Eduard Josep Bel Ribes

PLUG-IN PER LA GESTIÓ AUTOMATITZADA DEL NIVELL DE PRIVADESA ALS PORTALS WEB

TREBALL DE FI DE GRAU

Co-dirigit pel Dr. Jordi Castellà Roca
Co-dirigit per Cristòfol Daudén Esmel

Grau d'Enginyeria Informàtica

UNIVERSITAT ROVIRA I VIRGILI

Tarragona

2022

Agraïments

Al Jordi i al Tòful, per creure en mi des d'un principi.

Al meu pare, per haver-me ensenyat tantes coses, entre elles com d'apassionant pot arribar a ser la informàtica.

A la meva mare, per ser-hi sempre que fa falta.

Al Toni i la Natalia, per donar-me el seu suport als moments difícils.

Resum.

Cada cop és més freqüent la navegació per internet en busca d'informació o entreteniment. A causa d'això, també ha crescut el negoci de venda de les dades recol·lectades sobre els usuaris.

Des de l'aprovació del Reglament General de Protecció de Dades per part de la Unió Europea, els proveïdors de serveis han de proporcionar un mètode per la gestió de la seva política de privacitat i han d'obtenir el seu permís explícit si volen treballar amb les dades dels usuaris. Aquest permís l'obtenen a traves de pop-ups que apareixen cada cop que s'accedeix a una nova web. Generalment, per tal de no llegir les polítiques d'ús de dades i cookies, els usuaris tendeixen acceptar-ho tot.

En aquest projecte es proposa un plug-in per la gestió automatitzada de les polítiques de privacitat als portals web. A més a més, el sistema allotja els consentiments gestionats a la Blockchain mitjançant contractes intel·ligents. D'aquesta manera, es s'ofereix a l'usuari la possibilitat de consultar les polítiques acceptades per cada lloc web gestionat.

Aquesta eina ha estat provada en un entorn real i dona resposta a un 58,9% dels pop-ups que apareixen mentre naveguem.

Resumen.

Cada vez es más frecuente la navegación por internet en búsqueda de información o entretenimiento. A causa de esto, también ha crecido el negocio de venta de los datos recolectados sobre los usuarios.

Desde la aprobación del Reglamento General de Protección de Datos por parte de la Unión Europea, los proveedores de servicios deben proporcionar un método para la gestión de su política de privacidad y deben obtener su permiso explícito si quieren trabajar con los datos de los usuarios. Este permiso lo obtienen mediante los pop-ups que aparecen cada vez que se accede a una nueva web. Generalmente, con tal de no leer las políticas de uso de datos y cookies, los usuarios tienden a aceptarlo todo.

En este proyecto se propone un plug-in para la gestión automatizada de las políticas de privacidad en los portales web. Además, el sistema aloja los consentimientos gestionados en la Blockchain mediante contratos inteligentes. De esta manera, se ofrece al usuario la posibilidad de consultar las políticas aceptadas para cada sitio web gestionado.

Esta herramienta ha sido probada en un entorno real y da respuesta a un 58,9% de los pop-ups que aparecen mientras navegamos.

Abstract.

Surfing the web searching for information or entertainment has become more common year by year. Due to this, the business of selling users data has also increased.

Resum

Since the General Data Purpose Regulation was approved by the European Union, service providers must offer a method for their privacy policy management and must also obtain their explicit consent if they want to work with users' data. This consent is obtained through pop-ups that appear each time the user accesses a new web. Usually, in order not to read data and cookies policies, users tend to accept everything.

This project proposes a plug-in to automatically manage privacy policies of webpages. Furthermore, the system hosts managed consents on the Blochchain through smart contracts. By doing so, the user is offered the chance to look up for managed policies of each handled website

This tool has been tested in a real environment and responds to 58,9% of the pop-ups that appear while we surf the web.

Índex

Índex de taules

Índex de figures

1 Introducció

Els usuaris d'Internet han pogut trobar-hi des del començament informació i serveis relacionats amb els seus interessos, necessitats, etc. En la majoria de casos, la informació i serveis són gratuïts, però algú s'ha de fer càrrec dels costos. Per tant, era i és necessària una font de finançament pel seu desplegament i manteniment. Una d'aquestes fonts d'ingressos ha estat l'allotjament d'anuncis. Una altra font de finançament han estat les dades dels usuaris, ja sigui perquè la pàgina les ha recollit o els usuaris les han proporcionat voluntàriament. A mesura que el nombre de serveis i usuaris ha anat creixent també ho ha fet el volum de recursos que se n'obtenia.

No obstant, aquestes dades recollides permeten la creació de perfils dels usuaris que poden atemptar contra la seva privadesa. A l'article [9] de l'Oficina de Seguretat de l'Internauta es detallen els tipus de cookies i per que serveix cadascuna d'elles.

A causa d'això, el parlament de la Unió Europea va aprovar el General Data Protection Regulation (GDPR [1]) al 2016, que va entrar en plena vigència al maig del 2018. Des de llavors, les empreses, organitzacions, institucions i organismes de la UE o amb negocis dins d'aquesta s'hi han hagut d'adaptar en un termini de dos anys. Aquest reglament estipula que els usuaris han de donar el seu consentiment per que es pugui fer ús de les dades que l'organització tingui sobre ells. La manera d'aplicar la nova normativa depèn de l'àmbit de cada organització. El consentiment ha de ser explícit per les dades que es recopilaran i s'ha d'informar de la finalitat per la que es volen.

Aquesta iniciativa vetlla pel dret a la privacitat virtual dels ciutadans, però les organitzacions segueixen generant i subhastant els perfils dels usuaris que accepten la seva política de privacitat. El model de negoci de les companyies que treballen amb grans volums d'informació, tenint en compte que generalment el públic desitja obtenir entreteniment o informació a cost nul, es sosté gràcies a la venda i gestió de la informació recavada sobre els usuaris. Com es pot veure a l'article [10] de *Lopdat*, una empresa especialitzada en l'àmbit de la Llei Orgànica de Protecció de Dades (LOPD), els propòsits que tenen les empreses al comprar perfils d'usuaris són, a grans trets, enviar-los missatges de text o trucar-los per oferir els seus productes. Però si el perfil que es té de l'usuari conté informació més sensible que el seu número de telèfon, com ara informació bancària o dades mèdiques, l'existència d'aquest perfil pot influir de manera molt negativa a la vida de l'usuari.

En el cas concret de les empreses que tenen presència a la xarxa, la manera que tenen per complir amb el GDPR és proporcionant un avís legal i permetent a l'usuari manegar la política de privacitat amb un pop-up[1] de gestió de cookies.

Aquests pop-ups molesten als usuaris i alenteixen la navegació. Cada pàgina té el seu pop-up i, generalment s'ha de gestionar abans d'accedir a la informació o servei. Segons un estudi [6] realitzat a webs europees gairebé dos anys després que entrés en vigor el GDPR, el 81% dels llocs revisats utilitzen notificacions per informar als usuaris sobre la seva política de cookies. Tenint això en compte, un usuari habitual d'Internet que s'informi a través de diferents fonts ha de gestionar les cookies de quasi cada web que visita com a mínim un cop, ja que d'acord amb la ePrivacy Directive [2], les cookies persistents haurien de caducar al cap de 12 mesos i passat aquest període l'usuari hauria de tornar a gestionar la política de privacitat del lloc web. A banda de la quantitat de gestions de cookies que l'usuari ha de

[1] Finestra emergent per notificar quelcom important i que roman fins una interacció de l'usuari.

realitzar, si aquest desitja rebutjar-les totes per tindre major control sobre les seves dades, molts llocs web ho posen relativament complicat, fent que rebutjar les cookies sigui fer diversos clics, mentre que d'altres directament no ofereixen la possibilitat de rebutjar-les, com podem veure a la Figura 1, extreta de l'estudi abans mencionat.

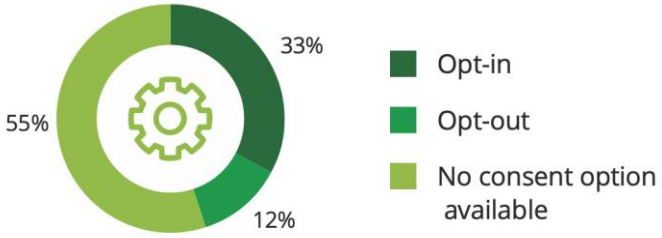

Figura 1. Gestió del consentiment de privacitat a diferents webs. Font: *Deloitte*

Amb tot això, els usuaris solen acabar acceptant-les totes perquè és el més fàcil i ràpid. A més a més, el volum de cookies gestionades manualment és tan elevat que s'acaben oblidant de quin tipus de cookies s'han acceptat i a quines webs.

La proposta [7] sobre la qual s'inspira aquest treball pretén donar resposta a aquestes necessitats.

Aquesta descriu un sistema que permet verificar els acords entre usuaris i proveïdors en relació a la custodia i processament de dades. El benefici que aporta la proposta és que ambdues parts puguin demostrar davant d'una autoritat el que es va acordar en cas de denúncia o negligència.

Per dur a terme això el sistema fa ús d'una Blockchain on cada consentiment amb els seus termes (duració, polítiques acceptades, etc.) es troba dins d'un Smart Contract d'accés públic, verificable, immutable i no repudiable. A més a més, l'usuari pot decidir en qualsevol moment si vol rescindir el consentiment o crear-ne un amb noves condicions.

1.1 Antecedents

Les pàgines web han d'oferir una gestió de les seves polítiques de privacitat mitjançant les cookies. Per tal de cobrir aquesta necessitat, sorgeixen els proveïdors de cookies (veure punt 1.1.1). A causa del creixent nombre de pàgines web amb pop-ups de cookies, s'han proposat diverses eines per fer-ne la gestió de forma fàcil (veure punt 1.1.2).

1.1.1 Els proveïdors de cookies

Hi ha empreses com *Didomi* [28] o *OneTrust* [29] que es dediquen a dissenyar els pop-ups de gestió de cookies i proporcionen els seus serveis a altres empreses per tal que els facin servir a les seves pàgines web. Aquestes empreses proveïdores tracten de complir amb el GDPR i ofereixen als seus clients la possibilitat de no preocupar-se del reglament.

Resta a disposició dels propietaris de pàgines web la possibilitat de modificar l'apartat visual i el contingut del pop-up, és a dir, quins tipus de cookies es faran servir.

Durant aquest treball anomenarem les empreses que es dediquen a proporcionar els formularis de cookies com a "vendors". Cada vendor fa el seu propi estàndard, llavors les solucions per tal de gestionar els formularis de cada web poden arribar a ser molt diferents.

1.1.2 Treball relacionat

La gestió de les cookies acostuma a incomodar als usuaris [8]. Per evitar-ho s'han proposat un seguit d'eines que faciliten la seva gestió. A continuació es presenta un breu estudi de les principals eines de gestió de cookies:

- Ninja Cookie [16]: rebutja les cookies no essencials.
- Super Agent [17]: permet triar quins tipus de cookies es volen acceptar o rebutjar.
- Auto Cookie Optout [18]: rebutja les cookies no essencials.
- Polish Cookie Consent [19]: accepta totes les cookies.

Durant l'estudi d'aquestes eines s'ha pogut observar que si bé totes gestionen alguns pop-ups de cookies, no totes són tan versàtils en quant al nombre de pàgines web amb les que poden interactuar.

Un cop resumit el seu comportament, a la Taula 1 es detallen altres aspectes d'aquestes eines:

Eina	Codi obert	Gratuïta	Té manteniment	Consulta del consentiment
Ninja Cookie	Sí	Parcialment	No	No
Super Agent	No	Sí	Sí	No
Auto Cookie Optout	Sí	Sí	Sí	No
Polish Cookie Consent	Sí	Sí	Sí	No

Taula 1. Característiques de les eines estudiades

Després d'estudiar les eines mencionades, podem concloure que cap d'aquestes ofereix la possibilitat de consultar el consentiment que gestionen. A més a més, hi ha una eina que no és de codi obert i, per tant, no es pot saber si recol·lecta dades dels seus usuaris mes enllà de les que s'informen a la seva pàgina web.

1.2 Motivació

Degut al GDPR hi ha hagut un gran augment dels llocs web que permeten la gestió de la seva política de privacitat a través de les cookies. Aquest fet és positiu sempre que s'ofereixi als usuaris denegar les cookies no necessàries de forma fàcil però, lamentablement no sol ser el cas. Es va realitzar un estudi [8] 30 dies després de l'entrada en vigor del GDPR sobre la interacció de més de 100.000 visitants de llocs web. Podem extreure com a conclusió que als usuaris els resulta tediós gestionar les cookies. Com es pot observar a la Figura 2 extreta de l'estudi, únicament el 0,5% dels usuaris van accedir a la configuració del pop-up per fer una gestió personalitzada, mentre que el 76% no va fer cap interacció amb el pop-up.

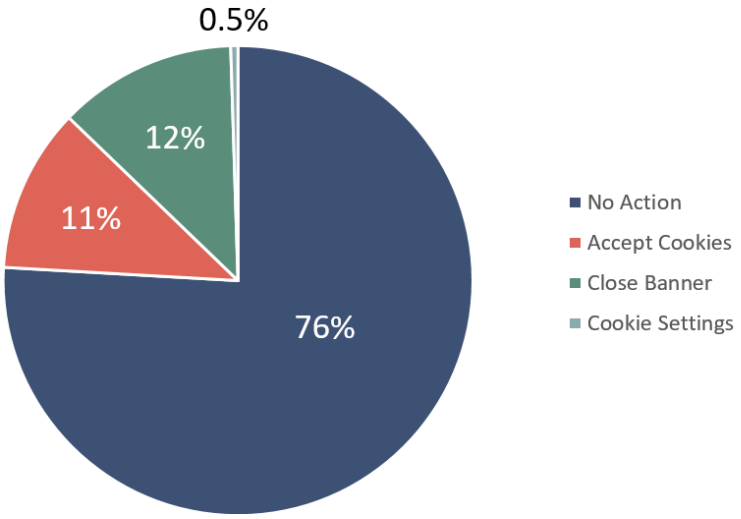

Figura 2. Interacció dels usuaris sobre els pop-ups de cookies. Font: *AmazeeMetrics*

A causa d'això i de l'estudi comentat al punt 1.1.2, sorgeix la motivació de proporcionar als usuaris una eina gratuïta de gestió automàtica de cookies.

1.3 Objectiu

L'objectiu del projecte és dissenyar i implementar part del sistema proposat a l'assaig de verificació d'acords en relació a la custodia i processament de dades [7] abans mencionat. La solució ha de permetre que donat un nivell de privadesa proporcionat per l'usuari, sigui capaç d'aconseguir:

- Una navegació per la web més fàcil i ràpida amb la satisfacció del nivell de privadesa especificat pels usuaris al donar el seu consentiment: acceptar les cookies automàticament.
- La consulta del consentiment donat: mitjançant un Smart Contract.
- L'avaluació del seu funcionament amb les principals webs amb pop-ups de cookies.

L'eina ha de permetre que els usuaris especifiquin el nivell de privadesa que volen, i actuar en conseqüència sobre les preferències de les cookies dels llocs que es visitin a partir d'aquell moment.

Aquesta eina ha d'interceptar els pop-ups de cookies, comprovar la política de privacitat que ha introduït l'usuari i, tenint en compte el contingut del pop-up i les preferències de l'usuari, determinar quina selecció s'ha de realitzar per tal de complir amb el seu propòsit, incrementant així la privacitat de l'usuari a la xarxa.

Com a sortida s'ha d'obtenir un Smart Contract i fer una transacció amb aquest a la Blockchain per deixar constància del consentiment proporcionat.

Finalment l'usuari, quan ho desitgi hauria de poder veure quina política de cookies s'ha acceptat per cada lloc web gestionat per l'eina.

1.4 Organització de la memòria

Tenint en compte que aquest treball de fi de grau tracta d'un sistema informàtic, es proposa un modelat del document de forma que prengui tota la rigorositat necessària per aprofundir en tots els aspectes que el projecte requereix.

A la Secció 2 es descriuen de forma breu les tecnologies que formen la base del projecte per una bona realització del codi font, necessàries per la comprensió de les decisions preses més tard.

A continuació, a la Secció 3 es presenta l'arquitectura del projecte i es detallen els requisits per cobrir les necessitats d'aquest. Tot seguit es mostra el disseny de l'estructura de la solució proposada seguit de la planificació del projecte.

Llavors, a la Secció 4, es troba la memòria d'implementació del projecte.

Seguidament, a la Secció 5 es demostra l'eficàcia del treball realitzat mitjançant unes demostracions a mode de joc de proves, aportant els resultats obtinguts.

Les conclusions obtingudes a l'acabar el projecte es troben, finalment, a la Secció 6.

2 Tecnologies

En aquesta secció es descriuen breument les diferents tecnologies emprades o que cal conèixer per una millor comprensió del projecte.

2.1 Plug-in

Un plug-in [11] és un software dissenyat per complementar un programa base, afegint-hi funcionalitats de les que no disposava inicialment. La idea que fa sorgir el concepte de plug-in és la de comunicar dos codis (programa base i codi nou) per tal que funcionin com si fos un sol programa. D'aquesta tasca se n'encarrega el programa base si està preparat per admetre plug-ins.

2.2 Cookies

Les cookies [12] són informació que queda desada al navegador web de l'usuari. Les cookies es desen per cada web concreta i es solen fer servir per tindre informació sobre accessos previs de l'usuari al lloc web i actuar en conseqüència, com ara, quin tema (clar o fosc) és l'últim que es va fer servir per visualitzar la web.

Un altre exemple són les cookies de sessió, que són les encarregades de que, un cop que l'usuari s'hagi identificat al lloc web, no se li torni a demanar identificar-se si aquest ha tancat la pestanya on hi ha la web o l'ha obert a una nova pestanya.

Pel cas que ens ocupa amb aquest projecte, ens centrarem en les cookies que desen les preferències respecte a la política de privacitat de l'usuari.

2.3 Blockchain

Blockchain [13] és un sistema amb arquitectura descentralitzada, és a dir, tots els nodes participants gestionen les dades, el processament i es coordinen en la presa de decisions. Així, si un dels nodes falla, la xarxa pot seguir operant sense cap mena de problema.

Tots els nodes d'una Blockchain emmagatzemen les transaccions fetes des de l'inici d'aquesta fins l'actualitat en blocs. Depenent de la Blockchain, els blocs tenen una mida diferent i cada cert temps la validesa i integritat del bloc es confirma per tots els nodes i es passa al següent.

2.4 Criptomoneda

Una criptomoneda [20] és una divisa virtual que utilitza mètodes criptogràfics per assegurar la integritat de les transaccions realitzades. Aquestes monedes virtuals s'utilitzen per realitzar transaccions controlades a través d'una base de dades descentralitzada, generalment una Blockchain.

2.5 Wallet

Una wallet [21] és una cartera virtual associada a un usuari de la Blockchain. Aquesta té la funció d'acumular, enviar i rebre criptomonedes. Una wallet té associades una clau pública, que es pot compartir amb tothom amb qui es vulgui realitzar una transacció i una clau privada per autenticar-se i que l'usuari pugui accedir als seus actius.

2.6 Smart Contract

Un Smart Contract [14] és un programa que s'executa a la Blockchain de manera transparent a l'usuari, capaç d'executar-se i fer-se complir per si mateix.

Aquests també poden ser creats i cridats per un usuari, són visibles per tots els usuaris de la Blockchain i el seu codi no es pot modificar degut a la naturalesa d'aquesta.

Els Smart Contracts podrien fer-se servir, per exemple, per manifestar la propietat d'objectes físics i virtuals, o per automatitzar herències, sent un document visible i possible de validar per tothom i reduint notablement els costos d'intermediaris com notaris o agències gestores.

2.7 Web3.js

Web3.js és una API[2] [3] que permet connectar el programa a una Blockchain, ja sigui local o remotament. Aquesta llibreria permet també crear un Smart Contract i fer la transacció d'aquest a la Blockchain.

2.8 Màquina virtual

Una màquina virtual [22] és la simulació d'un sistema computacional, pot executar programes com si fos un ordinador físic. La màquina virtual s'executa dins del sistema operatiu amfitrió.

[2] Application Programming Interface.

3 Disseny

En aquest punt s'exposa el disseny del projecte a diferents nivells, com són l'arquitectura d'aquest, els requeriments que s'han definit i les decisions de disseny respecte a l'eina a desenvolupar. Finalment es comenta la planificació del projecte.

3.1 Arquitectura del projecte

A continuació, es mostra la representació del disseny de l'arquitectura del projecte. Per tal de simplificar la seva visualització, s'ha dividit l'arquitectura en dues figures diferents. Inicialment, es mostra l'arquitectura de gestió de cookies (Figura 3), seguida de l'arquitectura per la consulta del consentiment (Figura 4). Finalment, es proporciona una breu descripció dels passos.

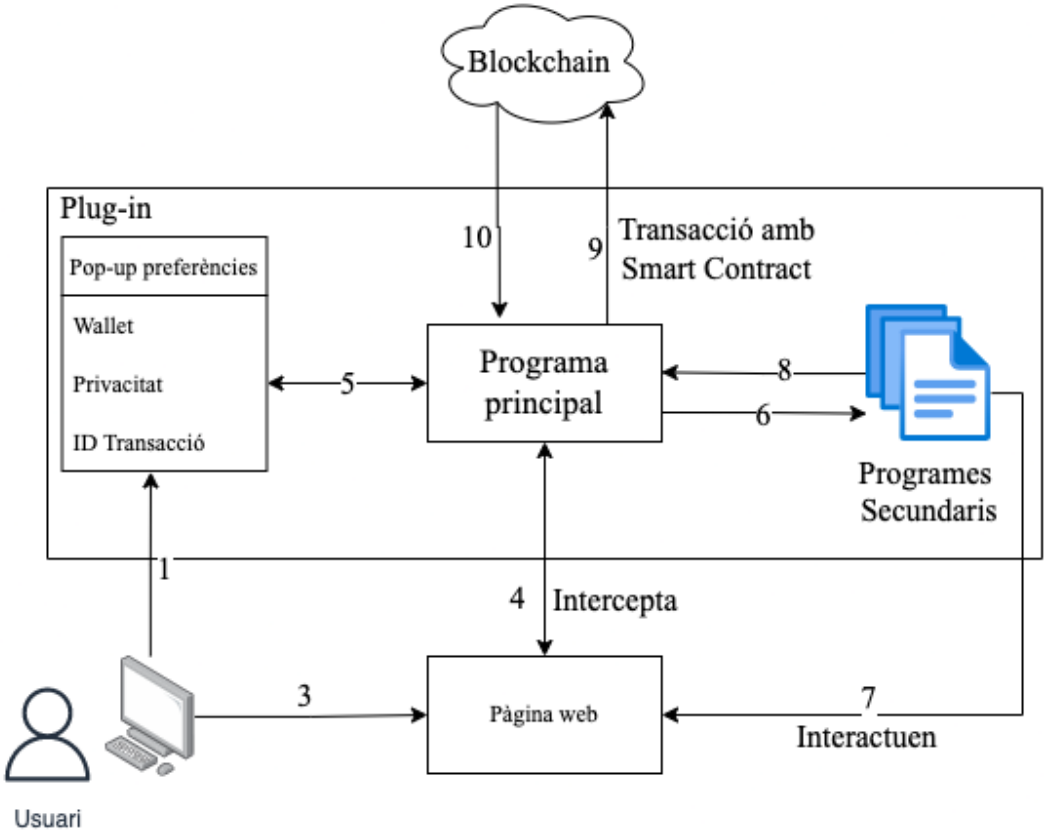

Figura 3. Arquitectura del projecte: gestió de cookies

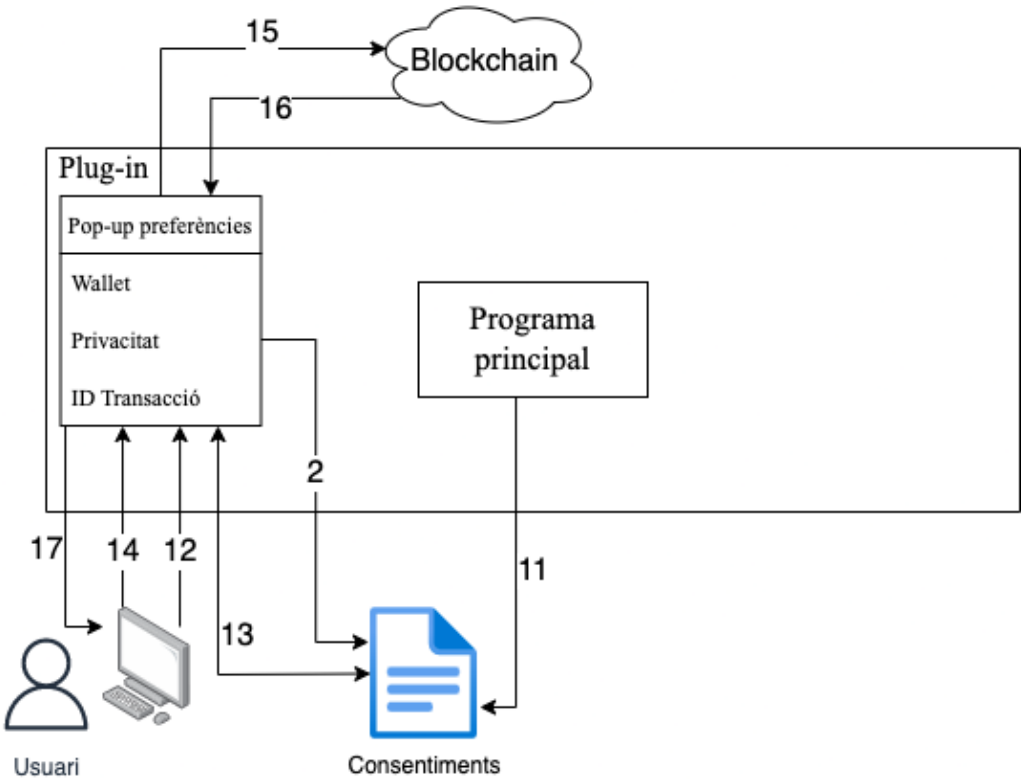

Figura 4. Arquitectura del projecte: consulta del consentiment

A continuació, es detallen breument els passos dels que consten els diagrames:

1. L'usuari introdueix les dades requerides al pop-up de preferències.
2. Es creen les llistes de consulta de consentiment.
3. L'usuari accedeix a una pàgina web amb pop-up de cookies.
4. El programa principal intercepta el pop-up i identifica de quin tipus és.
5. El programa principal consulta les dades que havia introduït l'usuari al pop-up de preferències.
6. El programa principal fa la crida al programa secundari pertinent.
7. El programa secundari interactua amb el pop-up de cookies trobat i en fa la gestió.
8. El programa secundari retorna al programa principal si s'ha realitzat la gestió correctament.
9. El programa principal fa la transacció de l'Smart Contract creat a la Blockchain.
10. La Blockchain retorna l'identificador de la transacció realitzada.
11. El programa principal desa l'identificador a les llistes de consentiments.
12. L'usuari interactua amb el pop-up per que es mostrin els consentiments gestionats.
13. El pop-up consulta les llistes de consentiment i les mostra.
14. L'usuari consulta al pop-up les llistes de consentiment i indica l'identificador de la transacció de la pàgina web sobre la que vol saber el consentiment donat.
15. El pop-up fa la consulta a la Blockchain.
16. La Blockchain retorna la política de privacitat que es va acceptar al pop-up.

17. El pop-up mostra a l'usuari quina va ser la política de cookies que es va acceptar a la pàgina web consultada.

3.2 Requisits funcionals

Als següents apartats es detallen els requisits funcionals dels grans punts que composen el treball.

3.2.1 Programes de gestió de cookies

Aquests programes, als que anomenarem "programes secundaris", han de poder gestionar les cookies dels diferents llocs web. Els programes han de complir els següents requisits:

R1.1. Els programes han de poder accedir a les dades introduïdes per l'usuari.

R1.2. Els programes han de poder seleccionar les opcions tal com ho faria l'usuari en funció de les dades.

R1.3. Els programes han de poder informar de si s'han gestionat les cookies correctament.

3.2.2 Programa de detecció de pop-ups

Aquest programa, anomenat "programa principal" d'ara en endavant, ha de detectar quin tipus de pop-up hi ha a la pestanya activa del navegador, si és que n'hi ha algun, i actuar en conseqüència. El programa ha de complir els següents requisits:

R2.1. El programa ha de poder accedir a les dades introduïdes per l'usuari.

R2.2. El programa ha de poder accedir al contingut web de la pestanya activa al navegador de l'usuari.

R2.3. El programa ha de poder identificar els pop-ups de diferents vendors suportats.

R2.4. El programa ha de poder executar el programa secundari pertinent en funció del vendor trobat.

R2.5. El programa ha de poder connectar-se a una Blockchain.

R2.6. El programa ha de poder crear un Smart Contract.

R2.7. El programa ha de poder crear una transacció a la Blockchain amb la informació necessària.

R2.8. El programa ha de poder modificar les llistes de consentiments gestionats.

3.2.3 Mètode d'introducció de dades i consulta del consentiment

Aquest mètode ha de permetre que l'usuari introdueixi informació rellevant pel funcionament del projecte. A més a més, ha de permetre la consulta dels diferents consentiments gestionats. El mètode ha de complir els següents requisits:

R3.1. El mètode ha de permetre que l'usuari indiqui els usos permesos en relació a les seves dades.

R3.2. El mètode ha de permetre que l'usuari modifiqui les dades en qualsevol moment.

R3.3. El mètode ha de poder accedir a les llistes de consentiments gestionats quan l'usuari ho demani.

R3.4. El mètode ha de poder connectar-se a una Blockchain.

R3.5. El mètode ha de poder consultar un consentiment gestionat a la Blockchain quan l'usuari ho indiqui.

R3.6. El mètode ha de poder mostrar el consentiment de forma clara per l'usuari.

3.3 Requisits no funcionals

Els requisits no funcionals han estat definits tenint en compte certs objectius d'eficiència, privacitat, usabilitat i dependències:

RNF1. El sistema ha de ser capaç de respondre al pop-up de forma ràpida

RNF2. El sistema no ha d'enviar cap informació a l'exterior d'aquest excepte a la Blockchain.

RNF3. Si té les dades a mà, l'usuari ha de poder tindre el sistema llest per funcionar en menys de 2 minuts.

RNF4. El sistema ha de poder seguir funcionant sense cap interacció de l'usuari que no sigui la inicial després d'aturades de la màquina.

RNF5. El sistema ha tindre la menor dependència possible respecte a llibreries i programes externs.

RNF6. El sistema ha de ser modular, per facilitar les actualitzacions d'aquest. És a dir, el sistema ha d'estar dividit en diferents subprogrames per facilitar les tasques de modificació i d'addició de noves funcionalitats.

RNF7. Tot el sistema haurà d'estar fet a prova d'errors i mostrar un missatge en cas de que succeeixi.

3.4 Decisions de disseny

Als objectius del projecte s'ha especificat que el sistema a implementar ha de gestionar les cookies dels portals web. Per tant, és necessari que el navegador incorpori una eina que modifiqui el seu comportament (secció 3.4.1). Per avaluar el comportament de l'eina cal disposar d'un entorn de proves (secció 3.4.2) que ha d'incloure una sèrie de màquines virtuals (seccions 3.4.3 i 3.4.4). Finalment és important fixar com ha de ser la seva interacció amb l'usuari (secció 3.4.5).

3.4.1 Tipus d'eina a desenvolupar

Des de l'inici del projecte s'ha tingut clar que el tipus d'eina a implementar ha de ser un plug-in per un navegador web. Els motius d'aquesta decisió són els següents:

- Facilitat d'instal·lació: La instal·lació d'un plug-in es composa de dos passos: cercar el plug-in a la pàgina d'extensions del navegador web i prémer el botó d'afegir al navegador.
- Multiplataforma: Els plug-ins s'instal·len al navegador, per tant, funcionaran a tots els sistemes operatius pels que funcioni el navegador web.

El plug-in s'ha de desenvolupar per funcionar dins del navegador web Mozilla Firefox. Les raons per les quals s'ha pres aquesta decisió es comenten a continuació:

- Firefox funciona pels tres grans sistemes operatius actuals: Windows, Linux i macOS.
- Mozilla és una organització sense finalitat de lucre. Depenen de les donacions per seguir funcionant i proveint productes gratuïts i de codi obert als usuaris. Degut a això no es veuen incentivats a recol·lectar dades dels seus usuaris per treure'n profit.
- Es tracta d'un navegador de codi obert[3].

3.4.2 Entorn de proves

Per tal d'iniciar el projecte sobre una base sòlida i funcional s'ha de construir un entorn de proves dins del programa de virtualització VirtualBox[4]. La decisió d'utilitzar aquest programa s'ha degut a les següents raons:

- Per tal de poder verificar el funcionament real del sistema cal tindre un entorn de proves que pugui emular diverses màquines alhora.
- VirtualBox permet interconnectar màquines virtuals simulant una subxarxa d'internet, entre d'altres opcions.
- Degut a la feina realitzada durant el grau d'Enginyeria Informàtica, el desenvolupador del projecte té la l'experiència de que es tracta d'un entorn de virtualització fiable i amb les funcionalitats necessàries per poder dur a terme el projecte.

Un cop comentats els motius de la tria de l'entorn de virtualització s'expliquen les decisions preses en relació a aquest per tal d'aconseguir un sistema que compleixi amb els requisits esmentats.

En primer lloc s'ha decidit crear tres màquines virtuals que serviran com a base per la resta del desenvolupament del projecte. Aquestes màquines són:

- Màquina "Client": ha d'allotjar el programa principal que interactuï amb les pàgines web i la Blockchain.
- Màquina "Servidor": ha d'actuar com a servidor d'una pàgina web pròpia, per comprovar la interacció del programa principal sobre ella.
- Màquina "Blockchain": aquesta màquina ha de ser l'encarregada d'allotjar una Blockchain on es facin les transaccions des del programa principal.

Un cop definides les màquines virtuals que s'han d'utilitzar, cal que aquestes es puguin connectar entre elles. VirtualBox ofereix diferents modes de connexió de xarxa per les seves màquines. Després d'estudiar les possibilitats, s'ha decidit utilitzar el tipus de connexió "Xarxa NAT[4]" per interconnectar les diferents màquines. La decisió ha estat presa degut a que aquest mode permet crear una subxarxa entre les màquines per tal que puguin interactuar entre elles i a més permet que tinguin accés a internet.

---

[3] Aquest codi es troba a la web https://searchfox.org/mozilla-central/source

[4] Network Address Translation.

3.4.3 Màquina virtual client

Al llarg d'aquest punt es comenten les decisions preses durant el projecte sobre el contingut de la màquina virtual client. Essencialment, aquestes són les decisions preses en relació al plug-in mencionat al punt 3.4.1.

3.4.3.1 Comunicació amb la Blockchain

Per tal de comunicar el plug-in amb la Blockchain s'ha decidit utilitzar la llibreria *web3.js* pels motius que es detallen a continuació:

- Està construïda per funcionar amb JavaScript, el llenguatge principal amb el que es programen els plug-ins.
- En comparació amb la seva competència, el projecte té un major nombre de contribuïdors.
- Permet compilar fàcilment els Smart Contracts per treballar amb ells a JavaScript.

Per la resta del projecte caldrà tindre en compte que la llibreria *web3.js* sols permet realitzar connexions amb la Blockchain d'Ethereum[5].

3.4.3.2 Disseny de l'Smart Contract

L'Smart Contract que ha d'utilitzar el sistema per desar la informació dels diferents consentiments gestionats per aquest, s'haurà de dissenyar amb l'entorn de desenvolupament Remix [23]. La decisió d'utilitzar aquest entorn s'ha pres tenint en compte els motius que es comenten a continuació:

- L'entorn permet programar i compilar els Smart Contracts.
- A més permet fer proves sobre l'Smart Contract programat mitjançant transaccions a una Blockchain de proves.
- Es tracta d'un entorn intuïtiu i online.

L'Smart Contract utilitzat al projecte s'haurà de programar amb Solidity. La decisió d'implementar-lo amb aquest llenguatge es deu a que aquest va ser desenvolupat per diversos col·laboradors del projecte Ethereum.

S'hauria de desar la mínima informació al contracte, ja que com més informació es desa, major és el cost econòmic de la transacció. Per aquest motiu, l'Smart Contract dissenyat hauria de desar únicament la tupla *URL*[6]*-Nivell de privadesa*, informació estrictament essencial per la futura consulta del consentiment gestionat.

Per tal de consultar aquest consentiment, el contracte hauria de disposar de dos mètodes de consulta, un per cadascuna de les dades introduïdes a la creació d'aquest.

[5] Es tracta d'una Blockchain com la que s'ha definit al punt 2.3, la seva particularitat és que permet l'ús de Smart Contracts. La seva criptomoneda s'anomena "Ether".

[6] Uniform Resource Locator.

3.4.3.3 Nivells de privacitat

Amb motiu de que l'usuari pugui decidir quins usos permet en relació a les seves dades, s'ha decidit dissenyar diferents nivells de privacitat. Aquests nivells s'organitzen de l'1 al 4 i com menor és el nivell triat, major és el nivell de privacitat que oferirà l'eina al fer la gestió de cookies. A continuació es defineixen les bases del disseny dels nivells de privacitat:

1. Rebutjar tot: si l'usuari indica que desitja aquest nivell de privacitat, l'eina hauria de denegar totes les cookies que hi hagi als pop-ups trobats.
2. Rebutjar cookies de perfil i socis[7]: si s'indica aquest nivell, l'eina hauria de rebutjar totes les cookies que siguin per realitzar un perfil de l'usuari i acceptarà la resta. A més a més s'haurien de rebutjar tots els socis de la pàgina web que s'estigui gestionant.
3. Rebutjar socis: amb la tria d'aquest nivell, l'eina hauria de rebutjar els socis però acceptar la resta de cookies.
4. Acceptar tot: si l'usuari tria aquest nivell de privacitat, l'eina hauria d'acceptar totes les cookies de la pàgina web que s'estigui gestionant.

3.4.3.4 Detecció de vendors

Amb l'objectiu de que l'eina sigui el més versàtil possible, s'ha decidit focalitzar la seva actuació sobre els vendors de cookies. D'aquesta manera s'aconseguiria gestionar el consentiment d'un major nombre de pàgines web que si investiguéssim el funcionament de pàgines que tenen el seu propi pop-up no estàndard.

3.4.3.5 Modularitat del sistema

Degut a que l'eina ha de treballar amb la gestió de vendors, s'ha decidit separar la gestió de cadascun en el seu propi fitxer. D'aquesta manera la tasca d'afegir la gestió d'un nou vendor al sistema es faria seguint els següents passos:

1. Crear el fitxer amb les instruccions de gestió del nou vendor.
2. Afegir l'identificador del vendor al mètode per la detecció d'aquest.

3.4.4 Màquina virtual Blockchain

En aquest punt queden reflectides la sèrie de decisions preses en referència al contingut d'aquesta màquina virtual.

Inicialment, la prova de connexió entre el programa principal i aquesta màquina s'hauria de dur a terme mitjançant el desplegament d'un servei web REST[8] per tal de comprovar la connectivitat entre el plug-in i un servei extern i degut també a la varietat de projectes de codi obert que ofereixen una implementació d'aquest servei llesta per fer servir.

[7] Els socis d'una pàgina web són les empreses amb les que la pàgina comparteix les dades obtingudes a partir de les cookies.

[8] REpresentational State Transfer

Posteriorment, s'ha decidit que es faci ús de la Blockchain de proves Ganache [5] pels següents motius:

- El programa permet iniciar una Blockchain de proves d'Ethereum ràpidament.
- A l'iniciar la Blockchain, es creen automàticament unes wallets amb les seves claus públiques i privades i una quantitat d'Ether associat a cadascuna d'elles. Això permet que es puguin fer proves sense cap mena de configuració prèvia.

3.4.5 Disseny de la interfície gràfica

Al projecte sols és necessari un element que disposi d'interfície gràfica, un pop-up que gestioni la introducció de dades i la consulta del consentiment gestionat.

Degut a que l'espai a un pop-up no és massa extens, s'ha de sintetitzar la informació que contingui. Aquest hauria de permetre que l'usuari introduís la seva wallet i el nivell de preferències desitjat.

Finalment, el pop-up hauria de ser capaç de permetre que l'usuari consulti el consentiment gestionat pel plug-in.

3.5 Cas d'ús

La previsió del Treball de Fi de Grau és la utilització a nivell usuari del navegador Mozilla Firefox per la seva versió d'escriptori. En aquest punt es detalla com serà el procés d'utilització del plug-in un cop s'hagi publicat la versió oficial per usuaris.

Quan un usuari vulgui fer ús del plug-in al seu navegador ha de seguir els passos habituals d'integració d'una eina d'aquest tipus. En primer lloc, es comenta el procés d'instal·lació, seguit de l'ús de l'eina. Finalment, es detalla el procés de desinstal·lació.

3.5.1 Instal·lació del plug-in

El pas inicial és la instal·lació del plug-in del projecte al navegador de l'usuari. Per fer-ho l'usuari ha de visitar la pàgina web [30] de complements del navegador i cercar el nom del plug-in. Finalment, ha d'oprimir el botó "Afegeix al Firefox".

3.5.2 Ús del plug-in

Un cop s'ha instal·lat el complement, és necessari que l'usuari introdueixi les dades requerides dins el pop-up pel correcte funcionament del plug-in, és a dir, la seva wallet i el nivell de privacitat desitjat. L'usuari pot modificar en qualsevol moment aquestes dades si així ho vol.

Posteriorment, a mesura que accedeix a diferents llocs web, l'usuari podrà veure que s'està realitzant una gestió automàtica dels pop-ups de cookies que s'allotgen a les pàgines web visitades.

Finalment, quan l'usuari ho desitgi, pot consultar qualsevol dels consentiments donats a cada una de les pàgines que el plug-in ha gestionat.

3.5.3 Desinstal·lació del plug-in

Per la desinstal·lació del plug-in, l'usuari ha de seguir els següents passos:

- Introduir "about:addons" a la barra de cerca del navegador.

- Cercar el plug-in del projecte i oprimir el botó de desplegament d'opcions addicionals.
- Seleccionar l'opció "Esborrar"
- Tornar a prémer "Esborrar" a la finestra emergent de confirmació que apareix.

3.6 Planificació del projecte

El projecte consta de les següents activitats:

1. Estudi de mercat: aquesta activitat consisteix en la recerca d'eines similars a la que es vol realitzar al treball. Això inclou: instal·lar-les, provar el seu funcionament real i classificar-les en funció de la seva similitud amb l'objectiu del projecte. Dintre d'aquest últim grup s'ha de fer la distinció entre els projectes que siguin de codi obert i els que no ho siguin per poder estudiar el seu funcionament a la fase 3 del projecte.
2. Crear l'esquelet de l'arquitectura: aquesta activitat consisteix en crear l'estructura bàsica de l'arquitectura del projecte per tal de poder començar a treballar sobre una bona base que funcioni correctament i reduir la cerca de futurs errors al codi que s'estigui programant i no a un possible funcionament erroni de l'estructura .
    a. Crear màquina virtual "Servidor": es tracta de crear una màquina virtual que actuï com a servidor per una web pròpia amb un pop-up de cookies amb la que es faran proves de funcionament del sistema.
    b. Crear màquina virtual "Client": aquesta màquina ha d'actuar com a ordinador de l'usuari del sistema final. Serà la màquina on es desenvoluparà tot el codi i es faran les proves de funcionament. Durant aquesta fase del projecte es farà servir per crear una eina que detecti exclusivament el pop-up de cookies de la web allotjada a la màquina virtual del servidor.
    c. Crear màquina virtual "Blockchain": es tracta de la màquina virtual on s'allotjarà una Blockchain de proves. A aquesta fase del projecte sols es farà servir per comprovar que es pot establir una connexió des de la màquina client.
    d. Connectar diverses màquines virtuals: aquesta tasca tracta de connectar la màquina virtual client amb les altres dues, per tal de tindre una base funcional del sistema.
3. Estudiar opcions de funcionament: aquesta activitat consisteix en estudiar el codi de les eines que s'hagin considerat a l'activitat 1 per tal de veure si totes les eines funcionen de la mateixa manera o cadascuna fa ús d'idees diferents. D'aquesta manera, es pot considerar quina és la manera més apropiada d'enfocar el problema tenint en compte les necessitats que ha de cobrir el projecte.
4. Implementar l'ús de la Blockchain: aquesta activitat consisteix en fer un ús de la Blockchain que compleixi amb els propòsits del sistema proposat.
    a. Ús de la Blockchain en local: durant aquesta tasca es vol aconseguir l'adaptació completa de la Blockchain amb la resta del sistema però executant-la a la màquina virtual del client per tal de descartar errors de connexió amb una màquina externa.

   b. Dissenyar un Smart Contract: es tracta de fer el disseny i creació d'un Smart Contract que emmagatzemi les dades que requereix el projecte a la Blockchain.
   c. Ús de la Blockchain en remot: a aquesta tasca es trasllada la Blockchain a la seva pròpia màquina virtual, comentada a la tasca 2.c, adaptant el que sigui necessari del programa base per un correcte funcionament.
5. Redactar la primera part de la documentació: durant aquesta activitat s'establirà l'estructura del document i es començarà a redactar la memòria del treball.
6. Gestió de diferents vendors de cookies: aquesta activitat consisteix en dissenyar i programar les parts del projecte amb les que l'usuari final podrà interactuar i que podrà veure, com ara amb quin nivell de privacitat vol que es gestionin els pop-ups de cookies, la pròpia gestió d'aquests o els consentiments gestionats que vulgui consultar.
   a. Dissenyar els nivells de preferències: aquesta tasca consisteix en definir diferents nivells de privacitat, decidint quins tipus de cookies s'acceptaran o es denegaran a cada nivell.
   b. Crear un mètode d'introducció de dades per l'usuari: es tracta de fer un mètode intuïtiu i simple que faciliti a l'usuari la tasca d'introducció de dades i la consulta dels consentiments gestionats.
   c. Programar la gestió de cookies per diferents vendors: durant aquesta tasca es programarà la gestió de consentiments pels vendors més habituals a les pàgines web.
7. Finalitzar la documentació: acabar de redactar la memòria afegint el treball que s'ha dut a terme, els jocs de proves i les conclusions.

A la Figura 5 es mostra de manera més visual la planificació del projecte.

ASUNTO	FECHA DE INICIO	FECHA DE FINALIZACIÓN
Estudi de mercat	22/03/2022	28/03/2022
Crear l'esquelet de l'arquitectura	29/03/2022	12/04/2022
Crear màquina virtual servidor	29/03/2022	01/04/2022
Crear màquina virtual client	01/04/2022	05/04/2022
Crear màquina virtual Blockchain	06/04/2022	09/04/2022
Connectar diverses màquines virtuals	10/04/2022	11/04/2022
Esquelet complet	12/04/2022	12/04/2022
Estudiar opcions de funcionament	13/04/2022	19/04/2022
Implementar ús de la Blockchain	16/04/2022	26/04/2022
Dissenyar Smart Contract	16/04/2022	17/04/2022
Ús de la Blockchain en local	20/04/2022	23/04/2022
Ús de la Blockchain en remot	24/04/2022	25/04/2022
Ús correcte de la Blockchain	26/04/2022	26/04/2022
Redactar la primera part de la documentació	27/04/2022	10/05/2022
Gestió de diferents vendors de cookies	27/04/2022	24/05/2022
Dissenyar els nivells de preferències	27/04/2022	28/04/2022
Crear un mètode d'introducció de dades per l'usuari	29/04/2022	03/05/2022
Programar la gestió de cookies per diferents vendors	04/05/2022	23/05/2022
Sistema funcional	24/05/2022	24/05/2022
Finalitzar la documentació	25/05/2022	09/06/2022
Entregar el projecte	10/06/2022	10/06/2022

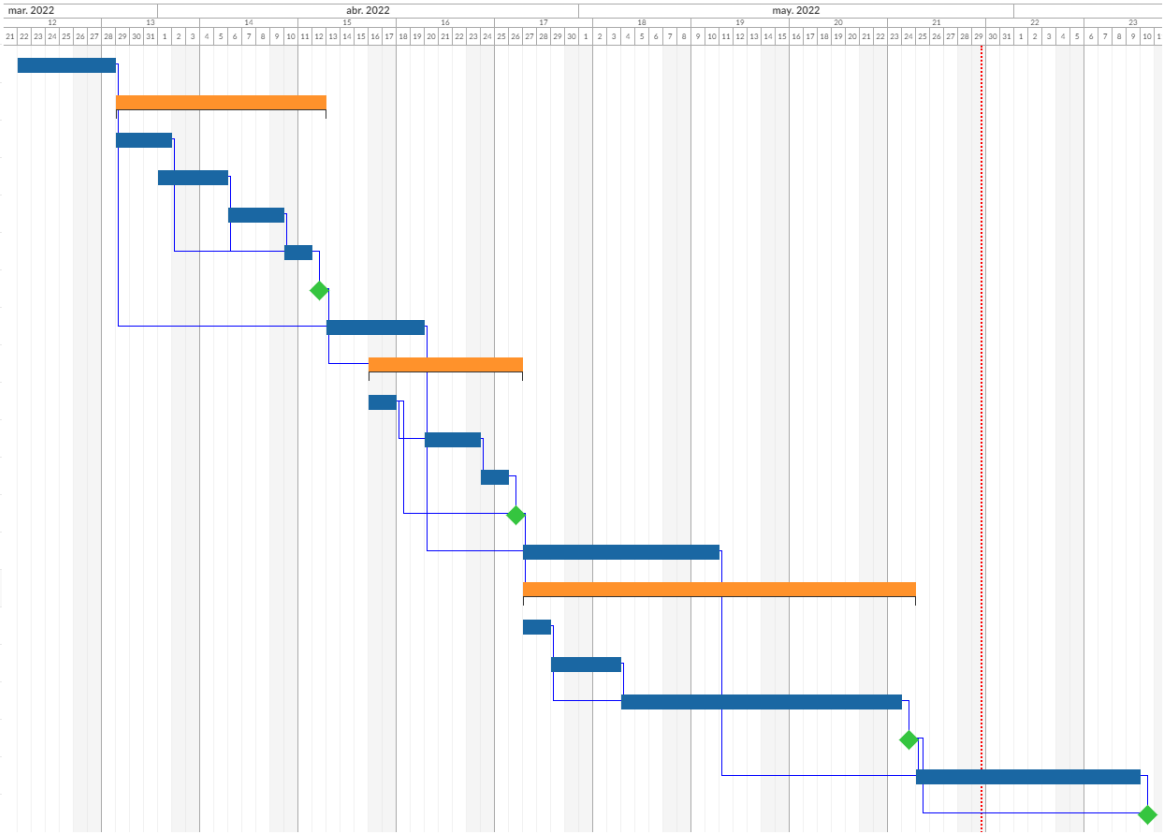

Figura 5. Planificació d'activitats del projecte

4 Implementació

L'arquitectura proposada s'ha desenvolupat en tres grans parts seguint la planificació detallada al punt 3.6. Inicialment, es comenta com s'ha construït l'estructura bàsica del sistema (veure secció 4.1). A continuació, es detalla com s'ha incorporat l'ús de la Blockchain dins d'aquest (veure secció 4.2). Finalment, s'explica el procés seguit per gestionar els pop-ups dels vendors suportats i la creació del pop-up d'introducció de dades (veure secció 4.3). El codi implementat es pot consultar al GitHub del projecte.

4.1 Implementació de l'estructura bàsica del sistema

Prèviament a la implementació de l'estructura bàsica del sistema s'han creat les màquines virtuals que la conformen i s'han interconnectat per tal que es puguin comunicar entre elles.

Posteriorment, s'ha procedit a realitzar la implementació d'una pàgina web per realitzar proves de funcionament del sistema (veure punt 4.1.1). A continuació, s'ha desenvolupat un servidor REST per provar la connexió entre aquest i el plug-in (veure punt 4.1.2). Finalment, s'ha implementat un plug-in bàsic que interactuï amb els dos elements comentats anteriorment (veure punt 4.1.3).

4.1.1 Implementació de la pàgina web

La pàgina web que s'allotja a la màquina virtual "Servidor" s'ha desenvolupat amb els llenguatges HTML[9], JavaScript i CSS[10]. A continuació, es descriuen les tasques que s'han realitzat per aconseguir el funcionament desitjat d'aquesta part del sistema.

El primer pas ha estat crear els fitxers que composen la pàgina web:

- Fitxer HTML: hi ha el contingut principal de la web a més del contingut del pop-up de cookies. Dins d'aquest fitxer s'especifica quin és el document d'estils a aplicar i quin és el document JavaScript associat.
- Fitxer CSS: conté els estils que s'apliquen als elements del fitxer HTML.
- Fitxer JavaScript: s'encarrega la lògica del pop-up de cookies. Aquest document conté tres funcions:
  - "`setCookie()`": desa un document de cookies al navegador de l'usuari quan ha acceptat la política de privacitat.
  - "`getCookie()`": comprova si l'usuari té desat del document de cookies d'aquesta pàgina de proves al seu navegador.
  - "`checkCookie()`": és la funció més complexa del document. Primer crida el mètode "`getCookie()`" per comprovar si l'usuari ja ha acceptat la política de privacitat. En cas que no l'hagi acceptat, mostra el pop-up a la web i la funció espera a que es produeixi un clic al botó d'acceptar. Quan això succeeix, es crida el mètode "`setCookie()`" i s'amaga el pop-up.

Un cop s'han implementat els documents que conformen la pàgina web, cal ubicar-los al directori "/var/www/html". Per tal que es pugui veure la pàgina des d'una altra màquina

[9] HyperText Markup Language.

[10] Cascading Style Sheets.

virtual s'ha de desplegar un servidor. Per dur a terme aquesta tasca s'ha fet servir Apache [24]. Per iniciar el servidor de proves amb Apache s'executa la comanda "`sudo service apache2 start`" a la terminal. El resultat obtingut es pot observar a la Figura 6.

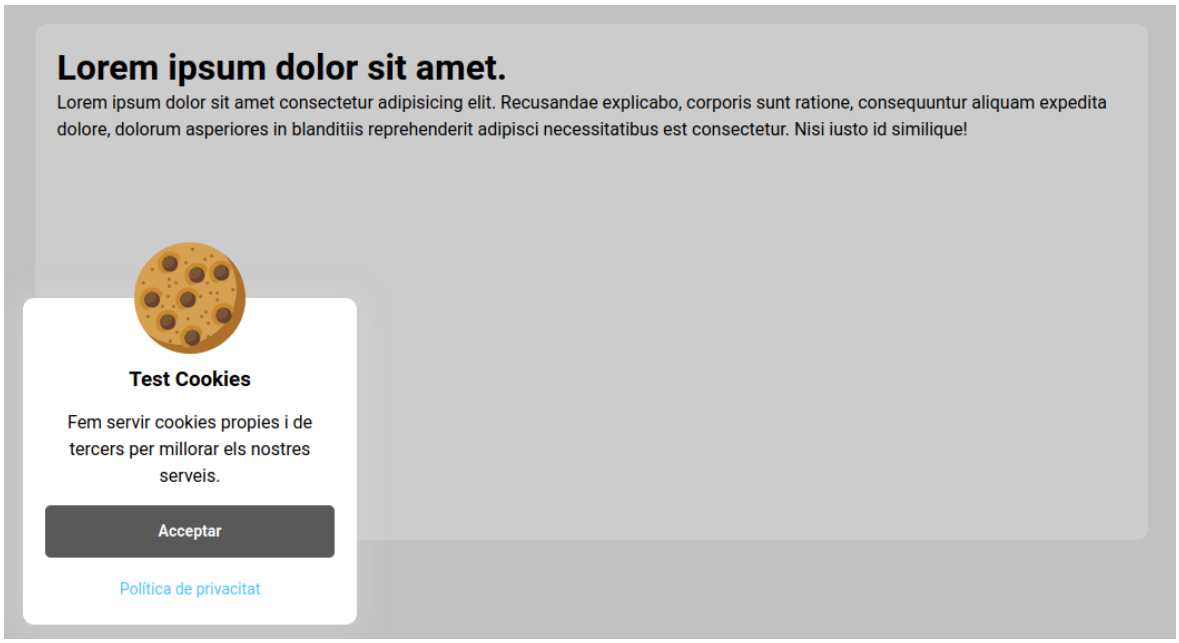

Figura 6. Contingut de la pàgina web creada

4.1.2 Implementació del servidor REST

Per tal de comprovar que el plug-in es pot connectar a la Blockchain en un futur, s'ha implementat un servidor REST a la màquina virtual "Blockchain". Aquest servidor funciona amb la API *Express* [25].

A continuació, es detalla el funcionament del fitxer de configuració del servidor REST anomenat "app.js":

- S'importa la llibreria *Express*.
- A continuació, es crea una instància de la llibreria a la constant *app*, que ens permetrà crear una funció que escolti a les peticions entrants.
- També es crea una variable associada al mètode "`Router()`" de la llibreria. Aquest mètode s'encarrega de les funcions d'encaminament del servidor.
- Amb el que s'ha detallat fins ara ja es pot crear el mètode de resposta de peticions del servidor. La funció, anomenada "`post()`" té el següent funcionament: Es connecta al directori "/test" del servidor i rep un objecte quan es produeix una petició. Finalment, retorna un objecte de resposta amb un text arbitrari cap al plug-in.
- Finalment es crea el mètode "`listen()`" que escolta les peticions que arriben al servidor.

El contingut del fitxer és prou simple, ja que per la comesa del projecte sols és necessari que quan el servidor rebi una petició del plug-in, li retorni una resposta bàsica.

Per desplegar el servidor REST cal executar la comanda "`node app.js`" a la terminal.

4.1.3 Implementació del plug-in de gestió de cookies

En aquest punt es detalla el funcionament del plug-in implementat a la fase d'implementació de l'estructura bàsica del projecte. Les tasques que realitza el plug-in en finalitzar aquesta fase són: interactuar amb el pop-up de la pàgina web de proves vista al punt 4.1.1 i establir una connexió amb el servidor REST comentat al punt 4.1.2.

En aquesta fase del projecte el plug-in està conformat per dos fitxers:

- "content.js": s'encarrega de la interacció amb el pop-up de cookies de la pàgina web i de la connexió amb el server REST.
- "manifest.json[11]": s'especifica l'organització dels fitxers del projecte per tal que el navegador es comporti correctament un cop instal·lada l'extensió. En aquesta fase del projecte, s'especifica que per qualsevol pàgina web visitada s'executi el fitxer "content.js".

A continuació, es comenta el funcionament del fitxer "content.js" amb major profunditat:

- Inicialment, s'introdueix l'identificador HTML del botó d'acceptar cookies a una variable amb la funció "`document.getElementById()`", on l'objecte "document" conté el codi HTML de la pàgina web.
- A continuació, s'aplica la funció "`click()`" a la variable que representa el botó d'acceptar cookies.
- Un cop gestionades les cookies, es fa una crida a la funció "`connectREST()`", enviant com a paràmetre la direcció IP[12] de la màquina virtual "Blockchain", juntament amb el directori "/test", on s'haurà de fer la petició.
- Dins de la funció "`connectREST()`", es fa una crida a la API *Fetch* [26] que es troba integrada als navegadors on s'especifiquen els següents paràmetres:
  - Direcció on s'ha de realitzar la connexió: aquesta s'ha rebut des de la crida comentada al pas anterior.
  - Tipus de petició a realitzar: s'ha de fer una connexió tipus "POST" contra el servidor REST, ja que és el tipus de petició pel que s'ha implementat el funcionament al punt 4.1.2.
  - Contingut de la petició: s'envia un text arbitrari.
- Finalment, s'espera a la resposta del servidor i es mostra a la consola del navegador quan es rep.

Per tal de poder carregar el plug-in desenvolupat com a complement temporal al navegador cal seguir els següents passos:

1. Obrir el navegador Mozilla Firefox.
2. Introduir "about:debugging#/runtime/this-firefox" a la barra de cerca del navegador.
3. Seleccionar la opció de "Carregar complement temporal".
4. Cercar la carpeta on es troben els fitxers del projecte i oprimir el botó "Obrir".

[11] JavaScript Object Notation.

[12] Internet Protocol.

4.2 Implementació de l'ús d'una Blockchain

Seguint la planificació del projecte, un cop s'ha desenvolupat l'estructura d'aquest es procedeix a implementar l'ús de la blockchain al plug-in. En aquest punt es comenten els passos que s'han realitzat per dur-ho a terme.

4.2.1 Implementació de l'Smart Contract

Com s'ha comentat al punt 3.4.3.2 de les decisions de disseny, l'Smart Contract que es fa servir al projecte s'ha implementat a l'entorn de desenvolupament Remix fent servir Solidity com a llenguatge de programació. A continuació, es detalla el funcionament del contracte:

- Constructor: s'utilitza per inicialitzar variables dins del contracte intel·ligent. El constructor del contracte implementat al projecte rep com a paràmetres d'entrada l'URL de la pàgina web de la qual s'ha gestionat el consentiment i el codi numèric que indica el nivell de privacitat escollit per l'usuari amb el qual s'ha fet la gestió. Dins del constructor s'emmagatzemen els paràmetres rebuts a dues constants dins del contracte per tal que romanguin inalterades i se'n pugui fer la consulta més endavant.
- Funció "`whichWeb()`": retorna l'URL que es troba emmagatzemada a una de les constants del contracte.
- Funció "`whichPreference()`": retorna el nivell de privacitat, emmagatzemat a l'altra constant.

Al compilar un Smart Contract amb Solidity es generen dos fitxers addicionals, l'"abi" i el "bytecode". Aquests documents són els que realment interactuen amb la Blockchain, degut a que Solidity és un llenguatge d'alt nivell. La manera com interactuen és la següent: El document "bytecode" és el codi que s'executa a la Blockchain i l'"abi" actua d'intermediari entre aquest i el codi del programa de l'usuari.

4.2.2 Implementació d'un ús local de la Blockchain

La interacció del plug-in amb la Blockchain s'ha implementat inicialment amb aquesta allotjada a la màquina virtual "Client" per tal que no es produïssin errors de connexió.

El primer pas a realitzar ha estat la instal·lació de Ganache a la màquina virtual "Client" per desplegar la Blockchain.

Seguidament, s'ha importat la llibreria *web3.js* al codi del plug-in amb la comanda "`require()`" de JavaScript però al provar aquest canvi carregant el plug-in al navegador s'ha trobat un error que indica que aquest mòdul no està suportat pel navegador.

Aquest problema s'ha pogut solucionar investigant a la pàgina web de la llibreria, on s'indica que dins d'un directori del seu projecte es troba el fitxer "web3.min.js". Aquest document és una versió reduïda de la llibreria que ens permet realitzar la seva importació de manera senzilla dins del projecte. La manera com s'ha importat el fitxer per obtenir el funcionament desitjat ha estat afegint la ruta on es troba el fitxer dins el document "manifest.json" del plug-in. D'aquesta manera s'aconsegueix que es carregui la llibreria abans d'executar el fitxer "content.js". Fent-ho així, el codi principal pot accedir a les funcions d'aquesta llibreria sense cap mena de problema.

Un cop s'ha importat la llibreria *web3.js* correctament, es procedeix a realitzar la connexió entre el plug-in i la Blockchain. Per dur a terme aquesta tasca, es segueixen els següents passos:

1. Crear la instància de la llibreria dins de la constant *web3* amb la comanda "`web3 = new Web3(url)`". El paràmetre URL conté la direcció IP on es troba allotjada la Blockchain.
2. Realitzar la petició de les wallets existents dins la Blockchain amb la comanda "`wallets = await web3.eth.getAccounts()`". L'operador "await" de JavaScript permet que el programa esperi a que es retorni d'una funció que executa accions fora del programa. Al rebre la resposta de la funció, es continua amb l'execució de la següent comanda.
3. Mostrar el contingut de la variable *wallets* a la consola del navegador per comprovar-ne el resultat.

El següent pas a realitzar un cop s'ha comprovat la connexió amb la Blockchain és fer ús de l'Smart Contract implementat al punt 4.2.1 per tal de realitzar transaccions amb els consentiments gestionats.

Al tractar d'utilitzar l'Smart Contract al plug-in mitjançant els documents "abi" i "bytecode" sorgeix un problema de compatibilitat amb el navegador: no es permet l'ús del mòdul natiu de JavaScript "fs" d'importació de fitxers.

La solució al problema ha estat encastar el codi d'ambdós documents dins el codi del plug-in, associats a les variables *abi* i *bytecode*.

Finalment, s'ha desenvolupat el codi pel desplegament de l'Smart Contract cap a la Blockchain. Els passos a seguir per dur-ho a terme es detallen a continuació:

1. Es crea una instància de contracte intel·ligent dins d'una variable amb la comanda "`contract = new web3.eth.Contract(JSON.parse(abi))`". La funció "`JSON.parse()`" transforma la cadena introduïda com a paràmetre en un objecte JavaScript.
2. Es prepara el contracte pel seu desplegament amb la comanda "`contract.deploy({data:bytecode,arguments:[privacitat,window.location.href]})`". Els paràmetres introduïts al camp d'arguments corresponen respectivament al nivell de privacitat i a l'URL de la pàgina web actual.
3. Es crida el mètode "`send()`" sobre el contracte per realitzar la transacció a la Blockchain amb els paràmetres següents:
    - "from : ac": on la variable *ac* conté la direcció de la wallet que realitzarà la transacció.
    - "gas[13] : estimatedGas": on *estimatedGas* és la quantitat de gas necessari per dur a terme la transacció. Aquest es calcula per la funció "`estimateGas()`" de la llibreria *web3.js*.
4. Quan es rep la resposta de la Blockchain conforme la transacció s'ha dut a terme correctament, es rep un objecte de tipus contracte que conté

[13] Fa referència a la comissió requerida per tal de dur a terme una transacció a la Blockchain d'Ethereum amb èxit.

l'identificador de la transacció a un camp. S'introdueix l'identificador al camp corresponent l'objecte *contract* creat al punt 1.

5. Un cop s'ha desat correctament l'identificador de la transacció realitzada es crida el mètode del contracte que retorna l'URL de la web gestionada. Aquesta acció es duu a terme mitjançant la comanda "`contract.methods.whichWeb().call()`".
6. Finalment, es mostra el valor que retorna la crida a la funció "`whichWeb()`" a la consola del navegador per comprovar-ne el resultat.

Un cop s'ha aconseguit implementar un codi que interactua correctament amb la Blockchain en local, cal traslladar-la a una màquina virtual remota i adaptar el codi del plug-in per tal que segueixi funcionant correctament.

4.2.3 Trasllat de la Blockchain a una màquina virtual remota

En aquest punt es mostra el procés d'adaptació del codi del plug-in per la correcta interacció amb una Blockchain a una màquina virtual remota.

El primer pas a realitzar ha estat la instal·lació de Ganache a la màquina virtual "Servidor" per desplegar la Blockchain.

Posteriorment, s'ha modificat el contingut de la variable *url* comentada al punt 1 de com importar la llibreria *web3.js*, a la secció 4.2.2. El seu contingut actual és "`HTTP://IP:8545`", on "IP" és la direcció IP de la màquina virtual "Servidor" i "8545" és el port on es connecta la Blockchain de Ganache.

El següent pas realitzat és l'execució de Ganache introduint la comanda "`ganache-cli -h IP`" a la terminal. Els paràmetres de la comanda es detallen a continuació:

- "`ganache-cli`": es tracta de l'entorn en consola de Ganache. També hi ha disponible un entorn amb interfície gràfica.
- "`-h`": indica que el següent paràmetre trobat és la direcció on escoltar les peticions. Es determina per tal que no funcioni localment com ho feia al punt 4.2.
- "`IP`": la direcció IP de la màquina virtual "Servidor".

Un cop s'ha seguit el procés detallat, es pot comprovar que el plug-in realitza la connexió i les transaccions amb la Blockchain correctament.

4.3 Implementació de la gestió i consulta del consentiment.

Un cop s'han implementat l'estructura del projecte i la interacció d'aquest amb la Blockchain, resta per implementar la part que dona sentit al treball: la gestió i consulta del consentiment.

En aquest punt es detalla com s'ha realitzat la seva implementació, dividint la feina realitzada en dos blocs: per una banda, es mostra el desenvolupament del pop-up per la introducció de dades i la consulta del consentiment (veure secció 4.3.1) i, per altra, es comenta la implementació de la gestió del consentiment pels diferents vendors suportats pel plug-in (veure secció 4.3.2).

4.3.1 Implementació del pop-up

En aquest punt es comenta la implementació del pop-up d'introducció de dades i consulta del consentiment gestionat. Aquest consta de dues planes:

- La pàgina d'introducció de dades. La implementació d'aquesta plana es troba detallada, en part, al punt 4.3.1.1. La part restant en referent al desenvolupament de la pàgina es troba al punt 4.3.1.2.
- La pàgina de consulta de transaccions. La implementació d'aquesta pàgina es troba detallada al punt 4.3.1.2.

A continuació, es comenten per separat les funcions d'introducció de dades i de consulta del consentiment.

4.3.1.1 Implementació de la introducció de dades al pop-up

Inicialment, s'ha desenvolupat el codi HTML amb el CSS corresponent per la introducció de dades. Aquest codi s'ubica exclusivament a la primera pàgina del pop-up.

A continuació, es comenta la implementació del codi HTML d'aquesta secció del pop-up:

- S'associa la pàgina amb un identificador anomenat *contingut* i s'indica que té la propietat de CSS "display" amb el valor "block". Amb això fem que la primera pàgina es vegi quan s'obre el pop-up.
- A continuació, es creen els camps d'introducció de text per la wallet i el nivell de privacitat amb els seus identificadors associats.
- Finalment, es crea el botó "Aplica" amb un identificador associat.

Tot seguit, es detalla el desenvolupament del codi JavaScript relacionat amb aquesta secció del pop-up:

- Inicialment, es comprova si l'usuari havia desat ja una wallet i un nivell de privacitat anteriorment fent ús de la funció "`browser.storage.local.get(ID)`". El camp "ID" representa l'identificador d'un dels dos camps d'introducció de text. En cas que s'hagin introduït els paràmetres anteriorment, s'escriuran els valors dins dels camps de text associats per tal que l'usuari pugui veure els valors que havia introduït.
- Seguidament, es crida la funció "`listenForClicks()`". El seu funcionament es comenta a continuació:
  - S'inicia un esdeveniment que controla si s'ha produït un clic al botó "Aplica" amb la comanda "`document.addEventListener("click", e)`". L'objecte "e" rep una notificació quan es produeix l'acció especificada.
  - Entra a un condicional que executarà la funció de gestió associada al botó "Aplica". El codi d'aquest és "`if(e.target.classList.contains(ID))`", on "e" és l'objecte creat anteriorment i "ID" és l'identificador associat al botó premut.
  - La funció associada al botó "Aplica" desa el text introduït per l'usuari als camps de "Wallet" i "Privacitat" a la memòria del navegador mitjançant la comanda "`browser.storage.local.set({clau: valor})`". A continuació, es detalla el contingut dels paràmetres:
    - "clau": conté el nom que associarem al camp que s'està desant.
    - "valor": conté el valor que s'ha introduït al camp.

En cas que el valor de la wallet canviï es reinicialitzen les llistes que desen la informació sobre el consentiment gestionat, ja que aquests no estan relacionats amb la nova wallet.

En aquesta secció s'ha desenvolupat el comportament del pop-up en referència a la introducció de la wallet i d'un dels nivells de privacitat detallats al punt 3.4.3.3. Quan l'usuari prem el botó "Aplica", les dades introduïdes es desen a la memòria interna del navegador. A la Figura 7 es mostra el resultat obtingut. Cal recordar que la implementació dels elements d'aquesta plana del pop-up que encara no s'han mencionat es troben detallats al punt 4.3.1.2.

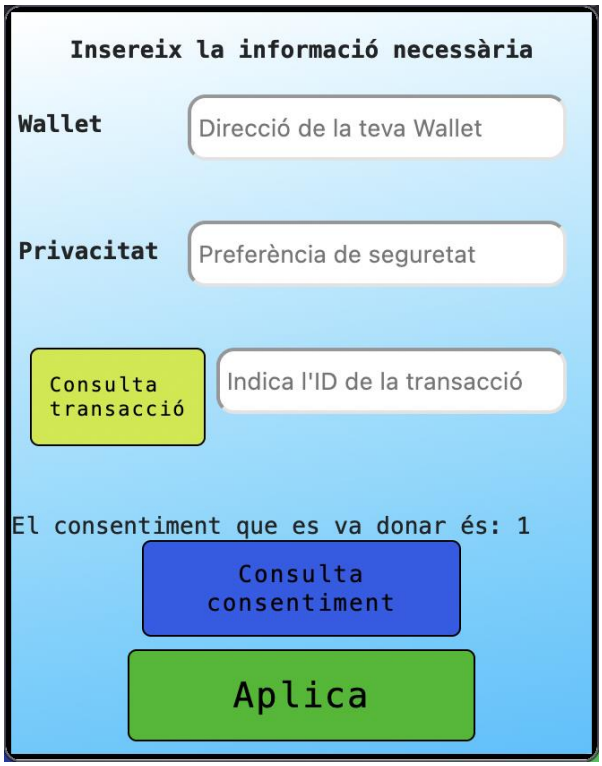

Figura 7. Pàgina d'introducció de dades del pop-up

4.3.1.2 Implementació de la consulta de consentiment al pop-up

El primer pas per la implementació de la consulta del consentiment ha estat desenvolupar el codi HTML amb el CSS associat. Aquest es correspon a la part que manca per explicar de la primera pàgina, vista a la Figura 7, i a la segona plana del pop-up en la seva totalitat.

A continuació, es comenta la implementació del codi HTML corresponent a la primera pàgina del pop-up:

- Inicialment, es creen el botó "Consulta transacció" i el camp d'introducció de text per la transacció a consultar. Ambdós amb els seus identificadors pertinents.
- Finalment, es crea el botó de "Consulta consentiment" amb el seu identificador.

Seguidament, es comenta el desenvolupament del codi HTML associat a la segona pàgina del pop-up:

- S'associa la pàgina amb un identificador anomenat *transaccions* i s'indica que té la propietat de CSS "display" amb el valor "none". Amb això fem que la segona plana quedi oculta quan s'obre el pop-up.
- A continuació, es crea el botó "Tornar" amb el seu identificador associat.
- Finalment, es crea una llista no ordenada sense contingut, associada a un identificador.

A continuació, es detalla el desenvolupament del codi JavaScript relacionat amb aquestes seccions del pop-up:

- Inicialment, es creen tres condicionals associats al mateix objecte "e" vist al codi JavaScript del punt 4.3.1.1, dins de la funció "`listenForClicks()`". Es recorda que aquest objecte rep quan l'usuari clica un botó del pop-up. Cadascun d'aquests condicionals està associat a un dels tres botons comentats anteriorment i, dins de cada condicional, es fa la crida a una funció que gestiona el comportament del pop-up quan es prem el botó associat.
- Funció associada a "Consulta consentiment":
  - Inicialment, amaga la primera pàgina canviant-li l'estat de la propietat "display" a "none" i mostra el contingut de la segona pàgina canviant-li el valor de la mateixa propietat a "block".
  - Posteriorment, pren el contingut de les llistes de consulta del consentiment. A continuació, es detalla el contingut d'ambdues:
    - "webPagesTFG": conté la llista d'URLs de les pàgines webs per les quals s'ha realitzat la consulta del consentiment.
    - "transactionIDsTFG": conté la llista d'identificadors de les transaccions realitzades.

    Cal esmentar que aquestes llistes es troben desades a la memòria interna del navegador.
  - Finalment, per cada element de les llistes es crea un element a la llista no ordenada que s'ha comentat a la implementació del codi HTML. Aquest element conté la tupla *URL-ID_Transacció*, on l'usuari pot seleccionar l'identificador desitjat i copiar-lo per tal de realitzar la consulta del consentiment que es va donar.
- Funció associada a "Tornar":
  - Inicialment, amaga la segona pàgina canviant-li l'estat de la propietat "display" a "none" i mostra el contingut de la primera pàgina canviant-li el valor de la mateixa propietat a "block".
  - Finalment, s'esborra el contingut de la llista no ordenada que s'ha omplert a la funció associada a "Consulta consentiment" per tal que no es dupliquin els elements mostrats si es torna a accedir a la segona plana.
- Funció associada a "Consulta transacció":
  - Inicialment, pren el contingut del camp de text on s'introdueix l'identificador de la transacció a consultar.
  - Es realitza la connexió a la Blockchain seguint el procediment vist a la secció 4.2.2 del document.
  - Com a paràmetre "address" del contracte s'estableix l'identificador de la transacció introduït per l'usuari. D'aquesta manera, el contracte que s'acaba de generar dins d'aquesta funció actuarà com si fos el contracte amb el que es va fer la transacció que es vol consultar.

- Es fa la crida al mètode "`whichPreference()`" del contracte. Aquesta crida produeix una consulta a la Blockchain.
- Quan es rep el resultat de la crida, es mostra dins el pop-up quin va ser el nivell de privacitat amb que es va gestionar el consentiment que s'ha consultat.
- En cas que es produeixi un error en relació amb la Blockchain, es mostra un missatge amb el codi d'error corresponent dins el pop-up.

A la Figura 7 mostrada anteriorment es pot observar el resultat de la implementació referent a la primera plana del pop-up. Quan l'usuari introdueix l'identificador de la transacció a consultar i prem el botó "Consulta transacció", es mostra el resultat sota del camp de text. Finalment, quan es prem el botó "Consulta consentiment", es mostra la segona pàgina del pop-up. A la Figura 8 es mostra el resultat de la implementació d'aquesta plana.

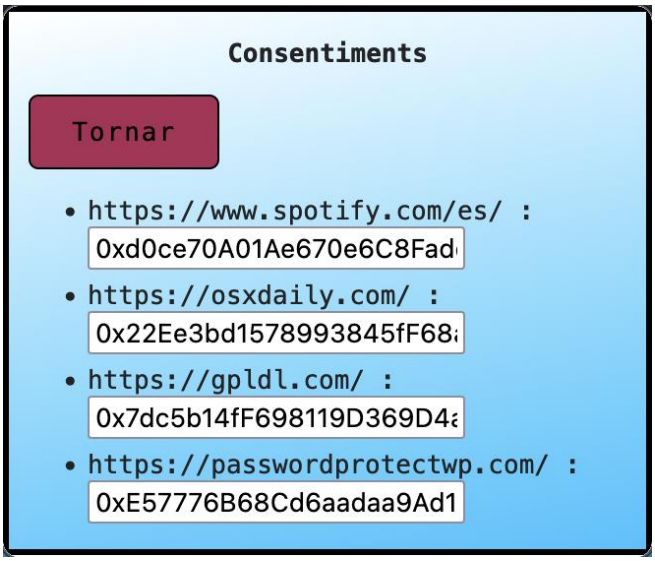

Figura 8. Pàgina de consulta de transaccions del pop-up

4.3.2 Gestió del consentiment pels diferents vendors

Durant el transcurs del projecte s'ha trobat un estudi [27] sobre la quota de mercat dels vendors de cookies. Aquest ha estat realitzat per la companyia *Wrappalyzer*, dedicada a la recol·lecció de dades sobre diferents tecnologies. Actualment, dins d'aquest estudi s'han analitzat 1.231.000 llocs web per la seva classificació. A la Figura 9 es pot observar el resultat obtingut.

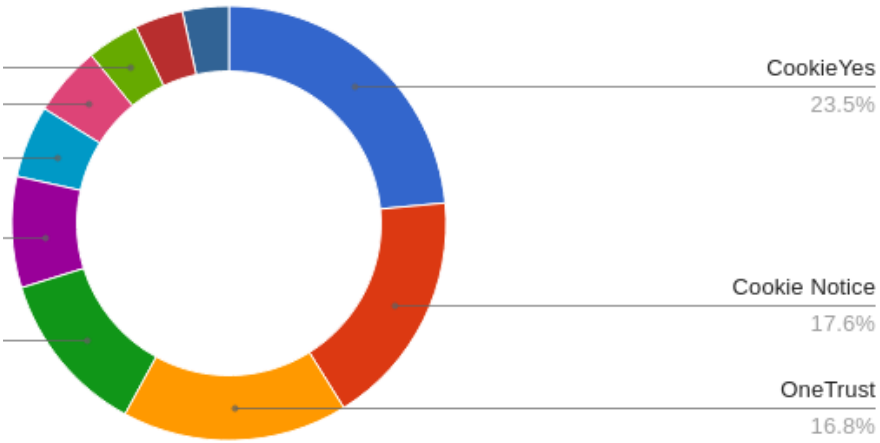

Figura 9. Quota de mercat dels vendors estudiats. Font: Wrappalyzer

Degut al gran nombre de vendors que hi ha al mercat, s'ha implementat la gestió del consentiment pels que tenen una major quota de mercat. Els vendors pels quals s'ha realitzat la implementació són els següents:

- *Didomi* (veure secció 4.3.2.2).
- *CookieYes* (veure secció 4.3.2.3).
- *CookieNotice* (veure secció 4.3.2.4).
- *OneTrust* (veure secció 4.3.2.5).

Com es pot observar a la Figura 9, el vendor *Didomi* no hi apareix. Això es deu a que es va implementar la seva gestió abans de descobrir l'estudi sobre les quotes de mercat comentat anteriorment. La tria d'implementar inicialment la seva gestió es va deure al fet que les webs més consultades pel desenvolupador a l'àmbit de la premsa empren aquest vendor.

L'estratègia general seguida pel desenvolupament de la gestió dels vendors suportats pel plug-in es mostra a la secció 4.3.2.1.

Prèviament a la implementació d'aquest punt, s'ha realitzat un estudi sobre el funcionament intern de les eines de gestió de cookies detallades a la secció 1.1.2 d'aquest document. Els tipus de funcionament que s'han trobat durant l'estudi són els següents:

- L'eina escolta les peticions que realitza la pàgina web a través de la xarxa. L'objectiu és trobar una petició coneguda associada a un dels vendors suportats per tal d'identificar-lo i fer-ne la gestió.
- L'eina busca els identificadors HTML dels pop-ups controlats dins del codi de la pàgina web actual. L'objectiu és el mateix que el del punt anterior amb la diferència que l'eina no treballa amb vendors, sinó amb una base de dades pròpia que conté els identificadors HTML dels pop-ups i la funció a executar per fer-ne la gestió.

Inicialment, es va implementar la primera opció per realitzar la detecció dels vendors, degut a que aquesta es produïa més ràpidament que esperant a que carregués el codi HTML de la pàgina.

Finalment, es va canviar el mètode de detecció utilitzat pel detallat a continuació, ja que no tots els vendors de cookies funcionen amb peticions de xarxa.

La tasca de detecció dels vendors que suporta el plug-in es duu a terme al fitxer "content.js". El procés seguit per la implementació d'aquesta tasca és el següent:

- S'ha creat una llista que conté les parelles clau-valor dels vendors suportats, on la clau és el nom de l'empresa proveïdora i el valor és l'identificador HTML del pop-up d'aquesta.
- Posteriorment, es fa la crida a la funció "`timeoutCall(list)`", amb la llista de vendors suportats com a paràmetre. Aquesta funció està ubicada al document "scripts.js", on es troben les funcions que s'utilitzen habitualment durant el projecte.
- Dins de la funció es cerca si hi ha algun dels identificadors de la llista de vendors al codi HTML de la pàgina web visitada per l'usuari. Si en 1 segon no se n'ha trobat cap, retorna un missatge a la consola del navegador. D'aquesta manera no es malbaraten els recursos de la màquina de l'usuari. En cas que trobi un vendor suportat, retorna el nom d'aquest.
- Finalment, s'executa un dels fitxers de gestió de consentiment en funció del vendor trobat.

Un cop explicat el mètode de detecció de vendors, es procedeix a comentar com s'ha implementat la consulta de consentiment al fitxer "content.js":

- Posteriorment a la detecció del vendor, es comprova que l'usuari hagi introduït els paràmetres "wallet" i "privacitat" al pop-up mitjançant la comanda "`browser.storage.local.get([camp])`", on "camp" és la clau que hem designat per aquests paràmetres al punt 4.3.1.1 dins del codi JavaScript. En cas que els paràmetres no siguin correctes es mostra un missatge d'error a la consola del navegador.
- Finalment, després de realitzar la transacció a la Blockchain com s'ha vist al punt 4.2.2, s'afegeix l'URL de la pàgina web a la que s'ha realitzat la consulta del consentiment dins la llista "webPagesTFG". Posteriorment, s'afegeix l'identificador de la transacció realitzada a la llista "transactionIDsTFG". Es recorda que aquestes llistes es troben emmagatzemades a la memòria interna del navegador.

4.3.2.1 Estratègia general per la gestió dels vendors suportats

En aquest punt es detalla quina ha estat l'estratègia que s'ha seguit per la gestió de tots els vendors suportats pel plug-in.

Primerament, es comprova si ja s'havia gestionat el consentiment per la pàgina web actual. Això es fa comprovant si aquesta té un document de cookies conegut associat. Degut a que hi ha vendors que no desen una cookie al navegador de l'usuari, s'ha creat una cookie pròpia anomenada "PluginTFG" per realitzar aquest control. Aquesta cookie es desa al navegador web de l'usuari quan s'ha realitzat la gestió del consentiment a la pàgina actual.

En cas que no s'hagi gestionat la pàgina actual anteriorment, es procedeix a comprovar el nivell de privacitat introduït per l'usuari al pop-up i es gestionen les cookies en funció d'aquest. Quan es gestionen les cookies amb un nivell de privacitat 4, sempre s'accepten totes.

Cal mencionar que durant la implementació de la gestió per tots els vendors s'ha realitzat una investigació exhaustiva sobre els identificadors associats a tots els botons que els composen i les diferents maneres d'interactuar amb ells.

A continuació, es detalla el funcionament de les funcions utilitzades recurrentment durant el desenvolupament de la gestió dels vendors:

- "`waitUntilFoundAndClick()`": rep per paràmetre l'identificador a cercar. Quan el troba dins del document HTML de la pàgina web actual, simula un clic de l'usuari. Quan ha realitzat totes les accions, retorna.
- "`waitUntilFixed()`": rep per paràmetre l'identificador a cercar. Quan troba l'element, comprova si té l'atribut CSS "position" amb valor "fixed". Fins que no es compleix la condició no retorna.
- "`waitUntilNull()`": rep per paràmetre l'identificador a cercar. Quan el troba, comprova si té valor "null", és a dir, que no és un objecte interactuable. Fins que no es compleix la funció no retorna.
- "`setCookie()`": crea la cookie "PluginTFG" mencionada anteriorment.

Quan finalitza la gestió del consentiment, es mostra un missatge a la consola del navegador, indicant quina acció s'ha dut a terme en funció del nivell de privacitat indicat.

4.3.2.2 Implementació de la gestió del consentiment per *Didomi*

A continuació, es detallen les particularitats a la implementació de la gestió d'aquest vendor. Pels nivells de privacitat 3 i inferiors, s'han els següents passos comuns:

1. Es prem el botó "Configurar", que mostra les opcions de gestió. Aquest s'oprimeix amb la funció "`waitUntilFoundAndClick()`".
2. Es realitza la mateixa acció sobre el botó "Veure socis".
3. Es selecciona l'opció de bloquejar tots els vendors.
4. Es prem el botó de desar i tornar enrere.

Pel nivell de privacitat 3, s'oprimeixen tots els botons d'acceptar dels diferents tipus de cookies mitjançant la funció "`waitUntilFoundAndClick()`". Finalment, es prem el botó "Desar".

La gestió del consentiment pel nivell de privacitat 2 d'aquest vendor s'ha implementat seguint els següents passos:

1. Denegar totes les cookies de cop amb la funció "`waitUntilFoundAndClick()`".
2. Acceptar una per una les cookies que no generen cap perfil de l'usuari.
3. Es prem el botó "Desar"

Per la gestió del consentiment al nivell de privacitat 1, s'oprimeixen tots els botons de denegar cookies mitjançant la funció "`waitUntilFoundAndClick()`". Finalment, es prem el botó "Desar".

Al finalitzar la gestió de qualsevol nivell de privacitat, es consulta si s'ha creat el document de cookies del vendor.

4.3.2.3 Implementació de la gestió del consentiment per *CookieYes*

A continuació, es detallen les particularitats a la implementació de la gestió d'aquest vendor.

En cas que no s'hagin gestionat les cookies del lloc web anteriorment, es crida la funció "`waitUntilFixed()`" degut a que s'han trobat pàgines web que no mostren el pop-up de gestió de cookies fins que l'usuari hi interactuï d'alguna manera. Així, el plug-in espera a que això succeeixi i, llavors comença la gestió del consentiment.

Pels nivells de privadesa 3 i inferiors es realitzen les següents accions comunes:

- Si el pop-up no disposa de botó de configuració de cookies, s'amaga modificant el seu atribut CSS "position" al valor "relative". Aquest tornarà a aparèixer a la pàgina si l'usuari la recarrega.
- Si el pop-up conté un botó per la configuració de cookies, el programa continua amb la seva gestió.

Degut a que aquest vendor no incorpora l'opció de gestionar els socis, pel nivell de privacitat 3 s'accepten totes les cookies mitjançant la funció "`waitUntilFoundAndClick()`" i es prem el botó "Desar".

Pel nivell de privacitat 2, s'accepten les cookies de funcionalitat i de rendiment mitjançant la funció "`waitUntilFoundAndClick()`" i es prem el botó "Desar".

Pel nivell de privacitat 1, simplement es prem el botó "Desar", ja que dins la configuració d'aquest vendor, totes les cookies es troben denegades per defecte.

Degut a que aquest vendor no desa el document de cookies al navegador de l'usuari, no tenim manera de comprovar que el codi s'ha executat correctament. Al finalitzar la gestió de qualsevol nivell de privacitat, es resol una "promise" per tal que el flux de treball del plug-in torni al programa principal. Una "promise" de JavaScript permet executar un codi seqüencialment i retornar en un punt desitjat. D'aquesta manera aconseguim que el codi de la gestió del vendor retorni en el moment apropiat.

4.3.2.4 Implementació de la gestió del consentiment per *CookieNotice*

Aquest vendor no incorpora les opcions de gestionar els socis o les cookies més enllà de l'opció de rebutjar-les. Aquesta opció no està disponible a totes les pàgines web. Per tant, la gestió del consentiment d'aquest vendor és prou simple en comparació amb els altres que es controlen.

A continuació, es detallen les particularitats a la implementació de la gestió d'aquest vendor.

Inicialment, s'executa la funció "`waitUntilFound()`" sobre l'identificador del pop-up, ja que no sempre es troba visible al carregar la pàgina. Un cop es pot interactuar amb ell, es procedeix a la gestió del consentiment.

En cas que el nivell de privacitat introduït per l'usuari sigui de 3 o inferior, es comprova si el pop-up ofereix la possibilitat de denegar les cookies. En cas que ho permeti, es deneguen mitjançant la funció "`waitUntilFoundAndClick()`" i es prem el botó "Desar". En cas contrari, s'amaga el pop-up canviant el seu atribut CSS "position" al valor "relative".

Igual que *CookieYes* (veure secció 4.3.2.3), aquest vendor tampoc desa les cookies al navegador de l'usuari, per tant, també es fa ús d'una "promise" per retornar al programa principal quan s'ha gestionat el consentiment.

4.3.2.5 Implementació de la gestió del consentiment per *OneTrust*

OneTrust és el vendor que més variants ofereix, ja que a la plana de configuració de les diferents cookies es poden trobar dos tipus d'organització diferents: per separat o tipus llista. A la variant tipus llista, tots els botons d'interacció es troben a la mateixa plana del pop-up. En canvi, a l'altra variant, s'ha de prémer la secció del tipus de cookies abans de poder interactuar amb el botó de gestió. A la Figura 10 es mostra la variant del pop-up on els botons estan separats.

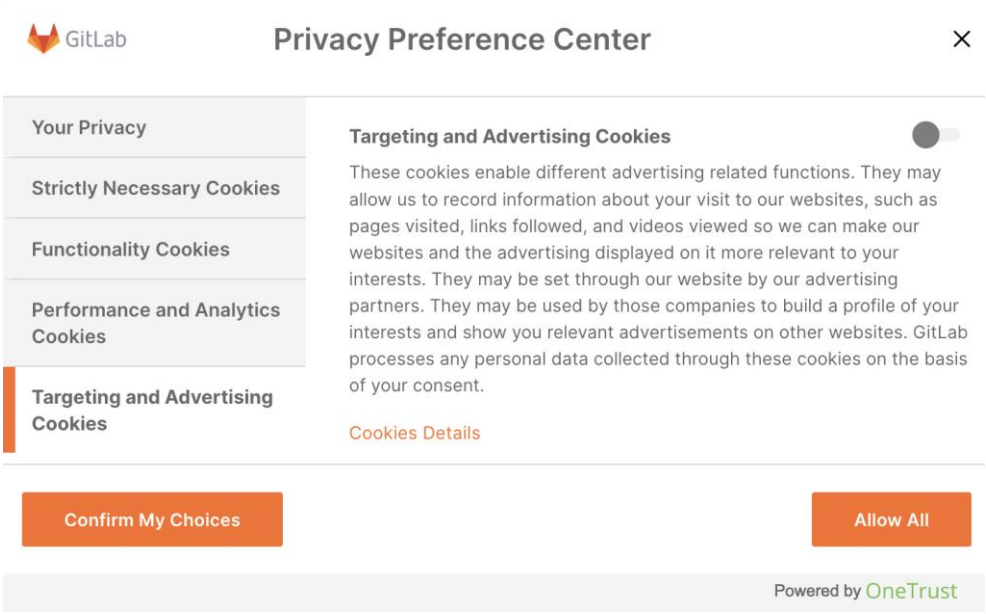

Figura 10. Variant de OneTrust amb els botons per separat

A continuació, es detalla la implementació comuna per la gestió del consentiment d'aquest vendor amb els nivells de privacitat 3 i inferiors:

- Inicialment, es comprova si disposa de botó per la gestió dels socis. En tal cas, es prem el botó i s'executa la funció "`waitUntilNull()`". Quan aquesta retorna, podem interactuar amb els socis de la pàgina web. Seguidament, es desactiven els botons "Interès legítim" i "Consentiment" en cas que estiguin activats. Finalment, es prem el botó que desa les preferències acabades de gestionar i mostra la plana de gestió de les cookies. En cas que no hi hagi un botó de socis, es prem el botó per la gestió de les cookies directament.
- Un cop es mostra la plana de gestió de cookies, es comprova si el contingut de la plana és de tipus llista o si es mostren les diferents cookies per separat. La diferència dins del codi entre les dues opcions és un petit canvi a la manera d'interactuar. La manera del plug-in de gestionar les cookies sempre simula el comportament d'un usuari, per tant, si les cookies es troben per separat, el programa haurà de clicar a cada secció del pop-up abans de gestionar la cookie en qüestió. Des d'aquest punt sols es comentarà la implementació per la gestió del pop-up tipus llista, ja que els canvis respecte a la gestió de l'altre tipus resideixen en com està construït.

Per la gestió del consentiment al nivell de privacitat 3, s'oprimeixen tots els botons de d'acceptar cookies comprovant abans la seva existència a la plana. Finalment, es prem el botó "Desar".

Pel nivell de privacitat 2 es realitzen les mateixes comprovacions. Es deneguen les cookies que creïn un perfil de l'usuari i s'accepta la resta. Finalment, es prem el botó "Desar".

Si l'usuari ha introduït el nivell de privacitat 1, es comprova l'existència de les cookies a la plana i, a continuació, es deneguen totes. Finalment, es prem el botó "Desar".

El vendor *OneTrust* no desa les cookies al navegador de l'usuari, per tant es fa ús d'una "promise" per retornar al programa principal un cop gestionades, d'igual manera que s'ha fet pels vendors CookieYes i CookieNotice (veure seccions 4.3.2.3 i 4.3.2.4).

5 Avaluació i resultats

Per poder avaluar un correcte funcionament del sistema proposat, es realitzen una sèrie de proves funcionals per cadascun dels punts que es detallen en aquesta secció.

5.1 Programa principal

S'han comprovat els possibles errors que el programa principal ha de poder manegar:

- Introduir una cadena o un nombre més gran que 4 al camp de text de privacitat del pop-up. El programa mostra un error a la consola del navegador.
- Introduir una direcció incorrecta al camp d'introducció de text de la wallet. El programa mostra un error a la consola del navegador.
- No s'ha introduït res dins els camps de text de wallet i/o privacitat. El programa mostra un missatge informatiu a la consola del navegador.
- No hi ha un vendor gestionat a la pàgina actual. El programa mostra un missatge informatiu a la consola del navegador.

Els resultats obtinguts són satisfactoris i compleixen amb els requisits del projecte, concretament amb el RNF7, detallat a la secció 3.3 del document.

5.2 Gestió dels vendors suportats

El mètode d'avaluació per la gestió dels vendors suportats, ha estat classificar les pàgines web trobades a l'estudi [27] sobre la quota de mercat dels vendors en funció dels següents paràmetres:

- Ofereix gestió: la pàgina permet la gestió de les preferències, és a dir, que s'ofereixen opcions de gestió a part del botó d'acceptar les cookies.
- Socis: la pàgina web comparteix les dades obtingudes amb els seus socis.

Finalment s'ha avaluat el funcionament de la gestió de consentiment tenint en compte els següents aspectes:

- Nivell de privacitat: fa referència al nivell introduït per la gestió del consentiment.
- Amaga pop-up: es determina si un cop s'ha gestionat el pop-up, aquest s'ha amagat.
- Fa transacció: el plug-in desenvolupat fa una transacció a la Blockchain amb el consentiment donat.
- Consulta: el nivell de privacitat que es mostra al fer la consulta del consentiment dins el pop-up del projecte.

A la Taula 2 es mostren els resultats obtinguts en relació amb la gestió del proveïdor de cookies *Didomi*. Com s'ha trobat un comportament homogeni a totes les pàgines, s'han fet les proves amb nivells de privacitat equitatius:

Web	Ofereix gestió	Socis	Nivell de privacitat	Amaga pop-up	Fa transacció	Consulta
marca.com	Sí	Sí	1	Sí	Sí	1
as.com	Sí	Sí	1	Sí	Sí	1
elpais.com	Sí	Sí	2	Sí	Sí	2

giphy.com	Sí	Sí	2	Sí	Sí	2
reverso.net	Sí	Sí	3	Sí	Sí	3
elmundo.es	Sí	Sí	3	Sí	Sí	3
bfmtv.com	Sí	Sí	4	Sí	Sí	4
societe.com	Sí	Sí	4	Sí	Sí	4

Taula 2. Resultats obtinguts amb la gestió del vendor *Didomi*

Un cop realitzades les proves per la gestió del vendor *Didomi*, s'observa que els resultats obtinguts són els que s'esperaven.

Els resultats obtinguts en relació amb la gestió del vendor *CookieYes* es troben a la Taula 3. El paràmetre "Socis" no es fa servir degut a que el vendor no permet la gestió d'aquests a cap dels pop-ups estudiats. A més a més, per les pàgines que no ofereixen una gestió del consentiment més enllà d'acceptar la política de privacitat, s'ha fet la prova amb el nivell 4 que realment accepta la política i també amb els altres nivells que simplement amaguen el pop-up.

Web	**Ofereix gestió**	**Nivell de privacitat**	**Amaga pop-up**	**Fa transacció**	**Consulta**
wpmet.com	Sí	1	Sí	Sí	1
sliderrevolution.com	Sí	2	Sí	Sí	2
tympanus.net	Sí	3	Sí	Sí	3
wpdatatables.com	Sí	4	Sí	Sí	4
bezkoder.com	No	4	Sí	Sí	4
		3	Sí	No	/
wpthemedetector.com	No	4	Sí	Sí	4
		2	Sí	No	/
styde.net	No	4	Sí	Sí	4
		1	Sí	No	/

Taula 3. Resultats obtinguts amb la gestió del vendor *CookieYes*

Un cop realitzades les proves, els resultats obtinguts són els esperats. La gestió produeix una transacció sempre que el pop-up ofereixi la possibilitat de gestionar les cookies. En cas contrari i, amb un nivell de privacitat inferior a 4, s'amaga el pop-up però no es realitza cap transacció a la Blockchain.

A continuació es mostren els resultats obtinguts a les proves realitzades sobre el vendor *CookieNotice*. Com s'ha comentat a la seva implementació (veure secció 4.3.2.4), aquest tipus de pop-up no ofereix la gestió dels socis, per tant, no es farà servir el paràmetre associat a aquests. A la Taula 4 es mostren els resultats de la seva gestió.

Web	Ofereix gestió	Nivell de privacitat	Amaga pop-up	Fa transacció	Consulta
gpldl.com	Sí	1	Sí	Sí	1
		2	Sí	Sí	2
wpbuffs.com	Sí	3	Sí	Sí	3
		4	Sí	Sí	4
mailtrap.io	No	1	Sí	No	/
osxdaily.com	No	2	Sí	No	/
searchengineland.com	No	3	Sí	No	/
booster.io	No	4	Sí	Sí	4

Taula 4. Resultats obtinguts amb la gestió del vendor *CookieNotice*

Els resultats obtinguts són els esperats. Sempre que s'ofereix la possibilitat de gestió, es fa una transacció. En cas que no s'ofereixi una opció més enllà d'acceptar les cookies, s'amaga el pop-up.

Finalment, a la Taula 5 es mostren els resultats obtinguts a les proves realitzades sobre el vendor *OneTrust*.

Web	Ofereix gestió	Socis	Nivell de privacitat	Amaga pop-up	Fa transacció	Consulta
fiverr.com	Sí	No	1	Sí	Sí	1
gitlab.com	Sí	No	2	Sí	Sí	2
app.slack.com	Sí	No	3	Sí	Sí	3
freepik.com	Sí	Sí	4	Sí	Sí	4
udemy.com	Sí	No	1	Sí	Sí	1
upwork.com	Sí	No	2	Sí	Sí	2
open.spotify.com	Sí	Sí	3	Sí	Sí	3
elementor.com	Sí	No	4	Sí	Sí	4

Taula 5. Resultats obtinguts amb la gestió del vendor *OneTrust*

Un cop realitzades les proves realitzades per la gestió del vendor *OneTrust,* s'observa que els resultats obtinguts són els que s'esperaven.

5.3 Interfície gràfica

Durant la fase d'avaluació, s'ha comprovat que el funcionament del botons és correcte i que el contingut de la llista de webs gestionades també ho es.

Es procedeix a comprovar els casos on pot fallar la implementació del pop-up:

- Al modificar el nivell de privacitat i prémer “Aplica”, es gestiona el consentiment de les següents pàgines visitades amb el nou nivell establert. Es comprova mitjançant el resultat de la transacció generada.
- Al modificar la wallet, la llista de consentiments es buida.
- Al consultar consentiments, tornar enrere i consultar-los novament, no es mostra la llista de consentiments duplicada.
- Quan s’introdueix un identificador de transacció incorrecte, es mostra un error dins el pop-up.

Els resultats obtinguts durant aquestes comprovacions han resultat satisfactoris i compleixen amb els requisits del projecte.

6 Conclusions

En aquest projecte, s'ha dissenyat una eina per la gestió automàtica de les polítiques de privacitat a través de les cookies que un usuari troba al navegar per internet. Aquesta eina consisteix en un plug-in desenvolupat per funcionar a un navegador, el qual s'encarrega de manegar els pop-ups de cookies de forma automàtica i transparent a l'usuari quan accedeix a diferents planes web, tenint en compte el nivell de privadesa desitjat per part del mateix usuari.

A més a més, davant l'actual model dels proveïdors de serveis, centrat en la gestió de polítiques de privacitat, l'eina proposada migra el consentiment donat en relació a aquestes a la Blockchain, mitjançant l'ús de contractes intel·ligents. Aquests, emmagatzemen la web a la qual s'ha accedit i el nivell de privadesa que s'ha tingut en compte durant el procés de gestió de les polítiques de privadesa. Finalment, l'usuari pot consultar quines polítiques de privacitat es van acceptar a les pàgines web gestionades per l'eina.

Per provar el funcionament del projecte a un entorn més realista, s'ha dissenyat un entorn de treball mitjançant l'ús de màquines virtuals que consisteix en:

- Una màquina que actua com a servidor per una pàgina web de proves
- Una segona màquina on s'allotja una Blockchain.
- Una última màquina on es desenvolupa el plug-in que interactua amb les altres dues i que, finalment, interactua amb webs allotjades a internet.

Com a resultat final, l'eina duu a terme aquesta gestió de les polítiques de privacitat al 58,9% de les webs visitades. Aquest resultat s'extreu tenint en compte els proveïdors de cookies pels que l'eina gestiona el consentiment i la quota de mercat que aquests representen a l'àmbit de les pàgines web.

Per últim, es vol comentar que hi ha molts proveïdors de serveis que no són massa honestos en quant a la gestió que ofereixen per les seves polítiques de privacitat. Durant la recerca del funcionament pels diferents vendors s'ha observat que associar el botó que tanca el pop-up a la funció d'acceptació de totes les cookies és una pràctica recurrent entre aquests proveïdors.

6.1 Treball futur

A continuació, es comenta el treball que es pretén realitzar de cara al futur:

- Implementar la gestió de més proveïdors de cookies per tal de manegar un major nombre de pàgines web.
- Traslladar el funcionament de l'eina a altres navegadors web per augmentar el nombre d'usuaris d'aquesta.
- Els contractes intel·ligents generats es troben publicats a la Blockchain, de forma que tothom hi té accés. Un sol contracte no conté més informació que la web visitada per un usuari, però, aquesta informació es pot considerar un quasi-identificador. Així, un atacant podria buscar a la Blockchain tots els contractes intel·ligents associats a una mateixa parella de claus i utilitzar-los per re-identificar un usuari, podent arribar a extreure informació delicada sobre aquest. Per tal d'evitar un atac d'aquesta mena, es pretén proveir al sistema actual d'un mòdul que s'encarregui de la generació i la gestió de parelles de claus, de forma que cada cop que es generi un nou contracte intel·ligent, aquest es publiqui a la Blockchain amb una nova parella de claus.

7 Referències

[1] GDPRinfo. https://gdprinfo.eu/ [Informació sobre el GDPR]

[2] GDPR. https://gdpr.eu/cookies/ [Informació sobre les cookies en relació amb el GDPR]

[3] ReadTheDocs. https://web3js.readthedocs.io/ [Informació sobre la llibreria web3.js]

[4] VirtualBox. https://www.virtualbox.org [Informació sobre VirtualBox]

[5] TruffleSuite. https://trufflesuite.com/ganache/ [Informació sobre Ganache]

[6] Deloitte. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-cookie-benchmark-study.pdf [Estudi sobre webs amb cookies a Europa]

[7] URV. https://crises-deim.urv.cat/web/docs/publications/conferences/1133.pdf [Proposta sobre la que es basa el projecte]

[8] AmazeeMetrics.https://www.amazeemetrics.com/en/blog/76-ignore-cookie-banners-the-user-behavior-after-30-days-of-gdpr/ [Estudi sobre la interacció dels usuaris amb els pop-ups]

[9] Oficina de Seguretat de l'internauta. https://www.osi.es/es/actualidad/blog/2018/07/18/entre-cookies-y-privacidad [Tipus de cookies]

[10] Lopdat. https://www.lopdat.es/noticias/que-hacen-con-nuestros-datos-en-internet [Article sobre la venda de dades]

[11] Ionos. https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-plugin/ [Explicació plug-in]

[12] Ayuda Ley Protección de Datos. https://ayudaleyproteccion datos.es/cookies/ [Explicació cookies]

[13] IBM. https://www.ibm.com/es-es/topics/what-is-blockchain [Explicació Blockchain]

[14] IBM. https://www.ibm.com/es-es/topics/smart-contracts [Explicació Smart Contracts]

[15] Profesional Review. https://www.profesionalreview.com/2018/12/16/conectar-maquinas-virtuales-en-red-virtualbox/ [Tipus de connexions a VirtualBox]

[16] Mozilla. https://addons.mozilla.org/es/firefox/addon/ninja-cookie/ [Extensió Ninja Cookie]

[17] Mozilla. https://addons.mozilla.org/es/firefox/addon/super-agent/ [Extensió Super Agent]

[18] Mozilla. https://addons.mozilla.org/es/firefox/addon/auto-cookie-optout/ [Extensió Auto Cookie Optout]

[19] Mozilla. https://addons.mozilla.org/es/firefox/addon/polish-cookie-consent/?utm_source=git [Extensió Polish Cookie Consent]

[20] Santander. https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas [Explicació criptomonedes]

[21] N26. https://n26.com/es-es/blog/que-es-un-wallet-de-criptomonedas#como-funciona-un-wallet-de-criptomonedas [Explicació wallet]

[22] VMWare. https://www.vmware.com/es/topics/glossary/content/virtual-machine.html [Explicació màquines virtuals]

[23] Ethereum. https://remix.ethereum.org/ [Entorn de desenvolupament Remix]

[24] Apache. https://httpd.apache.org/ [Informació sobre Apache]

[25] ExpressJS. https://expressjs.com/ [Informació sobre la llibreria Express]

[26] Mozilla. https://developer.mozilla.org/es/docs/Web/API/Fetch_API [Informació sobre la API Fetch]

[27] Wrappalyzer. https://www.wappalyzer.com/technologies/cookie-compliance [Estudi sobre la quota de mercat dels vendors]

[28] Didomi. https://www.didomi.io/es/ [Informació sobre Didomi]

[29] OneTrust. https://www.onetrust.es/ [Informació sobre OneTrust]

[30] Mozilla. https://addons.mozilla.org/es/firefox/ [Tenda d'extensions de Firefox]

[31] GitHub. https://github.com/EduardBel/TFGPlugin [GitHub del projecte]