Título

PABLO Blanco Peris

Máster en INGENIERÍA Informática, Facultad de Informática,

Universidad Complutense de Madrid



Trabajo Fin de Máster en Ingeniería Informática

Fecha

Director:

Adrián Riesco Rodríguez

Autorización de Difusión

Pablo Blanco Peris

Fecha

El abajo firmante, matriculado/a en el Máster en Investigación en Informática de la Facultad de Informática, autoriza a la Universidad Complutense de Madrid (UCM) a difundir y utilizar con fines académicos, no comerciales y mencionando expresamente a su autor el presente Trabajo Fin de Máster: “TÍTULO”, realizado durante el curso académico 20XX-20XX bajo la dirección de XXXX [y con la colaboración externa de dirección de YYYY] en el Departamento de Sistemas Informáticos y Computación, y a la Biblioteca de la UCM a depositarlo en el Archivo Institucional E-Prints Complutense con el objeto de incrementar la difusión, uso e impacto del trabajo en Internet y garantizar su preservación y acceso a largo plazo.

Resumen en castellano

[Enter abstract here, no longer than 350 words. Be sure to retain the Section Break below.]

Palabras clave

Resumen en inglés

[Enter abstract here, no longer than 350 words. Be sure to retain the Section Break below.]

Keywords

Índice de contenidos

[Autorización de Difusión ii](#_Toc8680869)

[Resumen en castellano iii](#_Toc8680870)

[Palabras clave iii](#_Toc8680871)

[Resumen en inglés iv](#_Toc8680872)

[Keywords iv](#_Toc8680873)

[Índice de contenidos 1](#_Toc8680874)

[Agradecimientos 2](#_Toc8680875)

[Chapter 1 - Introducción y motivación 3](#_Toc8680876)

[First-level Subhead (Heading 2 style) 3](#_Toc8680877)

[Second-level Subhead (Heading 3 style) 3](#_Toc8680878)

[Figures and Tables 4](#_Toc8680879)

[Chapter 2 - Preliminares 5](#_Toc8680880)

[Blockchain 5](#_Toc8680881)

[Tipos de blockchain 7](#_Toc8680882)

[Ethereum 10](#_Toc8680883)

[Chapter 3 - Diseño e implementación 12](#_Toc8680884)

[Chapter 4 - Demo 13](#_Toc8680885)

[Bibliografía 14](#_Toc8680886)

[Chapter 5 - 14](#_Toc8680896)

Agradecimientos

The Acknowledgement page is optional. If you include it, retain the Acknowledgements heading and enter your text here. If you do not include it, delete the entire page. Be sure to retain the Page Break that occurs after the List of Table page above.

# Introducción y motivación

desarrollar una aplicación móvil, concretamente para sistemas operativos iOS y que pretende útil y estable que proponeque puede ser utilizada a día de hoy en un ámbito concreto.

El sistema que se presenta en este proyecto consiste en una plataforma completa que proporciona un servicio de alquiler de coches a través de una aplicación móvil como *front-end*  (que gestiona las interfaces visuales) y un *Smart contract* dentro de la red *blockchain* Ethereum como *back-end* (que se encarga de la gestión de la información).

## Figures and Tables

Sample figures and tables are included in this template to show how they automatically generate entries in the List of Figures and List of Tables. For each figure and table in your document, you will need to insert a caption.

Figure 1.1 First Figure in Chapter 1

MP00640_

Table 1.1 First Table in Chapter 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A-D | A | B | C | D |
| 1 | A1 | B1 | C1 | D1 |
| 2 | A2 | B2 | C2 | D2 |
| 3 | A3 | B3 | C3 | D3 |

# Preliminares

En esta sección se incluye una descripción detallada de las tecnologías que han sido utilizadas para llevar a cabo la realización del proyecto descrito en este documento.

La tecnología principal en la que se basa este proyecto es *blockchain* [1], también conocida como cadena de bloques. El término blockchain se aplicó por primera vez en 2009 como parte del Bitcoin, aunque no hace mucho que ha empezado a escucharse con fuerza en la sociedad, sin embargo, la mayoría de la gente no sabe exactamente qué es el blockchain, para qué sirve o cómo funciona. En este trabajo se persigue el objetivo de explicar el blockchain con la mayor claridad posible para que cualquier persona con unos conocimientos básicos en informática sea capaz de entender sus beneficios y los usos que se le puede dar.

Esta tecnología se emplea dentro de este proyecto para soportar la estructura de datos y la información, a través de un Smart Contract se va a mantener la información dentro de la blockchain Ethereum, concretamente en Rinkeby, una cadena de bloques de *testing* proporcionada por Ethereum enfocada a desarrolladores.

## Blockchain

Aunque blockchain significa “cadena de bloques”, el propio nombre no deja muy claro qué es exactamente. Sin embargo, una vez entendido el contexto en el que se encuentra resulta más descriptivo.

El término blockchain empezó a escucharse con la revolución del *bitcoin*, ya que es la tecnología que está detrás de esta criptomoneda. Es una estructura de datos en la que la información contenida se agrupa en conjuntos, concretamente bloques, a los que se va agregando información relacionada con el bloque anterior, que, a su vez, contiene información relacionada con el bloque anterior a éste y así recursivamente, de manera que, debido a técnicas criptográficas, si un bloque es modificado modificaría todos los bloques posteriores, quitando así su validez. Estas cadenas de bloques se reparten entre nodos distribuidos en la red, comúnmente llamados mineros. Esta estructura persigue el objetivo de mantener una descentralización de la información y evitar dependencias con ciertos nodos, de manera que ningún nodo está por encima de otro y ningún nodo es indispensable para el correcto funcionamiento de la cadena, manteniendo así una estructura jerárquica horizontal. El intercambio de información se realiza de manera que, cuando un nodo añade un nuevo bloque, se lo comunica al resto de mineros de la red para que actualicen su cadena de bloques y así contengan todos la misma información.

De esta manera se crea un entorno distribuido en donde la cadena de bloques ejerce como una base de datos pública no con capacidad de asegurar la veracidad del contenido. Constantemente este libro digital de registros va creciendo añadiendo bloques a la cadena, las operaciones se van registrando de manera cronológica en la propia cadena, y se permite realizar un seguimiento sin la necesidad de registros centrales. Es importante destacar que los bloques tienen un orden cronológico dentro de la cadena y esto no se puede modificar ya que los bloques están interrelacionados entre ellos. Por ello, una vez que un bloque es considerado válido dentro de la red de nodos, siempre permanecerá en la cadena de bloques.

La tecnología blockchain es muy adecuada para los entornos en los que se quiera almacenar información de manera cronológica y se quiera garantizar la integridad de la información, imposibilitando la modificación de la información con el objetivo de garantizar una confianza distribuida en lugar de que quede depositada en una entidad certificadora.

Gracias a las funciones hash[[1]](#footnote-1) y la criptografía asimétrica que se emplean es posible implementar un registro contable distribuido, llamado *ledger*, que garantiza la seguridad y la integridad del dinero digital. Es por ello por lo que se está apostando a día de hoy en esta tecnología con las criptomonedas.

No es difícil actualmente leer noticias de proyectos nuevos o investigaciones acerca del blockchain. Empresas grandes o incluso gobiernos de algunos países están invirtiendo mucho dinero en esto, como, por ejemplo, el gobierno surcoreano ha anunciado hace relativamente poco que va a invertir en una “Estrategia de Desarrollo de Tecnología Blockchain” 207 millones de dólares en los próximos cuatro años. (21 - Jun - 2018 - “CriptoNoticias”, periódico digital que cubre toda la información referente a la tecnología blockchain).

Para evitar una entidad de confianza que centralice la información a la hora de garantizar la integridad de los datos por parte de todos los participantes de la red es necesario seguir un protocolo adecuado para todas las operaciones que se ejecuten sobre la blockchain. Gracias a esto se dice que la seguridad y la confianza de la tecnología dentro de todo el sistema se genera, se establece y se consolida por los propios miembros (los mineros). Incluso en un entorno en el que exista una minoría de nodos maliciosos por la red (nodos sybil) sería necesario que un atacante cubriera en mayoría la potencia de cómputo y presencia en la red que la que sumaría el resto de nodos combinados.

Gracias a esta características de confianza distribuida y mantenimiento de la integridad de los datos esta tecnología es útil en diferentes escenarios, como por ejemplo:

* Almacenamiento de la información, mediante la replicación de la información de la cadena.
* Confirmación de datos, mediante un protocolo de consenso entre los nodos participantes. El tipo de algoritmo más utilizado es el de prueba de trabajo (en inglés *proof of work*), en el que existe un proceso de validación de los nuevos bloques llamado minería.

Sin embargo, el blockchain está abarcando la mayoría de su peso en el ámbito financiero, en transacciones de dinero digital. Es por ello que no hace mucho comenzó la tendencia de las criptomonedas, que ha tenido y tiene mucha influencia a nivel mundial.

### Tipos de blockchain

Existen diferentes tipos de blockchain: blockchains públicas, blockchains privadas y blockchains híbridas. Cada una de ellas tiene características diferentes y, por tanto, tienen usos diferentes entre sí.

#### Blockchains públicas

Las blockchains públicas son accesibles para todo el mundo, lo único que se necesita para acceder a ellas es un ordenador y una conexión a internet. Bitcoin fue la primera blockchain pública, con la que nació en 2009 esta tecnología. De hecho, a día de hoy, esta criptomoneda es la más fuerte y las más consolidada de todas las blockchains públicas que se encuentran en activo. Otro ejemplo de blockchain pública es la criptomoneda Ethereum que es una de las más conocidas, ya que, ha sido el caso más exitoso de blockchain pública por detrás de Bitcoin. Cabe mencionar cuando se habla sobre blockchains públicas un grupo de criptomonedas que son mundialmente conocidas como Litecoin o Monero. A este tipo de cadenas también se las conoce como cadenas de bloques sin permisos.

Las cadenas de bloques públicas son mantenidas por todo aquel que quiera participar. En el caso de los Bitcoin, esto es posible gracias a los mineros, que deben contar con equipos con mucha capacidad de cómputo y por lo tanto gastar electricidad para poder mantenerlo. Sin embargo, esto no lo hacen gratuitamente, sino que existen ciertas recompensas cuando un nodo crea un bloque nuevo y lo añade a la cadena, por lo que se trabaja por incentivos. Esta parte se explicará un poco más adelante en la sección de Bitcoin.

Las blockchains públicas son, por tanto:

* **Descentralizadas**: evitando de esta manera la necesidad de una entidad central de confianza como podría ser un banco.
* **Distribuidas:** ya que, cada nodo de la red cuenta con una copia exacta de la cadena de bloques.
* **Consensuadas**: hay un consenso generalizado marcado por unas reglas para que las operaciones sean tomadas como válidas. Como por ejemplo un usuario no podría ejecutar una transacción en la que tratara de enviar más dinero del que realmente contiene.
* **Abiertas**: de manera que todo usuario que quiera es libre de participar de manera sencilla descargando el software necesario y realizando transacciones.
* **Seguras**: su seguridad es representada con la “verdad” que se encuentra en la integridad de los datos que se encuentran en ellas, así como la imposibilidad de modificación de datos anteriores.

Este proyecto se centra más en las blockchain públicas y concretamente utiliza la blockchain pública Ethereum.

#### Blockchains privadas

Estas cadenas de bloques se caracterizan porque el proceso de consenso que contienen, así como su participación, están limitados. De esta manera, solo ciertos usuarios tienen derechos para acceder a ellas, de hecho, lo normal es que al ser blockchains privadas, los usuarios que no participen en ellas no sean conscientes que existen.

En estas cadenas existen usuarios con diferentes permisos. Así, es posible que la lectura de la información de la blockchain esté limitada a ciertos usuarios.

Sin embargo, estas cadenas de bloques dejan de lado inevitablemente la descentralización del poder por lo que ya no se representaría el sistema como totalmente descentralizado.

Dentro de este grupo de blockchain existen variaciones, de manera que una cadena de bloques privada puede contar con un nivel de descentralización mayor o menor según la cantidad de entidades o grupos que formen parte del consenso.

Cuanta mayor sea la cantidad de figuras que forman parte del consenso, mayor nivel de descentralización. Por lo que existen blockchain privadas con una sola figura o entidad en el consenso que tenga permisos de escritura provocando así una cadena completamente privada y parcialmente centralizada.

Estas cadenas cuentan con las siguientes características:

* **Privadas:** no son accesibles para todo el mundo por lo que para mantenerlas es necesario definir unas entidades preseleccionadas**.**
* **Intereses:** los usuarios que mantienen estas bases de datos lo hacen por intereses propios como puede ser reputación.
* **Jerarquía:** existe una jerarquía de poder y permisos dentro de la cadena por lo que no todos los usuarios tienen por defecto los permisos de escritura. Además, el contenido de los bloques no es accesible para todos los participantes.

Algunas de las blockchains privadas más famosas a día de hoy son:

* Hyperledger, para la fundación Linux.
* R3, que se trata de un consorcio de bancos a nivel internacional para desarrollar soluciones bancarias a través de una blockchain privada.
* Ripple, una criptomoneda para realizar transferencias de dinero digital a nivel internacional.

#### Blockchains híbridas

Este tipo de cadenas de bloques son una combinación de las públicas y las privadas. En estas blockchains los nodos que participan han sido invitados previamente, sin embargo, todas las transacciones son públicas. De esta manera, los nodos se encargan de mantener y proporcionar seguridad a esta cadena, a pesar de que las transacciones sean públicas para el resto de usuarios.

Algunos ejemplos de blockchains híbridas son:

* BigchainDB.
* Evernym.

## Ethereum

Ethereum es una red pública y descentralizada de cadenas de bloques capaz de ejecutar código de programación de cualquier aplicación descentralizada. Esta plataforma permite compartir información con todo el mundo manteniendo su integridad ya que dicha información no puede ser manipulada ni modificada.[2]

Figure 2.1 First Figure in Chapter 2



Table 2.1 First Table in Chapter 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| E-H | E | F | G | H |
| 1 | E1 | F1 | G1 | H1 |
| 2 | E2 | F2 | G2 | H2 |
| 3 | E3 | F3 | G3 | H3 |

Note the figure and table captions above are automatically added to the List of Figures and List of Tables.

# Diseño e implementación

En esta sección se describe técnicamente el diseño completo de la plataforma ofreciendo una visión clara de la arquitectura del proyecto al completo y las tecnologías que han sido utilizadas para su implementación.

Tal y como se menciona en este trabajo anteriormente se han desarrollado dos secciones bien diferenciadas, que podrían dividirse en dos subproyectos: por una parte el *front-end* y por otra parte el *back-end*.

El *front-end* del proyecto consiste en la parte visual del proyecto, en este caso la aplicación móvil para dispositivos iOS. La totalidad del proyecto ha sido implementado con el lenguaje Swift en el entorno de desarrollo Xcode.

Swift, creado por Apple y presentado en 2014, es un lenguaje de programación orientado a objetos que cuenta con ciertas características que le hacen ser un lenguaje muy potente y restrictivo a la hora de programar con el fin de evitar código inseguro. Comprueba automáticamente desbordamiento de enteros y administra automáticamente la memoria a través de ARC (*Automatic Reference Counting*) eliminando la necesidad de utilizar punteros.

Este lenguaje está fuertemente “tipado” y es por ello que permite al propio compilador inferir el tipo de variables en tiempo de compilación sin asignarle un tipo por defecto. Permite enviar funciones o bloques de código como parámetros de otras funciones. Cuenta con un tipo de variable llamado Opcional que obliga al desarrollador a implementar un código seguro a partir de valores por defecto para poder compilar el código. [3]

La parte de *back-end* está desarrollada a través de un *Smart contract* en la red *blockchain* de pruebas de Ethereum llamada Rinkeby. El contrato inteligente con el que se realiza toda la gestión de alquiler de coches está desarrollado en Solidity.

# Demo

# Bibliografía

asdasd

[1] D. Tapscott, A. Tapscott, y J. M. Salmerón, La revolución blockchain: descubre cómo esta nueva tecnología transformará la economía global. Barcelona: Deusto, 2018.

[2] «Cuestiones básicas de Ethereum | Billetera de Blockchain». [En línea]. Disponible en: https://www.blockchain.com/es/learning-portal/ether-basics. [Accedido: 09-may-2019].

[3] C. G. García, J. P. Espada, B. C. P. G. Bustelo, y J. M. C. Lovelle, «Swift vs. Objective-C: A New Programming Language», IJIMAI, vol. 3, n.o 3, pp. 74-81, 2015.

asdasd

asdasd

###### Enter Your Appendix Title Here

Appendices must be identified by letters (A, B, etc.) rather than by numbers. For this reason, different style headings are used with appendices. (The style at the top of this page is “Appendix A - Heading 6.”)

First-level Subhead (Heading 7 style)

Within an appendix, Heading 7 is the style to use for all first-level subheads. If you need to add another subhead level within Heading 7, use Heading 8 as shown below.

Second-level Subhead (Heading 8 style)

Use Heading 8 for all second-level subheads within an appendix. If you need to add another subhead level within Heading 8, use Heading 9 as shown below.

Third-level Subhead (Heading 9 style)

If you need a third-level subhead in an appendix, use Heading 4.

Figures and Tables Within Appendices

When you first add a figure or table to an appendix, it will be numbered as though it were in a regular chapter. For example, when the figure below was first inserted, it became “Figure 4.1”. As a figure within Appendix A, it should be “Figure A.1”

To make this change, the codes in the caption labels must be modified, and it’s best to wait until all figures and tables have been added to appendices.

Figure A.1 First Figure in Appendix A

MP00640_

###### Enter Your Appendix Title Here

If you need additional appendices, use style “Appendix A – Heading 6” for the appendix heading. This will label appendices in alphabetical order (A, B, C, etc.).

1. Una función *hash* es una función computable mediante un algoritmo. Es una operación criptográfica que genera una especie de firma digital de un contenido. [↑](#footnote-ref-1)