



Criptomonedas Puig Coin

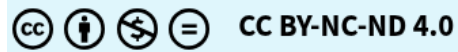
Sistemes Microinformàtics i Xarxes

Francisco J. Rodriguez Macia

Roderic Vicente Prunes

2D

SMX



Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International

Aquesta obra està subjecta a una llicència de [Reconeixement-NoComercial-SenseObraDerivada 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)

Espanya de Creative Commons

Resum del projecte

Aquest projecte tracta sobre la creació d'una criptomoneda per utilitzar a l'institut, amb la idea de que els professors puguin donar *tokens* als alumnes segons el seu criteri, amb l'objectiu d'implementar un sistema de recompenses i/o sistema de reputació pels alumnes, o fins i tot un sistema segur per posar nota als alumnes.

Paraules clau

Criptomonedas

BlockChain

Ethereum

Abstract

This project is about creating a cryptocurrency to be used at school, with the idea that teachers can give tokens to students at their discretion, with the goal of implementing a reward system and/or a reputation system for students, or even a way to implement a secure system to grade the students.

Keywords

Cryptocurrency

BlockChain

Ethereum

Índex

1 Introducció	1
1.1 Metodologia de treball	1
2 Descripció del projecte	2
2.1 Anàlisi de requisits	2
2.2 Tecnologies escollides	2
2.3 Estructura del projecte	3
2.3.1 Contracte intel·ligent	3
2.3.2 Node Ethereum	4
2.3.3 Interfície web	4
2.4 Funcionalitats	4
2.4.1 Transferència de <i>tokens</i>	4
2.4.2 Gestió de tokens pels professors	4
3 Conceptes i eines emprades	5
3.1 Blockchain i criptomonedes	5
3.1.1 Historia de la <i>blockchain</i>	5
3.1.2 Què és una <i>blockchain</i>	6
3.1.3 Criptomonedes i el seu funcionament	7
3.1.4 Sistemes de consens	8
3.1.5 Gas	8
3.1.6 Carteres digitals	9
3.2 Ethereum	10
3.3 Hardhat	10
3.4 Docker	11
4 Desenvolupament del projecte	12
4.1 Recerca sobre el tema del projecte	12
4.2 Implementació del node de prova	13
4.3 Creació de la interfície web	13
4.4 Dockerització	15
4.5 Proves	16
5 Conclusions	17
5.1 Conclusions generals del projecte	17
5.2 Consecució dels objectius	18
5.3 Valoració de la metodologia i planificació	19
5.4 Visió de futur	20
6 Annex	21
Deployment a la testnet Sepolia	21
Idees per l'utilització	22
7 Glossari	24
8 Bibliografia	25

1 Introducció

Aquest projecte tracta sobre la creació d'una criptomoneda per utilitzar a l'institut, amb la idea de que els professors puguin afegir o retirar *tokens* als alumnes segons el seu criteri, amb l'objectiu d'implementar un sistema de recompenses i/o sistema de reputació pels alumnes, o fins i tot un sistema segur per posar nota als alumnes.

Hem escollit aquest projecte perquè teníem curiositat per la tecnologia *blockchain* i volíem entendre millor com funciona en la pràctica. Ens interessava conèixer el seu impacte, no només en l'àmbit financer amb les criptomonedes, sinó també en altres sectors on la transparència, la seguretat i la descentralització poden tenir un paper clau, com l'educació, la traçabilitat de processos o la gestió de dades.

La idea era combinar la nostra curiositat amb un projecte pràctic que tingués aplicació real dins del nostre entorn escolar.

1.1 Metodologia de treball

La nostra metodologia de treball és majorment *waterfall* ja que s'adapta més al nostre projecte. Hem de treballar de manera secuencial per dur a terme els nostres objectius, sense el pas previ no podem fer el següent en la majoria de casos.

2 Descripció del projecte

2.1 Anàlisi de requisits

Requisits funcionals:

- Els professors poden enviar *tokens* als alumnes.
- Els alumnes poden consultar el seu saldo de *tokens*.
- Els alumnes poden transferir *tokens* entre si.
- La interfície web ha de ser fàcil d'utilitzar i tenir sistema de login.
- El sistema ha de registrar correctament totes les transaccions realitzades.

Requisits no funcionals:

La plataforma ha de ser segura i impedir accessos no autoritzats.
Ha de ser compatible amb navegadors moderns.

2.2 Tecnologies escollides

Hardhat: entorn de desenvolupament per a Ethereum.

Node.js: entorn per executar *scripts* de *deploy* i *backend*.

Ethers.js: biblioteca JavaScript per interactuar amb Ethereum.

HTML / CSS / JavaScript: per a la creació de la interfície web.

Ubuntu: sistema operatiu per executar el node local de prova.

2.3 Estructura del projecte

El projecte està organitzat en dos blocs principals: el bloc de *blockchain* i el bloc de pagina web.

El primer inclou el contracte intel·ligent escrit en Solidity, que es troba dins de la carpeta *contracts*. Aquest contracte defineix la criptomoneda, les seves funcions de transferència i la gestió de *tokens*. També inclou una carpeta *scripts*, on es troben els *scripts* per al desplegament del contracte i per a la gestió de la *blockchain* local, com ara el fitxer *deploy.js*. El fitxer *hardhat.config.js* conté la configuració necessària per al funcionament de Hardhat, definint la xarxa local, el compilador i altres paràmetres essencials per al desenvolupament.

El segon està compost per la interfície web que permet als usuaris interactuar amb la criptomoneda. Aquesta interfície inclou el fitxer *web.html*, que defineix l'estructura de la pàgina web amb els botons, la consulta del saldo i l'enviament de *tokens*. La comunicació amb el contracte es gestiona des del fitxer *app.js*, mentre que els estils visuals de la pàgina s'apliquen a través del fitxer *style.css*.

2.3.1 Contracte intel·ligent

Aquest contracte defineix el funcionament de la criptomoneda, que segueix l'estàndard ERC20, inclou totes les funcions necessàries per a la seva gestió. Els professors poden enviar *tokens* als alumnes segons criteris establerts, mentre que els alumnes poden consultar el seu saldo i realitzar transferències. El contracte assegura que totes les operacions es registrin a la *blockchain* i garanteix la integritat i seguretat de les transaccions.

2.3.2 Node Ethereum

Node Ethereum local, desplegat en un sistema Ubuntu utilitzant Hardhat. Aquest node permet simular la xarxa blockchain de manera controlada, proporcionant un entorn de proves

2.3.3 Interfície web

Desenvolupada amb HTML, CSS i JavaScript. Permet als usuaris interactuar amb el contracte intel·ligent. Inclou funcionalitats per connectar la cartera, consultar el saldo de *tokens*, enviar *tokens* a altres usuaris i visualitzar informació bàsica de les transaccions. La web actua com a capa intermèdia entre l'usuari i la *blockchain*, fent que el sistema sigui fàcil d'utilitzar per alumnes i professors sense necessitat de coneixements tècnics avançats.

2.4 Funcionalitats

2.4.1 Transferència de *tokens*

Els alumnes poden enviar *tokens* a altres companys, i els professors poden afegir *tokens* segons sigui necessari. Les transaccions es registren automàticament a la *blockchain*, assegurant que siguin segures.

2.4.2 Gestió de *tokens* pels professors

Els professors poden gestionar els *tokens* dels alumnes, és a dir l'addició i la de *tokens*, així com la consulta de l'historial de transaccions. Això permet establir un sistema de recompenses i reputació dins de l'institut, motivant els alumnes a participar activament i a seguir les normes establertes.

3 Conceptes i eines emprades

3.1 *Blockchain* i criptomonedes

3.1.1 Historia de la *blockchain*

La tecnologia *blockchain* té els seus orígens en investigacions sobre criptografia i sistemes distribuïts que es remunten als anys 90. L'any 1991, els investigadors Stuart Haber i W. Scott Stornetta van proposar un sistema per segellar documents digitalment de manera que no es poguessin modificar, utilitzant tècniques criptogràfiques similars a les que avui formen la base de la *blockchain*.

No obstant això, el concepte modern de *blockchain* no es va popularitzar fins al 2008 amb la publicació del document tècnic de Bitcoin per part de Satoshi Nakamoto. Aquest sistema introduïa per primera vegada una cadena de blocs descentralitzada que permetia realitzar transaccions digitals sense necessitat d'una autoritat central com un banc. El 2009 es va posar en marxa la xarxa de Bitcoin, convertint-se en la primera aplicació real de la tecnologia *blockchain*.

Posteriorment, el 2015 es va llançar Ethereum, que va ampliar les possibilitats de la *blockchain* més enllà de les criptomonedes. Ethereum va introduir els contractes intel·ligents, permetent executar programes dins la pròpia *blockchain* i obrint la porta a aplicacions descentralitzades (dApps).

Des d'aleshores, la tecnologia *blockchain* ha evolucionat ràpidament i s'ha aplicat en molts altres àmbits, com les finances descentralitzades (DeFi), els NFT, la gestió de dades, la traçabilitat de productes i els sistemes d'identitat digital. Avui en dia, és considerada una de les tecnologies emergents amb més potencial de transformació en diferents sectors.

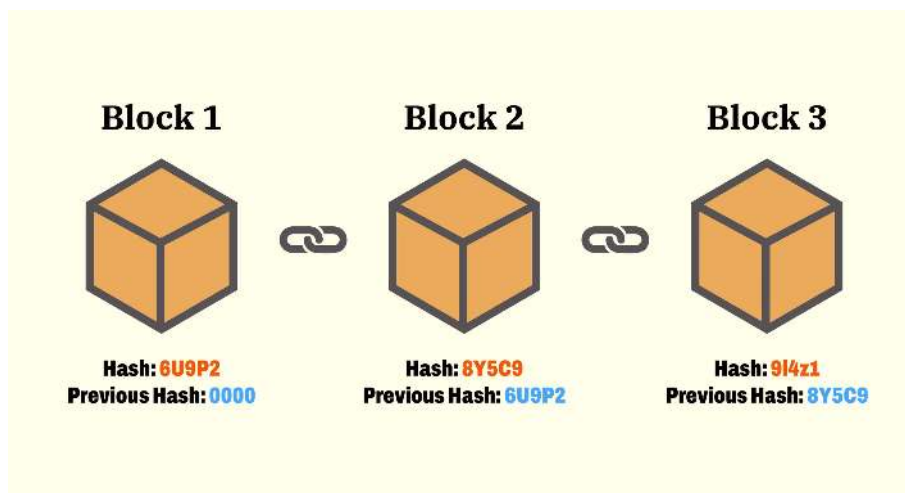
3.1.2 Què és una *blockchain*

Es una tecnologia que permet emmagatzemar informació de manera descentralitzada, segura i immutable. Funciona com un registre digital compartit entre múltiples dispositius (nodes) que validen i enregistren transaccions sense necessitat d'una autoritat central.

La informació s'organitza en blocs, que contenen un conjunt de transaccions.

Cada bloc està connectat amb l'anterior mitjançant un codi criptogràfic (hash), formant així una cadena. Aquesta estructura crea un sistema on, si algu intenta modificar un bloc, s'hagin de modificar tots els blocs posteriors a aquest, cosa que resulta quasi impossible.

A més de per criptomonedes, aquesta tecnologia també s'utilitza en altres àmbits, amb l'objectiu de garantir certa informació, ex: traçabilitat de productes, gestió d'identitats digitals, sistemes de vot electronic.



Funcionament basic d'una *blockchain*.

3.1.3 Criptomonedes i el seu funcionament

Les criptomonedes son “monedes” o *tokens* digitals que utilitzen la tecnologia *blockchain* per garantir la seguretat de les seves transaccions i controlar la creació de noves unitats.

Gràcies a aquesta tecnologia, no depenen de bancs ni governs.

El seu funcionament basic es:

- Un usuari envia criptomoneda a un altre.
- La transacció es validada pels nodes de la xarxa.
- La transacció s'inclou en un block que s'afegeix a la *blockchain*, d'aquesta manera registrada de manera immutable.

Per mantenir una xarxa extensa de nodes, es necessiten dispositius connectats a internet, que validin i registrin transaccions de manera continua.

Per tal que tots els nodes es posin d'acord sobre quines transaccions són vàlides, existeixen diversos sistemes de consens.

3.1.4 Sistemes de consens

Dos dels sistemes de consens més utilitzats son:

Proof of work (PoW): requereix que els nodes participants resolguin problemes matemàtics complexos mitjançant potència de càlcul, competint entre si per ser el primer. El guanyador serà el que validi el següent bloc de transaccions, i serà recompensat. Aquest procés però, requereix molta potència de processament i per tant, un elevat consum elèctric. Això és conegut com “mining”.

Proof of Stake (PoS): els participants bloquegen (*staking*) una quantitat de criptomoneda pròpia com garantia. La xarxa selecciona de manera pseudoaleatoria un validador per crear el següent bloc. La probabilitat de ser escollit està lligada a la quantitat de moneda bloquejada. Si el validador actua correctament, rep una recompensa.

També existeixen altres mètodes, com fer que cada node validi una transacció en un ordre acordat.

3.1.5 Gas

En moltes *blockchains* existeix el concepte de gas. El gas és una comissió que l'usuari ha de pagar per poder realitzar una operació dins la xarxa, com enviar criptomonedes o executar un contracte intel·ligent. Aquesta taxa serveix per compensar els validadors o miners pel treball computacional que realitzen i també evita l'ús abusiu de la xarxa (spam de transaccions). El cost del gas pot variar segons la congestió de la xarxa: quan hi ha moltes operacions, el preu augmenta perquè els usuaris competeixen per prioritzar la seva transacció.

3.1.6 Carteres digitals

Les *wallets* o carteres digitals, no guarden realment les monedes, sinó les claus criptogràfiques que permeten accedir-hi dins la *blockchain*. Cada usuari disposa d'una clau pública (adreça que pot compartir per rebre diners) i una clau privada, que ha de mantenir en secret perquè és la que li dóna control total sobre els seus fons. Si es perd la clau privada, no es poden recuperar les criptomonedes associades.

Això és un sistema de validació amb claus asimètric.

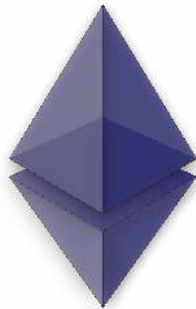


Metamask es una de les carteres digitals més conegudes

3.2 Ethereum

Ethereum és una plataforma de codi obert basada en tecnologia *blockchain* que permet la creació i execució de contractes intel·ligents (smart contracts) i aplicacions descentralitzades. A diferència d'una simple criptomoneda, Ethereum no només serveix per transferir valor, sinó que també funciona com un ordinador global descentralitzat on els programes s'executen de manera segura i immutable a la xarxa.

Ethereum va ser proposat l'any 2013 per Vitalik Buterin i es va llançar oficialment el 2015. La seva creació va suposar una evolució important respecte a *blockchains* anteriors, ja que va introduir la possibilitat de programar lògica complexa dins de la pròpia cadena de blocs mitjançant contractes intel·ligents escrits principalment en Solidity. Això va obrir la porta a molts casos d'ús més enllà de les criptomonedes, com ara finances descentralitzades, NFT, sistemes de votació o aplicacions de gestió de dades.



Logo Ethereum

3.3 Hardhat

Software d'entorn de proves que ens permet simular un desplegament de blockchain. Ofereix opcions flexibles i configurables per tot tipus de projectes. Els smart contracts es poden desplegar localment o en una testnet, Sepolia en aquest cas.



Hardhat

Logo de Hardhat

3.4 Docker

Docker és una plataforma de programari que permet crear, desplegar i executar aplicacions dins de contenidors. Un contenidor és un paquet lleuger i portàtil que inclou tot el necessari perquè una aplicació funcioni: codi, llibreries, dependències i configuració, sense la necessitat d'un sistema operatiu complet, sinó que comparteix el nucli del sistema amfitrió, cosa que el fa molt més eficient en consum de recursos. Això assegura que l'aplicació s'executi de la mateixa manera en qualsevol entorn, ja sigui a l'ordinador, en un servidor o al núvol, evitant així problemes de compatibilitat.

En el context del projecte, els contenidors s'utilitzen per separar i organitzar el node de blockchain i el desplegament del contracte, facilitant així la seva gestió.



Logo de docker

4 Desenvolupament del projecte

4.1 Recerca sobre el tema del projecte

Abans de començar el desenvolupament del projecte, es va realitzar una fase de recerca per entendre el funcionament de la tecnologia *blockchain* i de les criptomonedes. Es van estudiar conceptes clau com els contractes intel·ligents, el funcionament de la xarxa Ethereum i el paper dels nodes en la validació de transaccions. També es va investigar l'estàndard ERC-20 per comprendre com es defineixen i gestionen els *tokens* dins d'un ecosistema *blockchain*.

A més, es van analitzar eines de desenvolupament com Hardhat i biblioteques com Ethers.js, que permeten interactuar amb la blockchain des d'aplicacions web. Aquesta fase inicial va ser clau per establir una base sòlida de coneixements i decidir l'arquitectura del projecte.

Durant el procés de recerca i desenvolupament, també hem après nous conceptes de criptografia que desconeixíem, com la incorporació de *salt* en algunes funcions de derivació.

El concepte "salt" és una cadena de dades aleatòria que s'afegeix a la informació abans de ser "hashejada", amb l'objectiu d'augmentar la seguretat. Això evita atacs com les taules precomputades, ja que dos valors iguals no generen el mateix *hash* si tenen *salts* diferents. Aquest concepte ens ha ajudat a entendre millor com es protegeix la informació dins dels sistemes criptogràfics moderns.

4.2 Implementació del node de prova

Per al desenvolupament del projecte es va configurar un node local Ethereum utilitzant Hardhat. Aquest node simula una xarxa *blockchain* real però en un entorn controlat i sense costos de gas reals, fet que facilita el desenvolupament i les proves.

Un cop configurat Hardhat, es va desplegar el contracte intel·ligent ERC-20 sobre la xarxa local. Aquest node és l'encarregat de validar totes les transaccions, generar comptes de prova amb saldo inicial i mantenir l'estat de la *blockchain* durant les execucions.

Gràcies a aquest entorn, es poden provar funcionalitats com la creació de tokens, transferències entre usuaris i gestió per part dels professors de manera segura i immediata.

4.3 Creació de la interfície web

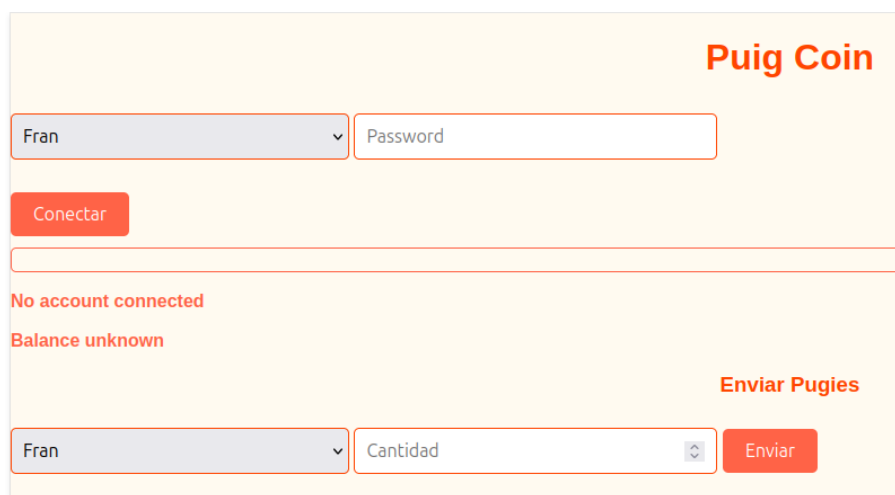
La interfície web del projecte s'ha desenvolupat utilitzant HTML, CSS i JavaScript, amb l'objectiu de crear una aplicació senzilla i intuïtiva que permet als usuaris interactuar amb la criptomoneda sense necessitat de coneixements tècnics avançats.

HTML i CSS s'han utilitzat per definir l'estructura i el disseny visual de la pàgina, incloent formularis i botons per a les diferents funcionalitats, com la consulta de saldo o l'enviament de *tokens*. D'altra banda, JavaScript ha estat clau per implementar la lògica de la interfície i la comunicació amb la *blockchain*.

Per connectar la web amb el contracte intel·ligent desplegat a la xarxa local Ethereum, s'ha utilitzat la llibreria Ethers.js. Aquesta permet enviar transaccions, consultar dades del contracte i interactuar amb el node de manera eficient.

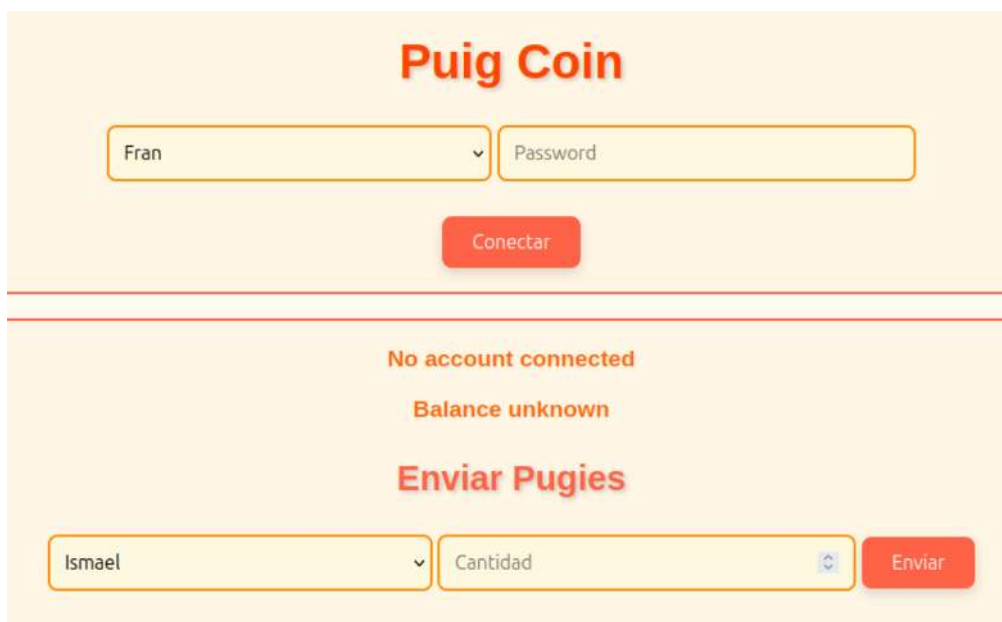
Entre les funcionalitats implementades a la interfície destaquen la connexió amb la cartera, la visualització del saldo de *tokens*, l'enviament de *tokens* a altres usuaris i la interacció amb les funcions específiques per als professors.

Durant el desenvolupament, JavaScript ha estat la part més complexa, ja que ha requerit entendre com gestionar esdeveniments, connectar amb la *blockchain* i tractar les respostes del contracte. Per això, s'ha combinat l'aprenentatge autònom amb l'ús de recursos externs i eines de suport per aconseguir una implementació funcional.



The screenshot shows the Puig Coin web interface. At the top right, the text "Puig Coin" is displayed in orange. Below it, there is a login form with a dropdown menu containing "Fran" and a "Password" input field. A red "Conectar" button is positioned below the login fields. A horizontal line separates the login section from the main content area. In the main area, the text "No account connected" and "Balance unknown" is shown in red. To the right, the text "Enviar Pugies" is displayed in orange. At the bottom, there is a transaction form with a dropdown menu containing "Fran", a "Cantidad" input field with a spinner, and a red "Enviar" button.

Primera iteració de la pàgina web



The screenshot shows the Puig Coin web interface with updated styling. At the top center, the text "Puig Coin" is displayed in orange. Below it, there is a login form with a dropdown menu containing "Fran" and a "Password" input field. A red "Conectar" button is positioned below the login fields. A horizontal line separates the login section from the main content area. In the main area, the text "No account connected" and "Balance unknown" is shown in red. Below this, the text "Enviar Pugies" is displayed in orange. At the bottom, there is a transaction form with a dropdown menu containing "Ismael", a "Cantidad" input field with a spinner, and a red "Enviar" button.

Segona iteració

4.4 Dockerització

Per facilitar el desplegament del projecte i assegurar que l'entorn de desenvolupament sigui reproduïble en qualsevol màquina, s'ha utilitzat Docker. Aquesta tecnologia permet encapsular totes les dependències del projecte dins de contenidors, evitant problemes de compatibilitat i simplificant el procés d'instal·lació i execució.

En el projecte s'han definit diferents imatges Docker que separen les responsabilitats principals del sistema:

Hardhat node:

Aquest contenidor executa un node local Ethereum utilitzant la comanda "npx hardhat node". Aquest node simula una *blockchain* de proves i escolta peticions a través del port 8545. La imatge instal·la les dependències del projecte i prepara l'entorn necessari per executar el node *blockchain* local.

Contract deployer:

Aquest contenidor s'encarrega del desplegament automàtic del contracte intel·ligent. Un cop iniciat, espera uns segons (sleep 10) per assegurar que el node de Hardhat estigui completament actiu. A continuació, executa el script:

```
npx hardhat ignition deploy --network testnet_docker  
ignition/modules/PGCToken.ts
```

Aquest procés compila i desplega el contracte ERC-20 dins la xarxa local de proves, automatitzant completament la posada en marxa del sistema.

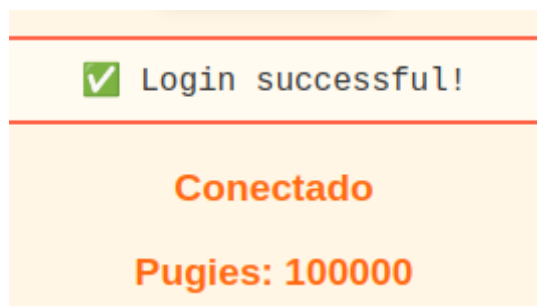
Orquestració amb Docker Compose:

Els contenidors es gestionen conjuntament mitjançant Docker Compose, que permet iniciar tant el node com el desplegador de contractes amb una sola ordre. Això garanteix que el contracte només es desplegui quan la *blockchain* està operativa, evitant errors d'inicialització.

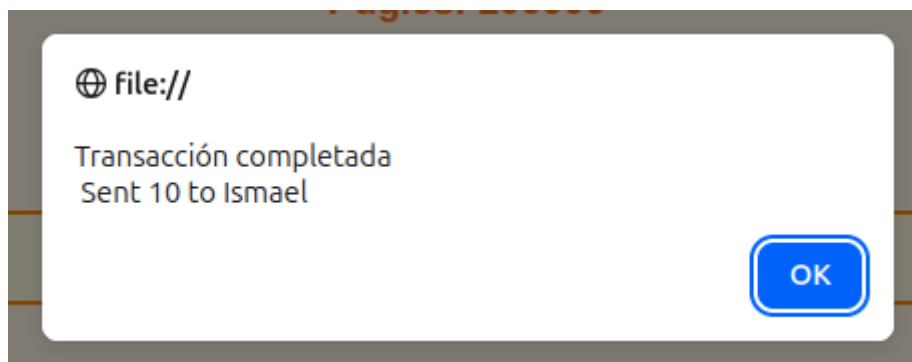
Gràcies a aquesta arquitectura basada en contenidors, el projecte és totalment portable, escalable i fàcil de desplegar en qualsevol entorn amb Docker instal·lat.

4.5 Proves

Un cop implementats els diferents components del projecte (contracte intel·ligent, node i interfície web), es van realitzar diverses proves per verificar el correcte funcionament del sistema.



En primer lloc, es van provar les funcionalitats bàsiques del contracte ERC-20, com la consulta de saldo i la transferència de *tokens* entre diferents comptes.



També es van fer proves d'integració entre la interfície web i la *blockchain*, comprovant que la comunicació mitjançant Ethers.js fos estable i que les accions realitzades des de la web es reflectissin correctament al contracte. Finalment, es van simular diversos escenaris d'ús per detectar possibles errors i assegurar l'estabilitat general del sistema.

5 Conclusions

5.1 Conclusions generals del projecte

El desenvolupament d'aquest projecte ens ha permès entendre de manera pràctica el funcionament de la tecnologia *blockchain* i com es pot aplicar en un entorn real com és un institut. Hem passat de conceptes teòrics com contractes intel·ligents, nodes o tokens ERC-20, a implementar-los en un sistema funcional basat en la xarxa Ethereum.

A nivell acadèmic, el projecte ens ha ajudat a consolidar coneixements de programació, xarxes i sistemes, així com a introduir-nos en eines professionals com Hardhat, Node.js i Docker. També hem après a treballar amb una arquitectura completa que integra *backend*, *blockchain* i interfície web.

A nivell professional, hem adquirit experiència en la resolució de problemes reals de desenvolupament, com la configuració d'entorns, la integració de sistemes distribuïts i l'automatització de processos mitjançant contenidors. A més, hem millorat la nostra capacitat de planificació de projectes tecnològics.

5.2 Consecució dels objectius

En general, s'han assolit els objectius principals plantejats a l'inici del projecte.

- S'ha creat una criptomoneda funcional basada en l'estàndard ERC-20.
- S'ha implementat un sistema on els professors poden donar *tokens* als alumnes.
- Els alumnes poden consultar el seu saldo i realitzar transferències entre ells.
- S'ha desenvolupat una interfície web que permet interactuar amb la blockchain de manera senzilla.
- S'ha configurat un entorn de proves local amb node Ethereum i Docker.

Inicialment teniem pensat implementació d'una *virtual wallet* (Metamask), però ens vam decantar per fer un sistema de login.

Durant el desenvolupament també es va investigar la possibilitat d'implementar una xarxa amb nodes de *blockchain* reals en comptes d'utilitzar únicament un entorn de proves local. Aquesta opció hauria permès una major descentralització i un funcionament més proper a un sistema real, però finalment no es va portar a terme per falta de coneixements avançats en configuració de xarxes distribuïdes i administració d'infraestructura. Tot i això, aquesta investigació ha servit per entendre millor l'arquitectura real de les blockchains i queda com una possible millora futura del projecte.

5.3 Valoració de la metodologia i planificació

La metodologia utilitzada ha estat principalment *waterfall*, ja que el projecte requeria una base sòlida abans de passar a les següents fases. Aquesta estructura ha estat adequada per entendre pas a pas els diferents components del sistema.

Tot i això, durant el desenvolupament s'han hagut de fer alguns ajustos respecte la planificació inicial, especialment en la integració entre la *blockchain* i la interfície web, on van sorgir dificultats imprevistes. També s'ha invertit més temps del previst en la creació i implementació de la pàgina web.

En general, la planificació ha estat útil com a guia, però és necessari mantenir certa flexibilitat per adaptar-se als problemes que van apareixent.

5.4 Visió de futur

Com a possibles millores futures del projecte, es podrien afegir diverses funcionalitats i expansions.

La principal millora seria passar de l'entorn de proves actual a una infraestructura basada en nodes reals de *blockchain*. En lloc d'utilitzar un node local simulat amb Hardhat, es podrien desplegar diversos nodes distribuïts en diferents màquines o servidors, creant així una xarxa més realista i descentralitzada.

A més, una altra millora important de cara al futur seria millorar la interfície web per fer-la més visual, moderna i atractiva per als usuaris. Actualment, la web està enfocada principalment a la funcionalitat, però es podria treballar en el disseny per fer-la més agradable d'utilitzar. La millora suposaria fer canvis dràstics amb CSS, organitzar els elements de manera eficient i possiblement l'ús de *frameworks* com Bootstrap o biblioteques modernes de *frontend*. L'objectiu seria aconseguir una experiència d'usuari més professional, fent que la interacció amb la criptomoneda sigui més clara, senzilla i visualment atractiva per a alumnes i professors.

També es podria desenvolupar un panell d'administració més complet per als professors, amb estadístiques, gràfiques i històric avançat de comportament dels alumnes.

Una altra línia de futur seria integrar sistemes d'identitat digital més robustos i millorar la seguretat del login.

6 Annex

Deployment a la testnet Sepolia

Després de realitzar les proves en l'entorn local amb Hardhat, es va desplegar la Puig Coin a la testnet Sepolia d'Ethereum per comprovar el funcionament del projecte en una xarxa *blockchain* real.

Sepolia és una xarxa pública de proves que permet desplegar contractes intel·ligents i executar transaccions sense utilitzar diners reals, fet que la converteix en una eina molt útil per al desenvolupament i testing de *blockchains*.

El primer pas va ser crear una cartera Ethereum amb les seves claus criptogràfiques corresponents. La clau pública funciona com l'adreça de la cartera, mentre que la clau privada permet signar transaccions i controlar els fons associats.

Posteriorment, es va obtenir ETH de prova mitjançant un *faucet*. Un *faucet* és un servei que distribueix petites quantitats de criptomoneda gratuïta dins d'una testnet. Aquest ETH no té valor econòmic real, però és necessari per pagar el gas de les transaccions i poder desplegar contractes intel·ligents.

Un cop configurada la cartera i obtinguts els fons de prova, es va configurar Hardhat amb les dades de connexió a Sepolia i la clau privada de la cartera.

Aquest procés va permetre verificar que la criptomoneda funcionava correctament fora de l'entorn local, validant transferències, saldos i interaccions amb el contracte dins d'una xarxa *blockchain* distribuïda real.

Idees per l'utilització

1. Sistema de reputació

El sistema pot ser utilitzat pels profes per tenir una idea de com de responsable es l'alumne amb una simple consulta.

2. Sistema per posar notes

Els professors podrien utilitzar el sistema per posar nota als alumnes de manera immutable i segura.

3. Sistema de punts per intercanviar

Es pot implementar un sistema en el qual els alumnes poden intercanviar puig coins guanyats amb bon comportament, responsabilitat i bones notes, per diferents recompenses que el centre pot oferir, incentivant el bon comportament i esforç als estudis:

- Marxar 5 minuts abans
- Triangle de xocolata o café gratis a la cantina
- Poder enviar tard una tasca
- Punt extra a una tasca
- Descompte 10% a la cantina
- Jugar a classe (sense molestar) un cop acabada la feina
- Pista a un examen

PUIG COIN STORE

INTERCANVIA ELS TEUS PUIG COINS PER RECOMPENSES!

RECOMPENSES DISPONIBLES

MARXAR 5 MINUTS ABANS  50 COINS	TRIANGLE DE XOCOLATA O CAFÉ GRATIS A LA CANTINA  70 COINS	PODER ENVIAR TARD UNA TASCA  60 COINS
PUNT EXTRA A UNA TASCA  80 COINS	DESCOMTE 10% A LA CANTINA  60 COINS	JUGAR A CLASSE (SENSE MOLESTAR) UN COP ACABADA LA FEINA  90 COINS
PISTA A UN EXAMEN  100 COINS	RECORDA! Els coins es guanyen i es canvien de manera justa i responsable. Fes que cada coin compti!	

Guanya coins amb bon comportament, responsabilitat i bones notes! 😊

BON ESFORÇ, MILLORS RECOMPENSES!

7 Glossari

Blockchain: registre digital descentralitzat on es registren totes les transaccions de manera segura i immutable.

Criptomoneda: moneda digital basada en tecnologia blockchain.

Token ERC20: tipus de token estàndard en Ethereum que permet transferències i compatibilitat amb altres contractes i carteres.

Ethereum: plataforma blockchain que permet crear i executar contractes intel·ligents.

Node: ordinador que forma part de la xarxa blockchain i valida transaccions.

Hardhat: entorn de desenvolupament per Ethereum que permet desplegar i provar contractes.

Solidity: llenguatge de programació per crear contractes intel·ligents a Ethereum.

Smart contract / Contracte intel·ligent: programa que s'executa a la blockchain amb regles predefinides.

Node.js: entorn de JavaScript per executar codi fora del navegador.

Sepolia: és una xarxa de proves pública que utilitza el protocol Ethereum i on pots aconseguir ETH de manera gratuïta. Es una eina ideal... per al desenvolupament i testing.

Faucet: servei que distribueix petites quantitats de criptomoneda gratuïta dins d'una xarxa de proves. Necesaries per interactuar amb la blockchain

8 Bibliografia

Nodejs: <https://nodejs.org/es>

Hardhat: <https://hardhat.org/>

Documentació ethereum: <https://docs.ethers.org/v5/getting-started/>

<https://docs.ethers.org/v5/getting-started/#getting-started--connecting>

Docker: <https://www.docker.com/>

RPC endpoint: <https://chainlist.org/chain/11155111>

Faucet:

<https://cloud.google.com/application/web3/faucet/ethereum/sepolia>

Generador de claus Ethereum: <https://vanity-eth.tk/>

Webs Demo/Github

<https://sepolia.etherscan.io/token/0x664f48e841ed383a93bffdaaf3b369fb36e4cb90>

<https://e338dc3c-02d1-4b8f-94ca.53af760a4161.bastion.elmeuescriptori.cat>

https://github.com/Blackknight333/puig_coin