

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

BLOCKCHAIN, SMART CONTRACTS Y DAPP: INMUEBLES TURÍSTICOS, PRÉSTAMOS Y SEGUROS

Autor: Teresa Rodríguez Benito

Director: Atilano Fernández-Pacheco Sánchez-Migallón Director: José Luis Gahete Díaz

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título “Blockchain, Smart Contracts y Dapp: Inmuebles Turísticos, Préstamos y Seguros” en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el curso académico 2018/19 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido tomada de otros documentos está debidamente referenciada.



Fdo.: Teresa Rodríguez Benito Fecha: 11/Junio / 2019

Autorizada la entrega del proyecto

LOS DIRECTORES DEL PROYECTO



Fdo.: Atilano Fernández-Pacheco Sánchez-Migallón Fecha: 11/ Junio / 2019



Fdo.: José Luis Gahete Díaz Fecha: 11/ Junio / 2019

**AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO**

***1º. Declaración de la autoría y acreditación de la misma.***

El autor D. Teresa Rodríguez Benito DECLARA ser el titular de los derechos de propiedad intelectual de la obra: “Blockchain, Smart Contracts y Dapp: inmuebles turísticos, préstamos y seguros”, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

***2º. Objeto y fines de la cesión.***

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

***3º. Condiciones de la cesión y acceso***

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar “marcas de agua” o cualquier otro sistema de seguridad o de protección.

b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.

c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.

d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.

e) Asignar por defecto a estos trabajos una licencia Creative Commons.

f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

***4º. Derechos del autor.***

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.

c) Solicitar la retirada de la obra del repositorio por causa justificada.

d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

***5º. Deberes del autor.***

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.

b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.

c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.

d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

***6º. Fines y funcionamiento del Repositorio Institucional.***

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

➢ La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.

➢ La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.

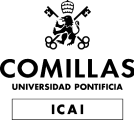
➢ La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro. ➢ La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 11 de Junio de 2019

**ACEPTA**

Fdo: Teresa Rodríguez Benito

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:



GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

BLOCKCHAIN, SMART CONTRACTS Y DAPP: INMUEBLES TURÍSTICOS, PRÉSTAMOS Y SEGUROS

Autor: Teresa Rodríguez Benito

Director: Atilano Fernández-Pacheco Sánchez-Migallón Director: José Luis Gahete Díaz

Madrid

“Para ser irremplazable, uno debe siempre ser diferente” -Coco Chanel

**BLOCKCHAIN, SMART CONTRACTS Y DAPP: INMUEBLES TURÍSTICOS, PRÉSTAMOS Y SEGUROS**

**Autor: Rodríguez Benito, Teresa.**

Director: Fernández-Pacheco Sánchez-Migallón, Atilano.

Director: Gahete Díaz, José Luis.

Entidad Colaboradora: ICAI – Universidad Pontificia Comillas

**RESUMEN DEL PROYECTO**

Con el fin de explotar la revolucionaria tecnología *Blockchain*, se plantea la creación de una plataforma descentralizada para aprovechar un nicho de mercado que está creciendo: los alojamientos turísticos. En el alcance se integran compradores y vendedores, así como, la interacción de este mercado con prestamistas y aseguradoras, posibilitando un sistema que reduce los costes de transacción y que es seguro, confiable, inmutable y transparente.

**Palabras clave**: Blockchain, Smart Contracts, Dapp, Ethereum, Rinkeby, Inmuebles, Seguros, Préstamos

**1. Introducción**

En la actualidad, el turismo es uno de los sectores primordiales en España, siendo el país con más influencia de este sector en su Producto Interior Bruto. [1] Además, se está produciendo un cambio de conducta en los turistas respecto a su alojamiento, albergándose cada vez una mayor proporción en apartamentos turísticos, como los ofrecidos por *Airbnb*. [2] Con el fin de mantener el gran aporte económico que genera el turismo, y adaptando la nueva actitud de los consumidores, se propone la introducción de la disruptiva tecnología *Blockchain*.

*Blockchain* es la tecnología que se encuentra detrás de las criptomonedas, como la popular *Bitcoin*. Permite eliminar el actor mediador de la transacción, puesto que es descentralizado; cada nodo de la red intercambia información con el resto y almacena una copia de los datos permutados. Debido a los algoritmos de consenso en uso y la criptografía utilizada, junto con la descentralización de la información, permiten mantener un sistema inmutable. Además, posibilita una reducción del coste de la transacción y una operativa disponible sin interrupción, a diferencia del sistema tradicional bancario. Asimismo, la integración con las cláusulas contractuales de *Blockchain*, *Smart Contracts*, se permite optimizar los procesos, puesto que se ejecutan al cumplir los requisitos diseñados de forma automática.

Por lo tanto, en este proyecto se integran los *Smart Contracts* y la tecnología *Blockchain* en una *Dapp*, para permitir una experiencia del consumidor agradable al disponer de una interfaz amigable, junto a la posibilidad de conectarse a través de una *Wallet HD*, con la que, registrándose con una única contraseña, permite almacenar todas las cuentas de cualquier red de forma segura y confiable.

**2. Definición del proyecto**

El objetivo principal del proyecto es utilizar las ventajas comentadas de la tecnología de *Blockchain* para gestionar el nicho de mercado de los inmuebles turísticos en España entre compradores-vendedores y arrendatarios-arrendadores, así como la posibilidad de obtener un préstamo y contratar una póliza de seguro para el inmueble deseado. Todo

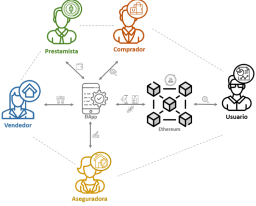
ello se basa en una aplicación descentralizada: *Dapp*, que registre de forma automática las transacciones realizadas si se cumplen las condiciones necesarias.

Para poder llevar a cabo el objetivo fundamental, en primer lugar se profundiza y documenta la tecnología *Blockhain* con su aplicación de *Smart Contracts*, con vistas a ser desplegado en la red de pruebas *Rinkeby*. Más tarde, se estudia y compara las plataformas para la aplicación de *Smart Contracts* en una *Dapp*, con el objeto de diseñar, desarrollar y testear el caso de uso en un nodo local. Por último, se realiza un despliegue en la red *Rinkeby*, para así analizar las transacciones en una red pública.

**3. Descripción del sistema**

Con el objeto de solucionar la gestión de inmuebles, préstamos y seguros, se desarrolla una plataforma *Blockchain* de forma distribuida.

El comprador publica en *Blockchain* un anuncio de un inmueble que desea vender a través de la *Dapp*. Por otra parte, la aseguradora puede publicar una oferta de póliza de seguro referente al inmueble visto en la *Dapp*. Con relación al comprador, si le interesa un inmueble, tendrá la opción de comprarlo sin necesidad de préstamo ni seguro, aunque si lo desea, podrá aceptar una oferta de las aseguradoras, así como publicar la necesidad de un préstamo con las condiciones que le interesan. En cuanto al prestamista, si le resulta ventajosa la oferta del prestatario, la puede aceptar para intercambiar *Ethers*. La siguiente figura muestran los diferentes actores de la aplicación junto al sistema descentralizado.



*Ilustración 1: Esquema del sistema*

Para resolverlo, se utiliza el framework de *Truffle* para fijar la estructura del proyecto, compilar y migrar los *Smart Contracts* desarrollados a través de *Atom*. Tras implementar *los Smart Contracts*, se necesita un nodo local de *Ethereum*, *Ganache*, para ejecutarlos y testearlos. Después, se realiza el despliegue y migración a través de un nodo remoto, *Infura*, en la *testnet Rinkeby*.

Por otro lado, en *Atom* se programa la parte del *front*: *HTML, CSS* y *JavaScript*. A través de *JavaScript*, junto a la librería *Web3.js*, el plugin de *Metamask* y el servidor de desarrollo *lite-server* de *Node.js*, se posibilita la unión de las partes tal como se muestra.

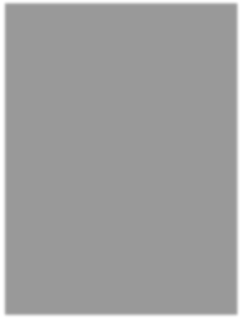


*Ilustración 2: Arquitectura Dapp*

**4. Resultados**

Se ha posibilitado utilizar *Blockchain* de forma transparente para el usuario a través de la *Dapp*. En ella, el comprador puede anunciar sus inmuebles y ser comprados por otros usuarios. Además, pueden solicitarse préstamos y contratar pólizas de seguro. También, se puede visualizar un registro histórico de las transacciones realizadas en la plataforma.

Se muestra un ejemplo de su utilización.



*Ilustración 3: Dapp*

Al realizarse el despliegue en *Rinkeby*, se puede observar que en los resultados se ha reducido los costes de las transacciones, se han evitado intermediarios, se ha almacenado en varios nodos la información, y se ha elevado la seguridad del sistema respecto a una aplicación tradicional.

**5. Conclusiones**

En esta iniciativa se observa cómo la gestión de inmuebles, préstamos y seguros puede reducir sus costes de tramitación basándose en la tecnología. Este proyecto supone una plataforma novedosa y única que posibilita interactuar a los compradores, vendedores, prestamistas y aseguradoras a través de *Blockchain* A parte de la implementación y el despliegue, el proyecto es un encuentro de información sobre las características de esta tecnología, sus mejores herramientas y sus aportaciones. Además, el análisis y diseño del caso de uso en detalle ha fomentado su aprendizaje y el uso de la disruptiva tecnología *Blockchain*, que reafirma la confianza y fiabilidad en las partes.

El presente proyecto sirve como punto de partida para implementar algunos de los trabajos futuros posibles indicados sobre la plataforma y su gestión. Con el fin de facilitar el progreso del proyecto, se ha entregados varios anexos para que cualquier persona sin experiencia y conocimientos de *Blockchain* pueda disponer de la instalación y funcionamiento del proyecto paso a paso para poder mejorarlo. Además de las contribuciones indicadas, el trabajo colabora con la sociedad aportando la información actualizada y contrastada para que las empresas españolas sigan invirtiendo en la tecnología como motor de mejora de los procesos.

**6. Referencias**

[1] [En línea]. Available: https://cepymenews.es/espana-pais-mundo-donde-turismo-aporta mas-al-pib-segun-la-ocde/ [Último acceso: 2 Junio 2019].

[2] [En línea]. Available: https://es.statista.com/estadisticas/802182/ingresos-anuales-de airbnb-en-espana/. [Último acceso: 31 Mayo 2019].

**BLOCKCHAIN, SMART CONTRACTS AND DAPP: TOURISM PROPERTIES, LOANS AND INSURANCES**

**Author: Rodríguez Benito, Teresa.**

Supervisor: Fernández-Pacheco Sánchez-Migallón, Atilano.

Supervisor: Gahete Díaz, José Luis.

Collaborating Entity: ICAI – Universidad Pontificia Comillas

**ABSTRACT**

In order to exploit the revolutionary *Blockchain* technology, the creation of a decentralized platform is presented to take advantage of a market niche that is growing: tourism apartments. The scope includes buyers and sellers, as well as the interaction of lenders and insurers at this market, making possible a system that reduces transaction costs and is safe, reliable, immutable and transparent.

**Keywords**: Blockchain, Smart Contracts, Dapp, Ethereum, Rinkeby, Real Estate, Insurances, Loans

**1. Introduction**

Nowadays, tourism is one of the most important sectors in Spain, being the country with the biggest influence of this sector in its Gross Domestic Product. [1] In addition, there is a change in the behavior of tourists regarding their accommodation, with a growing proportion of tourist apartments, such as those offered by Airbnb. [2] In order to maintain the great economic contribution generated by tourism, as well as adapting the new attitude of consumers, it is proposed the introduction of the disruptive *Blockchain* technology.

Blockchain is the technology behind cryptocurrencies, like the popular *Bitcoin*. It allows eliminating the mediating actor of the transaction, since it is decentralized; each node of the network exchanges information with the rest and stores a copy of the permuted data. Due to the consensus algorithms and the cryptography used, along with the decentralization of information, it allows maintaining an immutable system. In addition, it enables a reduction in the cost of the transaction and an operation available without interruption, unlike the traditional banking system. Furthermore, the integration with the contractual clauses of *Blockchain*, *Smart Contracts*, it allows optimizing the processes, since they are executed automatically when the configured requirements are met.

Therefore, in this project the *Smart Contracts* and the *Blockchain* technology are integrated in a *Dapp*, to allow a pleasant consumer experience by having a friendly interface, together with the possibility of connecting through an *HD Wallet*, with which registering with only one password, it allows to store all the accounts of any network in a safe and reliable way.

**2. Project definition**

The main objective of the project is to use the mentioned advantages of the *Blockchain* technology to manage the market niche of tourist properties in Spain between buyers sellers and tenants-lessors, as well as the possibility of obtaining a loan and contracting an insurance policy for the desired property. All this is based on a decentralized

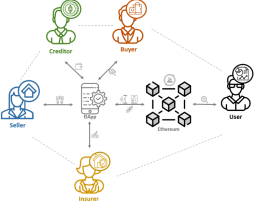
application: *Dapp*, which automatically records transactions made if the registered conditions are met.

In order to carry out the fundamental objective, *Blockhain* technology is first deepened and documented with *its Smart Contracts* application, in order to deployed in the *Rinkeby* test network. Later, the platforms for the application of *Smart Contracts* in a *Dapp* are studied and compared, in order to design, develop and test the use case in a local node. Finally, a deployment is made in the *Rinkeby* network, in order to analyze transactions in a public network.

**3. System description**

In order to solve the management of real estate, loans and insurance, a *Blockchain* platform is developed in a distributed way.

The buyer publishes in *Blockchain* an advertisement for a property that he wishes to sell through the *Dapp*. On the other hand, the insurer can publish an offer of insurance policy regarding the property seen in the *Dapp*. In relation to the buyer, if he is interested in a property, he will have the option of buying it without the need for a loan or insurance, although if he wish, he may accept an offer from the insurers, as well as publish the need for a loan with the conditions in which he is interested. As for the lender, if the borrower's offer is advantageous, he can accept it in order to exchange *Ethers*. The following figure shows the different actors of the application as well as the decentralized system.



*Ilustration 1: System scheme*

To solve the problem, *Truffle* framework is used to set the structure of the project, compile and migrate the *Smart Contracts* developed through *Atom*. After implementing *Smart Contracts*, a local *Ethereum* node, *Ganache*, is needed to run and test them. Then, the deployment and migration is performed through a remote node, *Infura*, in the *Rinkeby*

testnet.

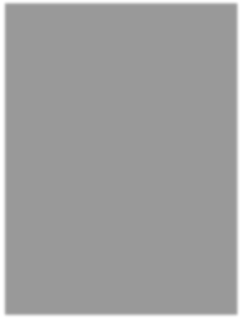
On the other hand, *Atom* is used to programme the front part: *HTML*, *CSS* and *JavaScript*. Through *JavaScript*, together with the *Web3.js* library, the *Metamask* plugin and the *Node.js lite-server* development server, it is possible to join the different parts as shown below.



*Ilustration 2: Dapp Architecture*

**4. Results**

It has been possible to use *Blockchain* transparently for the user through the *Dapp*. In the app, the buyer can advertise their properties and be purchased by other users. In addition, loans and insurance policies can be requested. Also, it is possible to view the historical record of the transactions made in the platform. An example of the *Dapp* developed is shown.



*Ilustration 3: Dapp*

When deployed in *Rinkeby*, it can be observed that as a result, the transaction costs have been reduced, intermediaries have been avoided, the information has been stored in several nodes, and the security of the system has been raised in comparison with a traditional app.

**5. Conclusions**

This initiative shows how the management of real estate, loans and insurance can reduce their processing costs based on this technology. This project supposes a new and unique platform that makes it possible to interact with buyers, sellers, lenders and insurers through *Blockchain*. Apart from the implementation and deployment, the project is a repository of information about the characteristics of this technology, its best tools and its contributions. In addition, the analysis and design of the use case in detail has fostered the learning and the use of the disruptive *Blockchain* technology, which reaffirms the trust and reliability of the parts.

The present project serves as a starting point to implement some of the possible future works indicated about the platform and its management. In order to facilitate the progress of the project, several annexes have been delivered so that anyone without experience and knowledge of *Blockchain* can make the installation and operation of the project step by step in order to improve it. In addition to the contributions indicated, the work collaborates with society by providing up-to-date and verified information so that Spanish companies continue investing in technology as an engine for improving processes.

**6. References**

[1] [En línea]. Available: https://cepymenews.es/espana-pais-mundo-donde-turismo-aporta mas-al-pib-segun-la-ocde/ [Último acceso: 2 Junio 2019].

[2] [En línea]. Available: https://es.statista.com/estadisticas/802182/ingresos-anuales-de airbnb-en-espana/. [Último acceso: 31 Mayo 2019].

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE LA MEMORIA*

***Índice de la Memoria***

***Capítulo 1. Introducción .................................................................................................. 13*** 1.1 Motivación del Proyecto ..................................................................................................... 15 1.2 Solución Propuesta .............................................................................................................. 17

***Capítulo 2. Descripción de las Tecnologías..................................................................... 21*** 2.1 Ethereum ............................................................................................................................. 21 2.2 Solidity ................................................................................................................................ 22 2.3 Truffle.................................................................................................................................. 23 2.4 Ganache............................................................................................................................... 24 2.5 Entorno de Desarrollo ......................................................................................................... 26

*2.5.1 Remix IDE ...................................................................................................................... 26 2.5.2 Visual Studio Solidity ..................................................................................................... 27 2.5.3 Editor Atom .................................................................................................................... 28 2.5.4 Comparativa................................................................................................................... 29*

2.6 Metamask ............................................................................................................................ 30 2.7 Web3.js................................................................................................................................ 31 2.8 EtherScan ............................................................................................................................ 32 2.9 Node.js................................................................................................................................. 33 2.10 Rinkeby ............................................................................................................................... 34 2.11 Infura ................................................................................................................................... 35

***Capítulo 3. Estado de la Cuestión.................................................................................... 37*** 3.1 Blockchain Respecto al Caso de Uso en España................................................................. 38 3.2 Blockchain Respecto a la Información Manejada en el Caso de Uso ................................. 42 3.3 Blockchain y la Universidad Pontificia Comillas ICADE-ICAI......................................... 45

***Capítulo 4. Definición del Trabajo .................................................................................. 47*** 4.1 Justificación......................................................................................................................... 47 4.2 Objetivos ............................................................................................................................. 49 4.3 Metodología......................................................................................................................... 50 4.4 Planificación........................................................................................................................ 52 4.5 Estimación Económica ........................................................................................................ 54

I

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE LA MEMORIA*

***Capítulo 5. Blockchain..................................................................................................... 57*** 5.1 Descripción General............................................................................................................ 57 5.2 Almacenamiento en Blockchain.......................................................................................... 59 5.3 Algoritmos de Consenso de las Redes Blockchain ............................................................. 65 5.4 Versiones de Blockchain ..................................................................................................... 67

*5.4.1 Criptomoneda................................................................................................................. 67 5.4.2 Smart Contracts.............................................................................................................. 69 5.4.3 Dapp ............................................................................................................................... 71*

5.5 Ico........................................................................................................................................ 73 5.6 Ventajas de Blockchain....................................................................................................... 74 5.7 Limitaciones de la Tecnología Blockchain ......................................................................... 76

***Capítulo 6. Análisis del Sistema....................................................................................... 79*** 6.1 Casos de Uso ....................................................................................................................... 79 *6.1.1 Caso de Uso Común ....................................................................................................... 79 6.1.2 Caso de Uso Vendedor................................................................................................... 80 6.1.3 Caso de Uso Comprador................................................................................................ 80 6.1.4 Caso de Uso Prestamista................................................................................................ 82 6.1.5 Caso de Uso Aseguradora.............................................................................................. 82* 6.2 Diagramas de Secuencia...................................................................................................... 83 *6.2.1 Diagrama de Secuencia Compra.................................................................................... 83 6.2.2 Diagrama de Secuencia Alquiler.................................................................................... 87* 6.3 Diagrama de Actividad....................................................................................................... 89 *6.3.1 Diagrama de Actividad Compra..................................................................................... 89 6.3.2 Diagrama de Actividad Alquiler..................................................................................... 92*

***Capítulo 7. Diseño ............................................................................................................ 95*** 7.1 Funcionalidades Comunes................................................................................................... 95 7.2 Funcionalidades de Vendedor ............................................................................................. 96 7.3 Funcionalidad de Comprador.............................................................................................. 96 7.4 Funcionalidad de Prestamista.............................................................................................. 98 7.5 Funcionalidad de Aseguradora............................................................................................ 98 7.6 Funcionalidad del Sistema................................................................................................... 99 7.7 Funcionalidad usuario con Privilegios ................................................................................ 99

II

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE LA MEMORIA*

7.8 Navegabilidad en la Dapp ................................................................................................. 100 ***Capítulo 8. Arquitectura................................................................................................. 103***

***Capítulo 9. Desarrollo de la Dapp.................................................................................. 109*** 9.1 Smart Contracts................................................................................................................. 109 9.2 Interfaz de Usuario ............................................................................................................ 113

*9.2.1 Página de Bienvenida................................................................................................... 113 9.2.2 Cuenta .......................................................................................................................... 114 9.2.3 Publicar........................................................................................................................ 115 9.2.4 Anuncios....................................................................................................................... 118 9.2.5 Préstamos..................................................................................................................... 119 9.2.6 Seguros......................................................................................................................... 120 9.2.7 Registro Histórico ........................................................................................................ 121*

***Capítulo 10. Despliegue en Rinkeby y Análisis de las Transacciones............................ 125*** 10.1 Despliegue de los Smart Contracts.................................................................................... 128 10.2 Flujo de Transacciones...................................................................................................... 133 10.3 Transacciones Internas de los Smart Contracts................................................................. 153

***Capítulo 11. Alcance Comercial ...................................................................................... 157***

***Capítulo 12. Conclusiones y Trabajos Futuros............................................................... 161*** 12.1 Conclusiones ..................................................................................................................... 161 12.2 Trabajos Futuros................................................................................................................ 165

***Capítulo 13. Bibliografía.................................................................................................. 171***

***A. Anexo A: Guía de Instalación para el Usuario........................................................ 181*** A.1 Atom.................................................................................................................................. 181 A.2 Ganache............................................................................................................................. 183 A.3 Node.js............................................................................................................................... 186 A.4 Truffle................................................................................................................................ 191 A.5 Estructura y Ficheros en el Proyecto................................................................................. 192 A.6 Git...................................................................................................................................... 195 A.7 Metamask .......................................................................................................................... 202

III

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE LA MEMORIA*

A.8 Infura Rinkeby................................................................................................................... 205

***B. Anexo B: Guía de Funcionamiento para el Usuario ............................................... 215*** B.1 Ejecución en Local a Través de Ganache.......................................................................... 215 B.2 Ejecución en Rinkeby........................................................................................................ 216

IV

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE ILUSTRACIONES*

***Índice de Ilustraciones***

Ilustración 1: Valoración del turismo en España 2017 por WEF........................................ 13 Ilustración 2: Gasto total de los turistas extranjeros que visitaron España en 2018, según el motivo principal del viaje ( millones de euros) [3] ............................................................. 14 Ilustración 3: Evolución anual de los ingresos declarados por Airbnb en España entre 2012 y 2017 (en millones de euros) [5]........................................................................................ 16 Ilustración 4: Evolución anual del número de turistas internacionales que alquilaron una vivienda en España de 2000 a 2018 (en millones) [6]......................................................... 16 Ilustración 5: Logo Ethereum.............................................................................................. 21 Ilustración 6: Logo Solidity [12]......................................................................................... 22 Ilustración 7: Logo Truffle [13] .......................................................................................... 24 Ilustración 8: Logo Ganache [14]........................................................................................ 25 Ilustración 9: Aplicación Ganache ...................................................................................... 25 Ilustración 10: Remix IDE [17]........................................................................................... 27 Ilustración 11: Visual Studio Solidity [19].......................................................................... 28 Ilustración 12: Atom Editor................................................................................................. 29 Ilustración 13: Logo Metamask [21]................................................................................... 31 Ilustración 14: Logo Web3.js .............................................................................................. 32 Ilustración 15: Logo Etherscan [23].................................................................................... 32 Ilustración 16: Transacción Etherscan [24]......................................................................... 33 Ilustración 17: Logo Node.js [26] ....................................................................................... 33 Ilustración 18: Logo Lite-server [27] .................................................................................. 33 Ilustración 19: Rinkeby estado de la red [29]...................................................................... 35 Ilustración 20: Logo Infura [30].......................................................................................... 36 Ilustración 21: Información en descubierto [55] ................................................................. 42 Ilustración 22: Identidad digital Blockchain [57]................................................................ 44 Ilustración 23: Logo Alastria [61]....................................................................................... 45 Ilustración 24: Kanban utilizado a través de Trello............................................................. 51 Ilustración 25: Diagrama de Gantt del proyecto.................................................................. 52

V

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE ILUSTRACIONES*

Ilustración 26: Nodo universitario Alastria ICAI [67] ........................................................ 58 Ilustración 27: Hash, la huella dactilar digital [68] ............................................................. 61 Ilustración 28: Se cambia información del bloque, hash no comienza por 0000 [68] ........ 62 Ilustración 29: Tras minar el bloque, hash comienza por 0000 [68]................................... 62 Ilustración 30: Cada bloque tiene hash anterior [68]........................................................... 63 Ilustración 31: Minar el bloque y los posteriores................................................................ 64 Ilustración 32: Diferentes tipos de algoritmos de consenso [69]......................................... 66 Ilustración 33: Valor Bitcoin durante los últimos tres años [70]......................................... 68 Ilustración 34: Comparación App y Dapp........................................................................... 71 Ilustración 35: Conjunto de Dapps [76] .............................................................................. 72 Ilustración 36: Caso de uso común...................................................................................... 79 Ilustración 37: Caso de uso vendedor.................................................................................. 80 Ilustración 38: Caso de uso comprador ............................................................................... 81 Ilustración 39: Caso de uso prestamista .............................................................................. 82 Ilustración 40: Caso de uso aseguradora ............................................................................. 83 Ilustración 41: Diagrama de secuencia compra (I).............................................................. 85 Ilustración 42: Diagrama de secuencia compra (II)............................................................. 86 Ilustración 43: Diagrama de secuencia alquiler................................................................... 88 Ilustración 44: Diagrama de actividad compra.................................................................... 91 Ilustración 45: Diagrama de actividad alquiler.................................................................... 93 Ilustración 46: Navegabilidad en la Dapp ......................................................................... 100 Ilustración 47: Arquitectura Dapp ..................................................................................... 103 Ilustración 48: Arquitectura Dapp con tecnologías........................................................... 103 Ilustración 49: Estructura del proyecto- Truffle ................................................................ 104 Ilustración 50: Metamask interacción Dapp...................................................................... 107 Ilustración 51: Página de bienvenida................................................................................. 114 Ilustración 52: Cuenta y saldo sin Metamask.................................................................... 114 Ilustración 53: Cuenta y saldo con Metamask................................................................... 115 Ilustración 54: Pestaña Publicar ........................................................................................ 115 Ilustración 55: Publicación anuncio .................................................................................. 116

VI

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE ILUSTRACIONES*

Ilustración 56: Solicitud préstamo..................................................................................... 117 Ilustración 57: Publicación póliza de seguro..................................................................... 117 Ilustración 58: Pestaña Anuncios ...................................................................................... 118 Ilustración 59: Comprar inmueble..................................................................................... 118 Ilustración 60: Pestaña Préstamos ..................................................................................... 120 Ilustración 61: Prestar dinero............................................................................................. 120 Ilustración 62: Pestaña Seguros......................................................................................... 121 Ilustración 63: Póliza de seguro ........................................................................................ 121 Ilustración 64: Pestaña Registro Histórico ........................................................................ 122 Ilustración 65: Registro histórico anuncios....................................................................... 123 Ilustración 66: Registro histórico préstamos..................................................................... 123 Ilustración 67: Registro histórico seguros......................................................................... 124 Ilustración 68. Cuentas existentes en Wallet..................................................................... 127 Ilustración 69. Transacción Rinkeby: generación Propiedad.sol ...................................... 128 Ilustración 70. Bloque generado en la red Rinkeby........................................................... 129 Ilustración 71. Transacción Rinkeby: generación Prestamista.sol .................................... 130 Ilustración 72. Transacción Rinkeby: generación Aseguradora.sol .................................. 131 Ilustración 73. Despliegue desde consola en la red Rinkeby ............................................ 133 Ilustración 74: Puesta en venta del primer inmueble......................................................... 134 Ilustración 75: Transacción Rinkeby: Venta primer inmueble.......................................... 135 Ilustración 76: Transacción Rinkeby: Log de eventos venta primer inmueble ................. 136 Ilustración 77: Cuenta de vendedor antes de realizar anuncio .......................................... 136 Ilustración 78: Cuenta de vendedor después de realizar anuncio...................................... 137 Ilustración 79: Dirección de vendedor en Etherscan......................................................... 137 Ilustración 80: Transacción Rinkeby: Alquiler segundo inmueble ................................... 138 Ilustración 81: Transacción Rinkeby: Seguro primer inmueble........................................ 139 Ilustración 82: Transacción Rinkeby: Log de eventos seguro primer inmueble ............... 140 Ilustración 83: Transacción Rinkeby: Préstamo primer inmueble .................................... 141 Ilustración 84: Transacción Rinkeby: Log de eventos préstamo primer inmueble ........... 141 Ilustración 85. Notificación de MetaMask previa a transacción ....................................... 142

VII

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE ILUSTRACIONES*

Ilustración 86: Transacción Rinkeby: Aceptación préstamo primer inmueble ................. 143 Ilustración 87: Transacción Rinkeby: Interna aceptación préstamo primer inmueble ...... 143 Ilustración 88. Contratación de póliza de seguro desde el Front....................................... 144 Ilustración 89: Transacción Rinkeby: Contratación seguro primer inmueble................... 145 Ilustración 90: Transacción Rinkeby: Interna contratación seguro primer inmueble ....... 145 Ilustración 91. Notificación de MetaMask a la hora de contratar el seguro...................... 146 Ilustración 92: Transacción Rinkeby: Compra primer inmueble ...................................... 147 Ilustración 93: Transacción Rinkeby: Interna compra primer inmueble ........................... 147 Ilustración 94: Transacción Rinkeby: Log de eventos compra primer inmueble.............. 148 Ilustración 95: Transacción Rinkeby: Alquiler tercer inmueble ....................................... 149 Ilustración 96: Transacción Rinkeby: Alquilado tercer inmueble..................................... 150 Ilustración 97: Transacción Rinkeby: Interna alquilado tercer inmueble.......................... 150 Ilustración 98: Transacción Rinkeby: Alquilado segundo inmueble ................................ 151 Ilustración 99: Transacción Rinkeby: Interna alquilado segundo inmueble ..................... 152 Ilustración 100: Transacción Rinkeby: interna del vendedor............................................ 154 Ilustración 101: Transacción Rinkeby: interna del comprador ......................................... 154 Ilustración 102: Transacción Rinkeby: interna del prestamista......................................... 155 Ilustración 103: Transacción Rinkeby: interna del asegurador ......................................... 155 Ilustración 104: Transacción Rinkeby: Cuenta Smart Contract Propiedad.sol ................. 156 Ilustración 105: Smart Contract Escrow [88].................................................................... 166 Ilustración 106: Stages de la normativa IFRS9 [89] ......................................................... 167 Ilustración 107: IPFS [90] ................................................................................................. 168 Ilustración 108: Smart Door [91] ...................................................................................... 169

VIII

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE TABLAS*

***Índice de Tablas***

Tabla 1. Comparativa entre entornos de desarrollo............................................................. 30 Tabla 2: Análisis dedicado a cada tarea............................................................................... 55 Tabla 3: Relación entre tiempo y coste ............................................................................... 55 Tabla 4. Flujo de transacciones ......................................................................................... 125 Tabla 5. Relación entre perfil y cuenta.............................................................................. 126 Tabla 6. Hash de las transacciones que han generado Smart Contracts............................ 132 Tabla 7. Cuentas sobre las que se han desplegado los Smart Contracts............................ 132 Tabla 8: Relación transacciones hash en el flujo Rinkeby ................................................ 153 Tabla 9: Relación tarea principal, objetivo y grado de cumplimiento............................... 165

IX

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE TABLAS*

X

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE FRAGMENTOS DE CÓDIGO*

***Índice de Fragmentos de Código***

Código 1: Fragmento versión Solidity............................................................................... 109 Código 2: Fragmento import ............................................................................................. 109 Código 3: Fragmento Propiedad.sol estructura ................................................................. 110 Código 4: Fragmento Propiedad.sol mapping ................................................................... 110 Código 5: Fragmento Asegurador.sol evento.................................................................... 110 Código 6: Fragmento desactivación Smart Contract......................................................... 111 Código 7: Fragmento Propiedad.sol vender Anuncio ....................................................... 111 Código 8: Fragmento Prestamos.sol obtener número de prestámos.................................. 112 Código 9: Fragmento Prestamos.sol aceptación préstamo ................................................ 112 Código 10: fragmento Asegurado.sol seguros publicados sin asegurado ......................... 112 Código 11: fragmento Propiedad.sol Obtener todas los anuncios..................................... 113 Código 12: Fragmento Javascript Web3.js [82]................................................................ 119 Código 13. Detalle despliegue en Rinkeby de truffle.js.................................................... 126

XI

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ÍNDICE DE FRAGMENTOS DE CÓDIGO*

XII

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

**Capítulo 1. INTRODUCCIÓN**

En España, el turismo tuvo un primer impulso de la mano de los romanos con los centros termales. Más tarde, a finales del siglo XIX, únicamente viajaban los aristocráticos a las aguas termales y zonas costeras como terapia, destacando las playas del norte: *Sardinero* y la *Concha*, mientras que en los siguientes años empezó a destacar

la zona del Mediterráneo, y, además, este turismo pasó a ser una fuente de ocio. Debido al período de guerra civil española, hasta los años cincuenta no se empezó a impulsar fuertemente la industria turística: transporte, restauración, hoteles… [1] hasta llegar a nuestros días.

Actualmente, el turismo es uno de los principales motores de la economía española. Según el estudio sobre competitividad turística elaborada por *World Economic Forum*, España recibió, en el año 2017, la friolera cifra de 68.521.255 de turistas internacionales, los cuales, de media, han generado 824,1$. Esto ha permitido clasificar a España en primera posición, frente a otros 136 países, destacando por su infraestructura turística, como se aprecia en la Ilustración 1. [2]

*Ilustración 1: Valoración del turismo en España 2017 por WEF*

13

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

Esta magnífica industria genera gran cantidad de servicios adjuntos. El turismo atrae a personas que están dispuestas a pagar más que un residente habitual puesto que la mayoría de los viajes de extranjero son por ocio, tal como se muestra en la gráfica de Ilustración 2. Para clarificar este hecho, nos situamos en la piel de un turista extranjero al viajar a otro país. Se necesita comprar los billetes de avión, necesita un taxi, Cabify o Uber para desplazarse del aeropuerto a su hotel, necesita reservar una habitación, realizará un gasto de restauración de esos días, con alta probabilidad comprará entradas a museos, concierto, o parques de atracciones, y realizará, seguramente, algunas compras de ocio.

*Ilustración 2: Gasto total de los turistas extranjeros que visitaron España en 2018, según el motivo principal del viaje ( millones de euros) [3]*

En 2018, la afluencia de turistas internacionales ha supuesto un aumento del 0,9% respecto al 2017. Este crecimiento ha supuesto aproximadamente 90.000 millones de euros más a la economía española, es decir, un 3,1% de ingresos turístico respecto al año 2017. Además, de la importancia de los ingresos del sector, el turismo permite impulsar y generar altas tasas de empleo, colaborando a la robustez de la economía española [4]

14

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

La afluencia de turistas produce efectos positivos como la activación y estimulación del comercio, del espíritu empresarial, de la creación de empleo, de generación de infraestructura nueva para uso turístico y el aumento de la recaudación de impuestos.

Además de la gran ayuda económica y generación de empleos que produce en España el turismo, la experiencia viajera ayuda a entender las diferencias de culturas, hechos históricos, estilo de vida y ser más respetuosos, tanto para el viajero como para la persona que le atiende para que disfrute de su estancia. En resumen, el turismo produce una fuente de bienestar en España.

***1.1 MOTIVACIÓN DEL PROYECTO***

Para mantener el liderazgo en el ranking, es necesario incluir diversos cambios junto a los nuevos avances tecnológicos para poder acelerar y optimizar los procesos, de tal forma que permita la consolidación de la rentabilidad del sector.

Actualmente, los alojamientos turísticos se encuentran liderados por el sector hotelero, aunque está comenzando un incremento moderado en España de los alojamientos realizados en viviendas propias, prestadas o alquiladas, tal como se demuestra con los ingresos de la plataforma *Airbnb* en la Ilustración 3. *Airbnb* es una plataforma que se encarga de enlazar a turistas que desean encontrar alojamiento a los anfitriones que poseen alojamientos, es decir, se trata de un alquiler temporal de un inmueble.

15

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

**

*Ilustración 3: Evolución anual de los ingresos declarados por Airbnb en España entre 2012 y 2017 (en millones de euros) [5]*

El segmento de los turistas internacionales son lo que más interesan en el turismo español debido a los beneficios que aportan. Este sector está dispuesto a pagar cada vez más por el alquiler de un alojamiento temporal en España tal como se muestra en la Ilustración 4.



*Ilustración 4: Evolución anual del número de turistas internacionales que alquilaron una vivienda en España de 2000 a 2018 (en millones) [6]*

16

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

Con el fin de aprovechar este nicho de mercado, se replantea dar un nuevo enfoque a las viviendas compartidas que supusieron un boom en los años 1980 y 1990 en España. Las viviendas aprovechas por turnos con fin turístico suponían un reparto de las cuotas como el IBI, comunidad, derramas de esa vivienda que únicamente se aprovechaba durante una o dos semanas al año. Sin embargo, estas viviendas compartidas han creado grandes discusiones como la fecha del disfrute, cuotas impagadas, contratos con perpetuidad, estafas… [7]

Es momento de plantearse: ¿cómo hacer un sistema transparente? ¿Cómo reflejar todas las transacciones de pago realizadas por la vivienda? ¿Se podría reflejar cuando el copropietario desea su período vacacional? ¿Se podría eliminar la empresa gestora? ¿Se podría limitar la duración del contrato?

Además, las organizaciones encargadas de certificar nuestra información, como el derecho de propiedad de un inmueble, almacenan información muy valiosa y confidencial, lo que puede suponer un riesgo, al dejar que un tercero sea propietario de información personal. En muchas ocasiones, estas organizaciones disponen de más información de la que necesitan para verificar la identidad, pudiendo regalar información extra a las entidades que solicitan información. ¿Deberíamos descentralizar esta información y únicamente permitir que el usuario sea el que decida a quién enseñarle qué información? ¿Podría existir un entidad descentralizada encargada de llevar a cabo la identidad digital?

Actualmente, la tecnología ha ayudado y fomentado al hombre en su día a día. Es por esta razón, que debemos recurrir a la tecnología para intentar solucionar ese mundo tan oscuro de los derechos de aprovechamiento por turnos de bienes inmuebles permitiéndonos mejorar todas las cuestiones planteadas previamente.

***1.2 SOLUCIÓN PROPUESTA***

Tal como se ha mencionado, existen diferentes opciones para disfrutar de un apartamento en régimen turístico. Sin embargo, aparecen distintos problemas; la inexistencia de una plataforma con transparencia donde se especifiquen los requisitos de

17

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

forma clara, como la gestión de suministros, cuotas de mantenimiento, acceso de servicios, o la duración del contrato, o la inexistencia de la posibilidad de compartir una vivienda sin la necesidad de tener una gestión económica tan elevada y de ser parte propietaria. Con el fin de solucionar los inconvenientes mencionados, se propone la realización de un sistema descentralizado, en el que se realice un aprovechamiento por turnos de inmuebles por distintos copropietarios a través de la realización de una aplicación descentralizada (*Dapp*) que ejecute *Smart Contracts*, basado en la emergente tecnología *Blockchain* en una red de pruebas de *Ethereum*: *Rinkeby*.

Al realizarlo a través de *Smart Contracts*, cláusulas contractuales ejecutadas automáticamente, se resuelven los problemas mencionados, y también se deposita confianza en el usuario, se produce una reducción de costes al disminuir los intermediarios y la automatización de pagos. Además, la tecnología *Blokchain* sobre la que se basa, permite verificar y validar la identidad del usuario para evitar suplantación de identidad, validar y verificar que no se ha alterado la información a través de algoritmos de consenso dispuestos en cada uno de los nodos de la red. Esta tecnología se basa en criptografía por lo que reduce el número de ataques y vulnerabilidades a la información almacenada. También, la *Dapp* permitirá al usuario una mayor comodidad y sencillez al poder almacenar sus claves criptográficas en una *Wallet*, así como confiar en la detección de errores y mejoras de la aplicación a través de un consenso al ser un sistema transparente de código *Open Source*, evitando estafas al estar controlada por muchos ojos.

Asimismo, si el comprador necesita un préstamo, la plataforma dispondrá de una sección para indicar qué condiciones e intereses está dispuesto a aceptar para que el prestamista acepte la entrega de la cantidad con la condición de que el prestatario la devuelva, cumpliendo las condiciones. Al realizarlo a través de esta majestuosa tecnología, proporciona una gran transparencia, inmutabilidad y rapidez al compararlo con el proceso de una hipoteca, así como la reducción de los gastos que conlleva.

También, para mejorar la eficiencia en los seguros de hogar, se realizarán las pólizas a través de *Smart Contracts* simplificando el flujo entre asegurador y asegurado, quedando registrados todos los posibles fraudes para poder evitarlos. El asegurador optimiza su intercambio de información y automatizar las pólizas en función de los

18

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

parámetros de caracterización del perfil de riesgo reduciendo las pérdidas por fraude. El asegurado tiene un notable mejoría en la experiencia del cliente al ser un proceso más simplificado y transparente

Actualmente, *Blockchain* tiene muchas puertas por abrir, al igual que sucedió en su momento con *Internet*, *Amazon* o *AirBnB*. A pesar de ciertos detractores acerca de la estabilidad y especulación de sus monedas, en los últimos días se ha visto como *Bitcoin* ha vuelto a resurgir después de la fuerte caída que tuvo, suponiendo este hecho un gran impulso para la tecnología. [8] Por ello, se pretende modificar el enfoque de los alojamientos turísticos, seguros y bancos a través de esta tecnología descentralizada.

En este documento, se presenta la información necesaria para comprender la seguridad, inmutabilidad y transparencia de la tecnología *Blockchain* junto a las herramientas que se han utilizado para implementarla. Además, se muestra el desarrollo del caso de uso clave planteado para esta tecnología junto a los posibles avances y mejoras de la emergente tecnología.

19

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

**Capítulo 2. DESCRIPCIÓN DE LAS TECNOLOGÍAS**

En este apartado se describen las tecnologías que han sido utilizadas a lo largo del desarrollo del proyecto; ya haya sido durante la fase de comparativa de las distintas tecnologías, o bien en la construcción de la plataforma descentralizada que se ha apoyado en el uso de *Smart Contracts*. Posteriormente, en el Capítulo 8. se observará la conexión e integración de las tecnologías utilizadas en el proyecto.

***2.1 ETHEREUM***

La idea de la plataforma de *Ethereum* fue concebida por Vitalik Buterin, un programador con nacionalidad ruso-canadiense. Sin embargo, el proyecto actual ha sido cofundado por Vitalik Buterin, Mihai Alisie, Anthony Di Lorio, Charles Hoskinson, Dr. Gavin Wood y Joseph Lubin. Buterin publicó el documento amarillo de Ethereum (donde los desarrolladores utilizan de referencia) y Mihai Alisie fundó *ConsenSys*, una compañía centrada en aplicaciones descentralizadas que resuelve problemas reales para organizaciones. [9]

*Ilustración 5: Logo Ethereum*

*Ethereum* surgió para una funcionalidad similar a *Bitcoin*, aunque para solucionar algo más complejo; permitir realizar una plataforma descentralizada donde se ejecutan *Smart Contracts*. Ethereum es la plataforma y *Ether*, *ETH* es su criptomoneda.

Las redes de *Ethereum* son creadas para transferir dinero y guardar información, y permiten crear interesantes aplicaciones. Hay muchas redes de *Ethereum*, algunas solo sirven para hacer código de prueba y transacciones de pruebas. De hecho, cada uno puede

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

crear su red privada de *Ethereum* en el ordenador y ser restringida o abrirla a más personas.

Se ha utilizado *Ethereum* en vez de *Bitcoin* porque la velocidad de las transacciones de *Ethers* es mucho mayor que la de *Bitcoins*, los *Smart Contracts* se encuentran integrados en la plataforma a diferencia de *Bitcoin* que precisa un software externo. También, cabe destacar que a diferencia de *Bitcoin* no existen límites de *Ethers*

y la recompensa por minería es mayor. [10] El proceso de minado en *Ethereum* al principio trabajaba a través de *Proof of Work* pero al tener un gran coste, la comunidad de *Ethereum* quiere explotar *Proof of Stake* al mejorar económicamente el proceso.

Las redes *Ethereum* están formadas por nodos, es decir, una máquina con conexión a *Ethereum* y software. Cada nodo funciona en un cliente *Ethereum* y cada uno tiene la copia de la información de la *Blockchain*. En *Ethereum*, el poder reside en cada uno de esos nodos pues es lo que permite no depender de un agente externo ya que la información se almacena encriptada de forma inmutable y segura. Además, *Ethereum* tiene un código open source y lo cambios de mejoras se deben llevar con el consenso de la mayoría se conocen como EIP: *Ethereum Improvement Proposal*.

***2.2 SOLIDITY***

Los *Smart Contracts* se desarrollan en el lenguaje de programación llamado *Solidity* en *Ethereum*. Es un lenguaje que se ha desarrollado en exclusiva para ejecutar los *Smart Contracts*. En el caso de otras plataformas se utilizan lenguajes de programación distintos como *C++, Golang, Ivy-lan* o *Javascript*, entre otros. [11]

Muchas veces se compara con el lenguaje *Javascript* al tener una sintaxis similar, aunque difieren en otros aspecto como que *Solidity* está fuertemente tipado.



*Ilustración 6: Logo Solidity [12]*

22

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

*Solidity* está en constante desarrollo y avance, es por ello que se puede especificar la versión que se utiliza en la parte inicial de cada fichero, para utilizar el compilador acorde a esto. Al no ser *Solidity* lo que se ejecuta en la red *Ethereum*, necesitamos un compilador. El compilador de *Solidity* lanza dos ficheros:

− ABI: *Application Binary Interface,* que se usa para trabajar con *Javascript* . Es similar a la *API* de las páginas web, es la parte que se utiliza para interactuar la *Dapp* con los *Smart Contracts.* Es similar a un interfaz para conectar el código de bytes real con *Javascript*.

− El código de bytes real: lo que se implementa en la red *Ethereum*

*Solidity* tiene la ventaja de proporcionar un medio confiable y seguro entre ambas partes. También, permite realizar herencia a distintos niveles. Otras función muy importante a destacar es que permite comunicarse con funciones seguras a través de *ABI*. Además, facilita la creación de bucles para los cuales se ha implementado un límite de *Gas* que se puede consumir en una transacción para evitar que sean infinitos.

La desventaja de este lenguaje radica en que no se puede modificar el contrato que se realizó puesto que se basa en la inmutabilidad. Otro inconveniente es el constante cambio en el que se encuentra actualmente, puesto que está en constante crecimiento y mejoría, por lo que sus bibliotecas no están consolidadas.

***2.3 TRUFFLE***

*Truffle* es un *framework* muy habitual en cualquier proyecto profesional y está muy documentado. Es una herramienta de línea de comandos que se utiliza para facilitar el desarrollo y ejecución de *Smart Contracts*. *Truffle* permite crear una estructura de proyecto: archivos y directorios, con unos simples pasos. También, facilita la configuración y conexión con la redes *Blockchain*.

23

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

**

*Ilustración 7: Logo Truffle [13]*

Dentro del entorno de Truffle de trabajo se encuentra:

− *Ganache*, que permite la ejecución de pruebas de forma local, tal como se explica en el siguiente apartado.

− *Drizzle*, que facilita la interfaz de usuario en la creación de una Dapp. Se trata de un conjunto de bibliotecas sobre las que se encargan de sincronizar y actualizar la información del *Smart Contract.*

− *Truffle Teams*, que posibilita supervisar el estado de la *Blockchain*. Visualizar el número de bloques creados, la cantidad de *Gas* utilizada, ejecutar test de manera automática, o vigilar eventos son algunas de sus funcionalidades.

*Truffle* aún se encuentra en desarrollo por lo que algunas funciones sobre *Truffle* no funcionan bien, por lo que es importante mantener la última versión.

***2.4 GANACHE***

Las redes están hechas por uno o más nodos. Un nodo es un máquina que corre un cliente *Ethereum*. Un nodo lo puede crear cualquiera, lo único que hay que hacer es encender el ordenador, descargar el software del cliente y conectarlo a la red *Ethereum*.

*Ganache* es un simulador del *Blockchain* de forma local, por ello no se tiene que pagar y se puede probar rápidamente. Por lo tanto, *Ganache* permite simular un nodo de Ethereum, aunque sin descargarte toda la *Blockchain* existente, a diferencia de *Geth* (cliente *Ethereum*), que es más lento y necesita bastantes recursos para su ejecución.

24

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

**

*Ilustración 8: Logo Ganache [14]*

Cada transacción hecha en *Ganache* se guarda por defecto en la memoria. En el momento que reseteas, se pierde todo en *Ganache*. Se está modificando esto para que en *Ganache 2* exista un *workspace* sobre el que trabajar. [15]

*Ganache* pertenece al *framework Truffle*. Existe la opción de utilizar *Ganache-cli*, que se utiliza a través del editor y la ventana de comando para ejecutar, compilar, probar y desplegar *Smart Contracts*, siendo un inconveniente su interfaz. Por ello, se ha trabajado de manera visual con *Ganache* tal como aparece en la Ilustración 9.

*Ilustración 9: Aplicación Ganache*

*Ganache* al ser una simulación de *Blockchain* en local, permite la creación de diferente número de cuentas, ajustar el puerto local, indicar el saldo de la cuenta, ver las diferentes transacciones realizadas, así como importar las diferentes cuentas a *Metamask*

25

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

a través de su clave privada. Por tanto, permite inspeccionar el funcionamiento de *Blockchain* y un control avanzado sin ningún coste para la fase de pruebas realizada antes de la implantación.

*Ganache* tiene la desventaja de que no es exactamente igual que la red principal *Ethereum* en el tema de la minería. En *Ganache* no hay mineros por lo que el rendimiento y rapidez de la red puede variar. El segundo inconveniente es que el límite de *Gas* de la red principal *Ethereum* puede ser modificado por los mineros, mientras que en *Ganache*

no ocurre.

***2.5 ENTORNO DE DESARROLLO***

Se presenta un análisis de los entornos de desarrollos posibles a emplear para seleccionar los recursos más apropiados:

**2.5.1 REMIX IDE**

Es un editor de texto con compilador realizado en el navegador que permite crear *Smart Contracts* de *Ethereum* en *Solidity*. Las ventajas que posee es que es muy sencillo de utilizar y posee una buena interfaz, como puede observarse en la Ilustración 10. Los problemas que presenta es que al funcionar sólo en el navegador, no testea correctamente los tiempos de transacciones. [16] Además, a la hora de testear los *Smart Contracts*, es necesario realizar diversos pasos, lo que supone incomodidad en un gran proyecto. A la hora de realizar una *Dapp*, supone una traba añadida, de manera que *Remix IDE* es un buen sistema como inicio a la programación de *Smart Contracts*, pero no es recomendable para realizar grandes desarrollos.

26

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

**

*Ilustración 10: Remix IDE [17]*

**2.5.2 VISUAL STUDIO SOLIDITY**

Es un entorno de desarrollo integrado que actualmente soporta *Solidity,* lo que permite desarrollar más fácilmente a través de diversas herramientas y desplegarlo en la nube de *Microsoft Azure*. Las ventajas que presenta es que se puede desarrollar en una red de pruebas o en la red principal de *Ethereum* y la facilidad añadida de diversas herramientas. Aunque su interfaz no es tan simple como la de *Remix IDE*, también es buena, como puede verse en la Ilustración 11. El gran problema que presenta actualmente es que está en pleno desarrollo y genera muchos problemas de extensiones. [18]

27

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

**

*Ilustración 11: Visual Studio Solidity [19]*

**2.5.3 EDITOR ATOM**

*Atom* es un editor de texto editable que permite tener una visualización de los diferentes paquetes, tal como se muestra en la Ilustración 12, y, unido al plugin *Atom Solidity Linter*, remarca el lenguaje *Solidity*. [20] Además, *Atom* se vincula fácilmente al *framework Truffle*, lo que permite ahorrar mucho tiempo al programador. Su interfaz permite visualizar el proyecto de manera cómoda. Asimismo, posee una gran cantidad de paquetes que se instalan fácilmente junto a gran cantidad de información. También, se puede personalizar diferentes paneles de visualización.

28

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

**

*Ilustración 12: Atom Editor*

**2.5.4 COMPARATIVA**

Es difícil, tomar la decisión correcta sobre el IDE de desarrollo, puesto que al no estar afianzadas, hay que enfrentarse a los diversos problemas que surgen en el uso de cada uno de ellos.

Como se quiere realizar el despliegue de una *Dapp* en la red de pruebas *Rinkeby*, se descarta la utilización de *Remix IDE* por complicar los pasos.

Respecto al trío *Atom-Truffle-Ganache* frente a *Visual Studio Solidity*, destaca el primero, a pesar de que su utilización es más compleja, permite una gran cantidad de

29

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

pruebas requeridas en este tipo de proyectos donde no funcionar como debe implica, muchas veces, un gran gasto económico.

En la tabla que se muestra a continuación, se han valorados distintos aspectos que caracterizan a los entornos de desarrollo. Estas características a valorar son cómo se integran todas las funcionalidades que se pueden llegar a obtener, la facilidad de desarrollo que muestra el entorno y la simplicidad del programa, la curva de aprendizaje a la que hay que enfrentarse, la facilidad y exactitud con la que se pueden analizar las transacciones de la red Ethereum desde la propia interfaz y por último la estabilidad que muestra en el mercado cada uno de estos entornos de desarrollo. Se han evaluado desde Muy Bajo en el peor de los casos hasta Muy Alto.

| ***Remix IDE*** | ***Microsoft Visual Studio Atom Editor*** |
| --- | --- |
| Muy Bajo | Alto |
| Medio | Alto |
| Bajo | Medio |
| Medio | Muy Alto |
| Medio | Bajo |

Integración Medio

Facilidad de desarrollo

Curva de

aprendizaje

Análisis de transacciones

Muy Alto Medio

Muy Alto

Estabilidad Alto *Tabla 1. Comparativa entre entornos de desarrollo*

***2.6 METAMASK***

*Metamask* es un *plugin* del navegador que facilita interactuar con la red de pruebas sin la necesidad de ser un desarrollador. *Metamask* es una cartera digital donde almacenar los *Ethers* a través de las claves de las cuentas. Se guardan de manera segura, puesto que acumula las claves en el navegador del usuario en vez de servidores remotos. A diferencia

30

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

de otro tipo de cuentas, como el email, una cuenta de *Metamask* se utiliza para todas las redes de Ethereum : red principal *Ethereum, Rinkeby, Ropsten, Kovan, Goerli*, y también a nivel local.

*Metamask* permite crear cuentas, importar cuentas a través de la clave privada y conectar con un monedero físico como *Ledger* o *Trezor*. En *Metamask*, al realizar las transacciones se indica el *Gas* que se utiliza para poder decidir sobre aceptarla o rechazarla.

*Metamask* se utiliza en la *Dapp* para que el usuario sin nociones de programación pueda realizar transacciones (enviar dinero, almacenar datos…) a través de una interfaz sencilla.



*Ilustración 13: Logo Metamask [21]*

Se ha preferido utilizar *Metamask* en lugar de *Mist Browser* para interactuar en la red *Ethereum* por encontrarse en una fase de desarrollo más avanzada.

***2.7 WEB3.JS***

A la red *Ethereum* se puede conectar a través de *Metamask*, que está disponible para cualquier usuario, o a través de *Web3.js*, que es recomendable para ser utilizado por programadores. *Web3.js* es un conjunto de bibliotecas que permite conectar las transacciones: enviar y recibir *Ether*, leer y escribir información en *Smart Contracts*, o la creación de *Smart Contracts* entre otros.

En el proyecto se ha utilizado para desarrollar un cliente que se relacione con la red Ethereum. Es decir, leer y escribir datos del servidor web (*npm lite server*), y leer y escribir en la red *Ethereum*. En el caso de enviar ciertos *Ether* a una dirección, primero

31

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

se envía al servidor *backend*. Este servidor utiliza la librería *Web3.js* para interactuar con cualquier red *Ethereum*, no solamente la red de *Ethereum* principal. El servidor *backend* utiliza esta librería *Web3.js* para crear lo que se llama el objeto transacción.



*Ilustración 14: Logo Web3.js*

***2.8 ETHERSCAN***

La herramienta *EtherScan* posibilita buscar la transacción realizada en la distintas redes de *Ethereum*, facilitando la transparencia, al ser externo a la *Fundación Ethereum*, permitiendo la indexación y la búsqueda de todas las transacciones en *Ethereum*. [22]



*Ilustración 15: Logo Etherscan [23]*

En Ilustración 16 se muestra arriba del todo la zona de búsqueda, en la que se puede buscar cualquier transacción, cualquier número de bloque, *token* o cualquier *hash*.

32

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

**

*Ilustración 16: Transacción Etherscan [24]*

***2.9 NODE.JS***

*Node.js* es un lenguaje de servidores que tiene diversas librerías. Es una herramienta de código abierto que posibilita ejecutar *Javascript* en el lado del servidor. Funciona para varias plataformas: *Windows*, *Mac OS x*, o *Linux* entre otros. [25]

 **

*Ilustración 17: Logo Node.js [26]*

*Ilustración 18: Logo Lite-server [27]*

*Node.js lite-server* es un servidor de desarrollo local permite, a la hora de realizar la *Dapp*, que los cambios se actualicen rápidamente respecto a los ficheros *Javascript*, c*ss* y *html*; es decir, que se recargan automáticamente. Para poder funcionar el servidor, se necesita tener previamente instalado *node.js*.

33

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

En el directorio del proyecto, se necesita instalar el servidor, y, tras la instalación, se abrirá automáticamente en el navegador la página *localhost:3000*. Dentro de la configuración del directorio del proyecto, se puede modificar diferentes parámetros, como por ejemplo, el puerto.

***2.10 RINKEBY***

Las redes *Ropsten*, *Kovan* y *Rinkeby* son todas redes de prueba. Estas redes se utilizan para probar código y obtener *Ether* gratuito para probar los *Smart Contrats*.

La red *Ropsten* ofrece *Proof Of Work*. En cambio, *Kovan* y *Rinkeby* ofrecen *Proof of Address*, que permite que no sean vulnerables a los ataques de spam. *Kovan* solamente soporta *Parity*, mientras que *Rinkeby* soporta *Geth*. Por ello, a pesar de tener un tamaño de almacenamiento menor *Rinkeby* que *Kovan*, ha sido elegida *Rinkeby* para implementar los *Smart Contrats* de prueba, puesto que no es necesario gastar dinero para realizar. [28]

En la Ilustración 19, se observa el estado de la red *Rinkeby*. Además, en su página web se posibilita obtener dinero en *Rinkeby*, a través de la publicación del número de cuenta a través un tweet y con un tiempo limitado para evitar saturar la red.

34

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

**

*Ilustración 19: Rinkeby estado de la red [29]*

***2.11 INFURA***

En el caso de realizar la implementación de la *Dapp* a nivel local, se ha utilizado *Ganache*, nodo de desarrollo local. Para poder hacer la implementación de la *Dapp* en una red de pruebas como *Rinkeby*, se utilizará *Infura*. Se ha decidido utilizar *Infura* en vez de *Geth*, puesto que *Geth* es un nodo que se instalaría de forma local, pero debe estar perfectamente sincronizado y actualizado para no ocasionar problemas. *Como Infura* es un clúster de nodos de *Ether*, se utiliza un nodo remoto de *Infura* en el proyecto para la implementación en la red de pruebas *Rinkeby*, para evitar los problemas de tener desactualizado las versiones con las bases de datos de los nodos si tuviera un nodo local instalado, así como para evitar problemas de capacidad de procesamiento.

En definitiva, *Infura* tiene una *API* donde *Web3.js* puede interactuar con la infraestructura de *Ethereum* con igual nivel de seguridad que si fuera en un nodo local. Además, la seguridad de *Infura* también reside en que sus claves privadas no son

35

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DESCRIPCIÓN DE LAS TECNOLOGÍAS*

almacenadas ni administradas por esta infraestructura, si no que se encarga un proveedor de *HD Wallet*.



*Ilustración 20: Logo Infura [30]*

36

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*INTRODUCCIÓN*

**Capítulo 3. ESTADO DE LA CUESTIÓN**

En los años 80, surgieron derechos de aprovechamiento por turno de bienes inmuebles, especialmente de uso turístico. Es decir, disfrutar de forma anual durante un período de ese inmueble durante un número determinado de años, gestionado por una promotora que indica las condiciones de cuota inicial, mensual y mantenimiento. Debido a las altas cuotas de gestión, engaños, fraudes por falta de regulación, imposibilidad de asistencia en el período otorgado, entre otros, han hecho que sus servicios hayan disminuido. [31]

Las viviendas de aprovechamiento por turnos de bienes se encuentran a cargo de una promotora o gestora. Esto supone unos elevados costes junto al mantenimiento anual de los mismos. Estas viviendas no pertenecen a los “copropietarios”, sino a la empresa gestora que se encuentra detrás de esto. [32] [33]

Actualmente, existen diferentes plataformas de software centralizado dedicadas a la oferta de alojamientos de alquiler turístico con impuestos de coste de gestión y sin opción de pertenencia a la vivienda, como *Airbnb*, fundada en 2007, o *HomeAway*, fundada en 2004, lo que supone un beneficio para el propietario del inmueble y la plataforma. [34] La plataforma más utilizada en España es *Airbnb*. *Airbnb* ingresa el 3% de comisión de cada reserva de los anfitriones, y en torno al 8% de los huéspedes. Los turistas suelen elegir *Airbnb* frente a un hotel por tener distintas prestaciones como cocina, piscina privada, lavadora… y por lo general un precio inferior al hotel. Los anfitriones prefieren alquilarlo de este modo que un alquiler anual para poder disfrutar ellos también de la vivienda y obtener una rentabilidad de alquiler mucho mayor.

Respecto a la tecnología, se ha de mencionar en orden cronológico la manera de realizar contratos. En primer lugar, los contratos no iban unidos a ninguna tecnología y se redactaban en lenguaje humano. Más tarde, surgen los contratos ricardianos, en los años 90. Son acuerdos fundamentados en un lenguaje informático vinculado a un lenguaje humano, permitiendo ser auditable por ambos, puesto que se ocupa de registrar las acciones e intenciones sin concernirle su ejecución. [35]

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

Más tarde, de la mano de Nick Szabo, se definió el concepto de *Smart Contract* en 1995 aunque la tecnología *Blockchain* surgió catorce años después. Los *Smart Contract s*on cláusulas contractuales programadas para ejecutarse automáticamente que no pueden ser detenidas. [36] El nombre otorgado ha recibido retoques de su pensador, Nick Szabo y de Vitalik Buterin, autor de la primera *Blockchain* con *Smart Contracts*.

*“Smart contract" is a very useful concept & phrase. “Smart” as in “smart phone” (shorthand for computerized phone), “contract”*

*meaning it does some important things we previously relied on*

*contracts to do for our deals, especially controlling assets &*

*incentivizing performance.*

*That said, if your dApp/persistent script doesn't control assets or,*

*short of invoking traditional law, incentivize performance, it's not a smart contract and you should call it something else.*

*Worrying about whether a smart contract is “legally enforceable” reflects a profound misunderstanding. The main relation of smart*

*contract to traditional courts is that smart contracts control burden of lawsuit. If "possession is 90% of the law”, then a good smart*

*contracts may be “99% of the law. – Nick Szabo [37]*

*To be clear, at this point I quite regret adopting the term “smart*

*contracts”. I should have called them something more boring and*

*technical, perhaps something like “persistent scripts” – Vitalik*

*Buterin [38]*

***3.1 BLOCKCHAIN RESPECTO AL CASO DE USO EN ESPAÑA***

Los sectores manejados en el caso de uso implementado en este proyecto corresponden al sector inmobiliario, al sector de la banca y al sector de los seguros. Por ello, se hará un repaso acerca de la tecnología *Blockchain* que existe en cada uno de ellos en España.

38

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

En España, están surgiendo diferentes soluciones utilizando *Blockchain* acerca de los inmuebles:

− *ProntoPiso* es una agencia inmobiliaria online que garantiza la venta de la vivienda en España en un período determinado, adelantando parte del importe de la transacción al propietario. [39] En octubre de 2018, *ProntoPiso*, con la tecnología proporcionada por *JLL*, comienza a realizar las tasaciones de viviendas a través de *Blockchain*, ahorrando costes y tiempo, simplificando el proceso de verificación y garantizando la seguridad de los datos. [40]

− En noviembre de 2018, la empresa española dedicada al negocio inmobiliario, *Metrovacesa*, ha lanzado sobre *Blockchain*, en primer lugar, la contratación de los suministros de la vivienda sobre *Alastria*. *Alastria* es una “red *Blockchain*/*DLT* semipública, independiente, permisionada y neutral, diseñada para ser conforme con la regulación existente, que permite a los asociados experimentar estas tecnologías en un entorno cooperativo” [41] Cabe destacar que el primer nodo universitario de *Alastria* se realizó en la Universidad Pontificia Comillas ICAI

ICADE. [42]

− El segundo lanzamiento de *Metrovacesa* ha sido dedicado a los inversores internacionales en vivienda sobre la red *Ethereum*, con el fin de agilizar el proceso de inversión únicamente a un sencillo paso, en vez de los tres pasos anteriores; oficina internacional, oficina española y promotora. Para ello se ha ayudado de la plataforma de inversión *Brickex* y de la consultora *Grant Thornton*. El proceso consiste en *tokenizar* los inmuebles, es decir, asignar un valor aceptado por una comunidad, y reflejarlos en una cuenta de *Metrovacesa* en *Blockchain*. A través de *Smart Contracts*, liberan los *tokens* cuando se cumplan las requisitos prefijadas en la compra. En caso que no finalice la venta, los *tokens* regresan a la cuenta de *Metrovacesa*. [43]

− El 19 de Marzo de 2019 se presentó en el *Demo Day*, en el campus de *Google* en Madrid la *start up: Real Fund.* Esta empresa se encarga de *tokenizar* los activos

39

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

inmobiliarios con el fin de invertir de forma sencilla en el tradicional sector inmobiliario. Además, cabe destacar que en el *Demo Day* se llevó a cabo la votación de los proyectos a través de *Blockchain*. Sus creadores José García Caballero y Juan Manuel Garrido han comentado la falta de marcos jurídicos completos para los proyectos de *Blockchain* en España. [44]

El sector de la banca en España se encuentra entusiasmado descubriendo y profundizando en posibles soluciones utilizando *Blockchain*. A continuación, se muestras datos relevantes sucedidos.

− En marzo de 2018, el Banco Santander y CaixaBank apuestan en un modelo de negocio que utiliza la tecnología *Blockchain* donde se necesita gran confianza, como es el comercio exterior y los avales internacionales. Además, BBVA comenta que *Blockchain* permitirá reducir costes y aumentar la productividad de procesos. Por otro lado, Bankia no deposita confianza en las criptomonedas por su gran riesgo y volatilidad. [45]

− En abril de 2018, BBVA junto a Indra realizaron el primer préstamo en *Blockchain* dentro de una organización, en este caso fue dentro de la entidad BBVA. [46] En este mismo mes, CaixaBank comenzó sus primeras transacciones en *Blockchain* de comercio exterior dentro de su consorcio *Batavia*. [47]

− En julio de 2018, el Banco Santander comenzó a descubrir *Blockchain* enfocado al mercado de valores, donde cambian *trading* de valores e instrumentos financieros a través de la creación de un equipo de Banca de Inversión Digital. [48] La entidad apuesta en este modelo de negocio que utiliza la tecnología *Blockchain* para aquellos que necesita gran confianza como es el comercio exterior y los avales internacionales. [45]

− En noviembre de 2018, BBVA formó parte del encuentro realizado para el lanzamiento de la *Asociación Internacional para Aplicaciones Blockchain* organizado por la Comisión Europea. El objetivo del encuentro es promover la

40

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

tecnología y facilitar la interoperabilidad entre las diferentes redes y entornos de desarrollo. [49]

− En febrero de 2019, el Grupo Santander, entidad crediticia más grande española, comenzó a focalizarse en reducir sus costes y evolucionar a un mejor aprovechamiento de la tecnología a través de un acuerdo con la entidad IBM que se apoyara en la tecnología *Blockchain*. El acuerdo está pactado en 700 millones de doláres. [50]

En España, están empezando a brotar situaciones de interés acerca de las aseguradoras con la tecnología *Blockchain*:

− A finales de 2017, Axa presentó un modelo en pruebas de un seguro para los vuelos retrasados en la red de *Ethereum*. El *Smart Contract* se encuentra conectado a varias bases de datos aéreas para verificar y validar la información de los vuelos. [51]

− En junio de 2018, Mapfre, aseguradora española de las más antigua que opera en España, comenzó a configurar un equipo de expertos en la tecnología *Blockchain* para proteger la seguridad de las operaciones y los activos de los clientes a través de la integración con otras tecnologías y recursos disponibles. [52]

− En noviembre de 2018, Axa, la primera compañía de seguros mundial, se unió a la red *Blockchain Alastria* para disponer de un entorno seguro y transparente. [53]

− En marzo de 2019, Seguros Santalucía ha premiado a cinco startups que aceleran la economía a través de la tecnología *Blockchain*. NodalBlock fue una de las startup premiadas que tiene relación con la protección de la identidad digital para los clientes de las pólizas; se encarga de proteger la identidad digital, emitir certificados y realizar firmas digitales. [54]

41

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

***3.2 BLOCKCHAIN RESPECTO A LA INFORMACIÓN MANEJADA EN EL CASO DE USO***

La sociedad cada vez se maneja más por internet, dejando información relevante al descubierto que en algún momento podría causarle algún disgusto. La huella digital cada vez es más completa, desde el *GPS* que tenemos en móvil que indica cuánto tiempo pasamos en cada sitio, qué zonas visitamos, el dinero que gastamos a través de tarjeta bancaria, con quién hablamos por *Whatsapp* o por *LinkedIn*, saber si acudiste a una manifestación, o a un acto en contra de una ideología de tu empresa… una cantidad de información que se obtiene a través de diferentes dispositivos como cámaras, móvil, ordenadores, altavoces, robots o radares de tráfico.

*Ilustración 21: Información en descubierto [55]*

Esta información no se puede despreciar, su valor y la explotación de esos datos puede ser muy valiosa. Tener la información minuto a minuto de lo que hace cada persona, de las llamadas que recibe, las que realiza, los mensajes entrantes o salientes, cuánto tiempo pasa en supermercado o en el gimnasio, el tiempo que se encuentra conectado a Internet o usando el móvil, cuando va en coche, equivale a tener un diario automático. Esto sería prácticamente una misión imposible sin los medios y dispositivos

42

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

electrónicos, puesto que ni el mejor espía sería capaz de recopilar tal cantidad de información.

Actualmente la seguridad y la privacidad van de la mano, puesto que un acceso indebido a los datos se convierte en uno de los mayores riesgos. Un ejemplo reciente sucedió en 2018, con la fuga de información de *Facebook* que afecto a más de 87 millones de personas, cuya información se utilizó para influir en resultados electorales y publicidad focalizada. [56]

Tradicionalmente, los organismos certificadores de información se encuentran en manos de una organización. Es decir, un tercero que se encarga de certificar y validar que el servicio o producto se corresponde con lo que se indica. La dependencia de un tercero para validar supone un coste alto y supone exponer información relevante a una entidad en la que confiar.

La tecnología *Blockchain*, es una herramienta muy potente al basarse en la criptografía permitiendo no exponer a la luz datos relevantes y sensibles. Es decir, un sistema de intercambio de información segura.

Una situación cotidiana sucede cuando, en el seguro de contratación de su casa, le realizan una fotocopia del DNI que contiene información de sus padres, fecha de nacimiento, lugar de nacimiento, o dirección entre otros datos, cuando realmente el seguro no necesitaba toda esa información, o el cliente no quería mostrarle toda la información. En cambio, si se utiliza la tecnología *Blockchain* para que solo la información necesaria pueda ser consultada, y la información privada no pueda ser consultada, se estaría reduciendo el peligro de exposición de información sensible, puesto que la información almacenada no depende un tercero que pueda vendernos en cierto momento, sino que se encuentra descentralizada. Es decir, se limitaría esta información a los organismos que contienen la información confidencial.

En la siguiente imagen, Ilustración 22, se muestra como un *DMV* es la entidad que certifica cierta información, en este caso es el DNI. El *DMV* usa claves vinculadas a su identificador descentralizado en la *Blockchain*, firmando la petición para que sea

43

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

inviolable y se sepa que fue emitido por *DMV*. El cliente tiene una *Wallet* para guardar sus solicitudes y puede usar claves vinculadas a un identificador descentralizado que pueda unir a su DNI. Cuando la entidad que necesita verificar, *BAR*, quiere comprobar que es mayor de edad, puede presentar la licencia de DNI. La *BAR* verifica que es cierto y que el *DMV* se la emitió, siendo el usuario el que la muestra. Otra solución, sería la utilización de un *token* para validar que la información ofrecida cumple con los requisitos.

*Ilustración 22: Identidad digital Blockchain [57]*

En mayo de 2018, nace la aplicación *Blockpass* que posibilita verificar la identidad y proteger la información de los usuarios. Se basa en un sistema para almacenar información descentralizada teniendo los usuarios control sobre su identidad digital, siendo estos los que deciden acerca de su identidad. De esto modo, ninguna entidad almacena sus datos confidenciales.

Por tanto, en el momento que un cliente envía datos para verificarse en *Blockpass* a través de plataformas de confianza, se almacena una copia local y se cifra con una contraseña creada por el usuario. Después, *Blockpass* recibe los datos, le realiza un *hash* y los elimina de sus servidores, quedando únicamente disponible para el usuario. De este

44

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

modo si se produjera un ataque en los servidores solo serían datos ilegibles. Así, sólo se compartirán con un tercero cuando el usuario lo desee. [58]

***3.3 BLOCKCHAIN Y LA UNIVERSIDAD PONTIFICIA COMILLAS ICADE-ICAI***

El pasado año 2018, la Universidad Pontificia Comillas se convirtió en la primera universidad en formar parte del consorcio *Alastria*, albergando un nodo de la red. Esta situación animó e impulsó a otras universidades a potenciar la economía española desde la tecnología *Blockchain*. [59]

*Alastria* es un ecosistema formado por diferentes entidades del sector energético, bancario, educativo y jurídico. El propósito de esta creación es generar un estándar que cumpla el marco jurídico español y europeo en el que puedan operar las diferentes entidades. [60]



*Ilustración 23: Logo Alastria [61]*

El pasado 4 de junio de 2019, se produjo la primera jornada de *Blockchain Economía* en la Universidad Pontificia Comillas. En ella se han reunido diferentes ponentes de distintas organizaciones y entidades: Alastria, CNMV, Colegio de Registradores de España, ICADE, Metrovacesa, Bankia, Eurogestión, Everis, Carex Logistics, Vottun, Proteum, ioBuilders, Blockchain Economía y Secretaría General del Tesoro y Financiación Internacional. De los ponentes ha destacado Amanjyot S. Johar, el principal inversor de *Proteum*. [62] *Proteum* es una *startup* de Silicon Valley que se

45

**UNIVERSIDAD PONTIFICIA COMILLAS** ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*ESTADO DE LA CUESTIÓN*

encarga de potenciar y asesorar a las empresas en la tecnología *Blockchain*. Actualmente, Amanjyot S. Joharse encuentra en búsqueda de iniciativas con cierta viabilidad en España para invertir hasta 20 millones de euros. [63]

46

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

**Capítulo 4. DEFINICIÓN DEL TRABAJO**

***4.1 JUSTIFICACIÓN***

Actualmente, a causa de la comodidad para obtener un perfil en internet, los casos de suplantación de identidad han crecido exponencialmente. Estas suplantaciones tienen diferentes objetivos; desde obtener información bancaria o personal hasta la realización de acosos. Para realizar la verificación de identidad, se está apelando de un tercero. Este problema lo soluciona la tecnología *Blockchain*, que facilita la verificación del usuario real para poder firmar la transacción evitando las amenazas y vulnerabilidades del segundo factor de autenticación, al utilizarse métodos criptográficos.

A menudo suele surgir problemas acerca de si ha sido *hackeado* o alterada cierta información. Este hecho es solucionado a través de *Blockchain*, porque la información se almacena como una estructura de datos donde no pueden ser alterados o eliminados, puesto que estos bloques se encuentran con un tiempo marcado al registrar en orden cronológico en diferentes nodos de la red. Además, a la hora de almacenar el bloque existen los algoritmos de consenso (*PoW* o *PoS*) para decidir, validar y verificar el bloque con gran confianza, evitando fraudes. El almacenamiento en diferentes nodos de la red permite no depender de terceros, ser descentralizado y poder recuperar los datos si hubieran sido eliminados en algún punto, similar a disponer de varias copias de seguridad.

Además, los algoritmos de validación de bloques *PoW* o *PoS*, conllevan a que hay mineros que validan esta información. Los mineros perciben retribuciones en *tokens* o *criptomonedas* por validar la información lo que fomenta la utilización de la *Dapp* ya que es el medio de compra o intercambio

Debido a la cantidad de ataques en internet y la gran vulnerabilidad, las compañías hacen hincapié en la seguridad de su almacenamiento de información. Es por ello que *Blockchain* aporta protección a la información al ofrecer la criptografía de clave pública y privada para las cuentas junto a los hashes. Es decir, los datos se encuentran encriptados para

47

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

todo usuario salvo el propietario. Respecto al almacenamiento de gran información, no está contemplado en el almacenamiento de la cadena de bloques. Es por ello que en el momento que se desea una gran información, se debe vincular un archivo al sistema *IPFS* y desde ahí se hará un *hash* al fichero.

Para evitar que se encubra información, la tecnología *Blockchain* es transparente, se posibilita observar la cadena de origen a fin.

Los *Smart Contracts* permiten no estar pendiente constantemente de una transacción y activarse cuando se cumplen ciertos requerimientos para enviar o recibir información o *Ethers*.

En la actualidad al entrar en una página web de compra, sólo confiamos en el pago a través de ella si se hace a través de una pasarela de pago de un tercero. En una *Dapp* se elimina la pasarela de pago realizándose de forma directa, es decir el usuario puede enviar o recibir *Ether* con un gasto muy bajo de *Gas*, lo que supone que sea prácticamente sin comisión.

Los usuarios cada vez que entran en una página web tienen que hacer el esfuerzo de registrarse o recordar su usuario y contraseña, puesto que dispone de innumerables contraseñas. Esta situación se evita con el uso de una *Dapp*, los usuarios no requieren registrarse debido a que con una única *Wallet* que se vincula a la *Dapp* dispones de tu clave pública y privada, sin necesidad de tener que recordar una cadena enorme. Actualmente existen inicios de sesión a través de ciertas redes sociales, y la diferencia es que una *Dapp* es descentralizada, es decir, si una red social deja de existir, podremos dejar de iniciar sesión con ella.

A diferencia de una aplicación actual, el código de una *Dapp* tiene que ser *Open Source*. El código del desarrollo debe estar disponible para mejorarse si se desea, aunque siempre en consenso debe decidirse si es una mejora oportuna. Esto permite crecer de forma exponencial, en comparación con un código que está disponible para un grupo reducido. Además, debe estar disponible la información del *backend*, es decir, los *Smart Contracts*,

48

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

para vigilar que no haya estafas o se robe información facilitando aún más la confianza de los usuarios.

***4.2 OBJETIVOS***

El objetivo principal es poner en práctica unas cláusulas contractuales que se ejecuten automáticamente, y permitan aprovechar inmuebles por turnos entre distintos copropietarios, asegurando una alta confianza entre los distintos copropietarios, y sin la necesidad de intermediarios. Con el propósito de desempeñar este propósito se deberán realizar los siguientes objetivos:

i. **Investigar la tecnología *Blockchain* y su aplicación de *Smart Contracts* con vistas a desplegar el caso de uso en la red de pruebas *Rinkeby***

Al tratarse de una tecnología emergente, se estudia el funcionamiento teórico con fin divulgativo y autodidacta para poder realizar su aplicación adecuadamente, para así ser capaz de realizar un despliegue satisfactorio sobre una red de pruebas de *Ethereum*: *Rinkeby*, donde se explorarán los diferentes intercambios y transacciones.

ii. **Estudiar y comparar las plataformas para la aplicación de *Smart Contracts* con objeto de diseñar, desarrollar y testear el caso de uso.**

Se estudia las plataformas desarrolladas sobre esta tecnología para poder utilizar la más conveniente al proyecto. Tras fijar la solución, se pone en práctica el desarrollo, a través del lenguaje *Solidity*. Tras obtenerlo, es necesario comprobar su funcionamiento, puesto que cualquier modificación en la red *Blockchain* implica un gasto de dinero, por lo que es muy importante asegurarse de que funciona en el modo que se desea antes de implantarlo en la red principal.

iii. **Solucionar el problema de gestión de inmuebles con tecnología *Blockchain***. Se fijan los requerimientos necesarios para la compartición del inmueble y se realiza un estudio legal de la solución. Se buscará el soporte a estas necesidades en la tecnología *Blockchain*.

49

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

***4.3 METODOLOGÍA***

Para poder cumplir los objetivos propuestos, el trabajo se desarrollará a través de la metodología descrita a continuación.

En primer lugar, en la etapa de investigación de la tecnología, se utilizará el método deductivo, puesto que se partirá del estudio de la tecnología *Blockchain* para centrarse después en los *Smart Contracts* de la red *Ethereum*, tanto en su contenido como en la tecnología. Más adelante, se deduce la forma de aplicar un caso de uso en particular de los *Smart Contracts*. [64]

Por otra parte, al tratarse de un proyecto individual basado en una tecnología emergente, debe considerarse la facilidad para poder adaptarlo a condiciones cambiantes de la tecnología empleando metodologías ágiles. Para ello, se va a utilizar la herramienta *Kanban,* que permite desmenuzar en una serie de pasos el proyecto para lograr el objetivo principal.

*Kanban* se basa en los siguientes principios:

i. Flujo de trabajo: visualizar lo que se realiza a diario.

ii. Limita la cantidad de trabajo que se puede realizar.

iii. Mejora el flujo: cuando se acaba una tarea, la siguiente tarea más importante que se encuentra atrasada se pone en marcha. [65]

Para poder realizarlo se utiliza una herramienta muy visual y sencilla: *Trello*, tal como se muestra en la Ilustración 24.

50

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

**

*Ilustración 24: Kanban utilizado a través de Trello*

Las tarjetas visuales se utilizarán con los siguientes fines:

• **Backlog**: lista de tareas que se deben realizar. Aparecer arriba del todo de la lista significa que se tiene que realizar con prioridad respecto a las que se encuentran en un lugar inferior.

• **To Do:** son las tareas que se mueven de *Backlog* a esta porque se han decidido realizar ahora, ya que se ha determinado que es el momento y se pueden conseguir realizar correctamente.

• **Doing**: tareas sobre las que se está trabajando. Son las tareas que al comenzarse a realizar pasan de encontrarse en *To Do* a esta lista.

• **Done**: son las tareas que ya se han completado. [66]

51

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

***4.4 PLANIFICACIÓN***

Dado que se dispone de un plazo limitado y un alcance relativamente cerrado en la

realización del proyecto, se muestra en la Ilustración 25, a modo informativo, el tiempo que se fijó al principio del mismo a la dedicación de las diferentes tareas para conseguir los objetivos marcados, a través de un diagrama de Gantt.

*Ilustración 25: Diagrama de Gantt del proyecto*

52

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

Tras finalizar el proyecto, se ha podido cumplir las tareas marcadas tal como se detalla a continuación:

En primer lugar, se definió el diseño y el alcance del proyecto para poder hacer frente a los costes, recursos, plazos y tareas.

Tras fijarse el alcance, se profundizó en la nueva tecnología de *Blockchain* tal como se detalla en las subtareas del *Kanban*: almacenamiento en *Blockchain*, ventajas de *Blockchain*, algoritmos de consenso de las redes *Blockchain*, *Smart Contratcs*, *Tokens*, *Dapp* entre otros.

Más tarde, se estudió y se aplicaron las tecnologías y herramientas de *Blockchain: Solidity, Truffle, Ganache, Metamask, Web3.js, Etherscan, Node.js, Rinkeby, Infura* y el entorno de desarrollo. De forma paralela al estudio, al tener ciertos conocimientos se decidió fijar la funcionalidad y el análisis del sistema detallando en diferentes casos de uso, diagramas de secuencia y diagrama de actividad.

Finalmente, la aplicación se diseñó y desarrolló de forma iterativa en un nodo local a través de *Ganache* para realizar las pruebas oportunas y comprobar su correcto funcionamiento. Además, en esta fase se decidió ampliar el objetivo de la planificación desarrollando una interfaz para poder interactuar cualquier tipo de usuario con los tres *Smart Contracts.* Tras funcionar adecuadamente, se desplegó en la red de pruebas *Rinkeby* de *Ethereum* a través de *Infura* para evitar desagradables problemas con la sincronización y actualización de los nodos.

Durante la realización del proyecto, se han establecido reuniones de seguimiento y encauzamiento del avance del mismo con los directores.

53

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

***4.5 ESTIMACIÓN ECONÓMICA***

En el apartado se presenta la estimación del coste económico del desarrollo del proyecto. En primer lugar cabe destacar que todas el software utilizado ha sido gratuito, por lo que el coste viene dado por el tiempo dedicado al proyecto de cada uno de los miembros del equipo.

A continuación, se presentan detalladas las tareas realizadas por el analista en el proyecto junto a sus horas para poder tener una vista completa del tiempo empleado.

***Tarea Horas***

Definición del proyecto 20

Síntesis y documentación de tecnología *Blockchain*

60

Comparativa técnica entre tecnologías 20 Aprendizaje y aplicación de *Solidity* 40 Análisis y gestión de inmuebles 55 Estudio y uso de *Metamask* 10 Estudio y uso del entorno de trabajo 32 Estudio y uso de *Truffle* 9 Estudio y uso de *Ganache* 12 Estudio y uso de *Etherscan* 12 Estudio y uso de *Javascript* 15

54

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*DEFINICIÓN DEL TRABAJO*

Despliegue en *Rinkeby* y análisis de las

12

transacciones

Elaboración de la memoria 60

Revisión de la memoria 20

Elaboración de la presentación 15

**Total 392**

*Tabla 2: Análisis dedicado a cada tarea*

Además del analista en el proyecto, se tiene que tener en cuenta el gasto del jefe de proyecto dedicado a las revisiones de documentación y supervisión del trabajo desarrollado. Es por ello que se ha procedido a reflejar en la Tabla 3, el coste de cada uno respecto a sus horas.

| ***Horas*** |
| --- |
| 392 |
| 30 |
|  |

***Integrante Coste/hora***

Analista 60 €

Jefe de proyecto 90 €

**Total 26.220 €**

*Tabla 3: Relación entre tiempo y coste*

Como se ha comentado anteriormente, todo el software utilizado ha sido gratuito, y además, no se ha entregado ningún hardware. Por tanto, el único coste que existe en este proyecto son los 26.220 € de personal.

55

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*BLOCKCHAIN*

**Capítulo 5. BLOCKCHAIN**

***5.1 DESCRIPCIÓN GENERAL***

*Blockchain* es un registro en todo momento de información. Cada bloque contiene un *timestamp* que posibilita ordenarlos cronológicamente y evitar remplazos puesto que cuando pertenecen a *Blockchain*, es muy difícil modificarlos. *Blockchain* es un sistema descentralizado que no depende de terceros. Los intercambios de información se realizan en el sistema, a través de transacciones como enviar y recibir criptomonedas, o realizar *Smart Contratcs* entre otros.

Al ser una tecnología reciente y aún no muy asentada, suele confundirse con el término *Bitcoin*. Cabe destacar que *Blockchain* es la tecnología que se encuentra por debajo de *Bitcoin*. *Blockchain* es imprescindible para poder almacenar o intercambiar *Bitcoins*, es decir, se puede usar *Blockchain* para otras criptomonedas como *Ethereum, Ripple, Litecoin*

o *Dash*.

La información almacenada dentro de cada uno de los bloques que conforman *Blockchain* depende del tipo de *Blockchain*. Existen tres tipos de *Blockchain*:

− ***Blockchain* pública:** cualquier persona tiene permiso para añadir un bloque a *Blockchain* o verificar un bloque. La utilización de las *Blockchain* públicas es gratuito y se recompensa a los mineros que se encargan de validar la información. Cualquier persona puede ver las transacciones, aunque recordando que estas transacciones aparecen de forma anónima.

− ***Blockchain* privada**: algunas personas autorizadas por una organización son las que pueden agregan un bloque a *Blockchain* o verificarlo. A pesar de pertenecer a una entidad para favorecer la transparencia, suele permitirse visualizar las transacciones a todos los usuarios. También, podría cerrarse el acceso a visualizar a todo el mundo.

− ***Blockchain* de consorcio o permisionadas**: surge de la fusión entre pública y privada. La constituyen un grupo de entidades, suelen tener una velocidad mayor al

57

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*BLOCKCHAIN*

tener un conjunto de nodos preseleccionados en varias organizaciones que se encargan de realizar el consenso y no encontrase en una única entidad. Un ejemplo de esta *Blockchain* de consorcio es *Alastria*, formado por importantes compañías, uno de los nodos de *Alastria* se encuentra en la Escuela Técnica Superior de Ingeniería, ICAI. [67]

*Ilustración 26: Nodo universitario Alastria ICAI [67]*

Al estar refiriéndonos a esta tecnología como almacenamiento de información, se puede caer en el gran error de asemejarlo a un almacenamiento compartido. Por ello, es importante señalar las diferencias entre ambos.

− En el caso de *Blockchain* cabe destacar que su replicación se basa en el sistema *P2P, peer to peer*. Se trata de clientes distribuidos que no necesitan un servidor para realizar el intercambio de información. En el momento que una persona desee pertenecer a la red tiene la opción de obtener la información de *Blockchain*

de principio a fin. Es decir, se realiza una replicación completa en cada nodo de la red. En el momento que se quiere añadir un bloque , cada nodo tiene que comprobar que no ha sido modificado y entre todos realizan un consenso acerca de su validez. Cabe señalar que modificar un bloque correctamente supone

58

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*BLOCKCHAIN*

modificar todos los bloques de la cadena y volver a realizar el algoritmo de consenso, *PoW* o *PoS*, para cada bloque de la cadena, lo que es prácticamente imposible hacer. En comparación con la base de datos compartida, la replicación se realiza a través de maestro-esclavo, haciendo que los datos del nodo maestro se repliquen en los servidores esclavos.

− Un diferencia muy significativa sucede en que *Blockchain* únicamente puede almacenar información en la cadena, y nunca podrá modificar o eliminar esa información mientras que en la base de datos compartida podrás alterarla.

− A la hora de producirse la validación de bloques es un algoritmo de consenso a nivel de *Blockchain*, por el contrario en la base de datos compartida, se crean reglas de validación, aunque a nivel local.

***5.2 ALMACENAMIENTO EN BLOCKCHAIN***

En el momento que se desea almacenar en *Blockchain* cierta información, se solicita ejecutar una transacción, ya sea a través de *Smart Contracts*, *Dapps* o criptomonedas. La información de la transacción se distribuye a cada uno de los nodos de la red *peer to peer*. Cada nodo se encarga de verificar y validar la transacción a través de los algoritmos de consenso (*PoW o PoS).* Tras verificar el correcto funcionamiento, se agrega el nuevo bloque a *Blockchain* donde no puede ser ya modificado.

Cuando creas una cuenta de *Outlook* y otra de *Gmail*, son cuentas independientes. En *Ethereum*, una cuenta se utiliza en todas las redes. Al crear una cuenta se crean tres partes distintas que constituyen la cuenta en la red Ethereum.

− **Dirección de la cuenta**: similar a la dirección de email o el nombre de usuario. Se puede compartir con cualquier persona y permite identifica con el resto. − **Clave pública y clave privada**: se combinan para crear una contraseña. Se utilizan para autorizar el envío de fondos de su cuenta a otras cuentas. La clave privada no se debe compartir nunca. Estas claves tienen una longitud muy grande, pues todo se almacena en hexadecimal, por ello se almacenan en *Wallet* digitales.

59

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*BLOCKCHAIN*

Al crear una cuenta sirve la misma dirección para todas las redes y sabemos que no se almacena en todas los *Ethers*. Esta información se indica en el *backend* de la aplicación tal como se detalla a continuación: en el *backend* se utiliza la librería *web3* para crea el objeto transacción y este objeto se envía a la red que hayamos indicado en el *backend*. En este proyecto se ha utilizado *Rinkeby*. Tras enviarse, se debe esperar a que el nodo que le ha llegado junte las transacciones que ha recibido, puede ser la que se está enviado y la de otros tres usuarios diferentes, y con todos ellos forme un bloque. La validación del nodo requiere tiempo pues necesita ciertos cálculos para resolver el algoritmo, proceso conocido como minería (*PoW*) o forjado (*PoS*). Es conveniente recordar que la red se comunica con un nodo y este con el resto de nodos. Finalmente, se produce correctamente y se devuelve un mensaje de éxito al navegador

A continuación, se analizan los parámetros de ese objeto transacción que es donde se indica los fondos que se envían de dinero junto a otras propiedades. Se crea una transacción siempre que haya un intercambio de dinero.

− ***Nonce***: es un cálculo que se lleva a cabo a través de los algoritmos de consenso para que de acuerdo a la información del bloque el hash comience por 0000. Es decir, los mineros intenten obtener el valor correcto en la red para obtener una retribución y un nuevo bloque.

− ***To*:** es la dirección a la cuenta donde se enviará cierta cantidad de *Ether.* − ***Value***: la cantidad de *Ether* que se quiere enviar desde el emisor.

− ***gasPrice****:* cantidad de *Ether* que el emisor está dispuesto a pagar por unidad de gas para procesar esta transacción.

− ***startGas/gasLimit****:* unidades de gas que la transacción consume.

60

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*BLOCKCHAIN*

− ***v,r,s***: son propiedades criptográficas generados para dar seguridad a la transacción. Los tres valores se usan para generar la dirección de la cuenta de la persona que hace

el intento de enviar el dinero. Si tienes la clave privada puedes generar v, r y s; pero

si tienes v, r y s **no** puedes generar la clave privada

A través de la aplicación creada por Anders Brownworth, se muestra el

funcionamiento de *Blockchain*. [68]. En primer lugar, a primera vista el hash se podría pensar que son números aleatorios. En cambio, es la huella digital de los datos digitales y es única en cada bloque. El hash reconoce tanto el bloque como su contenido. Si escribo en el bloque distinta información, el hash cambia. Por lo tanto, el hash es muy ventajoso cuando se quiere dar cuenta sobre si se han producido cambios; es una de las razones por la que *Blockchain* se considera inmutable.

En la Ilustración 27, la imagen de la izquierda muestra el hash y texto vacío. En la

imagen de la derecha, al escribir información, se observa como el hash se modifica.

*Ilustración 27: Hash, la huella dactilar digital [68]*

Al no tratarse de un bloque, sino que únicamente se observa el funcionamiento del

hash, no tiene por qué empezar por 0000. En la Ilustración 28 se puede identificar cómo el

61

**UNIVERSIDAD PONTIFICIA COMILLAS**

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI) GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

*BLOCKCHAIN*

bloque que no contiene información aparece firmado, mientras que en la imagen de la derecha se ha incluido información que aún no está firmada. Para ello, habrá que minarlo.

*Ilustración 28: Se cambia información del bloque, hash no comienza por 0000 [68]*

Tal como se aprecia en la Ilustración 29, después de minar el bloque, el hash

comienza por 0000 indicando que el bloque está firmado. A través de los algoritmos de consenso se ha configura un nuevo *nonce*.



*Ilustración 29: Tras minar el bloque, hash comienza por 0000 [68]*

62