Identity Management with Blockchain

Memoria del proyecto

Facultat d'informàtica de Barcelona
Universitat Politècnica de Catalunya

Trabajo realizado por:
Mario Salirrosas Aguirre

Dirigido por:
Manel Medina

Grado en Enginyeria Informàtica
Especialización en Tecnologías de la información

Barcelona, Junio 2018

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

Resumen

Este proyecto consiste en elaborar un prototipo como Proof of Concept para demostrar los beneficios que aporta una tecnología como la del blockchain al manejo de identidades.El prototipo desarrollado estará enfocado en el mundo de la búsqueda de empleo y en el que podremos ver como crear una identidad digital y asociar información propia de la identidad a una dirección ethereum, el poder de ser capaces de tener control sobre nuestra información en internet y de quién puede acceder como quien intenta acceder a ella, y finalmente ver el concepto de círculo de confianza en el manejo de identidades.

Resum

Aquest projecte consisteix en elaborar un prototip com Proof of Concept per a demostrar els beneficis que aporta una tecnologia com la del blockchain al maneig d'identitats. El prototip desenvolupat està enfocat al món de la recerca de feina i en el qual podrem veure com crear una identitat digital i associar informació pròpia de la identitat a una adreça ethereum, el poder de ser capaç de tenir control sobre la nostra informació a internet i qui pot accedir-hi a ella, i finalment veure el concepte de cercle de confiança en el maneig d'identitats.

Abstract

This project is based on elaborate a prototype as a Proof of Concept to prove the benefits that blockchain technology bring into identity management. The prototype implemented is focus in the world of recruitment in which we can see how to create an digital identity and associate information related to this identity to an ethereum address, the power to control our information in the internet and who is be able to see it as who want to access to it, y finally to see the concept of circle of trust applied into identity management.

Agradecimientos

Este trabajo de fin de grado representa la tarea realizada durante este último cuatrimestre de carrera, y la satisfacción de haber concluido el grado de informática después de tantos años en la universidad. Agradezco profundamente a mi tutor Manel Medina por haberme dado la oportunidad de realizar este trabajo enfocado en el mundo blockchain como también toda la ayuda proporcionada sin importar el momento.

Principalmente agradezco a mi mujer y a mi madre por haberme apoyado durante los momentos más críticos ya que sin ellas no lo habría finalizado. Además a amigos mejores como Benjamin, David, Alexander, Oscar y Jona por haberme ayudado y leído este trabajo.

No puedo dejar de mencionar a todas las personas que me han ayudado durante mis casi 8 años en la universidad y han hecho posible que escriba este proyecto, muchos de ellos no se acordaran de mi, pero yo si: Julita Corbalan, Fermin Sánchez, Josep Maria Barcelo, René Serral, Alex Pajuelo, Joan Carles Gil, Rene Alquezar, Jordi Martí, Gemma Sese y Rosendo Rey.

Para acabar, me gustaría dedicar una pequeña nota a mi madre: Mama, si, he logrado finalmente escribir el proyecto final de grado y por fin, tu hijo acaba la carrera. Te agradezco de todo corazón y eres una persona a la que admiro.

Índice

1. Contexto

1.1. Introducción

Existe una necesidad en el gobierno, servicios financieros y otras industrias de desarrollar un sistema para identificación seguro, escalable y moderno como también independiente del control por parte de gobierno. Este sistema debe mantener los derechos y proteger a los ciudadanos de cualquier tipo de e-crime que se pudiera producir. El fácil manejo y la seguridad que otorga la identidad digital es esencial para permitir el intercambio de documentos fiables, mensajes y transacciones entre las entidades de los sectores públicos y privados, teniendo siempre en cuenta a los ciudadanos. En el mercado actual existen muchas iniciativas que proveen identidades digitales y permiten identificación de usuarios o documento firmados, pero aún es difícil que exista una confianza entre los distintos proveedores y como también dar fiabilidad de las identidades de los distintos orígenes.

Muchas compañías sin saberlo mantienen información duplicada en los distintos servidores y no sincronizada o actualizada con los datos actuales. Este tipo de modelos centralizados son propensas a recibir ciberataques cosa que conlleva a una fuga de información. Pero a este problema le hemos de añadir que se puede producir corrupción de la información y que el mantenimiento de estos sistemas heredados es bastante alto.

Por lo tanto, una de las soluciones que surge de estos problemas, sería la creación de una herramienta capaz de crear identidades digitales seguras y la compartición de información de esta identidad sobre la red entre las distintas entidades o personas. Esto se logra gracias a la tecnología blockchain, que promueve la distribución de datos en la red de manera fiable, segura y immutable. Logrando así que no se produzcan fugas de información personal porque no tendría un punto central de almacenaje.

1.2. Objetivos

El principal objetivo de este proyecto sería construir un prototipo que demuestre la aplicación de manejo de identidades con blockchain. Para llevar acabo esto, se tendrán en cuenta los siguientes puntos para la construcción del prototipo.

1.1.1. Creación de identidad digital

1.1.2. Control de acceso a tus datos personales a otros usuarios.

1.1.3. Crear una red de círculos de confianza que aumenta tu fiabilidad.

1.3. Actores implicados

Las personas implicadas por este proyecto es muy diversa y amplia ,ya que el manejo de identidades utilizando la tecnología blockchain resulta bastante interesante como una apuesta hacia el futuro. A continuación, se detallaran esas personas o organizaciones en una mayor escala.

- Beneficiarios

Las personas que forman parte de una pequeña comunidad como hasta de las que conforman una gran ciudad o un país serán los que se beneficiaran del producto desarrollado porque les permitirá digitalizar, asegurar y manejar su identidad online para interactuar con el gobierno, administraciones públicas y otros sectores como compañías, comunidades o ciudadanos mismos.

- Audiencia

El Gobierno, comunidades o empresas es a quién va dirigido el sistema de manejo de identidades digitales de sus ciudadanos porque tener un sistema global y común de identificación, seguro y fiable resulta interesante porque otorga el control de la información expuesta en internet al ciudadano. Este sistema permitirá tener identificado a cada uno de los ciudadanos y impedir la suplantación de identidad.

- Usuarios

La **industria y los servicios** serán los que utilicen este producto ya que les permitirá crear soluciones para acelerar procesos que eran largos. Por ejemplo, una plataforma que permita arrendatario y arrendador firmar los documentos de alquiler, acelerando la contratación o una aplicación que sirve para certificar la identidad para realizar un examen.

2. Estado de arte

Es necesario integrar los mecanismos de identidad con las instituciones públicas y privadas para desarrollar sistemas de identificación de usuarios modernos, escalables y seguros a la vez que preservan los derechos de privacidad de los ciudadanos y facilitando la entrada a estos sistemas digitales de identificació. Los sistemas tradicionales de identificación digital han tenido muchas desafíos, principalmente para proporcionar responsabilidad, privacidad y seguridad.

Mientras se intenta solventar problemas asociados con el manejo de información, otros problemas han provocado que los métodos tradicionales sean problemáticos. El mantenimiento de las bases de datos que están centralizadas y puede provocar una fuga de información, la dificultad de usar los medios de identificación actual integrandolos con sistemas heterogéneos o la inseguridad cuando se han transacciones online. Se han intentando buscar soluciones basadas

en nuevas tecnologías como es el caso del blockchain. Han habidos algunas iniciativas como *bitnation*[1] que es una plataforma de gobernanza que permite el establecimiento de una nación descentralizada, voluntaria y sin fronteras (Decentralized Borderless Voluntary Nation o DBVN) utilizando la tecnología blockchain. Esta plataforma la intención que tiene es competir con las instituciones gubernamentales tradicionales, ofreciendo una alternativa de gobierno libre y equitativo. En Estonia[2] por ejemplo se ha creado un identidad virtual digital que se llama e-residency que permite a personas de otros países convertirse en residentes digitales pero no en su definición más tradicional, sino que permite realizar actividades comerciales a eses e-residentes. Además, existen otras plataformas interesante basadas en blockchain como *Shodcard*[3] que ofrece un aplicación móvil de autenticación y validación de identidad digital preservando siempre la privacidad y el control de tu identidad digital. *Shodcard* permite autenticarse en identidades sin necesidad de introducir tus credenciales,autenticar tu identidad mediante proceso en el que una autoridad fiable comprueba quién eres realmente y permite una entidad confíe en que dice que eres por que ya has sido identificado y validado por una tercera entidad fiable.

Otras aplicaciones están centradas en el derecho de propiedad como *binded*[4] que permite subir imagen en la red desde tu móvil, ordenador o tablet. Esta aplicación lo que hace crea una huella digital que lo sube al blockchain utilizando la tecnología del bitcoin, lo que te otorga a ti los derechos de autor. Como también otras app que permiten la economía compartida gracias a la utilización de smart contracts como es el caso de *Slock*[5] y que a su vez intenta conectar todas las cosas gracias a la integración de IoT. *Slock* automatizar que después de un pago y una cierta condiciones, se desbloquee la puerta o la electricidad se funcione en un departamento que alquilas similar a la plataforma Airbnb. Finalmente, esta *blockstack*[6] un tipo de enfoque distinto que fue la invención de una aplicación descentralizada con identidad, autenticación y un sistema de nombres de dominio.

[1] https://tse.bitnation.co/
[2] https://e-resident.gov.ee/become-an-e-resident/
[3] https://shocard.com/
[4] https://binded.com
[5] https://slock.it/
[6] https://blockstack.org/intro

Teniendo en cuenta los usos y aplicaciones de la tecnología Blockchain en el área de manejo de identidades y en el de otras aplicaciones. El objetivo principal de este proyecto será el de adaptar una solución existente y darle un nuevo enfoque para un tipo de sector más específico añadiendoles unas features específicas.

Partiendo de una aplicación como ShodCard para el manejo de identidades más el uso de los contratos inteligentes, se tratara de plantear un aplicación que sea utilizada en el mundo laboral, específicamente en el área de recursos humanos de una empresa en el cual se tratará de ayudar al proceso de recruitment y recompensas para los trabajadores de una empresa. Aparte de esto, nuestro prototipo será una dApp que es una aplicación descentralizada y solucionará un problema como es la recuperación de la identidad digital en caso de que se pierda el dispositivo donde se guarda la clave privada.

3. Alcance del proyecto

3.1. Alcance

En este proyecto se pretenden identificar las ventajas del uso de esta nueva tecnología llamada blockchain, así como también el uso de ethereum utilizando smart contracts para definir unas reglas dentro de este proyecto.
Para el desarrollo de esta propuesta de proyecto, se desarrollará un prototipo de un sistema de manejo de identidades que refleje las ventajas y principales características de integrar esta nueva tecnología.
En este desarrollo se pretende implementar una aplicación web que permita el manejo de usuario, permita obtener información de una persona como también autorizar quien la ve. Aparte como también desarrollar una sistema recuperación de la clave privada en caso de que se pierda el portatil, o sea sustraído y no se pierda toda tu información con el. La aplicación web consistirá de un sistema de autenticación y en el que cada usuario posea información útil como email, direccion, cumpleaños, nacionalidad, estudios universitarios,cuentas bancarias,usuario,estado

laboral actual, número de seguridad social y contraseña almacenados en el ordenador. Además este proyecto se focalizará en el mundo de la empresa, centrándose en la parte de procesos de selección y recompensas a sus trabajadores.

Por una parte en el proceso de selección, intentaremos utilizar realizar la verificación de los estudios realizados, la experiencia laboral pasada, motivos de baja de la empresa anterior, y valoración de la empresa anterior. Estos dos últimos puntos son opcionales ya que se dependerá de la empresa anterior pero la verificación de los estudios y la experiencia laboral se puede acreditar de manera tradicional, solo que en en nuestro usuario(empresarial) las empresas siguientes no tendrán que realizar estas comprobaciones ya que nosotros habremos comprobado. Por otra parte, las recompensas a sus trabajadores se podrá realizar mediante un contrato predefinido que a partir de unos X meses, si el Proyect manager valora con unos cierta puntuación, se le podrá aumentar el sueldo de manera automática como que estás valoración serán almacenadas en el usuario(empresa) para la consulta de las siguientes empresas. Esta aplicación también poseerá petición de información o de entrevista por parte de las recruiters al candidato, así el podrá rechazar o no con quien realizar una entrevista como la otorgación de información privada como email o numero de telefono.

3.2. Metodología y rigor

Como el proyecto se debe realizar dentro un marco de tiempo de 3-4 meses aproximadamente, el tiempo disponible es muy poco, se requiere una metodología que de desarrollo ágil. Además es una tecnología emergente por lo que aún no existe mucha información de como tratar la tecnologia a mi solución y con muchos problemas en el desarrollo, se ha de elegir una metodología que permita la constante modificación de requisitos. Para un buen desarrollo de nuestro sistema proof of concept para mas conveniente una metodología ágil. Existen diversas metodologías de este estilo, como Scrum, Extreme programming o Scrum XP, aunque son metodologías que requieren un mínimo de personas y unos hitos de 1-3 semanas. A pesar de todo esto, alguna de estas técnicas de desarrollo no son totalmente compatibles a un solo

desarrollador, se puede adaptar una metodología como la de scrum. En mi tiempo de vida laboral, no he visto muchas personas que se rijan al manual de scrum de manera religiosa, ya que es una metodología bastante flexible y parece la mejor candidata para el desarrollo de este proyecto.

Debido al tiempo poco tiempo que tenemos para desarrollar, se ha decidido por realizar hitos cortos de una semana para poder así adaptarse y hacer frente a los obstáculos que se puedan encontrar en el desarrollo. De esta manera, se podrá tener una mejor visión del estado del proyecto por parte del director. Se explicará de forma más detallada toda la planificación en el siguiente aparte.

Ahora definiremos las herramientas utilizadas en el desarrollo , los métodos de monitorización , las validaciones de resultados y los posibles obstáculos dentro de este proyecto.

3.2.1. Herramientas de desarrollo

Para el desarrollo del prototipo de manejo de identidades, se utilizaran para la capa de presentación, la interfaz, html, javascript, jquery y bootstrap. Para conectar nuestros datos con el backend desplegado en nuestra blockchain de pruebas, utilizaremos web3, javascript particularmente funciones promises y trufflejs. Y para el backend, se utilizara solidity de ethereum para escribir los contratos inteligentes. Además se utiliza metamask para el manejo de firma de transacciones de las cuentas ethereum.

Utilizaremos blockchain privadas, y cuando el sistema esté más estable subiremos el código de la interfaz como el controlador a un sistema distribuido de almacenaje de archivos llamado IPFS, y una blockchain de pruebas ropsten. Nunca subiremos nuestro sistema al una blockchain pública por temas de seguridad y gastos por el gas, es los gastos que cobra el sistema para desplegar algo en el blockchain.

Por último, utilizaremos como editores y corrector de errores, atom y remix.org. Atom utilizaremos para el desarrollo de todo el proyecto pero descubrir cualquier tipo de error de sintaxis escritos en los contratos inteligentes, remix es una herramienta bastante útil.

3.2.2. Herramientas para la monitorización y validaciones

Para la monitorización de nuestro proyecto, se hará mediante reuniones periódicas con nuestro director de proyecto definidas en el spring planning, llamadas tambien sprint review. Este tipo de reuniones con nuestro director nos ayudaran para detectar posibles desviaciones de nuestro proyecto. Las reuniones se harán ,teniendo en cuenta la disponibilidad de ambos, cada semana mediante la utilización de gmail, skype, hangouts o reuniones presenciales sin aplazarlos más de un o dos días del día definido del sprint review en nuestro spring planning.

Para un mayor visión del estado de nuestro proyecto a nivel digital, se utilizará una herramienta llamada icescrum ideal para la creación de historias, progresión y bloqueos durante el desarrollo. Y a nivel personal,se contará una pizarra de cartón en el que anotará las tareas que voy realizando, es más visual y más cómodo en ciertos momentos.

También se utilizará la herramienta gantt para consultarla si hay desviaciones de la planificación inicial en el diagrama de gantt que se desarrolla en otro punto del documento. En caso de ser necesario se utilizara herramientas de compartición de documentos como google drive para monitorizar el estado o la opinión de la memoria antes de ser entregada.

3.2.3. Validación de tareas

Para la validación de nuestros hitos realizados, se probará de manera manual la aplicación si se comporta de la manera adecuada cada vez que se realiza una funcionalidad nueva, un cambio en la interfaz o un nueva conexión con los contratos inteligentes en el conector.

Además de los pruebas manuales, también se intentará realizar pruebas automáticas a todo el sistema para ver su funcionalidad sin tener que repetir todo el rato nuestro sistema.

3.2.4. Obstáculos y riesgos del proyecto

Los riesgos del proyecto pueden ser los siguientes durante el transcurso del desarrollo:

- Las tecnologías para el desarrollo de la dApp es tan poco estandarizadas sin ninguna documentación oficial algunas y con demasiados bugs ya que no están demasiado maduras y aún están bajo desarrollo.

- El problema de las features de la Dapp pueden ser un problema ya que mi desconocimiento de la tecnología, puede producir realizar un proyecto demasiado grande para un solo desarrollador.

- El desconocimiento de las tecnologías implicadas.

- El entorno de prueba es demasiado lento y no se puede utilizar un entorno real porque para desarrollar aplicaciones en una red ethereum se necesita pagar el gas por las computaciones. El gas es el coste del uso de los smart contracts ya que realizan un cálculo, por eso se utilizan una red libre de coste como ropsten o una red privada.

- El poco tiempo disponible debido a que este proyecto se ha de realizar de manera real en 2 meses , y como tener en cuenta, las dificultades propias del desarrollador como estudios o que trabaja durante 8 horas cada dia.

4. Planificación de un proyecto

A continuación definiremos la metodología a seguir, las tareas principales en las que se ha dividido el proyecto y se mostrará la dependencia entre los distintas tareas mediante un diagrama de gantt.

Definir el tipo de metodología empleada para el proyecto, ha sido uno de los primeros momentos más críticos del trabajo final de grado. El debate estaba entre usar una metodología más tradicional, que sería cascada, o una de las metodologías ágiles, muy usadas en el mundo del software actualmente, ya que definiría el fracaso o victoria del desarrollo de este trabajo.

Después de tener en cuenta las desventajas y ventajas de usar una u otra, se decidió utilizar metodología ágil, en este caso, scrum . Las razones ,que llevaron a tomar esta decisión, fueron el conocimiento de esta metodología, el saber cómo adaptarla al proyecto, la redefinición de requisitos, el poder dividir el proyecto en hitos, y los hechos, de utilizar scrum , ha demostrado que agiliza y se hace entrega del producto a tiempo.

En los siguientes secciones se definirá las etapas por las que pasaran y la adaptaciones de scrum para un solo desarrollador. Como también los objetivos que se intentarán marcan en cada una de las etapas como la descripción de estas tareas que se llevarán a cabo.

4.1. Ciclo de vida

El ciclo de vida del scrum se llevará a cabo de la siguiente manera:

- El primer paso para llevar a cabo esta metodología, es crear un documento llamado product backlog,un lista de historias , mediante la definición de requisitos desde la perspectiva del usuario final y que sean claras para que el equipo scrum y los actores implicados puedan entender.El product backlog es realizado por el product owner en conjunto con el cliente. En este caso, el desarrollador actuará como productor owner, que es la persona encargada de tomar los requisitos teniendo en cuenta las necesidades del cliente. Y el cliente será nuestro director de proyecto.

- El siguiente paso después de priorizar las historias ,las historias son tareas definidas de manera muy general que pueden ser divididas en tareas más específicas más pequeñas, es dividir las historias en tareas que se irán añadiendo en sprints. Cada uno de estos sprints, estarán formados por tareas, se definen en los sprint planning mediante un sprint backlog definido por el scrum team. El sprint backlog en la lista de tareas en cada sprint.

- Después del sprint planning, son las reuniones pre desarrollo que se realizan al principio, se llevará a cabo el proceso de desarrollo con las figuras de los developers y scrum master. Este desarrollo estará marcado por los dailys que se llevarán a cabo a diario con la duración de 15 min máximo. En estas reuniones el scrum master hará de jefe y los developers tendrán que responder a preguntas : Que hiciste ayer? Que haras hoy? Has tenido algún bloqueo?.

- Al finalizar el sprint se realizaran el sprint review y el sprint retrospective. El sprint review ayudará a repasar lo que se logró, en este caso lo que se entiende como acabado, y lo que no se puedo acabar para pasarlo al siguiente sprint.En el sprint retrospective ayuda a dar criticas constructivas a problemas surgidos que puedan mejorarse para el próximo sprint planning y así poder incrementar el desarrollo y el valor del sprint.

- Una vez el scrum master haya identificado las mejoras que se deben llevan a cabo, el proceso volverá al primer paso y así de manera continua.

Para este proyecto,se ha realizado una serie de modificaciones para adaptar esta metodología de manera sencilla.

- El product owner será el director del proyecto.
- El development team y scrum master sera el estudiante solo.
- Los sprint planning se serán de una semana.
- Los Sprint review y los sprint retrospective quedarán reducidos a realizarlos cada 3-4 semanas con el director del proyecto para evaluar el proyecto y así obtener consejos sobre el desarrollo o redefinir el backlog, por si no se llegan a los objetivos.

4.2. Tareas principales

Se ha dividido las tareas en 3 secciones: Trabajo inicial, Construcción del proof-of-concept y documentar.

4.2.1. Trabajo inicial

En la primera parte del proyecto, vamos a definir el alcance del proyecto , crear una planificación del proyecto, y elaborar un plan económico como también evaluar si cumplimos con las competencias transversales de nuestra especialidad.

Gracias a este trabajo inicial,podemos establecer la base del que se sostendrá nuestro proyecto como también trazar unos pautas y objetivos por secciones.

- Contexto y alcance de nuestro proyecto
- Trazar el plan del proyecto.
- Sostenibilidad y presupuesto
- Borrado de presentación oral.
- Evaluar las competencias
- Entrega final y presentación oral.

Debido a la importancia de estar alineado con las competencias del proyecto, el estudiante realizará un reunión entre la presentación preliminar y la entrega final para poder garantizar la coherencia de las idas y la buena cohesión del proyecto.

Para llevar a cabo el correcto desarrollo se ha planteado una serie de pasos que ayudarán al desarrollo y finalización del proyecto.

Al principio del desarrollo, se estudiarán las distintas aplicaciones existentes en el mercado utilizando blockchain relacionado con el manejo de identidades para poder así elaborar un prototipo de aplicación con un valor añadido al existentes en el mercado más el uso de otras tecnologías como IPFS(sistema de archivos basada en un modelo distribuido) o contratos inteligentes. Para la realización de este prototipo, se deben tener en cuenta los distintos factores que implican un tipo de desarrollo más complejo o más sencillo, ya que los problemas principales son el tiempo limitado y el uso de una tecnología que aún es muy nueva y las herramientas existentes no son tan maduras o muy estables. Esta primera parte de toma de contacto tendrá una duración de una aproximado de un mes.

Los recursos utilizados son los siguientes:

- Recursos humanos
  - Tutor : Responsable de la traza y estrategia a seguir para el proyecto.
- Recursos hardware:
  - Portatil personal(Dell Latitude 3480 14", Intel Core i5-6200U 2.30GHz, 4GB, 500GB SSD)
- Recursos software:
  - Ubuntu 16,04.
  - Google Docs
  - Gmail,Whatsapp, Skype
  - Extensión drive chrome : Gantter
  - Google drive
  - Youtube.

4.2.2. Construcción del proof-of-concept

Durante esta etapa aprenderemos los conceptos de blockchain, ethereum, solidity y cómo aplicarlos en la validación de identidad.

Al principio del desarrollo, se estudiarán las distintas aplicaciones existentes en el mercado utilizando blockchain relacionado con el manejo de identidades para poder así elaborar un prototipo de aplicación con un valor añadido al existentes en el mercado más el uso de otras tecnologías como IPFS(sistema de archivos basada en un modelo distribuido) o contratos inteligentes. Para la realización de este prototipo, se deben tener en cuenta los distintos factores que implican un tipo de desarrollo más complejo o más sencillo, ya que los problemas principales son el tiempo limitado y el uso de una tecnología que aún es muy nueva y las herramientas existentes no son tan maduras o muy estables. Esta primera parte de toma de contacto tendrá una duración de una aproximado de un mes.

Se comenzará con un desarrollo sencillo siguiendo unos tutoriales de manejo de identidades y el uso de los frameworks que ayudan para el desarrollo de smart contracts o la interacción de los nodos dentro de un red blockchain. Después se tratará de estudiar el lenguaje solidity para implementación de smart contracts en el manejo de identidades. Una vez familiarizado con el entorno, se estudiará soluciones para la área de recursos humanos y sus funcionalidades para poder empezar a desarrollar el prototipo que se centrara en esta área específica. Este desarrollo tendrá dos entregas una primera que es el primer prototipo y luego su versión mejorada. Este proyecto se llevará a cabo mediante la metodología de scrum para poder partir el desarrollo en sprints y así poder llevar a cabo el proyecto de manera más fluida con el continuo feedback del director del proyecto.Esta parte de implementación del prototipo tendrá una duración de una aproximado de un mes.

- Tarea 1,2,3,4 Consistirá en aprender cómo programar con solidity en combinación con ethereum. Instalación del entorno de trabajo y lo necesario para llevar a cabo la implementación de este producto.
- Tarea 5: Llevaremos a cabo la definición de requisitos como también las etapas de desarrollo del producto.
- Tarea 6,7,8: Trataremos de elaborar un primer prototipo con el realizaremos una serie de pruebas para comprobar su funcionamiento. Después de comprobar el buen funcionamiento, acabaremos el prototipo y comprobaremos su funcionamiento en un entorno real como también la elaboración de una demo del producto.

Los recursos utilizados son los siguientes:

- Recursos humanos
    - Tutor : Responsable de la traza y estrategia a seguir para el proyecto.
- Recursos hardware:

  - Portatil personal(Dell Latitude 3480 14", Intel Core i5-6200U 2.30GHz, 4GB, 500GB SSD)

- Recursos software:
  - Ubuntu 16,04.
  - Google Docs
  - Gmail,Whatsapp, Skype
  - Solidity
  - Ethereum
  - Testnet
  - Go(posible)
  - Python(posible)
  - IDE
  - truffle
  - webjs
  - html/css/js

4.2.3. Documentación TFG

En esta parte del proyecto, se escribirá como el proceso de desarrollo del prototipo como también la definición de arquitectura y relación entre la tecnología implicada. Se desarrollará esta fase en 15 días trabajando 5 - 6 horas diarias.

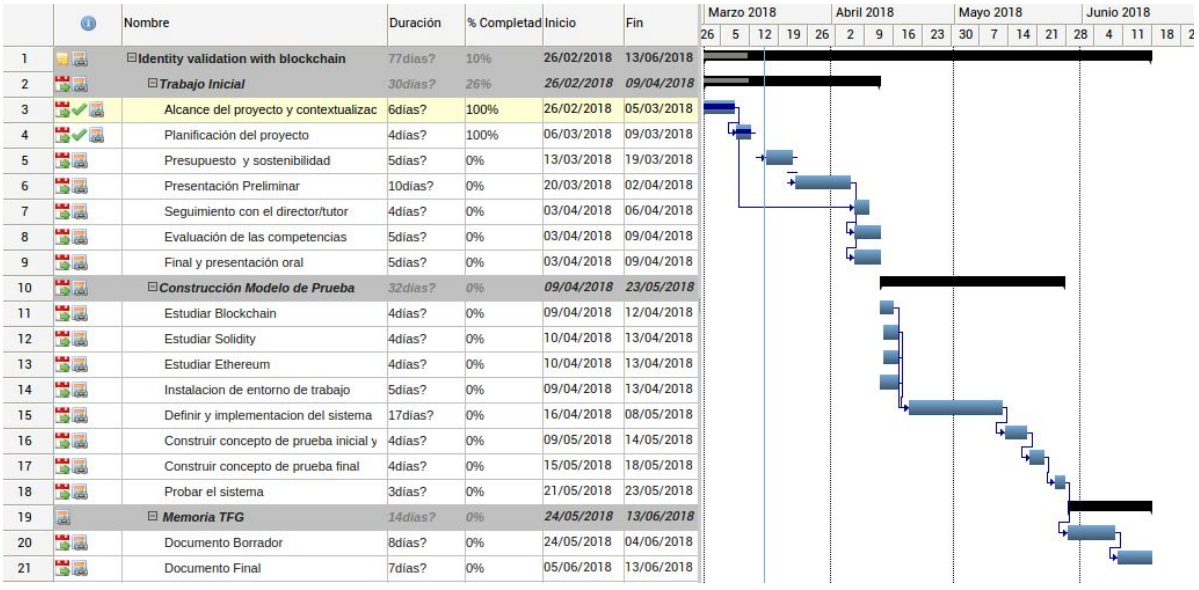
- Tarea 1: Consistirá en escribir el primer borrador del proyecto y unir la información del trabajo previo.
- Tarea 2: Consistirá en arreglar los fallos, finalizar las tareas de documentación pendientes y añadir detalles como : acknowledgements, abstracción y demás.

Los recursos utilizados son los siguientes:

- Recursos humanos
    - Tutor : Responsable de la traza y estrategia a seguir para el proyecto.
- Recursos hardware:
    - Portatil personal(Dell Latitude 3480 14", Intel Core i5-6200U 2.30GHz, 4GB, 500GB SSD)
- Recursos software:
    - Ubuntu 16,04.
    - Google Docs
    - Gmail,Whatsapp, Skype

4.3. Diagrama Gantt

En este diagrama de Gantt se puede apreciar las distintas tareas realizadas en cada una de las 3 fases explicadas previamente. A parte de esto, también se muestra el orden de precedencias asignado a cada una de las tareas.



	Nombre	Duración	% Completad	Inicio	Fin
1	Identity validation with blockchain	77días?	10%	26/02/2018	13/06/2018
2	*Trabajo Inicial*	*30días?*	*26%*	*26/02/2018*	*09/04/2018*
3	Alcance del proyecto y contextualizac	6días?	100%	26/02/2018	05/03/2018
4	Planificación del proyecto	4días?	100%	06/03/2018	09/03/2018
5	Presupuesto y sostenibilidad	5días?	0%	13/03/2018	19/03/2018
6	Presentación Preliminar	10días?	0%	20/03/2018	02/04/2018
7	Seguimiento con el director/tutor	4días?	0%	03/04/2018	06/04/2018
8	Evaluación de las competencias	5días?	0%	03/04/2018	09/04/2018
9	Final y presentación oral	5días?	0%	03/04/2018	09/04/2018
10	*Construcción Modelo de Prueba*	*32días?*	*0%*	*09/04/2018*	*23/05/2018*
11	Estudiar Blockchain	4días?	0%	09/04/2018	12/04/2018
12	Estudiar Solidity	4días?	0%	10/04/2018	13/04/2018
13	Estudiar Ethereum	4días?	0%	10/04/2018	13/04/2018
14	Instalacion de entorno de trabajo	5días?	0%	09/04/2018	13/04/2018
15	Definir y implementacion del sistema	17días?	0%	16/04/2018	08/05/2018
16	Construir concepto de prueba inicial y	4días?	0%	09/05/2018	14/05/2018
17	Construir concepto de prueba final	4días?	0%	15/05/2018	18/05/2018
18	Probar el sistema	3días?	0%	21/05/2018	23/05/2018
19	*Memoria TFG*	*14días?*	*0%*	*24/05/2018*	*13/06/2018*
20	Documento Borrador	8días?	0%	24/05/2018	04/06/2018
21	Documento Final	7días?	0%	05/06/2018	13/06/2018

Figura 1: Diagrama Gantt. Generado utilizando Gantter

Origen: Personal

5. Plan de acción y alternativas

El plan de acción que seguiremos esta definido en nuestro diagrama de gantt. Intentaremos seguir el plan trazado; pero esto dependerá de si el prototipo,es viable en el tiempo que nos hemos marcado.

La idea principal es utilizar elaborar un prototipo de validación de identidad con blockchain,utilizando ethereum,solidity desplegado en un red privada o red de pruebas como ropsten o rinkeby. Si vemos que ,por algún motivo, el proyecto se desvía debido al entorno de pruebas o por el desarrollo del prototipo con solidity. Entonces buscaremos alternativas en el despliegue del entorno de pruebas como crear nuestra propia red o cambiar de IDE de desarrollo como también el framework que nos permite conectar con el node en la red blockchain.. Por otro lado, si el problema es con el lenguaje, lo cambiariamos con otro también muy utilizado para el desarrollo de smart contracts como es serpent o python con algunas librerías. Gracias al tipo de metodología ágil que tenemos, podemos redefinir los requisitos y no desviarnos para así poder construir un prototipo.

Debido al corto tiempo de desarrollo se ha optado por utilizar metamask como manejo de firma de transacción en la red blockchain en vez de crear una propia.

Se intentará tener el prototipo como muy tarde el 15/05/18 , pero como hemos mencionado sino se llegase, se intentara buscar una alternativa o redefinir los objetivos para tener un prototipo más básico del planteado originalmente y así poder finalizar el proyecto en el tiempo justo.

6. Resumen sostenibilidad

La autoevaluación ha sido una forma de plantearse cómo se está enfocando el proyecto, si es sostenible o no, si tenemos en cuenta unos factores al desarrollar el proyecto y si conocemos o tenemos las herramientas suficientes para ver si nuestro proyecto es sostenible o no.

Las preguntas formuladas han sido de gran ayuda, ya que ha provocado plantearse qué puntos se han de tener en cuenta al momento de desarrollar el proyecto. A parte de esto, se ha descubierto que quizás no se tenía la capacidad de analizar bien el proyecto y cómo influirá al resto de la sociedad. El proyecto desarrollado tiene una gran impacto a nivel social, económico y medioambiental, ya que plantea una solución que beneficia de manera directa a los ciudadanos protegiendo sus derechos y privacidad, a nivel económico la reducción de costes y al nivel medioambiental la reducción de almacenamiento de información provocando de manera indirecta un gastos electrico menor.

En resumen, considerando la búsqueda hecha y toda la información obtenida de la tecnología que se utiliza para solventar un problema existente. Se llega a la conclusión ,de que aunque existen soluciones existentes, no se tienen en cuenta los factores que definen la sostenibilidad, sino que quizás solo el económico. Lo que se plantea ahora y se intentara conseguir es tener tener el máximo impacto positivo, teniendo en cuenta que hay tres pilares importantes en la sostenibilidad,y aunque en un principio no se tenía en cuenta la sostenibilidad para el proyecto, por el hecho de que no se valoraba y no se habían planteado estas preguntas.

7. Coste

7.1. Costes Directos

La sección se dividirá según las fases descritas en el entregables anteriores. Las personas implicadas en el proyecto son el tutor y el estudiante, que posteriormente definirán su rol dentro del proyecto.

En los recursos humanos teniendo en cuenta el metodología elegida,deberían existir los roles developer, product owner y scrum master. Pero como el proyecto es desarrollada por una sola persona, se harán las siguientes modificaciones.

- El desarrollador tendrá el rol suyo implícito y el de scrum master. Su sueldo se basará en el de un desarrollador junior que es 17.670 € brutos anuales.
- El tutor tendrá el rol de product owner, que será el que marque los requisitos del producto a desarrollar. Su sueldo no se tendrá en cuenta por el desconocimiento de este mismo.

Para calcular la amortización del ordenador personal, se ha usado la siguiente ecuación.

$$HTFG = \frac{CO}{HD * AU * 365}$$

HTFG = Horas utilizando el ordenador para el TFG.
CO = Coste ordenador.
HD = Horas utilizando el ordenador por dia.
AU = Años útiles portátil.

Suponiendo que se utiliza el ordenador una media de 8 horas diarias y los años útiles es de 5 - 6 años en los portátiles.

7.1.1. Trabajo Inicial

Recursos humanos

Para tener en cuenta el precio hora se tendrá en cuenta el sueldo neto mensual y dividirlo por una media de 160 horas mensuales.

Según la calculadora de sueldo neto se recibirá mensualmente 1.227,9€ por 12 pagas.

$$CH = \frac{SN}{160}$$

CH = Coste por hora

SN = Sueldo neto mensual.

	Rol	**Personas**	**Tiempo total**	**Coste(€/Horas)**	**Coste Total**
	Desarrollador	1	240 h	7,67(€)	1840.08(€)
	Product owner	1	-	-	-
Total					**1840.08(€)**

Recursos hardware

	Producto	**Unidades**	**Precio/Unidad(€)**	**Años útiles**	**Amortización**
	Ordenador	1	650	5	10.68(€)

	personal				
Total					**10.68(€)**

Recursos software

	Producto	**Unidades**	**Precio/Unidad(€)**	**Años útiles**	**Amortización**
	Google docs	1	-	-	-
	Skype	1	-	-	-
	Ubuntu 16.04	1	-	-	-
	Gmail	1	-	-	-
	Whatsapp	1	-	-	-
	Youtube	1	-	-	-
	Gantter	1	-	-	-
	Apogee	1	-	-	-
Total					0 (€)

TOTAL					**1850.76(€)**

7.1.2. Construcción de prototipo

Recursos humanos

	Rol	Personas	Tiempo	Coste	Coste Total
	Desarrollador	1	256 h	7,67(€)	1964.64(€)
	Product owner	1	-	-	-
Total					**1964.64(€)**

Recursos hardware

	Producto	**Unidades**	**Precio/Unidad(€)**	**Años útiles**	**Amortización**
	Ordenador personal	1	650	5	11.39(€)
Total					**11.39(€)**

Recursos software

	Producto	**Unidades**	**Precio/Unidad(€)**	**Años útiles**	**Amortización**

	Ubuntu 16.04	1	-	-	-
	Metamastk	1	-	-	-
	Google docs	1	-	-	-
	Solidity	1	-	-	-
	Testnet for Ethereum	1	-	-	-
	Web3	1	-	-	-
	JS/HTML/CSS	1	-	-	-
	Truffle Framework	1	-	-	-
	IDE - Atom	1	-	-	-
Total					0 (€)

TOTAL					**1976.03(€)**

7.1.3. Memoria

Recursos humanos

	Rol	Personas	Tiempo	Coste	Coste Total
	Desarrollador	1	112 h	7,67(€)	859.04(€)
	Product owner	1	-	-	-

Total					**859.04(€)**

Recursos hardware

	Producto	**Unidades**	**Precio/Unidad(€)**	**Años útiles**	**Amortización**
	Ordenador personal	1	650	5	4.98(€)
Total					**4,98(€)**

Recursos software

	Producto	**Unidades**	**Precio/Unidad(€)**	**Años útiles**	**Amortización**
	Google docs	1	-	-	-
	Skype	1	-	-	-
	Ubuntu 16.04	1	-	-	-
	Gmail	1	-	-	-
	Whatsapp	1	-	-	-
	Apogee	1	-	-	-
Total					0 (€)

TOTAL					**861.02(€)**

7.2. Costes Indirectos

Los costes indirectos, a tener en cuenta en este proyecto, son la electricidad y internet. No se considerará los desplazamientos como coste indirecto porque se realizan pocos desplazamientos al mes y es despreciable.

- Consumo eléctrico

El kWh según el gobierno de españa es de 0.12088 e/kWh, por lo tanto, para un proyecto de 608 horas el precio total es: 73,50 euros

- Acceso a internet.

El internet según la fuente consultada varía desde 36,89 hasta 57 euros, por lo que se ha elegido la media entre el máximo valor y el menor valor, que sería de 47 euros mensuales.
El coste de internet total durante todo el proyecto sera : (47*12*608)/365*8 = 117.43 euros

7.3. Total Costes indirectos y directos

	Recursos	**Coste Total**
	Recursos directos	4687.81
	Recursos indirectos	190.93
TOTAL		**4878.74(€)**

7.4. Costes Contingencia

Las contingencias de este proyecto se han calculado en base al presupuesto realizado anteriormente. En nuestro caso el porcentaje será bajo debido al nivel de detalle de dicho presupuesto. El porcentaje final calculado es del 11%. Lo que nos da un c**oste de contingencias** de 536,58€.

	Justificación	**Porcentaje Coste**	**Coste(€)**
	Proyecto bien detallado.	11%	536.58

7.5. Costes de incidencia

En esta sección de incidencias vemos possible 1 factor que podrían influir en el desarrollo del TFG. No se considera los fallos del sistema ni los de almacenaje de la documentación ya que cada dia se hacer subidas a github y la documentación se hace directamente en la nube.

- **Falta de tiempo en el desarrollo del prototipo**

Se añadirá más horas de desarrollo los fines de semana, en caso que, se estime que no se llegan a objetivos de cada sprint en la parte del desarrollo del prototipo.

Añadiremos 20 horas más por semana en un total de 6 semanas de la fase de desarrollo, del tal modo que, las horas totales de esta fase serían: 120 horas.

	Causa	**Solución**	**Duración**	**Coste(€)**
	Falta de tiempo en la fase desarrollo del prototipo	Trabajar los fines de semana 20 por semana durante 6 semanas.	120 h	920.4(€)

7.6. Total Costes

El objetivo de este proyecto es crear un prototipo usando tecnologías de código abierto. una de los problemas que podríamos enfrentarnos es que el entorno de pruebas sea poco estable para el desarrollo de la aplicación y que tengamos que ir al entorno real, pero no lo veo probable ya que nuestra dapp es bastante ligera. Si así fuera el caso, la otra alternativa sería colaborar con alastria que tiene un ecosistema blockchain para el desarrollo de aplicaciones pero deberíamos hacer algunos cambios en el proyecto y también tendría cero costo para nosotros. Otro de los problemas que podría ocurrir es que tuviéramos que añadir más horas en el desarrollo,si se

estima que no se llega a los objetivos pero teniendo en cuenta que ese coste ya se tiene en cuenta en el de posibles incidencias, no afectaría mucho. Aparte de eso, se tiene en consideración que solo ocurra estas horas extras en la fase de creación del prototipo ya que las otras fases habrá tiempo suficiente para la finalización sin problemas de los objetivos.

	Recursos	Coste Total
	Costes directos y indirectos	4687.81€
	Costes de contingencia	536.58€
	Costes de posibles incidencias	920.4 €
TOTAL		**6144.79(€)**

8. Sostenibilidad

Se describirán las reflexiones sobre los distintos aspectos que se tienen en cuenta en la sostenibilidad y como el proyecto los tiene en cuenta.

8.1. Ambiental

- **PPP**

El impacto medioambiental de la realización del proyecto es casi despreciable pero igualmente para la reducción máxima de gasto energético y usar los recursos de manera adecuada sin desperdiciar, hemos apagado usado el ordenador solamente para escribir el proyecto teniendo apago el resto de tiempo. Igualmente si volviésemos a plantearnos el proyecto de nuevo, no hay nada en el que pudiera escatimar ya que usamos los recursos necesarios y además solo es una persona dedicada al proyecto.

- **Vida Útil**

El proyecto intenta resolver un problema que tenemos centralizando la información y permitiendo una fuga de información.A parte de esto también reduce mejora mucho el modelo actual ya que reduce el número storage actual ya que la información está descentralizada en los diferentes nodos de la red.

Los recursos que se utilizaran durante la realización del proyecto son solamente el portátil personal y en algún momento el móvil para grabar el video de la presentación. Estos aparatos tiene un impacto despreciable.

Resumiendo, creo que mi solución daría una mejora sustancial si se implementara a nivel mundial ya que el almacenamiento de información seria en los mismos nodos repartidos, sin la necesidad de mantener a almacenamiento de información gigantescos.

8.2. Económico

- **PPP**

El coste del proyecto es relativamente pequeño teniendo en cuenta que solo lo realiza un programador. Los costes no se puede reducir más de lo que hemos descrito en los descrito previamente.

- **Vida útil**

El proyecto reduce considerablemente el gasto que conlleva mantener unos servidores en los que se almacena la información, como estos mismos productos como también la gente que lo mantiene.

8.3. Social

- **PPP**

El proyecto a nivel personal creo que el proyecto será un tema complicado de llevar pero que me aportará muchos conocimientos de una tecnología innovadora y que será muy utilizada en un futuro cercano.

- **Vida útil**

El proyecto resuelve un problema importante en la sociedad y creo que de los aspectos que se tiene en cuenta en la sostenibilidad, es el que más afecta. El proyecto protegerá a los ciudadanos el poder de controlar su información privada y de saber con quien compartirla como también de darles la privacidad que ellos necesitan.
En si, existe proyectos reales que intenta cubrir estas necesidades, pero que no funcionan ya que han habido fallos en el sistema o fallos humanos que provocaron el fallo.

8.4. Matriz de sostenibilidad

	PPP	**Vida útil**
Ambiental	Consumo diseño	Huella Ecológica

	8	18
Económico	Factura 7	Plan de viabilidad 17
Social	Impacto personal 10	Impacto social 19

Total	**79**

9. Diseño

Para comenzar con el diseño, se ha tenido que definir primero el sistema. El sistema se basa en una aplicación dapp(aplicación descentralizada) conectado a un node ethereum y a una red distribuida de archivos. Los usuarios son capaces de conectarse mediante un navegador para realizar todos las acciones descritas más abajo.

Se tomó la decisión de una aplicación dapp porque corren en redes de sistemas descentralizados y su código es abierto. Además gracias a que es una aplicación distribuida se beneficia del hecho de que la aplicación es escalable y tiene una alta disponibilidad de datos.

Las dapps necesitan de un usuario conectados en a la aplicación dapp que esta a su vez se conectara a una node de la red distribuida. La aplicación para hacerla puramente distribuida está conectada su interfaz está almacenada en el IPFS distributed file system y nuestro backend estará desplegado en la red blockchain, específicamente testnet ropsten, para que así se puedan comunicar cuando las dos estén subidas en la red.

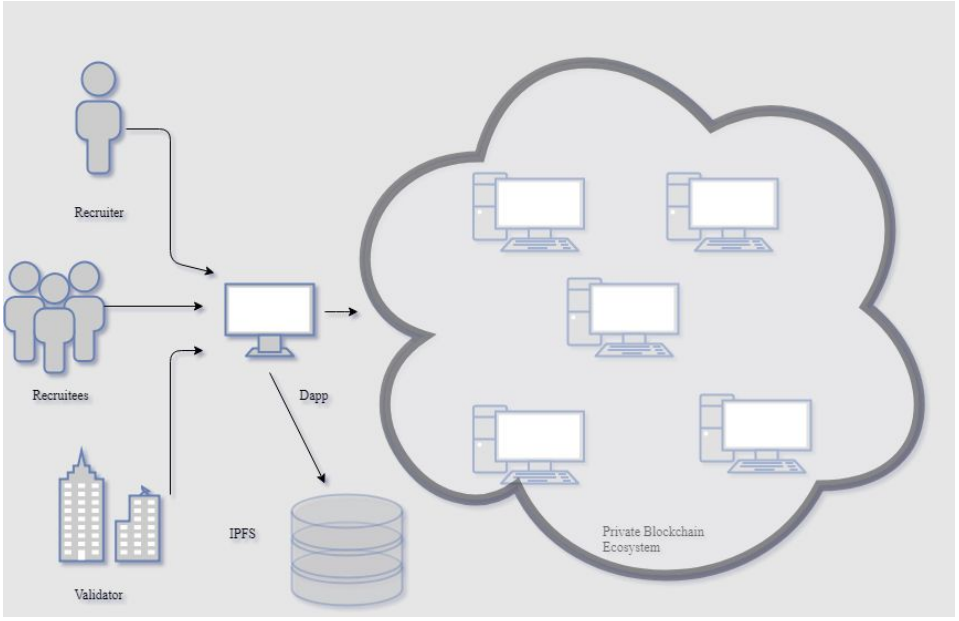


Figura 2: Vista del todo sistema elaborado por draw.io

Con el fin de cumplir con los requisitos de manera más eficiente y a la vez quedar dentro del marco de complicidad y relevancia esta es la arquitectura que es a la vez eficaz y estructuralmente semejante a las aplicaciones usadas en vida real.

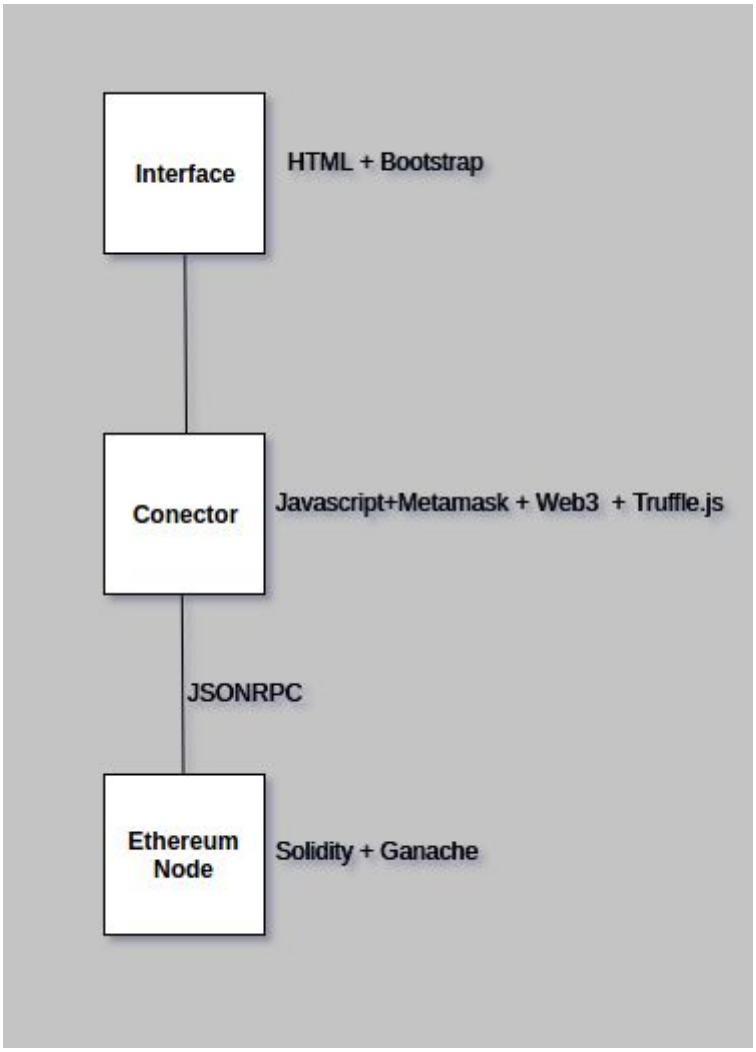


Figura 3: Arquitectura Generado utilizando draw.io

La aplicación está dividida en tres partes: interfaz de usuario - que está hecha de tal forma que no necesita servidor o hosting, solo el acceso a blockchain - , el conector implementado con extensión de navegador Metamask - que permite acceder a blockchain- y librería web3 - que traduce el API de blockchain in gRPC- , y en la parte de blockchain se usa el entorno de desarrollo Truffle - en particular el simulador de red de blockchain privada Ganache.

9.1. Interfaz

Las tecnologías web tienen el mérito de ser la tecnología más utilizadas y accesibles para los para el usuario final, teniendo en cuenta que casi cada ordenador tiene un navegador. Esta aplicación aprovecha de desarrolladas librerías de JavaScript que permiten modificar el estado de la página según el estado del blockchain. Debito que la página no carga ningunos otros ficheros no tiene tráfico adicional.

El HTML de la página contiene una carcasa de la interfaz que se estiliza con CSS de bootstrap.

JavaScript implementa todas las funcionalidades que no son necesarias para ejecutar en el blockchain como generación de los elementos HTML para facilitar las transacciones de usuario y representar los datos del contrato de manera adecuada. JavaScript toma el papel principal aquí ya que es gracias a él que no se requiere ningún servidor adicional para servir las páginas durante el uso de la web por el usuario.

En conclusión es una interficie autónoma que usa el Navegador Web como interpretador de los lenguajes y no tiene limitaciones en cuanto a distribución, es decir se pueden usar tanto servidores convencionales, servicios que ofrecen almacenamiento de datos gratuitos o las tecnologías distribuidas de P2P tales como IPFS y BitTorrent que además verifican los datos de la página automáticamente.

9.2. Conector

Metamask es un puente al blockchain que en nuestro caso nos permite usar los contratos de Ethereum a través del navegador sin que necesitemos de tener un Nodo de Ethereum entero. El hecho que baja la barrera de entrada para el usuario ya que instalación y mantenimiento de un nodo requiere conocimientos específicos y tiempo.

Por otro lado Metamask es un monedero de Ethereum ja que maneja las transacciones avisando al usuario tanto del hecho de que la transacción está a punto de transcurrir como de los gastos que lleva dejando que el usuario tome la decisión final. En ethereum cualquier transacción monetaria está iniciada por el dueño de monedero, mientras el que el receptor no tiene que iniciar ninguna acción - Metamask asocia las imágenes a los dos permitiendo al usuario distinguir las personas de forma gráfica para evitar estafas y confusiones.

web3.js es una librería que implementa el API de blockchain en JavaScript y permite implementar transacciones. Sigue siendo necesario tener un node entero si la librería se usa por sí misma. Todas las llamadas al blockchain reflejan la misma estructura y forma que tienen en solidity.

9.3. Ethereum node

La simulación de la red se hace mediante en entorno de desarrollo Ethereum Truffle, en particular con la utilidad llamada Ganache que permite simular el blockchain con las cuentas ya existentes. Este utilidad es necesario por la razón que una simple transacción cuesta dinero y un error en el contrato puede costar una importante cantidad de dinero. El segundo beneficio es que durante el desarrollo accelera las confirmación de los bloques lo que permite que las transacciones se confirman en menos de 3 segundos.

La fiabilidad del contrato se consigue a medidas de las tecnologías blockchain, en nuestro caso Ethereum, que van confirmar las transacciones descritas de tal manera que el coste de falsificación es superior al beneficio conseguido con la última, por un lado. Por otro lado carece de los costes adicionales, a diferencia de la escritura, permite un acceso inmediato e ilimitado al contrato elevandolo a la categoría de un documento público que es fácil de consultar, tener en cuenta y que es de fianza. Por otro lado es contraproducente guardar en la máquina distribuida de Ethereum datos adicionales que no requieren fiabilidad crítica ya que supone un coste elevado comparado con otras tecnologías más convencionales.

Tener una dirección de Ethereum es el requisito para poner en marcha la aplicación. Es la pieza que va une el resto de las datos alrededor de sí.

Para preservar la fiabilidad del sistema y prevenir el abuso del mismo se puede poner restricciones a las dirección o al conjunto de las direcciones que participan en una interacción, aprovechando que la lectura no tiene ningún coste adicional y se pueden hacer todas las confirmaciones necesarias. Por ejemplo, se puede requerir que las direcciones registradas tengan un mínimo arbitrario de Eth para ser mostrados e interactuar con otros usuarios o depositarán una suma que se les devolvería después de un tiempo o en caso de borrar su cuenta.

Para preservar la privacidad de los usuarios su dirección se va ocultar la dirección ya que compartirla significa compartir toda la historia financiera asociada la dirección. Esto se puede mejor creando una cuenta nueva en Ethereum ya que este proceso tendrá un coste adicional mínimo. En lugar de la dirección se usará un entero que también corresponderá al orden en que se han registrado los usuarios.

Tanto la dirección como el número de usuario pueden ser vinculados con los datos personales del usuario, más en adelante la identidad. La identidad no puede ser consultado a no ser que hay una solicitud explícita confirmada por el usuario que va revelar su identidad.

En este caso el usuario que envía la solicitud es el recruiter el usuario que la recibe será el recruitee. Por razones de convenio la solicitud no podrá ser borrada pero el recruitee siempre podrá rechazarla o aceptarla, incluso varias veces a la vez.

El acto de registrarse, enviar un solicitación y aceptar o rechazarla supone un coste adicional que será pagado en Ether. Este proceso de confirmación de la transacción está controlado por metamask de forma explícita y muestra el valor de la transacción.

Una vez el recruiter tiene acceso al perfil del recruitee podrá acceder a sus datos personales incluido la dirección.

No se le llevara ninguna operación computacional o lógica de importancia inferior a crítica o de alta demanda de recurso computacionales.

9.4. Diagrama

Podemos observar en este apartado como interactúan las diferentes "clases" en los smart contracts. Se ha definido una clase principal **identity** en el que se controla el manejo de la identidad.

A continuación definiremos las clases restantes, haciendo una pequeña descripción:

- Access

Es la clase que tienes la funciones para controlar las accesos que recibe un usuario y el manejo de la aceptación y la denegación de permisos para ver el perfil público.

- Validation

Es la clase encargada de controlar las validaciones que se otorga al usuario para poder así lograr, una identidad fiable y dar confianza a las personas que acceden.

- Experience y Education

Son las clases encargadas de controlar la información extra y ver quién ya ha validado o no estos campos en el usuario.

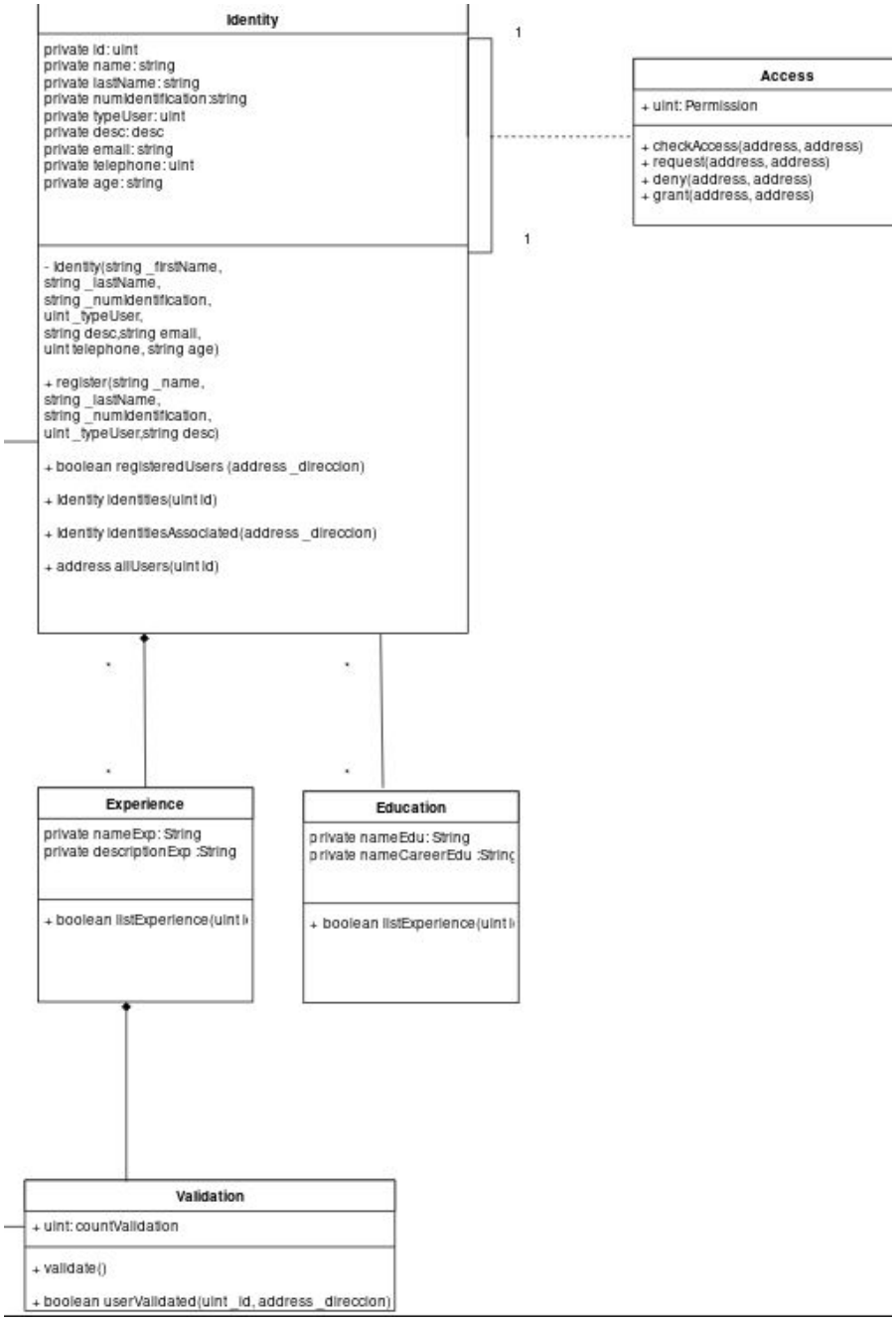


Figura 4: Diagrama de clases elaborado por draw.io

9.5. Casos de uso

Se ha definido los casos de uso de la aplicación porque es fundamental tener bien definidos los requerimientos del programa para su buen desarrollo. Se ha tenido en cuenta que en el desarrollo tres tipos de usuarios posibles en la aplicación: **Recruiter**, **Recruitee** y **Validator**. Los nombres significan Reclutador ,Solicitante y validador, este último es una entidad pública que validara datos asociados a el.

A continuación se ha mencionan de manera detallada los casos de uso que se ha tenido en cuenta para el concepto de prueba.

Caso	Register new user
Actor	Usuario no registrado
Flujo	Cuando se abra la página, se ve la **página para registrarse.** **Todos los usuarios deberán registrarse para utilizar la aplicación.** 1. El recruitee abre la aplicación.Debe crear una identidad para poder asociar una identidad a tu dirección ethereum. 1.1. El usuario debe de elegir que tipo de usuario es. 1.2. El usuario debe rellenar los datos necesarios en la páginas de creación de identidad. Los datos necesarios, es el nombre, apellidos, número de identificación . 1.3. El usuario debe apretar el botón de crear identidad. 1.4. La aplicación abra creado una identidad, y una vez vuelvas a entrar ya no hará falta que crees una identidad. 2. El recruiter abre la aplicación. Debe crear una identidad para poder asociar la información de la empresa a una dirección ethereum. Los pasos a seguir son los mismos que en crear identidad por el recruitee.

	3. El validador abre la aplicación. Debe crear una identidad para poder asociar la información de la entidad pública a una dirección ethereum. Los pasos a seguir son los mismos que en crear identidad por el recruitee.

Caso de uso	Create CV
Actor	Usuario registrado - Recruitee
Flujo	El usuario está en la página Profile **Un recruitee** puede crear un CV. 1. El usuario debe rellenar los datos necesarios del CV 2. La pagina mostrara 2 campos: a. El campo trabajo con dos campos a rellenar: nombre de la empresa y puesto de trabajo. b. El campo educación con dos campos a rellenar: Nombre de la universidad y carrera hecha. 3. El usuario debe rellenar información adicional para crear el CV como email, edad y teléfono. 4. El usuario debe apretar crear CV para crear el CV y así activar que está buscando trabajo.

Caso de uso	Validate education to a recruitee
Actor	Usuario registrado - Recruitee
Flujo	El usuario está en la página CV. Un recruitee en la página CV podrá solicitar a una entidad tercera, en

	este caso, la nuestra es una entidad pública para validar la información. 1. El usuario presiona sobre el botón validar información de la educación. 2. La entidad debe aceptar o denegar esta solicitud 3. Cuando la entidad haya aceptado o denegador: a. Si ha validado debe haber un visto verde esto se podrá visualizar en la página pública del usuario. b. Si no lo ha validado, no aparece nada.esto se podrá visualizar en la página pública del usuario.

Caso de uso	Validate work experience to a recruitee
Actor	Usuario registrado
Flujo	El usuario está en la página CV. Un usuario cualquiera, excepto el usuario dueño del perfil, podrá validar la información de la experiencia laboral. 1. El usuario debe hacer presionar el botón que se encuentra a lado de la experiencia laboral. 2. El usuario ve como el contador ha aumentado, ya que se van sumando las validaciones de todos los usuarios, esto se podrá visualizar en la página pública del usuario.

Caso de uso	Records of incomings requests - Accept
Actor	Usuario registrado
Flujo	El usuario está en la página notifications. Un usuario ve la lista de solicitudes que ha recibido para acceder a su perfil público. Cada fila de la lista se debe seleccionar aceptar o

	rechazar solicitud. 1. El usuario debe denegar la solicitud que viene del usuario que quiere acceder a su información. 2. Una vez se ha elegido, el usuario que solicita, podrá acceder a una perfil privado del usuario.

Caso de uso	Records of incomings requests - Deny
Actor	Usuario registrado
Flujo	El usuario está en la página notifications. Un usuario ve la lista de solicitudes que ha recibido para acceder a su perfil público. Cada fila de la lista se debe seleccionar aceptar o rechazar solicitud. 3. El usuario debe aceptar la solicitud que viene del usuario que quiere acceder a su información. 4. Una vez se ha elegido, el usuario que solicita, podrá acceder a una perfil privado del usuario.

Caso de uso	Request information

Actor	Usuario registrado - Recruiter - Recruitee
Flujo	El usuario está en la página de recruitees. Un usuario,excepto el validator, puede ver la lista de usuarios buscando trabajo.Estos usuarios previamente deben estar registrado y deben haber creado un CV. 1. El usuario ve un listado de usuarios buscando trabajos, presiona en el botón request de un usuario para solicitar ver su información privada. 2. Una vez se haya aceptado la solicitud, el usuario ve un botón view profile. 3. El usuario presiona sobre el botón y se abre una nueva página. 4. La nueva pagina tendra toda la información privada.

10. Desarrollo

El desarrollo se puede dividir en dos partes relacionadas: el desarrollo del interfaz y el del contrato. Ambos se distinguen tanto en las utilidades necesarias como editores y depuradores, como en el método de desarrollo: el Contrato es lo que se escribe primero y el interfaz es lo que se adapta a él.

10.1. Ganache

Es la primera herramienta que tiene que ser ejecutada ya que simula el blockchain y al minero que confirma las transacciones. Desde ahí se cojen las claves privadas para

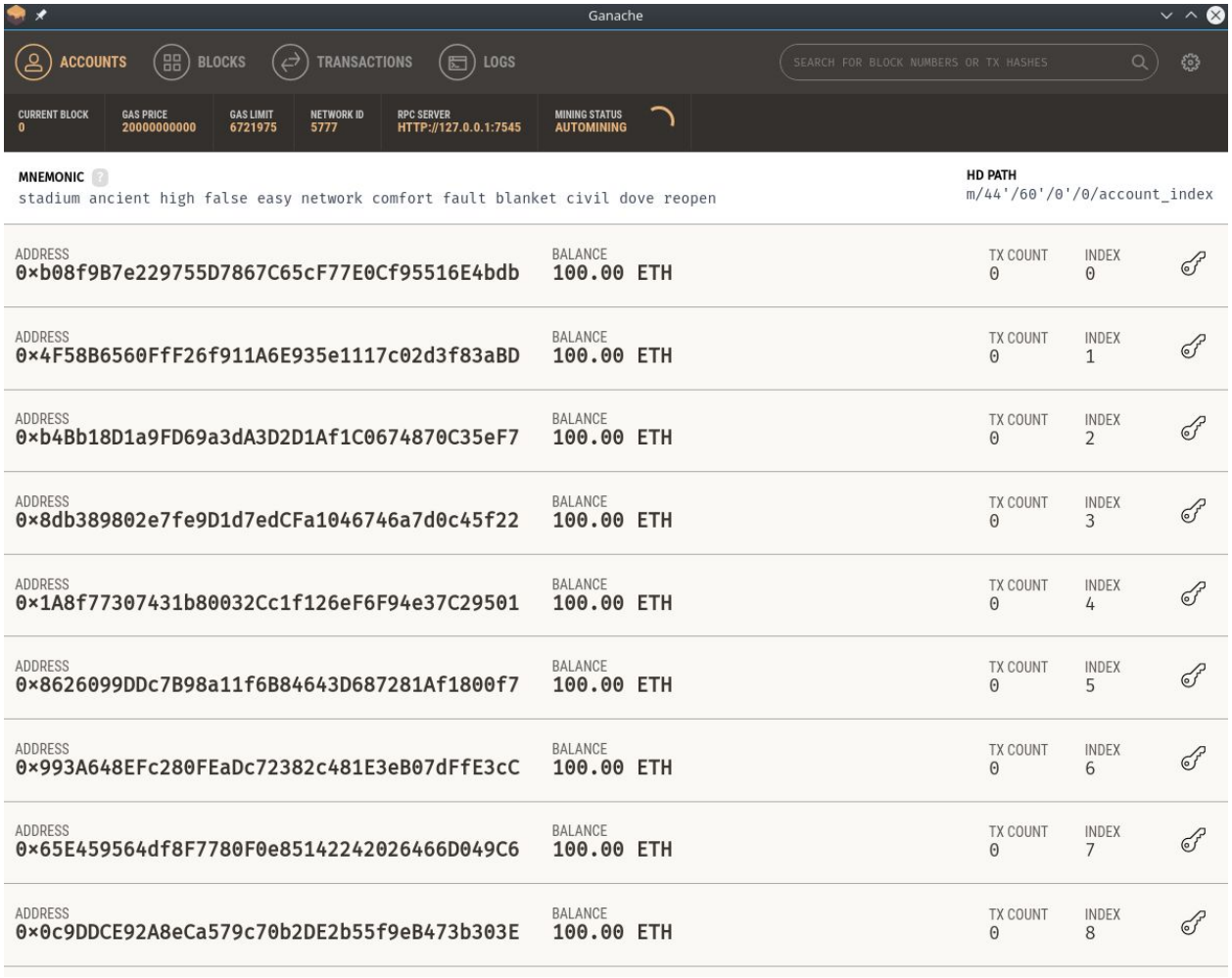


Figura 5: Ganache

10.2. Contrato Ethereum

El contrato es el parte crítica de la aplicación que guarda los datos importantes como los datos públicos personales de los usuario y defina la reglas y el contexto de la interacción. Como el editor se usaba el editor oficial Remix que compila el código a medida de que este se está escribiendo sacando las notificaciones en la barra lateral.

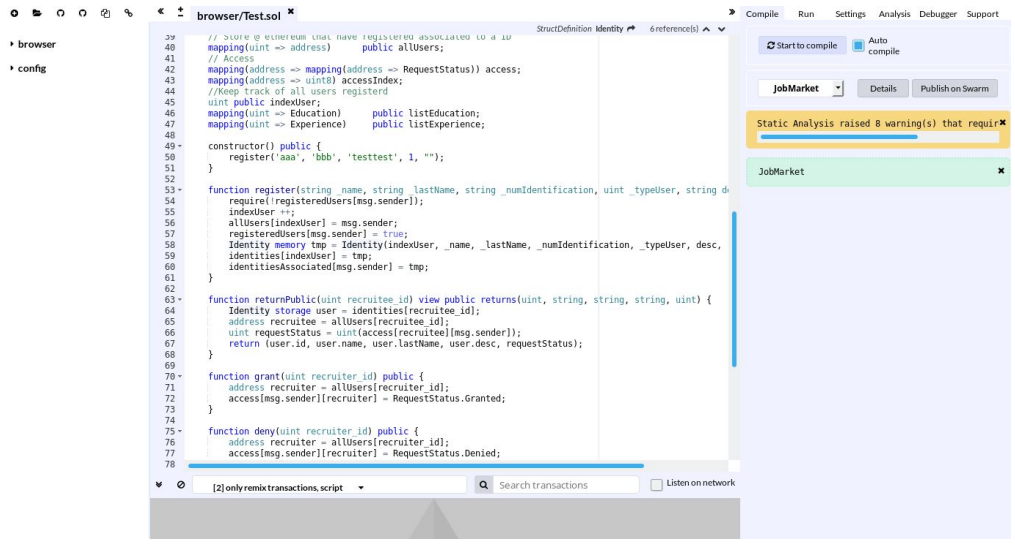


Figura 6:Contrato en remix para depurar.

El contrato se validaba en el console donde se llamaban sus funciones con diferentes valores.

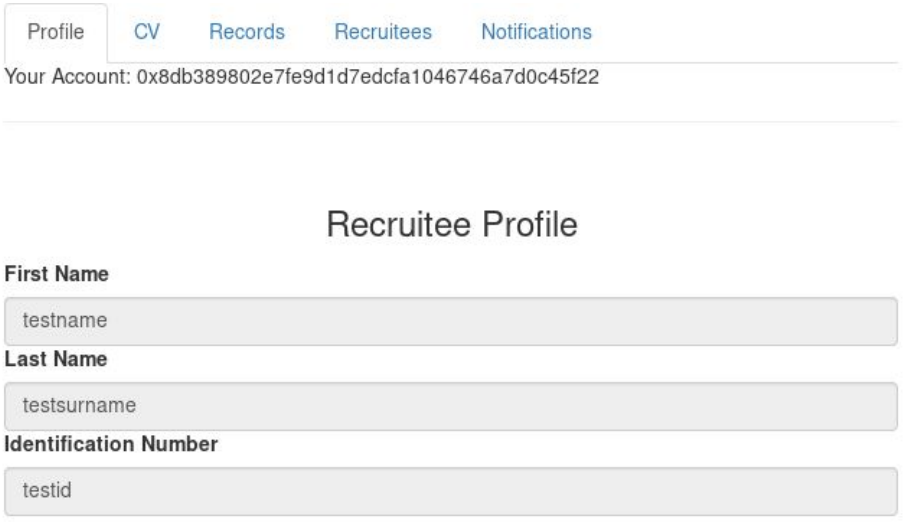


Figura 7: Usuario Creado

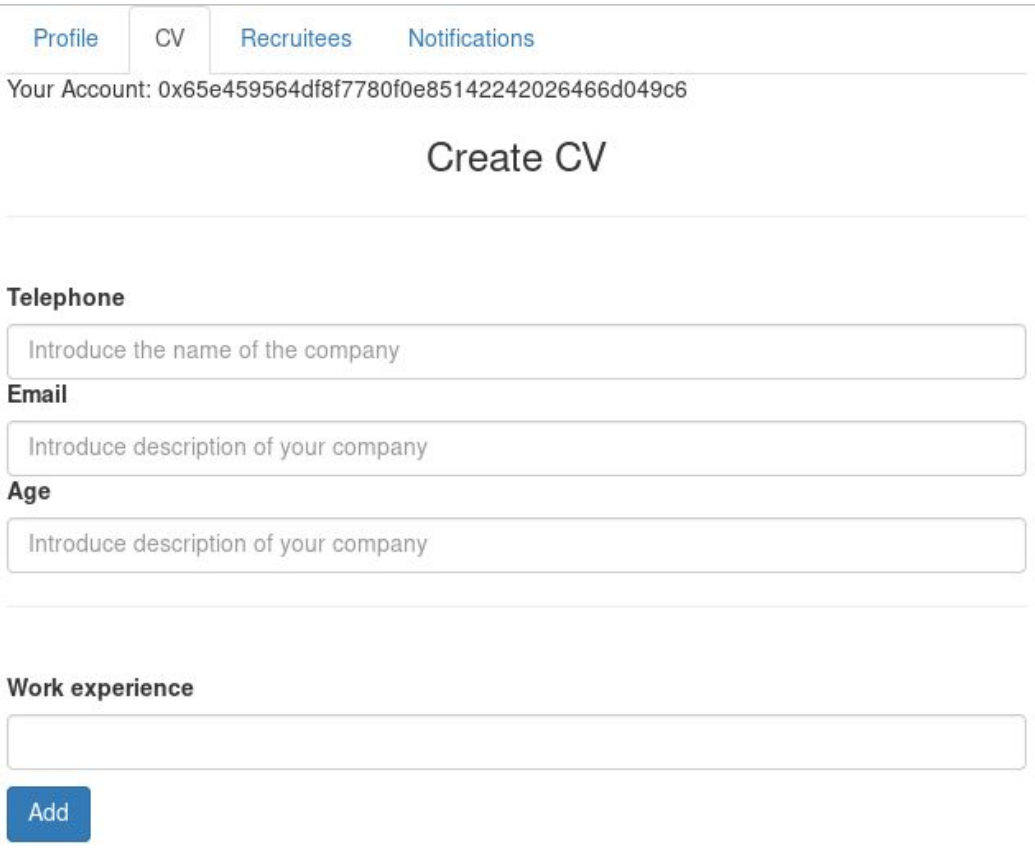


Figura 8: Registro

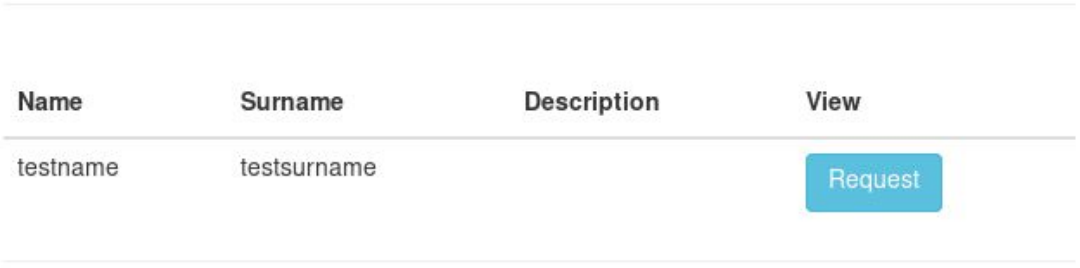


Figura 9: Lista de usuarios en búsqueda de trabajo

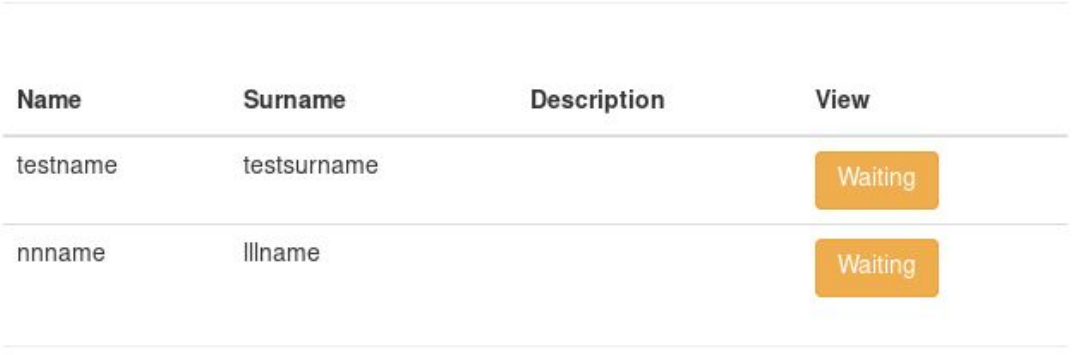


Figura 10: Lista de usuarios en búsqueda de trabajo con solicitudes pendientes de aprobar

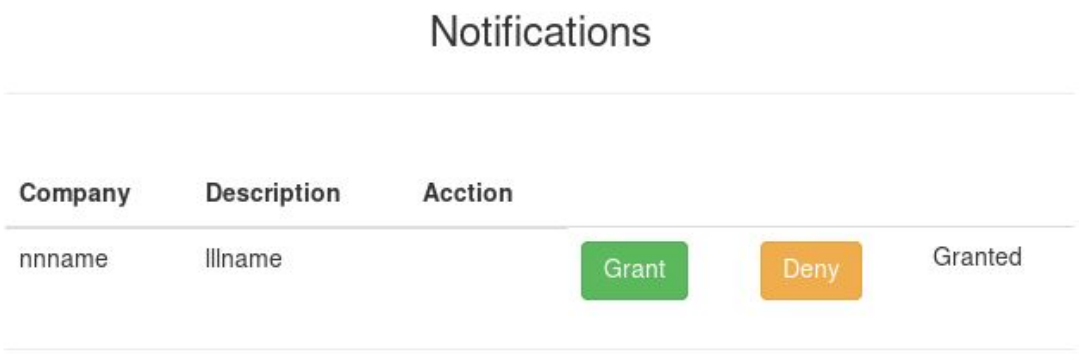


Figura 11: Lista de solicitudes que llegan al usuario

Un escenario típico necesitará dos personas, un recruiter y un recruitee. Ambos entrarán en la página y facilitarán sus datos para presentarlos a otros usuarios. Una vez registrado el recruitee se rellena su CV y esperá hasta que el recruitor le envía una solicitud en la página donde está listado.

Recruiter entrará podrá enviar las solicitudes en la página llamada “Recruitees” y entonces esperará hasta que los recruiters aceptan o rechazan su solicitud. Las solicitudes en nuestro caso no serán borradas pero el recruitee siempre podrá cambiar el estado de la solicitud. Siempre y cuando la solicitud es aceptada el recruiter podrá acceder al perfil de recruitee y entrar en contacto con el usando los datas que el último ha presentado ahí.

11. Obstáculos

Durante la realización del proyecto han ido apareciendo diversos obstáculos y desviaciones que han afectado algunos aspectos del desarrollo definidos en la planificación inicial.

A continuación se mencionara aquellos que se consideran más relevantes y han tenido un impacto dentro de la elaboración del desarrollo. Se tiene que tener en cuenta que han habido agentes externos que también han provocado al cambios en la planificación inicial.

- Cambio del lenguaje de del desarrollo de la interfaz del sistema.
- Cambio de la utilización de la red blockchain

  de una blockchain privada generada por una herramienta llamada ganache a montar una red blockchain propia desde cero.
- Cambio de la herramienta de framework de desarrollo de blockchain.
- Cambio de trabajo como agente externo
- El problema de debuggear las herramientas.
- El desconocimiento del sistema a desarrollar y la complejidad.

12. Conclusiones

Los objetivos principales de este proyecto eran la creación de una identidad única, la asociación de información a esta identidad, control de quién puede acceder a tu información privada y de poner en práctica el concepto de círculo de confianza aplicada en el manejo de identidades. Con este proyecto se han intentado dar un nuevo enfoque al desarrollo de las aplicaciones y las posibles soluciones que existen con blockchain referido al mundo de la identidad digital.Durante el desarrollo de esta prueba de concepto, las metodologías ágiles han sido de gran ayuda, y sobretodo, de la una tabla en el que mantener actualizada el estado del proyecto y en el que poder percibir los posibles bloques o desviaciones. Estas desviaciones quedan explicadas en un punto superior, pero gracias al feedback del director, la ayuda de la comunidad blockchain, mi asistencia a reuniones blockchain y mis horas depurando han podido ser superadas.

Como he podido explicar en el apartado mejoras posibles, tengo una idea más clara de el potencial de esta tecnología aplicada en el mundo digital, pero no solo al de la identidad digital, sino como percibimos el mundo digital haciéndolo más seguro y dejanos el control a nosotros. Aunque tengo que resaltar es una tecnología por la que están apostando muchas empresas, pero que ha de mejorar ciertos aspecto como algoritmo de consenso que trae mucho debate.

Finalmente, los resultados de este prototipo son los esperados se ve que existen un gran serie de posibilidades que pueden mejorar el prototipo, permitiendo así, hacer una aplicación descentralizada capaz de ser comercializada.

13. Futuras mejoras

Dado el tema del proyecto y su infinita mejorar respecto a temas de identidad, y mejoras para la

anonimidad para los usuarios de la aplicación, han aparecido durante el desarrollo de todo el proyecto, una serie de ideas posibles para mejorar la aplicación descentralizada.

- Añadir a la aplicación un sistema de creación de una dirección secundaria para no exponer la primera a todos los procesos y en caso de perdida, solo perder en el aparato la clave de la dirección secundaria y no la primera de la cuenta ethereum.
- Añadir una capa de seguridad añadiendo un 2FA(factor authentication) que es parecido a lo que hace gmail cuando pides que te envie un mensaje para que envie un codigo y lo escribas en la página web para poder acceder. Esto se logra añadiendo una aplicación móvil que haría que estaría conectada a nuestra aplicación mediante un servidor que enviaria todas las peticiones a nuestro aplicación móvil, y se tendría que verificar o no que la persona que está accediendo es la persona asociada a esa cuenta.
- Añadir un sistema de recuperación de clave privada pero añadiendo un challenge que sería enviado a 3 personas favoritas elegidas para la recuperación de la cuenta.

14. Bibliografía

1. *Contributors. "Introduction — Ethereum Homestead 0.1 documentation." Ethdocs.org. Accessed 1 Mar. 2018. <http://www.ethdocs.org/en/latest/introduction/index.html>*
2. *N.a. "What is Ether." Ethereum.org. 15 Feb. 2018. Web. 1 Mar. 2018. <https://www.ethereum.org/ether>*
3. *"Solidity." Solidity - Solidity 0.4.21 Documentation, solidity.readthedocs.io/en/v0.4.21/.*
4. *Tikhomirov, Sergei. "Ethereum: State of Knowledge and Research Perspectives - Semantic Scholar." Semanticscholar.org. n.d. Web. 1 Mar. 2018.*
5. *François Zaninotto. "The Blockchain Explained to Web Developers, Part 1: The Theory." Marmelab.com, 28 Apr. 2016, https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-the-theory.html. Accessed 1 Mar. 2018.*

6. N.a. "Who are Stakeholders and what is their role?." University-essays.tripod.com, http://university-essays.tripod.com/stakeholders.html. Accessed 1 Mar. 2018.
7. Wikipedia Contributors. "Decentralized application." Wikipedia, the Free Encyclopedia, 9 Mar. 2018, https://en.wikipedia.org/wiki/Decentralized_application. Accessed 4 Mar. 2018.
8. Ethereum. "ethereum/wiki." GitHub, https://github.com/ethereum/wiki. Accessed 4 Mar. 2018.
9. https://www.computer.org/csdl/proceedings/p2p/2001/1503/00/15030101.pdf. Accessed 4 Mar. 2018.
10. Wikipedia Contributors. "Blockchain." Wikipedia, the Free Encyclopedia, https://en.wikipedia.org/wiki/Blockchain. Accessed 5 Mar. 2018.
11. CoinDesk. "How bitcoin mining works - CoinDesk." CoinDesk, 6 Aug. 2013, https://www.coindesk.com/information/how-bitcoin-mining-works/. Accessed 6 Mar. 2018.
12. Andrew Tar. "Proof-of-Work, Explained." Cointelegraph, https://cointelegraph.com/explained/proof-of-work-explained. Accessed 6 Mar. 2018.
13. Cointelegraph. "What is Bitcoin Mining." Cointelegraph, https://cointelegraph.com/bitcoin-for-beginners/what-is-mining. Accessed 6 Mar. 2018.
14. Claresullivana. "E-residency and blockchain." Sciencedirect.com, 3 May 2017, https://www.sciencedirect.com/science/article/pii/S0267364917300845. Accessed 6 Mar. 2018.
15. "Sueldos en Programador/a junior en España | Indeed.es." Indeed.es, https://www.indeed.es/salaries/Programador/a-junior-Salaries. Accessed 19 Mar. 2018.
16. Ediciones El País. " Calculadora sueldo neto." EL PAÍS, 18 Mar. 2018, https://cincodias.elpais.com/herramientas/calculadora-sueldo-neto/. Accessed 20 Mar. 2018.
17. Comparadorluz.com. "Precio kWh electricidad." Comparadorluz.com, 3 Dec. 2013, https://comparadorluz.com/faq/precio-kwh-electricidad. Accessed 19 Mar. 2018.
18. N.a. "Comparar - Tarifas Internet y Telefonía - Rastreator.com™." Tarifas-adsl-fibra.rastreator.com,

https://tarifas-adsl-fibra.rastreator.com/datos-comparativa?product=7#Q1. Accessed 19 Mar. 2018.

15. Lista de imágenes