25	Pàgina de les ICO	3	T13	58,5

Figura 34: Resum de tasques de programació actualitzades (1)

T26	Pantalla de campanyes creades	6	T20	117
T27	Pantalla de campanyes preferides	10	T21	195
T28	Pantalla de respostes a un comentari	5	T17	97,5
T29	Tests als contractes intel·ligents	10	S'han anat fent fins que s'han implementat la resta de tasques	195
T30	Consultar MATIC acumulat a una ICO	3	T13	58,5
T31	Nom d'usuari i color no s'actualitzen en canviar de compte	5	T15	97,5
T32	Enllaços a webs externes incorrectes	1	T20	19,5

Figura 35: Resum de tasques de programació actualitzades (2)

13.4 Gantt resultant

A continuació, es troba el diagrama de gantt resultant del projecte. Es poden observar algunes petites diferències amb l'inicial, però el canvi dràstic s'ha donat amb l'addició de totes les noves tasques que podeu trobar dins del requadre verd.

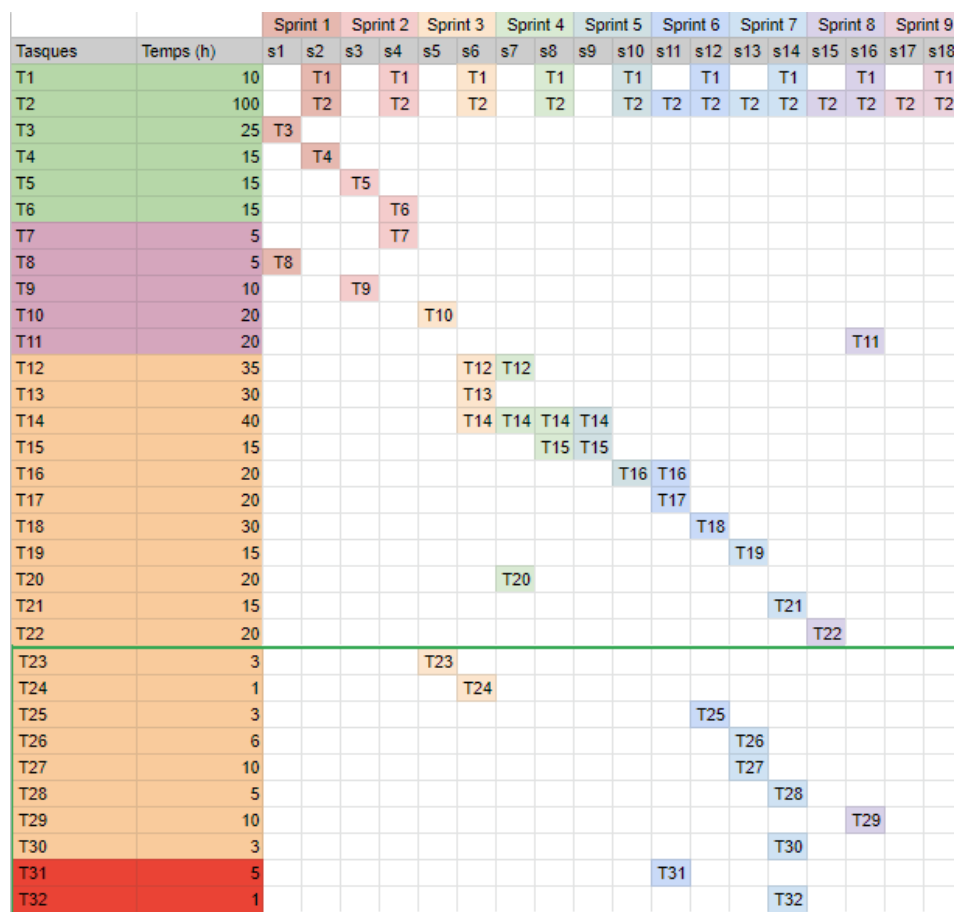


Figura 36: Gantt de la planificació resultant del projecte. Elaboració pròpia

13.5 Desviacions en el pressupost

En aquest apartat es mostrarà la taula pressupostària (Figures 37 i 38) amb totes les modificacions adients. S'han actualitzat els costos de cadascuna de les tasques, les contingències i s'han eliminat els imprevistos.

Activitat	Import (€)	Observacions
T1	195	
T2	1950	
T3	487,5	
T4	292,5	
T5	292,5	
T6	292,5	
T7	97,5	
T8	97,5	
T9	195	
T10	390	
T11	390	
T12	682,5	
T13	585	
T14	780	
T15	292,5	
T16	390	
T17	390	
T18	585	
T19	292,5	
T20	390	
T21	292,5	
T22	390	
T23	58,5	
T24	19,5	
T25	58,5	
T26	117	
T27	195	
T28	97,5	
T29	195	
T30	58,5	
T31	97,5	
T32	19,5	Activitats que estan al diagrama de Gantt
Total CPA	10666,5	

Figura 37: Pressupost final dividit en partides (1). Elaboració pròpia

Cost Genèric 1:	60,17	
Cost Genèric 2:	86€	Amortització fixada en un 26%.
Total CG	146,17	
Contingència	1621,9005	Fixat un nivell de contingència del 15%. (Total CPA + Total CG) *15%
Total	12434,5705	

Figura 38: Pressupost final dividit en partides (2). Elaboració pròpia

Les despeses finals han sigut de 12434,58 €, amb una desviació de 371,9 € (2,9%). Per tant, s'han gastat 371,9 € menys, que podran ser invertits a posar el projecte en producció.

14 Integració de coneixements

En aquest projecte s'han hagut d'integrar conceptes de diverses disciplines i branques de la informàtica: enginyeria de software, gestió de projectes informàtics, tecnologies de la informació, xarxes, enginyeria de requisits i disseny de pàgines web.

He aplicat coneixements adquirits durant el grau d'enginyeria informàtica, ja sigui com a matèria d'algunes assignatures o aprenent pel meu compte fora de l'àmbit de la universitat.

Pel que fa a la interfície d'usuari, he aplicat alguns principis de disseny d'interfícies d'usuari. Aquest coneixement el vaig adquirir a l'assignatura "d'Interacció i Disseny d'interfícies" (IDI).

Havia tingut experiències prèvies fent *front-ends* a algunes assignatures i també durant les meves pràctiques a l'empresa G+D Mobile Security. A l'assignatura "Aplicacions i Serveis web" (ASW) vaig tenir l'oportunitat de fer el meu primer client JavaScript amb Angular.

Un dels conceptes més innovadors del projecte, el qual encara no havia posat en pràctica a la universitat, ha sigut la creació d'aplicacions descentralitzades i la integració amb la cadena de blocs d'Ethereum. Per informar-me d'aquestes noves tecnologies he hagut de fer alguns cursos i llegir guies via internet. Concretament, vaig fer un curs de desenvolupament *full stack* d'una aplicació web3, on vaig descobrir Remix IDE, Solidity, ReactJS i Openzeppelin. També vaig desenvolupar un *marketplace* de NFT molt senzill, amb el que vaig agafar pràctica abans de començar a implementar el meu projecte.

He utilitzat la metodologia àgil de treball SCRUM. Aquesta la vaig descobrir a "Gestió de projectes de software" (GPS) i la vaig posar en pràctica per primer cop a "Projecte d'enginyeria de software" (PES), on vaig haver de treballar juntament amb altres 6 estudiants. També vaig seguir aquesta metodologia durant les meves pràctiques d'empresa. Tot i que he fet el projecte sol, m'ha sigut de molta ajuda per planificar-me els esprints i per saber a quin ritme estava treballant.

Per a la identificació de requisits funcionals i no funcionals, he emprat pràctiques apreses a assignatures com "Enginyeria de requisits" (ER). Alguns exemples són la definició dels casos d'ús, la descripció de les tasques o la identificació dels requisits no funcionals seguint el patró Volere.

Durant tot el projecte, he intentat utilitzar eines de codi obert. Una característica fonamental de les aplicacions descentralitzades és que son *open-source*, i per això he volgut que totes les tecnologies utilitzades durant el desenvolupament de l'aplicació també ho fossin. Aquesta conscienciació del

moviment del programari lliure i del programari de codi obert la vaig adquirir a l'assignatura "Software lliure i desenvolupament social" (SLDS).

15 Conclusions

15.1 Competències tècniques

Durant el transcurs del projecte s'ha treballat en algunes competències tècniques associades al projecte i relacionades amb l'enginyeria de *software*. A continuació, es justificarà el grau de compliment de cadascuna.

CES1.1: Desenvolupar, mantenir i avaluar sistemes i serveis software complexos i/o crítics. [En profunditat]

Aquest projecte està construït sobre la tecnologia de la cadena de blocs. Aquesta té bastants peculiaritats i construir una pàgina web que interaccioni amb ella pot resultar bastant complex en relació amb la web convencional.

També es duen a terme transaccions de criptomonedes. Aquest punt és crític, donat que si alguna cosa fallés, portaria molts problemes, ja que estem parlant de transaccions econòmiques.

CES1.2: Donar solució a problemes d'integració en funció de les estratègies, dels estàndards i de les tecnologies disponibles. [Bastant]

S'han hagut d'integrar els contractes intel·ligents amb el client JavaScript. Els contractes, en ser compilats, generen una interfície binària anomenada ABI (*Application Binary Interface*) amb JSON. Aquesta és la forma estàndard d'interaccionar amb contractes que es trobin en l'ecosistema Ethereum. En aquesta, es troben definides les funcions del contracte. Un cop compilat, cal desplegar-los a una cadena de blocs. Durant el desenvolupament es duia a terme a una xarxa local, i finalment s'ha desplegat a la xarxa de test Mumbai.

El client utilitza la llibreria ethers.js i l'ABI generat anteriorment per crear un objecte JavaScript que representa el contracte i els seus mètodes. L'eina Metamask fa de proveïdor de web3, és a dir, permet la connexió del client amb la cadena de blocs i signar les transaccions.

CES1.3: Identificar, avaluar i gestionar els riscos potencials associats a la construcció de software que es poguessin presentar. [En profunditat]

En aquesta memòria es poden trobar tots els riscos identificats a l'inici del projecte, concretament a l'apartat 6.

Primer es parla de la poca experiència que tinc com a desenvolupador d'aplicacions de la web3 i de com tinc algunes fonts d'informació que m'ajudaran a poder construir una aplicació descentralitzada durant el projecte. També es comenta que vaig sobreestimar les tasques relacionades amb tecnologies que no coneixia.

Seguidament, es comenta que tinc marge per allargar la implementació, ja que als últims esprints tinc planificada una càrrega de treball menor.

També es comenta el risc del preu volàtil de les criptomonedes. Es comenta que si el preu del MATIC pugés dràsticament, es plantejaria canviar de xarxa. També es diu que si el projecte no es posa en producció en acabar el treball de fi de grau, es desplegaria en una xarxa de test i el preu del MATIC no seria un problema perquè seria gratuït.

CES1.4: Desenvolupar, mantenir i avaluar serveis i aplicacions distribuïdes amb suport de xarxa. [En profunditat]

Una aplicació descentralitzada, que és justament el que s'ha construït durant el transcurs d'aquest projecte, no deixa de ser un tipus d'aplicació distribuïda que s'executa en una xarxa P2P, en el cas del projecte la xarxa Polygon, de l'ecosistema Ethereum.

CES1.5: Especificar, dissenyar, implementar i avaluar bases de dades. [Bastant]

A la memòria es pot trobar el model de dades de l'aplicació a l'apartat 10.2. En aquest, es poden trobar totes les estructures de dades necessàries i imprescindibles pel projecte, com les campanyes, les ICOs, els comentaris, les notificacions o els usuaris.

Aquesta base de dades no s'ha implementat com es faria en una pàgina web convencional, sinó que s'ha dut a terme mitjançant els contractes intel·ligents. Algunes estructures de dades s'han definit mitjançant *structs* a

dins d'un contracte intel·ligent, i altres són un contracte intel·ligents per si sols (ICOs).

En aquests, també s'hi han definit tots els mètodes per interaccionar amb les dades, sigui per modificar-les o per consultar-les.

CES1.6: Administrar bases de dades (CIS4.3) [Bastant]

Els contractes intel·ligents, que són l'equivalent a la base de dades del projecte, han sigut desplegats a la xarxa Polygon. Aquests tenen una adreça permanent i la informació és immutable gràcies a la tecnologia de la cadena de blocs i a la prova de treball (*Proof of work*).

CES1.7: Controlar la qualitat i dissenyar proves en la producció de software. [En profunditat]

S'han dut a terme tests exhaustius sobre els contractes intel·ligents. Cadascun dels mètodes ha sigut testat de forma individual. A més a més, s'han testat algunes funcions conjuntament, simulant l'execució de la pàgina web.

Pel que fa al client JavaScript s'han dut a terme proves manuals perquè es volia que l'experiència de l'usuari fos el millor possible.

CES2.1: Definir i gestionar els requisits d'un sistema software. [En profunditat]

S'han definit els requisits funcionals i no funcionals als apartats 3.2 i 3.3.

Els requisits funcionals s'han definit en forma de casos d'ús, mitjançant un Diagrama de casos d'ús i la descripció *brief style* de cadascun. Els no funcionals s'han adaptat a partir de la plantilla Volere.

S'han complert tots els casos d'ús, ja que es van identificar les tasques del projecte a partir d'aquests. També s'han tingut en compte tots els requisits no funcionals perquè el software tingués la màxima qualitat possible.

CES2.2: Dissenyar solucions apropiades en un o més dominis d'aplicació, utilitzant mètodes d'enginyeria del software que integrin aspectes ètics, socials, legals i econòmics. [En profunditat]

Donat que el concepte de criptomonedes està guanyant importància aquests últims anys, apareixen moltes informacions de països que les han prohibit o d'altres que ja les estan utilitzant com a moneda vehicular. Pel que fa a Espanya i a la unió europea, no hi ha regulació de cap classe, per la qual cosa legalment no hi ha cap mena de problema en fer transaccions mitjançant criptomonedes.

Tots aquests aspectes s'han tingut en compte a l'hora de definir l'abast i els requisits del projecte. El *software* construït permet a les organitzacions recaptar fons pels seus projectes, per la qual cosa econòmicament pot resultar molt beneficiós per aquestes.

15.2 Valoració personal

L'elaboració d'aquest projecte ha sigut una de les experiències més enriquidores d'ençà que em vaig embarcar en el món de la informàtica. Abans de començar-lo, no coneixia la gran majoria de conceptes clau per a la implementació d'una aplicació d'aquestes característiques. Mai n'havia construït cap que interactués amb una cadena de blocs ni havia escrit contractes intel·ligents, per la qual cosa, des de l'inici vaig haver d'informar-me en profunditat i consultar una gran quantitat d'articles i de tutorials per a poder dur a terme el projecte.

Tota aquesta informació sobre les cadenes de blocs i la web3 m'ha permès formar una opinió elaborada respecte al tema. He estat captivat pels ideals de la comunitat web3, ja que busquen una descentralització de la informació i les finances, que permet combatre el poder d'algunes grans empreses i organitzacions.

Malgrat tot, he trobat que la web convencional resulta més eficient i útil en segons quins casos. Per exemple, el sistema de la signatura de transaccions de la web3 resulta més aviat molest a l'hora de fer un simple comentari o configurar el perfil d'usuari. Hi ha projectes que, per evitar aquesta signatura de transaccions i per estalviar taxes a l'usuari, guarden part de les dades en un servidor centralitzat. Aquesta solució, tot i resoldre el problema parcialment, va en contra dels principis de les aplicacions descentralitzades, per la qual cosa crec que cal un llarg procés de reflexió i de cerca de solucions descentralitzades per a aquests d'inconvenients.

D'altre banda, he après a utilitzar des de zero algunes tecnologies molt emprades al món laboral com React. Aquest fet m'ha obert les portes a moltes entrevistes de feina i m'ha dotat d'eines molt útils per enriquir el meu perfil professional. L'experiència en la implementació d'aplicacions descen-

tralitzades també em serà útil en un futur, ja que sembla que aquest tipus de tecnologia va a l'alça i moltes *startups* s'estan dedicant a aquest sector.

Pel que fa a projectes personals, tinc pensat continuar involucrat en la comunitat web3. Crec que pot ser una de les tecnologies del futur, tot i que encara té algunes mancances, i crec que seria un error desvincular-m'hi sent coneixedor del seu potencial i els ideals que persegueix.

En conclusió, ha resultat molt interessant combinar els coneixements adquirits durant el grau d'enginyeria informàtica, tant en la implementació de la web com en la redacció de la memòria escrita del projecte. El resultat ha sigut altament satisfactori i em sento orgullós d'haver après tants conceptes i tecnologies durant aquests mesos.

15.3 Futur del projecte

El procés que s'havia ideat pel projecte encara no s'ha completat. Es vol implementar una funcionalitat perquè els usuaris puguin crear la seva pròpia ICO a través d'un formulari, de la mateixa manera que amb les campanyes de finançament.

En el moment de la presentació d'aquesta memòria, encara no s'ha posat el projecte en producció. Els contractes intel·ligents estan desplegats a una xarxa de test a Polygon anomenada Mumbai Testnet, que utilitza tokens que no tenen cap valor real.

Per tant, els següents consistiran en investigar com crear aquestes ICOs de forma automàtica i desplegar els contractes a la xarxa de Polygon. Un cop fet, només caldrà afegir les noves direccions dels contractes intel·ligents al client JavaScript i ja estarà posat en producció, utilitzant MATIC amb valor real.

Annexos

Annex 1: Repositori GitHub de l'aplicació web

Repositori de codi obert de l'aplicació web, implementada durant el transcurs d'aquest projecte:

<https://github.com/arnauboy/crowdfunding-dapp>

Annex 2: Accés a l'aplicació web

Enllaç per accedir a l'aplicació web. En el moment en el qual s'entrega aquest treball, encara estan els contractes intel·ligents desplegats a la xarxa de test Mumbai, tot i que en un futur es trobaran a Polygon.

<https://ivoryfund.netlify.app/>

Annex 3: Llicència de l'aplicació

MIT License

Copyright (c) 2022 ArnauTheCoder

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE

OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Referències

- [1] Xataka. Qué es blockchain: la explicación definitiva para la tecnología más de moda. <https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>. [En línia; consultat el dia 23 de febrer de 2022].
- [2] Ethereum. Bienvenido a Ethereum. <https://ethereum.org/es/>. [En línia; consultat el dia 24 de febrer de 2022].
- [3] IG. ¿Qué es Ethereum y cómo funciona?. <https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona>. [En línia; consultat el dia 24 de febrer de 2022].
- [4] Bit2Me. ¿Qué es una cadena lateral o sidechain?. <https://academy.bit2me.com/que-es-cadena-lateral-sidechain/>. [En línia; consultat el dia 15 de març de 2022].
- [5] Bit2Me. Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?. <https://academy.bit2me.com/que-son-los-smart-contracts/>. [En línia; consultat el dia 28 d'abril de 2022].
- [6] The Dapp List. What are Dapps? All you need to know about the Decentralized Applications. https://thedapplist.com/learn/what-is-dapp/?utm_source=google&utm_medium=cpc&utm_campaign=what_is_dapp&utm_id=dapp&utm_term=dapp&utm_content=text_ad. [En línia; consultat el dia 28 d'abril de 2022].
- [7] Universo Crowdfunding. ¿Qué es el crowdfunding? <https://www.universocrowdfunding.com/que-es-el-crowdfunding/>. [En línia; consultat el dia 15 de març de 2022].
- [8] Economipedia. Empresas más grandes del mundo 2021. <https://www.europapress.es/economia/noticia-numero-start-ups-espana-ascendio-23000-informa-db-20210616135407.html>. [En línia; consultat el dia 17 de març de 2022].
- [9] El rincón del emprendedor. Las 6 mejores plataformas de crowdfunding. <https://rincondelemprendedor.es/6-mejores-plataformas-de-crowdfunding/>. [En línia; consultat el dia 17 de març de 2022].
- [10] The New York Times. ¿Qué es la web3? <https://www.nytimes.com/es/interactive/2022/03/29/espanol/web3-que-es.html>. [En línia; consultat el dia 24 de febrer de 2022].

- [11] Tech Target. What is a walled garden?. <https://www.techtarget.com/searchsecurity/definition/walled-garden>. [En línia; consultat el dia 05 de maig de 2022].
- [12] Star Citizen Wiki. Star Citizen. https://starcitizen.fandom.com/wiki/Crowdfunding_campaign. [En línia; consultat el dia 05 de maig de 2022].
- [13] Investopedia. Initial Coin Offering (ICO). <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>. [En línia; consultat el dia 05 de maig de 2022].
- [14] James Robertson & Suzanne Robertson. Volere Requirements Specification Template Edition 16—2012 . https://www.volere.org/wp-content/uploads/2018/12/template_es.pdf. [En línia; consultat el dia 18 de maig de 2022].
- [15] Expansión. ¿En qué países son ilegales las criptomonedas?. <https://expansion.mx/tecnologia/2021/09/27/en-que-paises-son-ilegales-las-criptomonedas>. [En línia; consultat el dia 28 de febrer de 2022].
- [16] El Español. La existencia de las ‘shitcoins’ aumenta la desconfianza hacia los crypto activos. https://www.elespanol.com/invertia/mercados/20211119/existencia-shitcoins-aumenta-desconfianza-criptoactivos/628187753_0.html. [En línia; consultat el dia 23 de febrer de 2022].
- [17] Talent. Salario medio para Programador .net en España, 2022. <https://es.talent.com/salary?job=programador+.net>. [En línia; consultat el dia 10 de març de 2022].
- [18] Medium. Estimating Smart Contract Costs. <https://medium.com/scrappy-squirrels/estimating-smart-contract-costs-f65acf818c26>. [En línia; consultat el dia 10 de març de 2022].
- [19] CHC. Cuánta electricidad consume un ordenador. <https://chcenergia.es/blog/cuanto-consume-un-ordenador-o-pc/>. [En línia; consultat el dia 6 de març de 2022].
- [20] Ser autónomo. ¿Cómo se calcula la amortización?. <https://www.serautonomo.net/%C2%BFcomo-se-calcula-la-amortizacion.html>. [En línia; consultat el dia 10 de març de 2022].
- [21] Crypto Wikipedia. What is Polygon (MATIC)? <https://crypto-wikipedia.com/what-is-polygon-matic/>. [En línia; consultat el dia 19 de maig de 2022].

- [22] Openzeppelin. Contracts. <https://docs.openzeppelin.com/contracts/4.x/>. [En línia; consultat el dia 20 de maig de 2022].
- [23] Choose a license. MIT License. <https://choosealicense.com/licenses/mit/>. [En línia; consultat el dia 19 de maig de 2022].
- [24] Netlify. Terms of Use Agreement. <https://www.netlify.com/legal/terms-of-use/>. [En línia; consultat el dia 19 de maig de 2022].
- [25] Polygon Inc. Terms of service. <https://polygon.io/terms>. [En línia; consultat el dia 19 de maig de 2022].
- [26] FIB Facultat d'Informàtica de Barcelona. Normativa del treball final de grau del grau en enginyeria informàtica de la FIB. https://www.fib.upc.edu/sites/fib/files/documents/actes/normativatfg-gei_document_final.pdf. [En línia; consultat el dia 19 de maig de 2022].

