



UNIVERSIDADE DA CORUÑA

MEMORIA EXPLICATIVA DOS  
ASPECTOS ESPECÍFICOS DO SOFTWARE LIBRE  
E ACTIVIDADE PÚBLICA DO PROXECTO  
FIN DE CARREIRA EN ENXEÑARÍA INFORMÁTICA

**Pasaporte dixital de vacinación COVID-19  
baseado en Blockchain, con criptomoeda  
asociada a modo de incentivo e aplicación  
móbil para o seu uso**

**Estudante:** Mauro Alberto de los Santos Nodar

**Dirección:** Tiago Manuel Fernández Caramés

A Coruña, outubro de 2021.

# Índice Xeral

---

<b>1</b>	<b>Memoria explicativa</b>	<b>2</b>
1.1	Resumo . . . . .	2
1.2	Introdución e desenvolvemento do PFC . . . . .	2
1.2.1	Motivación e obxectivos . . . . .	2
1.2.2	Aspectos técnicos relativos ao PFC . . . . .	3
1.3	Xustificación do uso de software Libre no PFC . . . . .	5
1.4	Software Libre utilizado no proxecto . . . . .	6
1.5	Licenza Open Source utilizada no PFC . . . . .	7
1.6	Actividade Pública . . . . .	8
1.6.1	Distribución do código . . . . .	8
1.6.2	Publicidade, difusión e contactos . . . . .	8
1.7	Conclusións e traballo futuro . . . . .	9

# Memoria explicativa

---

## 1.1 Resumo

Debido á recente aparición da pandemia da COVID-19, as vidas de todos nós deron un xiro radical e na sociedade actual xurdiron novas etapas acompañadas de novas necesidades. Este traballo arranxa unha delas creando unha solución *Open Source*, libre, transparente e accesible para calquera potencial usuario arredor do mundo. Dita solución aportará un sistema de certificados dixitais para o seguro almacenamento e compartición de datos médicos relacionados ca COVID-19, co fin de demostrar de forma inequívoca, infranqueable e segura a inmunidade ou falta de virus, baseándose na tecnoloxía Blockchain e nos seus beneficios inherentes, presentando un sistema de incentivos cunha criptomoeda propia para recompensar aos usuarios que o empreguen e creando dúas aplicacións móbiles distribuídas para o seu uso.

## 1.2 Introducción e desenvolvemento do PFC

### 1.2.1 Motivación e obxectivos

O proxecto nace ca idea de facer fronte ás notábeis consecuencias que a pandemia deixou na vida de todas as persoas ao redor do mundo, véndose reflexadas a todos os niveis e áreas da nosa sociedade. De feito, orixináronse nela unha serie de fases, entre as que destacamos as actuais e futuras etapas de vacinación e post-vacinación da poboación. Con elas preséntase un problema co cal lidar: o adecuado tratamento da información respecto ás vacinas e probas e a óptima utilización da mesma. Isto, sumado á clara precariedade tecnolóxica do sistema sanitario, ás cuestionábeis solucións adoptadas e aos problemas actuais de non-vacinación e restricións sociais, sumado ao gran potencial de novas tecnoloxías como Blockchain e temáticas emerxentes na sociedade como as criptomoedas, anima a pensar nunha solución que trate xa non só os datos respecto ás vacinas, senón todos aqueles que xiren en torno á COVID-19, dunha forma máis moderna, óptima, descentralizada e segura, e que ao mesmo tempo, in-

centive o seu uso ca finalidade de crear situacións sanitarias máis controladas e polo tanto, seguras. Vemos así como o obxectivo principal do proxecto é a mellora da sociedade e a axuda á situación actual de loita fronte a pandemia, creando unha solución única no campo e sendo indispensable polo tanto que conte cun carácter aberto, libre e non-restritivo, para poder ser difundida, verificada, mellorada e depurada co principal obxectivo da súa futura implantación e uso. En canto aos obxectivos máis técnicos, podemos destacar:

- **A creación dunha Blockchain privada** que permita incorporar todos aqueles datos médicos e de vacinación máis relevantes, asociados sempre de forma unívoca e segura ao cidadán, con datos como poden ser as datas das doses recibidas, o tipo de vacina, o centro na que foi administrada ou as últimas probas COVID-19 realizadas, á súa vez co seu tipo, data e resultados.
- **A creación dunha criptomoeda**, despregada sobre a Blockchain anteriormente mencionada, que terá como obxectivo actuar a modo de incentivo para o cidadán, sendo adxudicada certa cantidade dela á conta de cada usuario por diversos motivos: uso do pasaporte de vacinación, inoculación dunha dose, realización dunha proba, etcétera. Promóvese así o uso do sistema, a vacinación da poboación, a creación de ambientes seguros e a compartición segura de datos médicos relacionados ca COVID-19.
- **A creación de dúas *Decentralized applications* (Dapps) móbiles**, deseñadas e implementadas nun entorno **multi-plataforma**, as cales se comuniquen ca Blockchain para facilitar e acercar o uso de toda a infraestrutura detallada anteriormente tanto á parte dos cidadáns como á parte médica, permitindo realizar accións como por exemplo: lecturas de pasaportes, actualización dos mesmos ao acudir a centros médicos, envío e recepción da criptomoeda, etcétera.
- **A elección dunha licenza *Open Source* axeitada e una selección tecnolóxica libre**, ca finalidade de poder, una vez finalizado o proxecto, facelo público e accesible, para crear así una comunidade que o verifique, mellore e depure sen rastro de opacidade e que o acerque a todos os rincóns do mundo que se viron afectados pola pandemia, contribuíndo á xestión da mesma.

### 1.2.2 Aspectos técnicos relativos ao PFC

#### Deseño e Implementación

A Figura 1.1 amosa a arquitectura de comunicacións do sistema proposto, onde vemos os principais módulos xunto cos seus compoñentes e as relacións entre os mesmos. Concretamente, amósanse xunto cas diferentes partes implementadas e as súas respectivas tecnoloxías:

- Unha **Blockchain privada** creada en **Ethereum** ca ferramenta **Geth**. A súa correcta configuración foi realizada a través dun *JSON* que define o seu *Genesis Block*. Despre-gouse xunto con diversos nodos mineiros que aceptan diferentes tipos de transaccións.
- **Smart Contracts**: desenvoltos en **Solidity** dende o IDE online de **Remix**. Ditos *smart contracts* implementan todas as funcionalidades do sistema. Cabe mencionar: os contratos de rexistro médico, para consultar a información dun rexistro ou escribir e/ou actualizar a información médica do mesmo; o da criptomoneda, habilitando un sistema de incentivos polo uso do sistema e permitindo o libre comercio ca mesma; e por último, o contrato do *Faucet*, ferramenta creada para o outorgamento baixo demanda de *Ether* aos diferentes usuarios do sistema.
- **Dúas apps móbiles** multiplataforma desenvoltas con *Kotlin* en **KMM** (*Kotlin Mobile Multiplatform*) para modularizar o proxecto e separar as funcionalidades de lectura para os pacientes e de escritura para os CDCs (*Centers for Disease Control*).

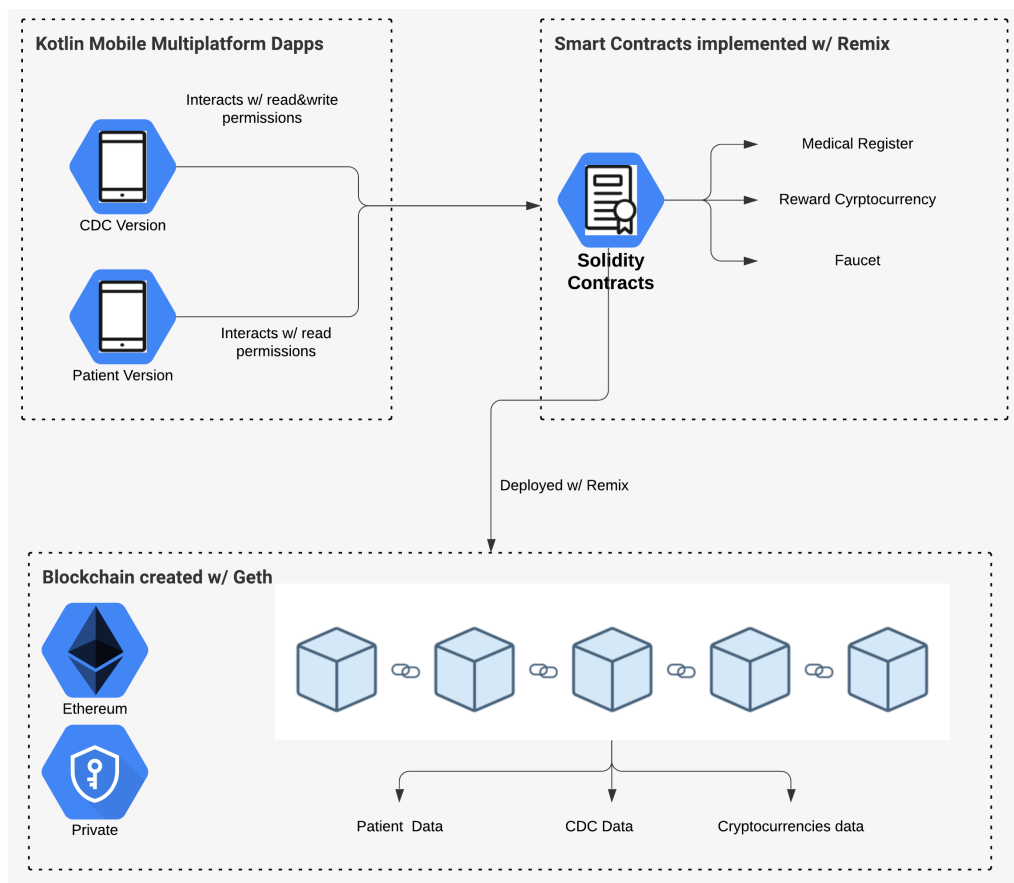


Figura 1.1: Arquitectura do proxecto.

### Exemplos de uso

A Figura 1.2 amosa un exemplo do fluxo de diferentes interaccións co sistema proposto. Catro casos de uso son ilustrados de maneira secuencial: (1) Un paciente acude por primeira vez tras descargar a app a un CDC, é engadido ao sistema dende a app CDC e o seu rexistro médico é creado así como (2) actualizado cunha dose inoculada, recibindo por elo o incentivo correspondente. A continuación, (3) comercia libremente ca criptomoeda dende a súa app, enviándolla a outro usuario (e.g., nun bar, hotel ou transfirella a un amigo). Por último, (4) o paciente deixará consultar a súa información médica, recibindo tamén o seu incentivo correspondente e deixando acceder aos seus datos COVID-19 á app que lle leu o seu pasaporte, por exemplo, no control de acceso a un evento.

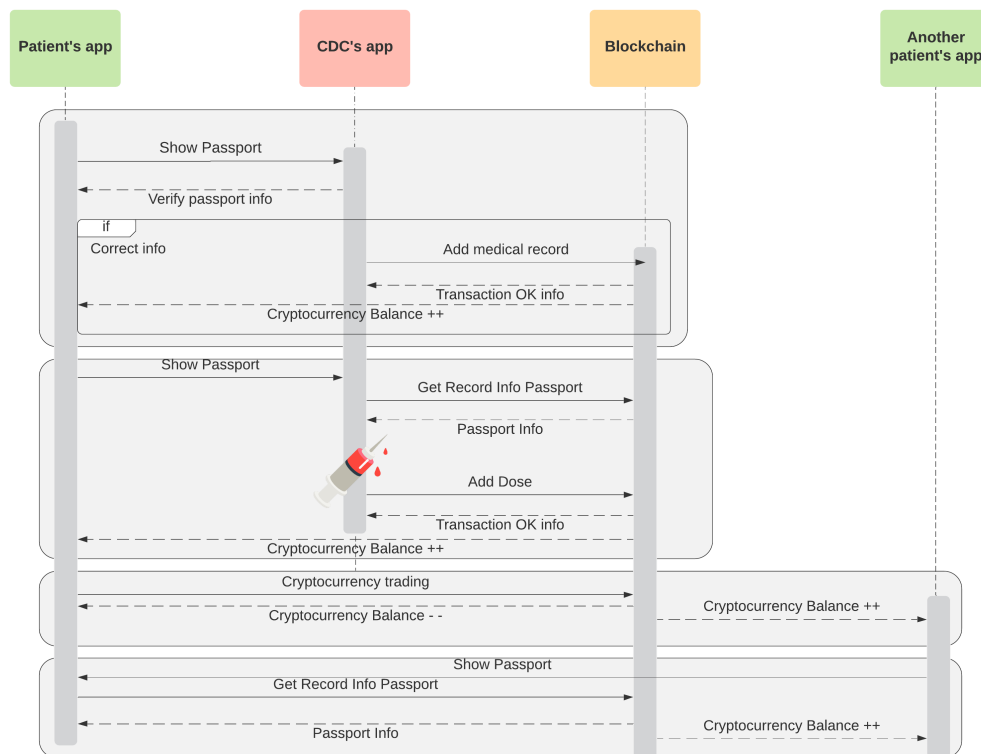


Figura 1.2: Diagrama de fluxo de diversos casos de uso.

### 1.3 Xustificación do uso de software Libre no PFC

Que o proxecto sexa integramente *Open Source* será chave, primeiro de todo pola difusión que isto conleva. Como ben se recalca durante toda a memoria, a finalidade ca que nace é a de

axudar á sociedade, aliviar e mellorar situacións actuais e en definitiva, contribuír a recuperar a maior normalidade posible ao redor de todo o mundo. Para conseguir isto, é fundamental que dito traballo sexa aberto, para chegar así a máis lugares e poder ser compartido, editado, e para como ben dixemos antes, que haxa unha comunidade traballando por melloralo e poñelo en marcha. Deberá tamén ser libre e gratuíto, para non poñer barreiras de ningún tipo na súa evolución. Dende un primeiro momento, como ben se especifican nos obxectivos principais, é fundamental dito carácter, xa non só por ética, se non porque todo o mundo se veu afectado pola pandemia, e toda mellora respecto a ela é unha boa noticia para todos. A maiores, facer público o código supón dotar ao proxecto dunha gran transparencia e serve para evitar posibles suspicacias do uso dos datos, polo que en conclusión, fomentar unha solución libre, pública e accesible por calquera, a cal poda ser mellorada e implantada sen requisitos, será chave.

## 1.4 Software Libre utilizado no proxecto

Na totalidade do proxecto foron empregadas ferramentas, librerías e linguaxes *Open Source* para seguir a tendencia comentada. Temos a continuación unha táboa co software utilizado, xunto cas súas licenzas e as posibles dependencias ou incompatibilidades acompañadas de posibles solucións.

Software	Licenza
Ethereum	GNU GPLv3
Solidity	GNU GPLv3
KMM	Apache 2.0
GEth	LGPL-3.0
Remix	MIT
Android Studio	Apache 2.0
Web3j	Apache 2.0
Metamask Mobile	Licenza Open Source asimilable a CC BY-NC-SA
Firebase	Copyright

Para o caso de *Firebase*, dicir que foi incorporado ao proxecto polo feito de que é ensinado nunha das mencións da carreira á que pertence o TFG, e aportaba polo tanto valor ao traballo ao facer uso das competencias específicas obtidas de cursar dita mención, pero para unha solución real poderíamos usar calquera outro tipo de base de datos, sexa tradicional, como *PostgreSQL* ou *MariaDB*, ambas *Open Source*, ou unha alternativa online como é ***Supabase*** (Apache 2.0), opción a cal está a ser sopesada para realizar a portación dende *Firebase*. Vemos por tanto, como a única peza non *Open Source* do proxecto, é totalmente prescindible e foi empregada por razóns externas ao traballo, ademais de que existen solucións libres para

sustituíla sen ningunha consecuencia e xa se está a contemplar a migración a unha delas.

En canto ás linguaxes utilizadas, recalcar tamén que todas elas son abertas e de licenza libre. Cada una foi empregada para implementar cada un dos módulos do traballo, polo que era fundamental que foran *Open Source* para acadar ese grao de software libre na totalidade do proxecto. Maioritariamente utilizamos:

- **Kotlin**, no novidoso proxecto de *Kotlin Mobile Multiplatform* para a implementación de todo o código das *Dapps* móbiles híbridas en *Android* e *iOS*.
- **Solidity**, para a implementación de todos os *Smart Contracts* (creación e xestión da criptomoeda propia, entre outras cousas) e o código referente a Blockchain.

Podemos destacar que, aínda que pequeno, o proxecto aporta valor ás comunidades destas linguaxes, as cales son relativamente recentes e pequenas, como a de *Solidity*, debido á novidade das tecnoloxías Blockchain e máis aínda da implementación propia de *Smart Contracts*, e sobretodo a de *KMM*, en *alfa* dende finais de 2020 e do cal apenas se podían atopar exemplos de código, e moito menos proxectos de mediana ou gran envergadura e que por riba, foran totalmente libres. Polo que utilizar estas linguaxes libres e recentes axudou ao crecemento e mellora de ambas, e en consecuencia, da comunidade de software libre en xeral.

### 1.5 Licenza Open Source utilizada no PFC

A licenza escollida para todo o proxecto, baixo a cal está todo o repositorio contedor do mesmo, foi a **GNU General Public License version 3 (GNU GPLv3)** por varios motivos:

- É una das licenzas de código aberto por excelencia, a cal garante a todos os usuarios a liberdade de poder usar, compartir e modificar o software, e polo tanto, melloralo, satisfacendo así todos os requisitos e obxectivos nomeados anteriormente.
- Protexe o proxecto co *copyleft*: como ben dixemos, a pandemia non fixo restricións de ningún tipo, polo que dito proxecto, despois de ser mellorado ou depurado de calquera maneira por calquera persoa, non deberá tampouco ser restrinxido a ninguén que queira ou necesite usalo, polo que necesitamos que a nosa licenza asegure que calquera proxecto derivado del sexa tamén libre, aspecto chave e que a *GNU GPLv3* cumpre.
- Compatibilidade: esta licenza permite combinar código baixo outras licenzas co código publicado baixo a *GNU GPLv3*, para así crear un proxecto máis amplo e totalmente libre, obxectivo que identificamos dende un primeiro momento e que necesitabamos que a nosa licenza satisfixera pola selección tecnolóxica comentada anteriormente.



## 1.6 Actividade Pública

### 1.6.1 Distribución do código

Como mencionamos antes, todo o contido do Traballo de Final de Grao, tanto a memoria completa entregada na facultade, como o artigo científico redactado en inglés a modo de resumo, como as presentacións de ambos documentos, xunto con todo o código fonte de todos os módulos do proxecto (incluíndo as diferentes linguaxes mencionadas) e todos os elementos necesarios para o despregue e posta en marcha de forma autónoma e independente da infraestrutura creada (*scripts*, ficheiros de configuración, etcétera), pódense atopar no repositorio público de **GitLab** (*Open Source*), baixo a licenza *Open Source GNU GPLv3* no seguinte link: <https://gitlab.com/maurodelossantos/coronapassport.git>.

Cabe destacar tamén que a partires da entrega de dito traballo, todo mantemento e actualización do proxecto estase a facer a través de ditos repositorios cas súas ferramentas, aínda que a partires desta publicación usarase tamén a *Forxa* de *mancomungal* para crear comunidade arredor do proxecto e aportar calquera mellora posible.

### 1.6.2 Publicidade, difusión e contactos

Dito proxecto, pode atoparse tamén dispoñible na páxina web persoal do autor do mesmo: <https://mauopi.ddns.net>, e segue a ser perfeccionado e mellorado de forma continua xa que unha vez finalizada a súa entrega e presentación, a difusión e mellora do mesmo converteuse nunha prioridade. Para isto, leváronse a cabo varias iniciativas:

1. Dito proxecto foi aceptado e presentado no congreso científico XoveTIC este mesmo mes de outubro.
2. Publicouse un artigo *Open-Access* a modo de resumo do mesmo na revista *MDPI Engineering Proceedings* baixo a licenza *Creative Commons Attribution License (CC BY)*.
3. Como plans académicos de futuro, contéplase facer unha publicación máis extensa nunha revista de maior impacto científico, complementando o proxecto realizado cun apartado de métricas de rendemento.
4. Participación na *Cátedra R en Ciberseguridade* como potencial mellor TFG aplicado dentro da temática de ciberseguridade.
5. Participará tamén, por levar a calificación de Matrícula de Honra, no premio a mellor proxecto aplicado da Facultade de Informática de A Coruña.
6. E obviamente, a parte da súa participación no concurso a mellor PFC de SW Libre, estase á espera de confirmación de diferentes eventos para o software libre que ocorreron

en anos anteriores (como podería ser a *OSHWDem* ou a *Coruña Hacks*, ou calquera outro novo evento que xurda nun futuro, para participar neles e darlle difusión e crear comunidade arredor do mesmo).

## 1.7 Conclusións e traballo futuro

Vemos entón como se describiu un sistema de pasaporte dixital para a COVID-19 que consta de dous módulos: un referente á Blockchain e outro relacionado co desenvolvemento de *Dapps* móbiles multiplataforma. Tras combinalos, conséguese crear un potente sistema que mellora e soluciona certas situacións actuais ca pandemia COVID-19, tanto dende unha perspectiva tecnolóxica (cun novo sistema de almacenamento da información COVID-19), como médica (favorecendo a comprobación e creación de situacións de baixo risco sanitario) e social (eliminando ou aliviando restricións así como beneficiando economicamente tanto a clientes como a empresas). Todo isto, cunha elevada complexidade técnica, ao utilizar novidosas e disruptivas tecnoloxías baixo o carácter *Open Source* que caracteriza ao proxecto. Ademais, o sistema proposto ten unha utilidade maiúscula, ao dar unha solución a un dos problemas actuais máis investigados e nacer cando apenas había un estado da arte. Por último, respecto ás liñas futuras a seguir, será chave o desenvolvemento para sistemas *iOS* en *KMM* para obter así ese carácter multiplataforma. Igualmente, deberase afondar na mellora da xestión das conexións ca cadea e ter un maior control de ambas apps en diferentes aspectos, como no outorgamento das contas CDC, ou nas restricións de obtención de incentivos.

Para finalizar, e no tocante ao carácter libre do mesmo, deberemos destacar que a difusión, o crecemento e a mellora do proxecto, motivados polo seu carácter *Open Source*, serán claves para un hipotético futuro uso real e a gran escala. E é que conseguimos crear un proxecto usando múltiples e novas tecnoloxías, todas elas libres, creando finalmente unha solución que tamén o é. Contribuímos por tanto á sociedade, á comunidade do software libre, pero sobretudo, puxemos o primeiro gran de area con este proxecto, o cal realmente comeza a partir de agora, abríndoo de forma íntegra para todo o público, para que comece ser accedido, depurado e mellorado e así crear unha extensa comunidade arredor del que se beneficie e beneficie ao resto de persoas co uso.