Trabajo Fin de Máster

Máster Universitario en Ingeniería de Telecomunicación

Estudio y aplicación de Sistema Electoral basado en Blockchain

Autor: Daniel López Gómez

Tutor: Francisco José Fernández Jiménez

Dpto. Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2019

Trabajo Fin de Máster
Ingeniería de Telecomunicación

Estudio y aplicación de Sistema Electoral basado en Blockchain

Autor:
Daniel López Gómez
(danlopgom@gmail.com)

Tutor:
Francisco José Fernández Jiménez
Profesor colaborador

Dpto. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2019

Trabajo Fin de Máster: Estudio y aplicación de Sistema Electoral basado en Blockchain

Autor: Daniel López Gómez

Tutor: Francisco José Fernández Jiménez

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2019

El Secretario del Tribunal

"Conocimiento es poder.
Conocimiento compartido
es poder multiplicado."

Robert Noyce

Agradecimientos

Este breve espacio queda reservado para agradecer su apoyo a aquellas personas que han hecho posible la realización de este proyecto.

Al tutor de este trabajo, Francisco José Fernández Jiménez. Por, desde el primer momento en que hablamos, guiarme y ayudarme con el proyecto. He podido comprobar como a lo largo de estos meses ha estado siempre dispuesto a resolver las dudas que me han surgido y a indicarme constantemente cualquier tipo de mejora.

A mis profesores, desde el colegio hasta la universidad. Todos me han aportado, en mayor o menor medida, conocimientos y valores que me han ayudado tanto profesional como personalmente.

A mis amigos, especialmente a Francisco Jesús Marchal, Francisco José Pérez y Javier Soriano, sin los cuales hubiera sido infinitamente más difícil llegar hasta aquí.

Y por último, y no menos importante, a mi familia. A mi hermana Cristina y a mis padres Antonio e Isabel. Por dármelo absolutamente todo a cambio de nada. Nunca podré agradeceros lo suficiente todo lo que hacéis por mí.

Daniel López Gómez

Sevilla, 2019

Resumen

A lo largo del documento lo que el lector encontrará es el análisis de la situación respecto a los sistemas de votación existentes y la tecnología que se ha incluido en los últimos años, además de describir cómo se ha creado un nuevo sistema basado en tecnología Blockchain.

A continuación, una descripción en líneas generales de la estructura del documento:

En primer lugar, se analiza el Estado del Arte tanto de los sistemas de votación a nivel mundial y nacional como de la tecnología Blockchain, y se justifica el motivo por el que ambos conceptos pueden unirse.

Posteriormente se presenta una Prueba de Concepto que trata de demostrar la posibilidad real de que un sistema de estas características puede llegar a implementarse y se presentan los resultados obtenidos con la aplicación desarrollada.

Y por último, se detallan las conclusiones obtenidas de la realización del trabajo.

Abstract

Along the document what the reader will find is the analysis of the situation regarding the existing voting systems and the technology that has been included in recent years, as well as describing how a new system based on Blockchain technology has been created.

A general description of the structure of the document:

Firstly, the State of Art of global and national voting systems and Blockchain technology is analyzed, and it is justified why the two concepts can be brought together.

Subsequently, a Proof of Concept is presented that tries to demonstrate the real possibility that a system of these characteristics can be implemented and the results obtained with the developed application are detailed.

And finally, the conclusions drawn from the project.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

If you can't explain something in simple terms,
you don't understand it.
- Albert Einstein -

Desde su lanzamiento en 2009 por parte de Satoshi Nakamoto (identidad a día de hoy desconocida), Bitcoin ha supuesto una auténtica revolución en diversos aspectos:

En el **aspecto económico**, se ha comprobado la posibilidad real de crear una forma de dinero puramente *peer-to-peer* que permite la transferencia de valor entre diferentes partes sin necesidad de pasar a través de una institución financiera, algo que siempre había resultado imprescindible hasta el momento.

En el **aspecto tecnológico**, ha resultado ser la primera gran aplicación de la tecnología Blockchain demostrando, gracias a todos los años que lleva funcionando, su seguridad y robustez a pesar de ser un sistema íntegramente digital.

Aunque si bien es verdad, a día de hoy Bitcoin no es ampliamente usado por la mayoría de la sociedad, motivado principalmente por el carácter meramente especulativo que ha tenido en los últimos tiempos, su potencial a medio-largo plazo es bastante amplio mientras la comunidad que lo desarrolla, mantiene y participa siga con las metas con las que fue ideado. De hecho, el mismo Vitalik Buterin, creador de Ethereum -la otra gran criptomoneda-, se preguntaba[1] si realmente estaban justificados los 0,5 billones de dólares de capitalización que había alcanzado el mercado de las criptodivisas.

A pesar del futuro, o no, que puedan tener tanto Bitcoin como el resto de las criptomonedas como alternativa al dinero fiduciario con el que tratamos hoy en día, lo que sí ha supuesto es la constatación de la posibilidad de crear un sistema de registro de datos de manera segura mediante Blockchain. Este hecho está abriendo un mundo de posibilidades donde se puede aplicar dicha tecnología en otros muchos ámbitos, siendo solo algunos ejemplos:

- En **servicios de salud**, para almacenar los registros médicos de los pacientes. Por ejemplo, MedRec, es una solución basada en Blockchain con este propósito.
- En **logística**, para guardar toda la información que se crea durante el transporte de mercancías. Por ejemplo, la compañía Maersk, una de las más grandes en cuanto a transporte marítimo, ha creado junto a IBM la solución TradeLens.
- En **arte**, para poder verificar quiénes fueron los anteriores propietarios de una obra. Por ejemplo, Blockchain Art Collective.

[1] https://twitter.com/VitalikButerin/status/940744724431982594

Otro ámbito donde se puede llegar a aplicar Blockchain, y cuya demostración es el propósito de este trabajo, son los sistemas de votación.

1.1 Objetivo y motivación

Este proyecto viene motivado por diversas razones:

La primera de ella es la **escasa modernización** del sistema de votación existente en España. Como se verá más adelante, este es uno de los motivos por los que la participación en los continuos sufragios que ocurren en nuestro país sea escasa, sobre todo por parte de los ciudadanos que residen en el exterior. El acceso al sistema de votación a veces resulta complicado dependiendo de las circunstancias y, a pesar de los avances tecnológicos que han ido apareciendo en la sociedad en las últimas décadas, no se ha tratado realmente de poner remedio a esta situación.

A este hecho se le suma la **aparición de la tecnología Blockchain**, la cual, a pesar de ser *relativamente* nueva, debido a los conceptos sobre los que se construye –y que se verán a lo largo del documento– muchos expertos la reconocen como la tecnología ideal para el almacenamiento de datos en el futuro.

Además, y al hilo de lo comentado anteriormente, otra motivación bastante importante que se ha encontrado a la hora de realizar este proyecto ha sido el hecho de que hasta el momento no se ha encontrado **ningún trabajo relacionado con la tecnología Blockchain** en la Escuela Técnica Superior de Ingeniería, tal y como se puede ver en la siguiente búsqueda realizada en sus archivos:

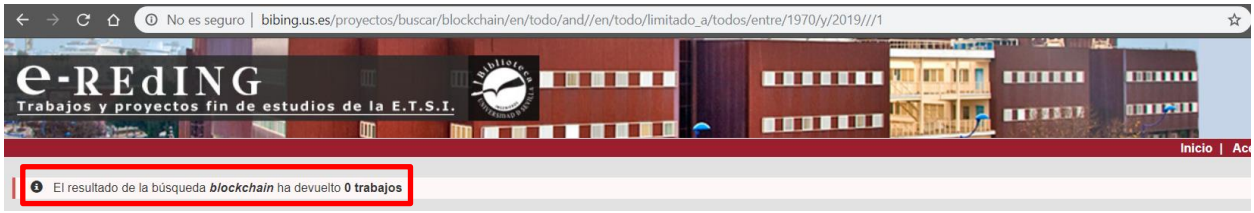


Figura 1. Búsqueda de proyectos relacionados con Blockchain en los archivos de la E.T.S.I.

Todas estas razones han sido motivación fundamental para la realización de este proyecto y han propiciado que, por lo tanto, el objetivo de este trabajo sea tanto el de **analizar** como el de **demostrar** mediante una **Prueba de Concepto** cómo se podría usar la tecnología Blockchain en un sistema de votación como las Elecciones en España con el fin de facilitar el acceso al voto en un sociedad cada vez más global y avanzada tecnológicamente.

1.2 ¿Por qué unir Sistema Electoral y Blockchain?

A modo de resumen, el proceso seguido para el recuento de votos en las elecciones en España es el siguiente:

- Una vez se acaba la jornada y se cierran los colegios electorales, el presidente de la Mesa electoral extrae las papeletas de los sobres y nombra en voz alta el partido que aparece en ellas, todo ello con miembros de los partidos políticos presentes.
- Cuando la urna ha quedado vacía, el presidente de la Mesa anuncia los resultados de la votación creando el acta de escrutinio, una copia de la cual también será repartida a los miembros de los partidos políticos.
- El acta se entrega en un Juzgado y posteriormente se distribuye a una empresa que crea una base de datos con el propósito de poder conocer los resultados electorales pocas horas después de haber cerrado los colegios electorales.
- Tres días después del día de elecciones se realiza el Escrutinio General y definitivo en un acto público y sobre las actas que fueron recogidas. En este acto participan también los partidos políticos y

ciudadanos que quieran acudir. De este modo se certifica que los resultados provisionales son los mismos que los definitivos.

Estos pasos, y la cierta transparencia con la que se hacen, permiten que la sospecha de fraude sobre el proceso electoral español no sea demasiado grande.

¿Entonces por qué podría/debería abrirse la posibilidad del voto electrónico en España?

Los motivos son varios:

Añadir la posibilidad del voto electrónico por Internet **no implicaría quitar la posibilidad del voto presencial**. Ambos pueden complementarse tal y como se detallará posteriormente que ocurre en Estonia. De hecho, podría seguir teniendo preferencia el voto presencial frente al remoto.

En los últimos tiempos es conocida la desafección que tiene una buena parte de los jóvenes hacia la política, tal y como se puede ver en el siguiente gráfico:

Figura 2. Intención de voto elecciones 2016. Fuente: larazon.es

La visión de algunos expertos es que no se puede seguir votando en el siglo XXI como en el siglo XIX y es por ello que creen que la introducción del voto por Internet podría cambiar esta situación: "la democracia electrónica es una vía interesante para el presente y un futuro no muy alejado, por los colectivos jóvenes y los de las áreas dispersas, donde es mucho más difícil acudir a los colegios electorales", asegura Ángel Valencia, catedrático de ciencia política en la Universidad de Málaga [1].

También cabe añadir que según el Instituto Nacional de Estadística, en España en el año 2017 el **84,6%** de la población de 16 a 74 años ha utilizado Internet en los últimos tres meses [2] y esta cifra se prevé que aumente año a año, por lo que el acceso a Internet no es un problema real para su implementación.

Además, desde el Ministerio del Interior se asegura [3] que "buena parte de este conjunto de actividades, procesos y documentación [sobre gestión electoral] se repite proceso tras proceso" por lo que "este carácter repetitivo hace de la gestión electoral un campo en el que la utilización de herramientas informáticas resulta idónea."

1.2.1 Tecnología Blockchain aplicada a las Elecciones

El motivo por el que Blockchain podría ser la tecnología ideal para poder implementar el voto electrónico es básicamente porque permite la seguridad, anonimato y transparencia que requiere un proceso tan exigente como es un proceso electoral.

1.2.1.1 Seguridad

La dependencia mediante hashes entre los bloques que conforman una cadena de bloques hace que se detecte la más mínima alteración de cualquier dato contenido en la cadena. Haciendo de este modo imposible el poder modificar un solo voto sin ser detectado.

Además, el esquema de criptografía asimétrica utilizado en la cadena de bloques es ampliamente usado a día de hoy. De hecho, es el esquema criptográfico usado para el certificado digital de la FNMT (Fábrica Nacional de Moneda y Timbre).

1.2.1.2 Anonimato

Al igual que ocurre en Bitcoin, el registro de transacciones (en elecciones, votos) guarda únicamente las claves públicas de los sujetos que intervienen en la operación. Debido a que la clave pública es una ristra de caracteres alfanuméricos, no será posible correlar dicha clave con su dueño, permitiendo el anonimato necesario en una votación.

1.2.1.3 Transparencia

Puesto que la información accesible a todo el mundo sería únicamente la clave pública del votante, a la vez que se garantiza su anonimato, se permitiría a cada ciudadano (el cual es conocedor de su clave pública) verificar cómo ha sido contabilizado su voto incluso una vez se hayan escrutado todos los votos y publicado los resultados.

1.2.2 Algunos proyectos existentes

En los últimos años han aparecido algunos proyectos con el objetivo de implementar una solución que permita votaciones mediante la tecnología Blockchain. Algunos de estos ejemplos pueden ser democracy.earth (código abierto) o votem.com (código cerrado).

Nota: aprovechando este apartado, cabe decir que si en algún momento Blockchain -o cualquier otra tecnología- llega a utilizarse para un proceso con la necesidad de tanta transparencia como unas elecciones, esto debería hacerse con código abierto y accesible a todo el mundo. De este modo se permitiría encontrar posibles fallos en la aplicación usada, además de que se hace imposible para el usuario confiar en código al que no se tiene pleno acceso.

1.2.3 Argumentos en contra

Ante la llegada de una tecnología tan nueva a un campo tan antiguo como es un proceso electoral, es lógico que haya puntos de vista discrepantes sobre la inclusión, no solo del voto electrónico en general, sino más aún de la tecnología Blockchain. Es entendible y razonable.

Si pensamos en por qué el voto presencial mediante papeleta es con el que más cómodo se siente la gente hoy en día, esto parece ser debido fundamentalmente a dos factores:

1. Es el método que se ha usado siempre y hasta ahora nunca se ha detectado un posible fraude (en España).
2. Es un proceso simple que todo el mundo entiende.

El punto número 1 es cierto, pero no debería ser excusa. Como ya se ha comentado en apartados anteriores, la

poca participación que ha tenido siempre el voto de los españoles en el extranjero debería ser suficiente para poder plantear la necesidad de un método de votación alternativo.

El punto número 2 es igualmente cierto. Blockchain, como cualquier tecnología nueva y disruptiva, no es sencilla de entender en un primer momento, pero tampoco debe ser una excusa. Los conceptos que se usan, y que se comentarán en capítulos posteriores (criptografía asimétrica, función hash o red peer-to-peer) no son conceptos nuevos. De hecho, cualquiera en España puede realizar acciones confidenciales a través del certificado digital emitido por la FNMT, el cual se utiliza para realizar operaciones confidenciales a través de páginas webs de instituciones públicas como la Agencia Tributaria, la Seguridad Social o los Registros Mercantiles.

Además, la casualidad ha querido que al momento de escribir estas líneas (noviembre de 2018) se produzcan las elecciones legislativas de Estados Unidos. En ocasiones como éstas es común que salgan a la luz artículos que debaten sobre nuevas formas de votación, posibles fraudes que se pudieran producir, etc y esta vez no ha sido distinto. En esta ocasión algunos expertos han alzado la voz contra aquellos que piensan que la tecnología Blockchain puede servir en hacer los procesos de votación mejores:

Figura 3. Tweet de Angela Walch, profesora de The St. Mary's University School of Law en San Antonio. Fuente: twitter.com

Traducción: Es ridículo. Por favor, dejad de recomendar la tecnología blockchain para casos de uso críticamente importantes, como votar en elecciones públicas, cuando todos los expertos discrepan. Engañar sobre esto a políticos y al público es irresponsable.

Figura 4. Tweet de Andreas M. Antonopoulos, conocido defensor de Bitcoin y profesor en el programa de maestría de Moneda digital de la Universidad de Nicosia. Fuente: twitter.com

Traducción: De acuerdo. La votación no se mejora con blockchains (no en cualquier momento pronto al menos). Vendedores de aceite de serpiente engañando a los legisladores crédulos.

Opiniones como las anteriores justifican la aparición de la Prueba de Concepto para demostrar cómo se podría llevar a cabo un proceso de estas características.

2 ESTADO DEL ARTE

Democracy is the worst form of government,
except for all the others.
- Winston Churchill -

2.1 Estado del Arte del voto

2.1.1 Definición de voto

El voto, según la Real Academia Española, es la expresión pública o secreta de una preferencia ante una opción. Parte esencial en cualquier sistema democrático, gracias al voto se pueden tomar decisiones de manera equitativa y haciendo valer el punto de vista de cada individuo.

Aunque existen muchos contextos en los que se puede realizar una votación, este proyecto se ideó teniendo como referencia un sistema de votación como el de las **Elecciones Generales de España**, las cuales sirven a los ciudadanos para elegir sus representantes públicos.

Para que este sistema de votación se considere propio de una democracia, el voto debe cumplir las condiciones de ser: **universal**, todo el conjunto de la ciudadanía tiene derecho a voto; **libre**, cada votante debe elegir libremente su opción; **igual**, cada votante cuenta con un único voto; **directo**, el voto debe ser efectuado por cada ciudadano de forma directa, sin intermediarios; y **secreto**, el votante tiene derecho a que nadie conozca el sentido de su votación.

Estas características, las cuales garantizan que un sistema de votación sea totalmente democrático, estarán presentes durante todo el proyecto.

2.1.2 Tipos de votación en el mundo

A la hora de realizar el voto no todos los ciudadanos tienen la misma facilidad para acceder al sistema de votación y esto, unido al avance de la tecnología, ha hecho que existan diferentes maneras en que se pueda participar en un sufragio. A continuación veremos una posible clasificación:

2.1.2.1 Voto presencial

Voto por papeleta

Sistema tradicional de voto consistente en la introducción en una urna de una papeleta con la opción que ha elegido el votante.

Voto electrónico

La primera vez que se introdujo la electrónica fue durante la década de 1960 mediante el sistema de voto electrónico en papel al realizar el conteo de votos mediante escaneo óptico y electromecánico. El votante marca a mano tarjetas o láminas de papel que posteriormente el sistema analiza para contabilizar el voto. Estos sistemas incluían votación mediante máquina de votar o tarjetas perforadas, sistemas de votación de escaneo óptico, sistemas de marcado y escaneo óptico y más tarde sistemas de votación con lápiz óptico.

Posteriormente también aparecieron los sistemas de voto electrónico de **registro directo**. La máquina de votar electrónica de registro directo (DRE, del inglés Direct-Recording Electronic) consiste en una pantalla y componentes mecánicos (botones) o eléctrico-ópticos (pantalla táctil) mediante los cuales el votante realiza la acción de votar.

Figura 5. Urna electrónica usada en Sistemas de voto electrónico de registro directo. Fuente: wikimedia.org

2.1.2.2 Voto a distancia

Voto por correo

En el caso de solicitarlo, el votante puede recibir las papeletas mediante correo y éste enviará su opción por correo postal, sin necesidad de asistencia personal a una mesa electoral.

Voto por poder

Para emitir un voto por poder el votante designa a alguien como apoderado, autorizándolo a votar en su lugar. El problema del voto por poder es que no permite verificar que, en una votación secreta, el apoderado vote en el sentido indicado por el poderdante. No obstante, esta modalidad es utilizada en varios países, como Albania, Canadá, China, Gabón, India, Rusia, Reino Unido o Estados Unidos.

Voto electrónico por Internet

En esta modalidad tanto la autorización como el propio acto de votación se realizan a través de Internet. Se verá en profundidad en capítulos posteriores.

Voto consular

A este método se le denomina voto consular porque normalmente el votante emite el voto en la sede del consulado de su país.

2.1.3 Tipos de votación en España

En España, la Constitución recoge (Art. 23) que “los ciudadanos tienen el derecho a participar en los asuntos

públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal." Ese periodo, que en el artículo 68 se define en un máximo de cuatro años, marca el tiempo (en circunstancias normales) en las que los ciudadanos españoles participan en las elecciones generales, autonómicas y municipales. (Además también participan en las europeas, pero éstas se celebran cada cinco años)

El organismo encargado del proceso electoral en España es la **Junta Electoral Central** que es el órgano superior de la Administración Electoral y, según se define en su propia página web, su "fundamental misión" es la de "velar por la transparencia y objetividad del proceso electoral".

En dicha página web se definen para España hasta tres tipos de votación:

- **Ejercicio del voto en la Mesa Electoral:** el voto tradicional mediante el depósito de papeleta en una urna de manera presencial.
- **Voto por correspondencia:** el votante que prevea que en el momento de las elecciones no va a poder acudir a su colegio electoral podrá emitir su voto por correo, previa solicitud a la Delegación Provincial de la Oficina del Censo Electoral.
- **Voto de personas que viven en el extranjero** (C.E.R.A. - Censo de los Electores Residentes-Ausentes): votación mediante correspondencia o en urna, previa inscripción a C.E.R.A, la cual es obligatoria para los españoles que residen permanentemente en el extranjero.

2.2 Voto Electrónico por Internet

Si bien existen tres formas de voto electrónico, tal y como se ha diferenciado en el capítulo anterior:

- Escaneo óptico.
- Registro directo (DRE).
- Voto a través de internet.

En este capítulo nos centraremos en éste último al ser el único que se realiza a distancia, siendo en los dos primeros necesaria la presencia física del votante.

Se denomina al voto por Internet cuando el ciudadano hace uso de redes telemáticas tanto para la autorización como para realizar la propia acción del voto. A diferencia del voto meramente electrónico, el votante puede votar a distancia con el único requisito de tener acceso a Internet.

Este caso estaría concebido como un sistema integral que incluye todo el proceso de entrada de voto, registro de votos, cifrado de datos, transmisión a servidores, y finalmente consolidación y tabulación de los resultados electorales.

2.2.1 Sistema público en Estonia

Si bien el voto electrónico ha sido usado en multitud de países del mundo a lo largo de las últimas décadas, tal y como se puede ver en la siguiente imagen:

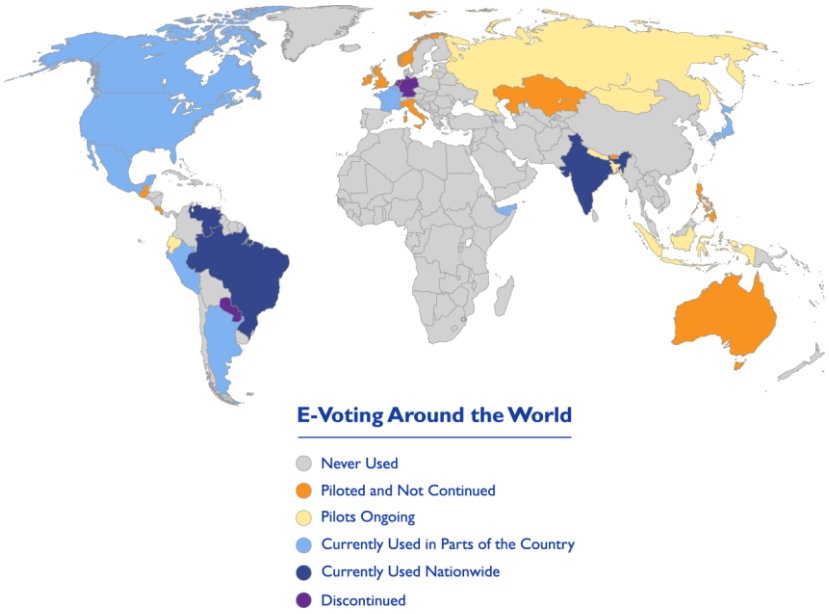


Figura 6. Uso del voto electrónico en el mundo. Fuente: ndi.org

Sólo en algunos de estos países como Canadá, Suiza o Estonia se ha considerado o se considera introducir la modalidad de voto electrónico vía Internet.

Por ejemplo, en **Canadá** en el año 2003, doce municipios permitieron este método a sus ciudadanos en las elecciones municipales [4]. Además **Suiza** lleva desarrollando desde 2004 un plan estatal (que tiene como *deadline* finales de 2019) para poder votar de manera telemática [5].

Sin embargo, el país europeo referente en cuanto al voto electrónico vía Internet es **Estonia** y a continuación lo veremos más en detalle.

A nivel mundial, **Estonia** es el país pionero en cuanto al sufragio vía Internet. En el año 2005 tuvieron lugar las primeras elecciones municipales en las que se podía elegir esta opción para realizar el voto y posteriormente -dos años más tarde- fue aplicado también en unas elecciones parlamentarias.[2]

Las fases en las que se divide un proceso electoral cualquiera son las siguientes:

- Declaración de las elecciones
- Registro de los candidatos
- Preparación de la lista de los votantes
- Periodo de votación
- Conteo de votos
- Publicación de resultados

El sistema que veremos a continuación se centra únicamente en las tres últimas fases, necesitando como requisito fundamental que las listas de votantes y candidatos estén preparadas y sean consistentes.

2.2.1.1 Descripción del sistema

El sistema es denominado “Sistema de sobres” (Envelope Scheme) y se basa en el esquema tradicional de criptografía asimétrica:

[2] La web a través de la que los ciudadanos realizan las votaciones en Estonia es https://www.valimised.ee/en

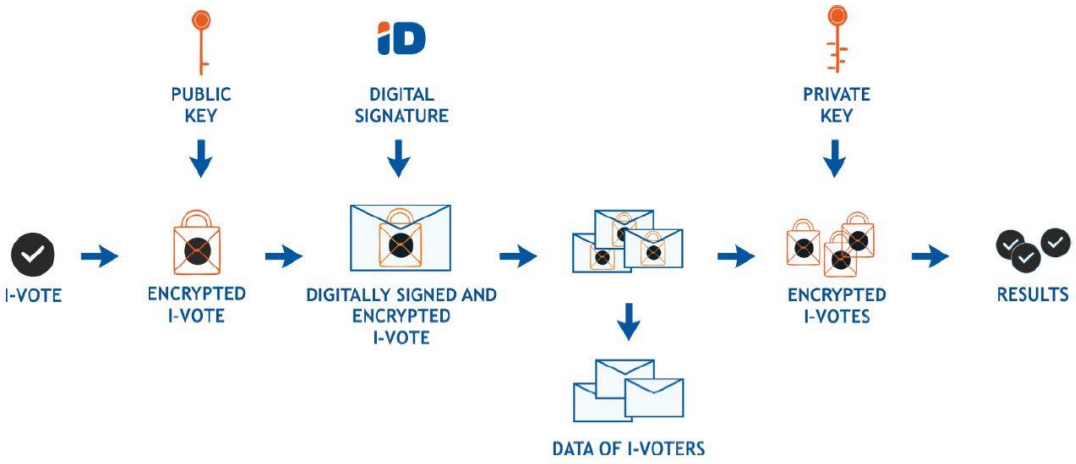


Figura 7. Envelope Scheme. Fuente: valimised.ee

Tal y como se puede ver en la Figura 3, una vez que el votante emite el voto, éste pasa por diferentes procesos:

- En primer lugar, el voto es cifrado con la clave pública específica de las elecciones.
- Una vez cifrado, se "envuelve" con la firma digital del votante y es enviado a los servidores centrales.
- En los servidores centrales se comprueba la legitimidad del votante y se eliminan los posibles votos dobles.
- Después se elimina la firma digital del votante.
- Finalmente, se descifra con la clave privada de las elecciones obteniendo el voto final.

2.2.1.2 Principales actores del sistema

El actor principal es el **Organiser** y tiene como cometido designar el resto de roles, además de poseer el elemento más importante de todo el sistema: la clave privada de las elecciones. Los actores que forman parte del sistema se pueden ver representados en la siguiente Figura:

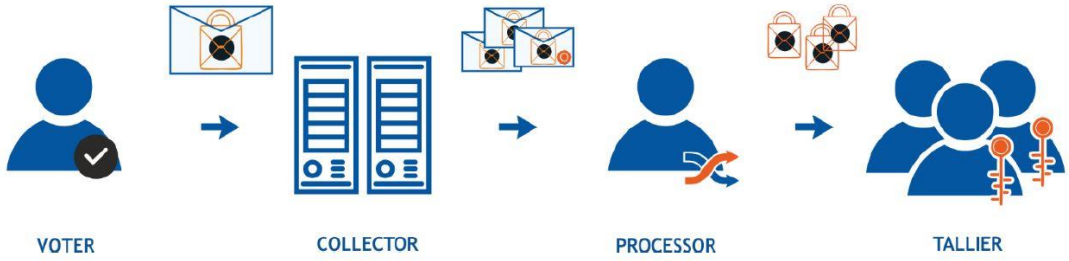


Figura 8. Principales actores en el Envelope scheme. Fuente: valimised.ee

- **Voter:** es el ciudadano que vota. Elige su opción, la cual es cifrada y firmada digitalmente para posteriormente pasarla al Collector. El votante puede verificar la integridad del voto mediante un dispositivo diferente al que ha emitido el voto.
- **Collector:** servidor que ayuda al votante ofreciéndole la lista de candidatos y verificando la integridad de su voto si éste lo solicita.
- **Processor**: entidad que verifica la firma digital y la integridad del voto, elimina votos dobles y la posible dualidad voto remoto-presencial, anonimiza el voto eliminando la firma digital y mezcla los votos para que no haya una posible correlación votante-voto.

- **Tallier**: parte del Organiser que posee la llave privada del proceso electoral y que es capaz de obtener el voto en claro una vez este ha sido anonimizado y mezclado.

Además, también debería existir la figura del Auditor, el cual se encarga de que el proceso se lleve a cabo correctamente por parte de todos los actores.

2.2.1.3 Periodo de votación

Se puede realizar de dos maneras:

- La votación electrónica se realiza **días antes** de la votación presencial. En caso de que algo falle en la votación electrónica, ésta se puede anular parcial o totalmente teniendo la votación presencial como alternativa.
- La votación electrónica se realiza **en paralelo** a la presencial. En este caso si un votante votara de ambas formas solo se tendría en cuenta la votación presencial.

2.2.1.4 Posibles preguntas que pueden surgir

¿Cómo se garantiza que el votante no ha sido coaccionado por una tercera persona?

¿Cómo podríamos asegurarnos de que el votante no ha votado bajo la amenaza de alguien si el único testigo es la pantalla del dispositivo? La solución es bien sencilla: el votante puede votar tantas veces como quiera, únicamente contabilizando el último. Y no solo eso, además se prioriza siempre el voto presencial frente al remoto.

¿Cómo se garantiza que el voto no ha sido manipulado una vez lo ha emitido?

El votante tiene la posibilidad de verificar su voto (en este caso hasta el Collector) mediante un dispositivo distinto al utilizado para votar, por si éste se hubiera visto comprometido.

2.2.1.5 Algunos puntos a mejorar

El votante no puede comprobar su voto final ya que la verificación de su voto es realizada en el Collector, el cual posteriormente envía el voto a otros actores.

2.2.2 Implementación en España

En España, tal y como se ha visto en el apartado *Tipos de votación en España*, todavía no se contempla el voto electrónico a pesar de diversas peticiones que se han realizado en los últimos años, como por ejemplo la de la Comisión de Peticiones del Parlamento Europeo [6] o la de la propia Junta Electoral [7].

Estas peticiones son consecuencia sobre todo debido a la poca participación que normalmente tienen los votantes en el extranjero (**4.95%** en 2011, **4.73%** en 2015 y **6.3%** en 2016) [8], tal y como se puede ver en la siguiente Figura, cuyos datos se han obtenido de la web del Ministerio del Interior del Gobierno de España:

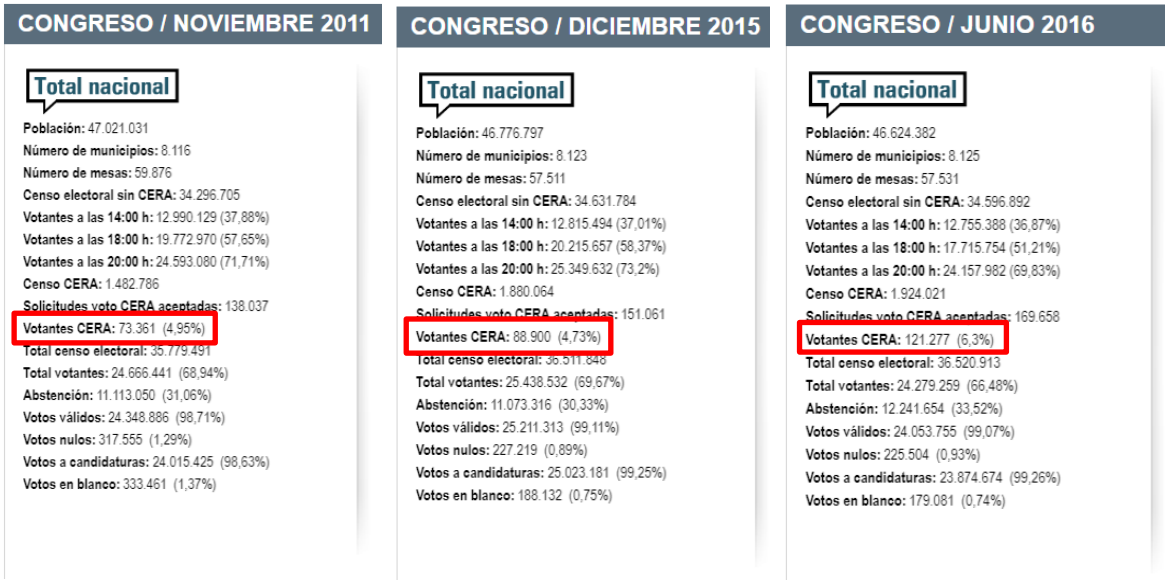


Figura 9. Participación en las elecciones al Congreso de España en 2011, 2015 y 2016. Fuente: mir.es

2.2.3 Compañías relacionadas

Además del sistema público en Estonia, en las últimas décadas han surgido diversas compañías en el ámbito privado que ofrecen soluciones para facilitar el sistema de votación electrónico vía Internet [9].

Algunos ejemplos pueden ser la española Scytl que participó en las elecciones presidenciales de EEUU del año 2012 [10] (y a la que recientemente se le encontró un fallo de seguridad en el sistema de votación ideado para Suiza [11]) o Polyas, la cual surgió en 1996 a raíz de la primera votación organizada en Finlandia.

2.3 Estado del Arte de Blockchain

2.3.1 Breve introducción a Bitcoin

El 31 de octubre de **2008**, Satoshi Nakamoto (nombre ficticio de una persona o grupo de personas) publicó el documento *Bitcoin: A Peer-to-Peer Electronic Cash System* [12] a través de una lista de correo sobre criptografía.[3] En dicho documento se describía cómo se creaba "una forma de dinero en efectivo electrónico puramente peer-to-peer" y que "debería permitir enviar pagos online directamente entre las partes y sin pasar a través de una institución financiera".

Aunque en el documento se utilizan conceptos ya existentes en aquel momento como *red peer-to-peer*, función *hash* o sistema de *criptografía asimétrica*, nunca antes se había vislumbrado la posibilidad real de que existiera dinero puramente electrónico y que además pudiera ser viable sin necesidad de intervención de una tercera parte en la transacción entre dos sujetos.

2.3.2 La cadena de bloques

El histórico de todas las transacciones realizadas en Bitcoin queda reflejado en un gran libro contable, público y distribuido. Ese gran libro contable es lo que se denomina la *cadena de bloques* y, como su propio nombre indica, está formada por bloques los cuales contienen transacciones realizadas por los usuarios.

Aunque su aplicación más famosa es Bitcoin, puede ser ampliamente usado en cualquier ámbito que sea

[3] https://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22

necesario el almacenamiento de datos de forma segura.

Este concepto se verá con más detalle en el siguiente apartado *2.3.4 Definición de Blockchain.*

2.3.3 Usuarios/Direcciones

Para poder participar en transacciones del protocolo de Bitcoin es necesario, tanto para enviar como recibir, crearse lo que se denomina una wallet (del inglés, cartera). Una wallet no es más que la generación de un par de claves siguiendo el sistema de criptografía asimétrica, de modo que cada usuario tendrá asignadas dos claves: la clave pública y la clave privada.

La **clave pública** (también llamada dirección) es la encargada de cifrar la información. Esta clave será, como su propio nombre indica, conocida por cualquier persona que quiera enviar información al dueño de la clave privada asociada a dicha clave pública. Es una ristra de entre 27 y 34 caracteres alfanuméricos, comenzando por el número 1 o el 3 y que representa el destino de un pago de bitcoins.

La **clave privada** es la encargada de descifrar la información. Debe ser conocida **única y exclusivamente** por el usuario. Es la parte más sensible del sistema ya que es la clave que te hace dueño de la información que se cifra con la clave pública, es decir, la pérdida de la clave privada es la causante de la pérdida, en este caso, de bitcoins.

La siguiente imagen representa el esquema de criptografía asimétrica que se acaba de detallar:

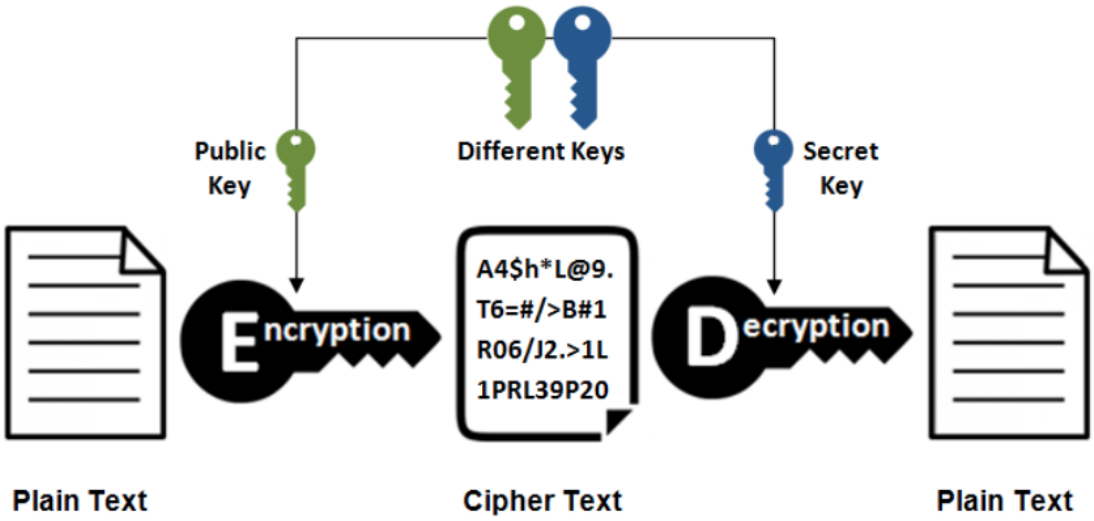


Figura 10. Esquema de criptografía asimétrica. Fuente: medium.com/@cesar_m

Aunque exponer todos los conceptos técnicos subyacentes que posibilitan Bitcoin no es objetivo de este trabajo, merece la pena mencionar que para la generación de claves se sigue el algoritmo ECDSA (**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm) basado en criptografía de curva elíptica.

Anonimato en Bitcoin

Aunque, como se apuntó en apartados anteriores, todas las transacciones realizadas en Bitcoin son públicas y conocidas por cualquiera, esto no impide obtener un cierto grado de privacidad y anonimato en cuanto a conocer quiénes son los individuos que participan en dicha transacción.

Como el propio libro blanco (whitepaper) de Bitcoin indica: “La necesidad de anunciar públicamente todas las transacciones excluye este método [limitar el acceso a la información a las partes implicadas y a un tercero de confianza], pero aun así se puede mantener la privacidad rompiendo el flujo de información en otro punto: manteniendo las claves públicas anónimas.”

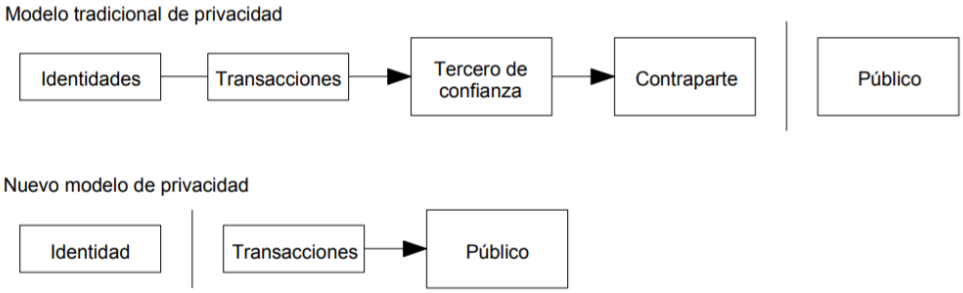


Figura 11. Comparación entre el modelo de privacidad tradicional y en Bitcoin. Fuente: bitcoin.org

En la Figura 7 se puede observar lo anteriormente comentado; si bien en el modelo tradicional de privacidad prácticamente todos los datos son privados (identidades, transacciones …) gracias a que existe un "Tercero de confianza", en Bitcoin al no existir esta entidad, lo único que se mantiene privado es la identidad de las partes mientras que todas las transacciones son públicas y conocidas por el público.

De modo que cualquier usuario que evite la correlación clave pública – usuario, podría, en principio, mantenerse anónimo en la red de Bitcoin.

2.3.3.1 Transacciones

Las transacciones son el elemento fundamental del sistema ya que es lo que permite la transmisión de valor entre usuarios.

En Bitcoin, cada transacción contiene entradas (inputs) y salidas (outputs). En una transacción se gastan bitcoins previamente recibidos en una o varias transacciones anteriores, por lo que el input de una transacción siempre será el output de otra. Este hecho se puede ver reflejado en el siguiente ejemplo:

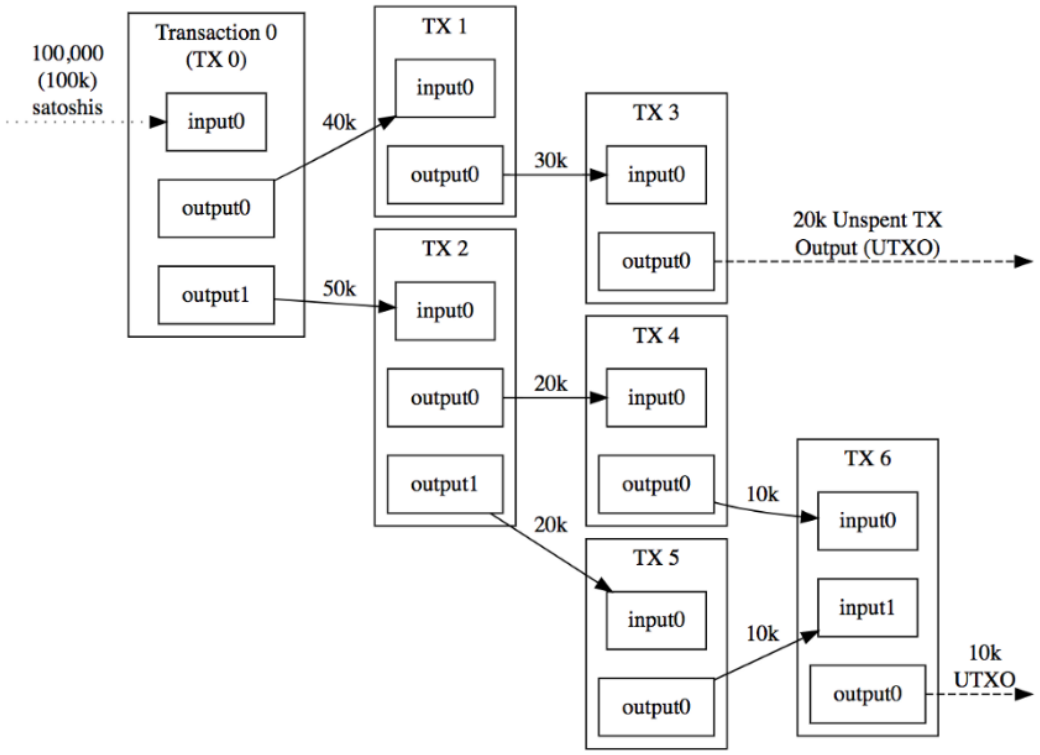


Figura 12. Ejemplo del modelo UTXO usado en Bitcoin (notar que el transaction fee es de 10k satoshis[4]).
Fuente: bitcoin.org

Además, una sola transacción puede generar varios outputs (por ejemplo haciendo un envío a varias direcciones diferentes).

Este modelo es el denominado UTXO (Unspent Transaction Output), el cual es diferente al modelo tradicional basado en el balance, usado por ejemplo en el entorno de Ethereum y en el sistema tradicional bancario, en el que en una cuenta se guarda el balance total disponible del usuario.

2.3.3.2 Prueba de Trabajo

Un sistema de Prueba de Trabajo (Proof of Work) es un sistema que requiere que el usuario de un servicio realice algún tipo de trabajo que tenga cierto coste.

En el protocolo de Bitcoin, y de las criptomonedas que son minadas en general, el sistema de Prueba de Trabajo es utilizado con dos propósitos. El primero de ellos, para la **creación de nuevas unidades monetarias**. Cada vez que un nuevo bloque es *minado*, el nodo que crea dicho bloque recibe 12.5 BTC. El segundo propósito es el de **verificar las transacciones** que realizan los usuarios.

A continuación explicaremos ambos conceptos un poco más detallados.

Creación de nuevos bloques

Cualquier nodo que colabore con la red contiene una copia del "gran libro contable" y puede añadir un bloque que contenga transacciones realizadas por los usuarios. Estos nodos que añaden bloques se llaman **mineros**.

Los mineros son nodos que ceden su capacidad de cómputo para mantener el sistema de Bitcoin. Con esa capacidad de cómputo, los mineros realizan una especie de "carrera" entre ellos. La "carrera" en la que participan los mineros consiste en encontrar, a partir de los datos propios del bloque más un campo a rellenar (denominado

[4] 1 satoshi = 1e-8 BTC

nonce) un hash que empiece por una determinada cantidad de ceros. A medida que aumenta el número de ceros requeridos al inicio de ese hash -cuya cantidad vienen impuesta por el propio protocolo Bitcoin- más difícil será obtener ese hash, siendo esto lo que se denomina la dificultad de minado.

El primero que resuelve este "problema matemático", añade el siguiente bloque a la cadena de bloques de Bitcoin y, a cambio, recibe una cierta cantidad de bitcoins como recompensa (12.5 BTC en el momento de escribir estas líneas). Este sistema basado en ceder capacidad de cómputo a cambio de una recompensa es lo que se denomina **sistema de prueba de trabajo** (del inglés Proof-of-Work).

Una vez un nodo ha minado un bloque, éste es distribuido al resto de nodos de la red los cuales comprueban que ese bloque es válido y lo añaden a su propia copia del gran libro contable, procediendo a resolver el siguiente "problema matemático" con el que añadir un nuevo bloque.

Llegados a este punto podría pasar que **dos nodos de la red minaran dos bloques diferentes a la misma vez**, dando como resultado dos cadenas de bloques distintas. Resolver este conflicto es fácil: siempre prevalece la cadena de bloques de mayor longitud.

A medida que se vayan añadiendo bloques a las diferentes cadenas de bloques, llegará un momento en el que una de ellas contenga más bloques que las demás. En ese caso se tomará como principal aquella cadena de bloques de mayor longitud.

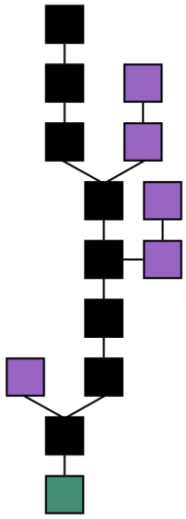


Figura 13. Representación de ramificación de bloques en Blockchain. Fuente: wikipedia.org/wiki/Bitcoin

En la imagen anterior se puede observar la cadena principal en negro, la cual es la serie más larga desde el origen (en verde). Los bloques huérfanos aparecen en color morado.

Por ello, para asegurarse de que una transacción está contenida en la cadena de bloques principal y no en una secundaria, las casas de cambio[5] aceptan una transacción cuando está contenida en un bloque con un determinado número de bloques posteriores (lo que equivale a decir con un determinado número de *confirmaciones*).

Verificación de transacciones

Lo que se consigue con la verificación de una transacción es simplemente validar que ésta ha sido realizada única y exclusivamente por la persona que dice ser el emisor, es decir, lo que se está haciendo es comprobar que la transacción ha sido firmada con la clave privada del emisor, pero sin conocer dicha clave privada.

[5] https://bitcoin.org/en/exchanges

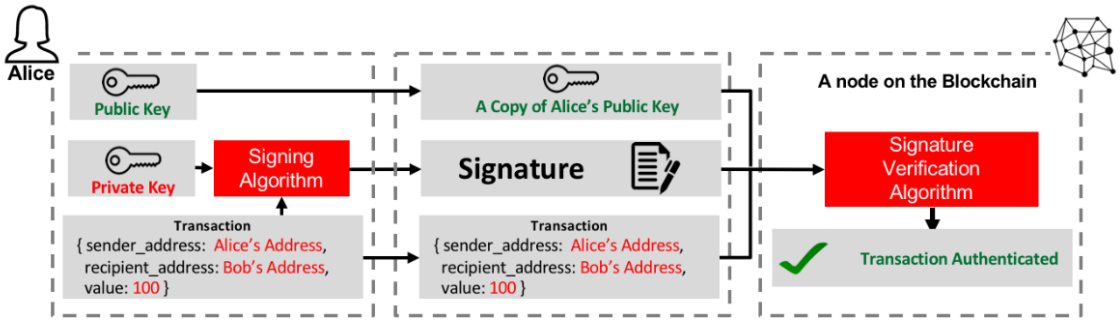


Figura 14. Proceso de autenticación para las transacciones en Blockchain. Fuente adilmoujahid.com

En la imagen anterior tenemos el ejemplo de que Alice transfiere un valor de 100 a Bob. Alice lo que hace es firmar con su clave privada la transacción que quiere hacer, creando la firma, en la cual se usa de manera implícita la clave privada. Con el algoritmo de verificación, cualquier nodo que reciba la **clave pública** de Alice, la **firma** que acaba de generar y la **transacción** original que fue firmada, puede comprobar que dicha transacción fue firmada con la clave privada de Alice, sin necesidad de conocerla.

2.3.3.3 Puntos débiles

Como cualquier sistema, el protocolo de Bitcoin y su funcionamiento cuentan con ciertos puntos débiles y aspectos a mejorar.

Alta latencia

Al realizar una transacción en Bitcoin ésta sigue el siguiente proceso:

1. El usuario genera la transacción.
2. La transacción se transmite a los nodos de Bitcoin.
3. Los nodos deben minar un bloque en el que la transacción ha sido incluida.
4. Una vez el bloque ha sido minado por un nodo, se transmite al resto de nodos.
5. La cadena en la que ha sido incluido el bloque debe confirmarse como la cadena principal.

Por lo tanto, todos estos pasos, llevan un tiempo que hace que las transacciones en Bitcoin no sean inmediatas y tarden generalmente entre 6 y 16 minutos[6].

Capacidad de procesado

No solo una transacción tarda en ser confirmada en la cadena, sino además el número de transacciones capaces de ser procesada por la red es bastante limitado, tal y como veremos a continuación.

El tamaño máximo de un bloque en el protocolo de Bitcoin es de 1 MB, lo que hace que en la actualidad el número de transacciones medio incluido en cada bloque sea de aproximadamente 2000 transacciones por bloque. Si de media se añade un bloque a la cadena cada 10 minutos, esto hace que cada minuto se procesen alrededor de 200 transacciones, un número claramente inferior a las decenas de miles de transacciones que es capaz de procesar, por ejemplo, el protocolo de Visa por segundo.

[6] https://www.blockchain.com/es/charts/median-confirmation-time

Escalabilidad

Éste es uno de los principales problemas de Bitcoin actualmente.

Si de media se añade un bloque a la cadena cada 10 minutos y en la actualidad cada bloque ocupa como máximo 1 MB, esto significa que cada hora la cadena puede llegar a aumentar su tamaño en 6 MB haciendo que a fecha de abril de 2019 ocupe ya **211.6 GB**, tal y como se puede ver en la siguiente gráfica:

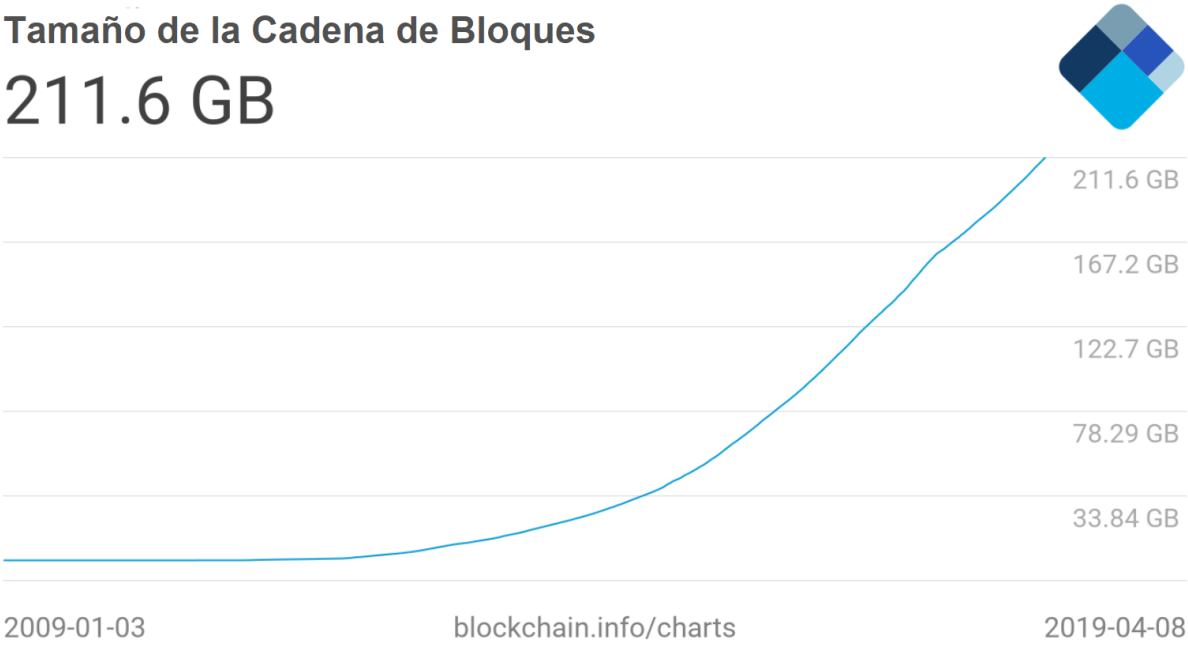


Figura 15. Tamaño de la cadena de bloques de Bitcoin. Fuente: blockchain.com

Para solucionar este problema, además de los anteriormente mencionados, a lo largo de los últimos años han ido surgiendo diferentes soluciones. Un ejemplo es el **Protocolo Lightning** [13], lo cual es una red construida sobre la propia red de Bitcoin con el objetivo de permitir realizar pagos de manera casi instantánea.

Además, el hecho de que existan estas limitaciones también ha hecho que aparezcan otras criptomonedas cuyos puntos fuertes argumentan ser los puntos débiles de Bitcoin, e incluso han ido apareciendo diferentes *forks*[7] al propio protocolo Bitcoin.

2.3.4 Definición de Blockchain

Blockchain (cadena de bloques) es una estructura con datos los cuales están contenidos en bloques cuya información depende de los bloques anteriores de la cadena.

[7] Se denomina fork o bifurcación cuando se crea un proyecto en una dirección distinta del proyecto principal).

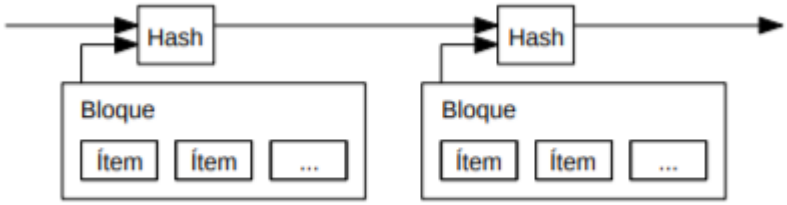


Figura 16. Representación de la cadena de bloques. Fuente: bitcoin.org

Como se puede observar en la Figura anterior, la información del *bloque n-1* que es usada posteriormente por el *bloque n* es el hash.

Una función hash es un algoritmo que tiene como entrada un conjunto de datos y obtiene como salida una cadena de caracteres de longitud fija. Por ello también se les llama funciones resumen. Las principales características de una función hash es que cualquier mínimo cambio en los datos de entrada hace que los datos de salida cambien. Este hecho se puede observar en los siguientes ejemplos:

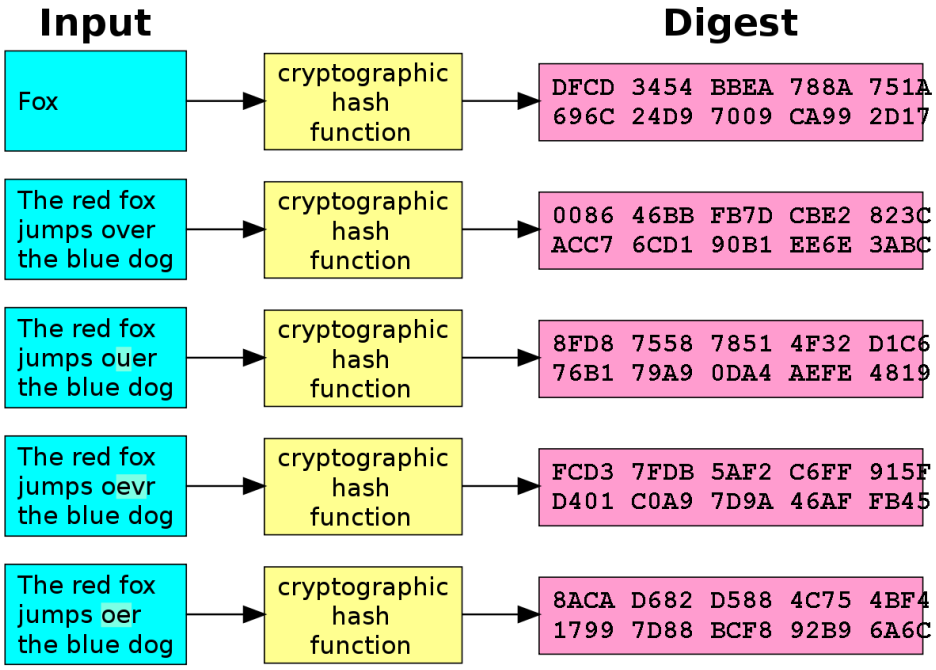


Figura 17. Representación de función hash. Fuente: wikipedia.org

De este modo se consigue que cualquier mínimo cambio en los datos contenidos en el *bloque n* se vea reflejado en todos los bloques posteriores a él en la cadena.

2.3.5 Clasificación

A día de hoy existen múltiples clasificaciones, no existiendo un gran consenso en cuanto a la forma de clasificar las cadenas de bloques. A continuación se expondrán algunas, pero es posible encontrar infinitas clasificaciones dependiendo de distintos parámetros, por ello para una mayor extensión de posibles clasificaciones se remite al lector, por ejemplo, a [14].

2.3.5.1 Según el acceso a los datos

Esta clasificación se basa en la posibilidad (o no) de acceder a los datos que contiene la cadena de bloques,

pudiendo implementar una **cadena de bloques pública**, una **cadena de bloques privada** o una solución intermedia entre ambas.

En general, los sistemas más conocidos de Blockchain están asociados al concepto de redes públicas en la que cualquiera puede participar como nodo en el sistema, sin embargo, esto no siempre es así y por ello a continuación se presentarán los distintos tipos de Blockchain que existen en la actualidad.

Blockchain pública

Son las cadenas de bloques en las que se puede participar simplemente descargándose el código y corriéndolo en un dispositivo propio para participar como un nodo más de la red.

Algunos ejemplos -y los más famosos- de Blockchain pública serían: Bitcoin, Ethereum, Monero…

Blockchain privada

En este caso es una única organización la que goza de los permisos de escritura en la cadena de bloques mientras que los permisos de lectura pueden ser totalmente públicos o simplemente asignados a otra entidad distinta.

Un caso de uso puede ser por ejemplo la gestión de una base de datos cuya auditoría pudiera ser pública o cometido de una entidad externa a la que se encarga de la gestión.

El uso de una cadena de bloques privada puede ser de utilidad puesto que se seguiría disfrutando de algunas de las características propias de la tecnología Blockchain ya que, por ejemplo, se tendría una serie de nodos que verificarían los datos que se están almacenando. Esto podría ser un arma de doble filo -al igual que podría pasar en un sistema centralizado- ya que un fallo de seguridad de los nodos podría comprometer el escenario.

Este modelo de cadena de bloque es usado, en estos momentos, sobre todo por el sector financiero. Algunos ejemplos:

- **One Pay FX**: solución basada en Blockchain para transferencias internacionales del Banco Santander.
- **Quorum**: solución basada en Blockchain creada por el banco JP Morgan.
- **Ripple (XRP)**: tercera criptomoneda con más volumen a día de hoy (solo por detrás de Bitcoin y Ethereum).

Blockchain híbrida o federada

Son parecidas al caso anterior (las cadenas de bloques privadas) pero en este caso los permisos de escritura residen sobre un grupo.

2.3.5.2 Según los permisos

En este caso el permiso se refiere a si se pueden generar bloques y añadirlos a la cadena de bloques.

Existen las **cadenas de bloques sin permisos** en las que cualquiera puede participar, normalmente incentivando a la participación con recompensas (Bitcoin por ejemplo remunera con 12.5 BTC a cada nodo que añade un bloque).

O también existen las **cadenas de bloques con permisos** en las que solo participan las entidades autorizadas para ello (este tipo es usado por ejemplo por las entidades financieras).

2.3.5.3 Según modelo de cambio de estado

Cambio de estado **basado en el gasto de salidas de transacciones** o **UTXO** (Unspent Transaction Output). Este modelo es característico de las cadenas de bloques que se usan para el "dinero electrónico". Al contrario de lo que se podría pensar, los bloques no contienen el saldo total de los sujetos, sino todas las transacciones que han sido realizadas por ellos. De este modo si se quiere calcular el saldo total que tiene uno de los sujetos,

simplemente hay que comprobar las transacciones en las que ha participado y hacer la suma total.

También existe el cambio de estado **basado en mensajes**. En este caso el orden de los mensajes se representa mediante un consenso en la cadena de bloques y es posible calcular el estado final a partir de los mensajes que son contenidos por todos los bloques.

2.3.6 Usos de Blockchain

Aunque Bitcoin es el ejemplo más conocido de la aplicación de Blockchain, a día de hoy existen múltiples campos donde ya se está aplicando su uso.

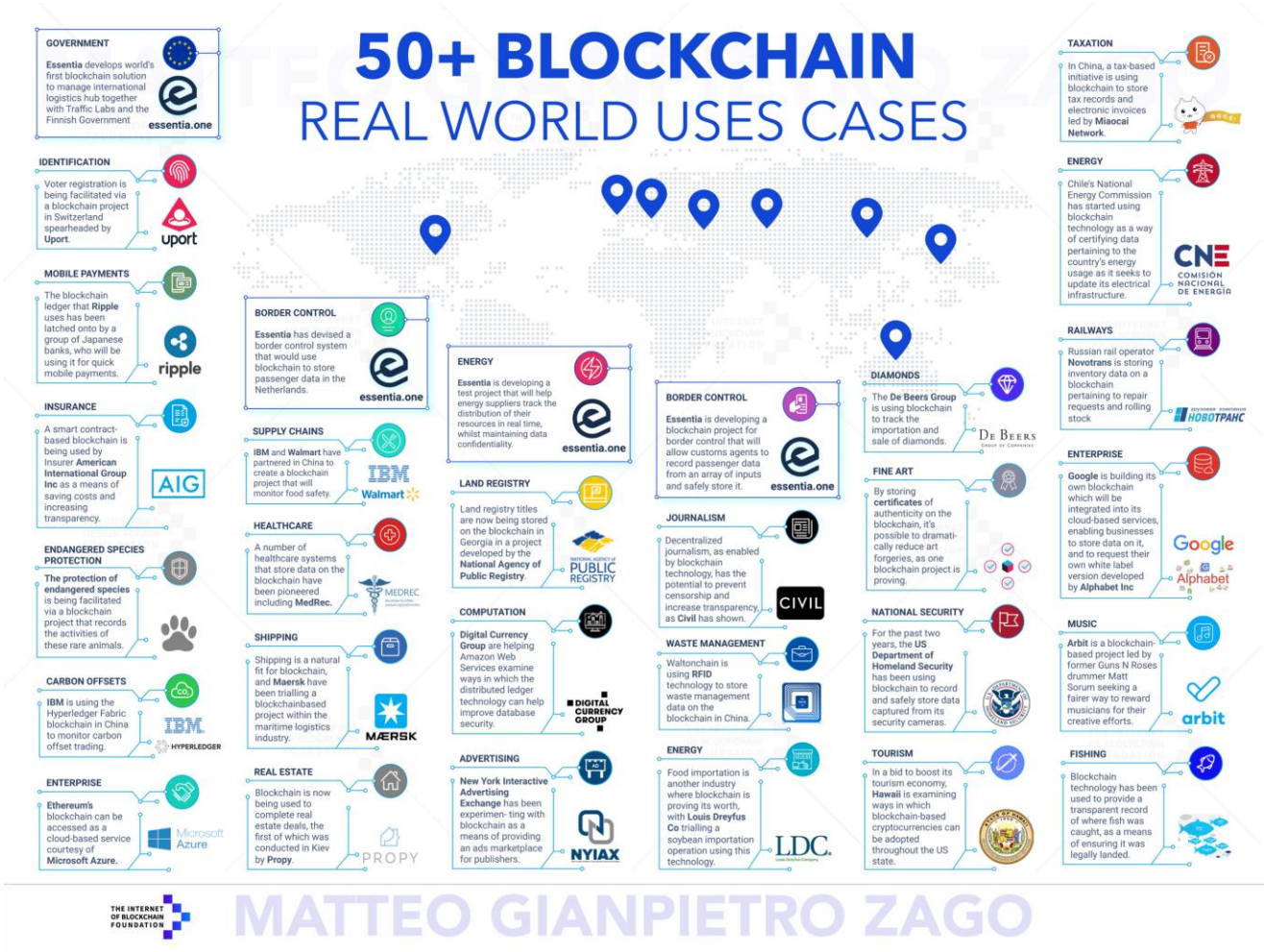


Figura 18. Ejemplos reales de aplicación de Blockchain. Fuente: https://medium.com/@matteozago

Como se puede observar en la imagen anterior, los campos donde se aplica la cadena de bloques son bastante diversos: pagos mediante móvil, transporte, registros médicos, periodismo…

Además de que los potenciales campos donde se puede aplicar Blockchain son amplios, también son muchas las grandes compañías que están explorando esta tecnología para aplicarla a sus respectivos proyectos. La siguiente Figura muestra un listado publicado por la revista Forbes de 50 de estas compañías [15]:

Figura 19. Lista de 50 compañías con proyectos relativos a Blockchain. Fuente: forbes.com

Por lo tanto, tal y como se ha visto en las imágenes anteriores, el potencial ofrecido por Blockchain parece bastante amplio. Sin embargo a día de hoy existen dos áreas principales donde ya se está usando dicha tecnología, y que se detallarán a continuación.

2.3.6.1 Criptomonedas

Aunque Bitcoin es la criptomoneda por excelencia debido a que fue la primera que apareció y a que en estos momentos cuenta con una cuota de mercado de aproximadamente el 52%, posteriormente han ido apareciendo muchas otras.

En este apartado vale la pena mencionar también la aparición en 2015 del ecosistema **Ethereum**, una cadena de bloques inspirada en la de Bitcoin, pero con la finalidad de crear un lenguaje universal que permite la creación de aplicaciones descentralizadas (Đapps) que alojen contratos inteligentes (Smart Contracts).

Las dos anteriores, Bitcoin y Ethereum, son las dos criptomonedas por excelencia, sin embargo, a lo largo de los últimos años han ido apareciendo múltiples de ellas (en estos momentos hay listadas 2066 criptomonedas y

tokens en Coinmarketcap[8]), siendo algunos ejemplos destacables[9]:

- **Ripple** (XRP): cuyo objetivo es enrutar los pagos entre pares de manera más rápida y eficiente que el resto de criptodivisas.
- **Monero** (XMR): criptomoneda enfocada principalmente a la privacidad y el anonimato basándose en un tipo de firma digital denominada firma en anillo.
- **Litecoin** (LTC): moneda electrónica basada en Bitcoin, diferenciándose de éste último en algunos aspectos técnicos.

2.3.6.2 Aplicaciones decentralizadas y contratos inteligentes

En este apartado se describirán dos grandes conceptos derivados de la aparición de Ethereum y que se nombraron en el apartado anterior: aplicaciones descentralizadas (Đapps) y contratos inteligentes (Smart Contracts).

El primero de ellos (Đapps) hace referencia a una app que no depende de un sistema central, sino de la comunidad de usuarios que la utilizan. La aplicación descentralizada puede ser una app móvil o una aplicación web que interactúa con un contrato inteligente para llevar a cabo su función.

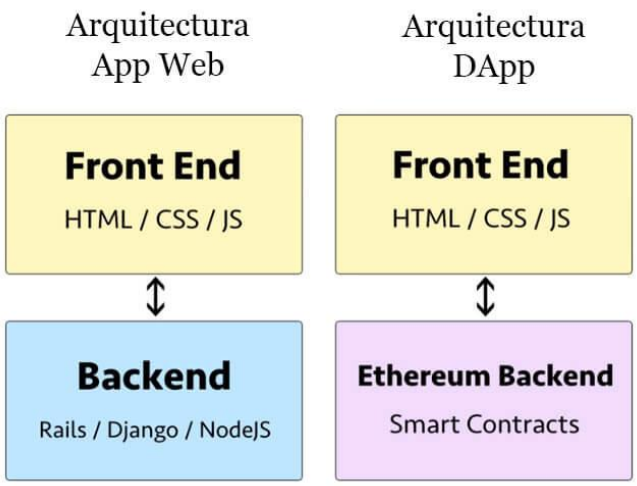


Figura 20. Comparación entre aplicación web y aplicación descentralizada. Fuente: miethereum.com

Como se puede observar en la Figurar anterior, a diferencia de lo que podría ser, por ejemplo, Facebook, una aplicación descentralizada no cuenta con un Backend en unos servidores como punto único de apoyo. Por el contrario, las Đapps se construyen sobre una red descentralizada de nodos, siendo la más famosa y utilizada la de Ethereum.

Por otro lado, un **contrato inteligente** es un programa informático que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes. Su funcionalidad es idéntica a la del operador condicional "if else" ampliamente usado en los lenguajes de programación, en el cual se ejecutan sentencias siempre que se cumpla una cierta condición.

2.3.7 Herramientas de código abierto

A pesar de, como ya se ha comentado en ocasiones anteriores, la tecnología Blockchain es relativamente nueva,

[8] https://coinmarketcap.com/all/views/all/
[9] Al resto de criptomonedas, aparte de Bitcoin, también se les denomina "Altcoins"

en los últimos tiempos han surgido diferentes herramientas y soluciones con las que poder construir un escenario que se sirva de ella siendo algunos ejemplos: Hyperledger [16], Corda [17], EWF (Energy Web Foundation) [18] o Multichain [19].

3 PRUEBA DE CONCEPTO

If I had asked my customers what they wanted, they would have said: a faster horse.

- Henry Ford -

En el presente capítulo se detallará una Prueba de Concepto (PoC, del inglés Proof of Concept) que sirve para mostrar cómo se ha construido un sistema de votación basado en Blockchain desde cero. A lo largo de este apartado se verá tanto la parte que se presenta al votante, como el funcionamiento de los nodos que componen la parte interna del Sistema.

La solución se ha realizado en el lenguaje de programación Python y a lo largo del capítulo se irán mostrando porciones del código que se utiliza de modo que se complemente con la explicación de los distintos componentes del Sistema.

Cabe aclarar también que durante la realización de la PoC no se ha buscado ofrecer una interfaz gráfica pulida como la que probablemente se mostraría al usuario en el caso de realizar su implementación final. Por el contrario, lo que sí se ha buscado ha sido ofrecer **toda la funcionalidad** de modo que demuestre, desde un punto de vista técnico, todas las características de las que consta el proyecto.

3.1 Introducción

Como planteamiento inicial para el posterior desarrollo del proyecto, se han tenido en mente los conceptos descritos en la primera parte de este documento: un sistema de elecciones mediante voto por Internet como el implementado en Estonia y un sistema mediante Blockchain como el usado en Bitcoin.

Con esta base como punto de partida se ha desarrollado una PoC que permita entrever como pudiera hacerse un sistema complejo que pudiera implementarse para dar solución a la problemática en España de que no exista un método de votación segura por Internet.

3.1.1 Escenario a simular

El escenario ideal que se pretende simular es un sistema que consta fundamentalmente de dos partes. Una primera parte sería una red de nodos gestionados por el Estado y conectados entre sí en una red peer-to-peer, los cuales recibirían constantemente (durante el día de votación) miles y miles de votos, los cuales serían verificados, validados y añadidos a una gran "base de datos". Esta base de datos podría ser consultada y verificada directamente por los ciudadanos en tiempo real.

La segunda parte de la que constaría el sistema sería la parte visible a los votantes. Esta parte consistiría en una aplicación para móvil o una aplicación web a la que accederían los ciudadanos y que utilizarían con el objetivo de registrarse, realizar la votación y también para comprobar que su voto se ha registrado correctamente en el sentido en el que fue emitido.

3.1.2 Suposiciones y limitaciones

Una vez se ha explicado el sistema ideal que se pretende simular, la PoC que ha realizado contará claramente con las limitaciones -tanto temporales como materiales- propias de lo que es un Trabajo Fin de Máster. Por lo tanto, hay algunos aspectos que se han tenido que suponer y que habría que tener en cuenta a la hora de pasar de una mera Prueba de Concepto a una implementación real.

Una de estas suposiciones tiene que ver con las **comunicaciones**. En la PoC se utilizarán varios nodos simultáneos, los cuales procesarán los votos que vayan recibiendo. Sin embargo, todos estos nodos estarán concentrados en una única máquina. Es por ello que no se han estudiado las características propias de un sistema de comunicaciones entre entidades ni los posibles protocolos a usar.

Otro aspecto que se ha tenido que suponer ha sido el de la **seguridad**. Este es un aspecto de gran importancia ya que, como se verá posteriormente, en el caso de que se consiga comprometer cualquier de los nodos, éste podría añadir votos ilegítimos a la cadena de bloques. A pesar de ello, sí que cuenta con características de seguridad propias de un sistema con Blockchain, como es el detectar cualquier alteración de los datos registrados o que, como ya se ha comentado anteriormente, cada ciudadano puede verificar su propio voto con el fin de cerciorarse de que éste no ha sido manipulado.

3.1.3 Requisitos

Además, se han definido una serie de requisitos de los que debe hacer cumplimiento el sistema para que satisfaga con unas características necesarias mínimas.

Uno de estos requisitos es que el votante que se registre haya sido previamente **validado por un tercero**. En este caso se pensó en la FNMT y su certificado digital. El certificado digital es un instrumento ampliamente usado en España para realizar operaciones confidenciales a través de páginas webs de instituciones públicas como la Agencia Tributaria, la Seguridad Social o los Registros Mercantiles.

Otro requisito que se ha tenido en cuenta para la realización del trabajo ha sido el relativo al **procesado de votos**. En el sistema ideal que se tiene como base se procesarían miles de votos por segundo, sin embargo, si bien con las limitaciones propias de este trabajo eso es difícilmente simulable, sí que se ha establecido como requisito que se puedan procesar una cierta cantidad de votos por segundo llegando hasta las varias decenas.

3.1.4 Sistema basado en Blockchain privada

Aunque en general los sistemas más conocidos de Blockchain están asociados al concepto de red pública éste no es el único modelo de cadena de bloques existente.

Tal y como se ha explicado en el apartado sobre Clasificación de Blockchain, existen diferentes puntos de vista a la hora de utilizar el mismo concepto de almacenar datos en una cadena de bloques y cada una de ellas puede ajustarse mejor a cada necesidad dependiendo de la casuística.

3.1.4.1 Resiliencia

Puesto que la solución es escalable y el sistema se puede diseñar para que conste de tantos nodos como se deseen, se puede afirmar que sería totalmente resiliente ya que el fallo de uno de los nodos no afectaría al funcionamiento del escenario. Para ello, se podría implementar que cuando uno de los nodos caiga, la información que tendría

que ser procesada por éste pase por el resto de nodos que sí funcionan, haciendo muy difícil que el sistema deje de dar servicio en algún momento.

3.1.4.2 Seguridad

A diferencia de una Blockchain pública en la que los nodos (mineros) son anónimos, en este caso se puede conocer quién o quienes participan en el sistema.

De esta manera se imposibilita la opción de que aparezca alguna entidad con fines maliciosos en la estructura. Por lo tanto, como se ha explicado en apartados anteriores, el uso de una Blockchain privada haría al sistema inmune al clásico ataque por 51%, ya que solo participarían nodos confiables, evitando que un posible atacante modifique la cadena a su antojo.

3.1.4.3 Precio

Una Blockchain privada generalmente es más barata que una pública.

Este hecho es fácilmente entendible puesto que en las soluciones públicas se incentiva a la participación mediante el pago a los mineros (por ejemplo en Bitcoin con 12.5 BTC) además de la alta tasa/cuota (fee en inglés) que deben pagar los usuarios a los mineros por cada transacción que realizan (en estos momentos próximo a los 20 $ de media[10]).

Por lo tanto, el uso de una Blockchain totalmente pública por parte de una institución también pública no solo podría hacerla vulnerable al ataque por 51% ya comentado, sino que incrementaría el coste de la solución por el pago a los posibles participantes.

3.1.4.4 Ejemplo de aplicaciones

Algunas entidades famosas ya usan la estructura de Blockchain privada.

Por ejemplo, **Ripple (XRP)**, la tercera criptomoneda más importante, utiliza un sistema privado. **One Pay FX**, la solución basada en Blockchain para transferencias internacionales del Banco Santander también es privada. **Quorum** es otra solución basada en Blockchain privada creada por el banco JP Morgan.

3.2 Entidades del Sistema

En este apartado se describirán las distintas entidades que forman parte del Sistema.

3.2.1 Cliente

Es la aplicación visible al votante y se utilizará para poder realizar la acción del voto.

```
============================== [MENU] ==============================
1. Registrar votante   (Votantes: 50)
2. Votar               (Candidatos: 3)
3. Mostrar resultados  (Bloques: 51)
4. Simular votación
0. Exit
====================================================================
Introduzca su opcion [0-4]:
```

Figura 21. Aplicación del cliente. Comando: `python cliente.py 1`

[10] https://www.blockchain.com/es/charts/cost-per-transaction

Las principales funcionalidades de las que consta la parte de la aplicación del cliente, y que se detallarán posteriormente, son:

- Registrar al votante.
- Votar.
- Mostrar resultados.
- Simular votación (usada en la PoC, esta opción no se implementaría en la aplicación final).

La aplicación podría implementarse como interfaz gráfica ya sea en una aplicación móvil que los votantes se podrían descargar en sus propios móviles o en una interfaz web pública.

El código de la aplicación del cliente se recoge en el fichero `cliente.py` y se ejecuta con el comando:

```
python cliente.py [n]
```

siendo [n] el número de nodos que se van a crear.

3.2.1.1 Opción 1: Registrar votante

A continuación se presenta el diagrama de flujo que ayuda a entender cómo sería el proceso para el registro del votante para que éste pueda realizar la votación:

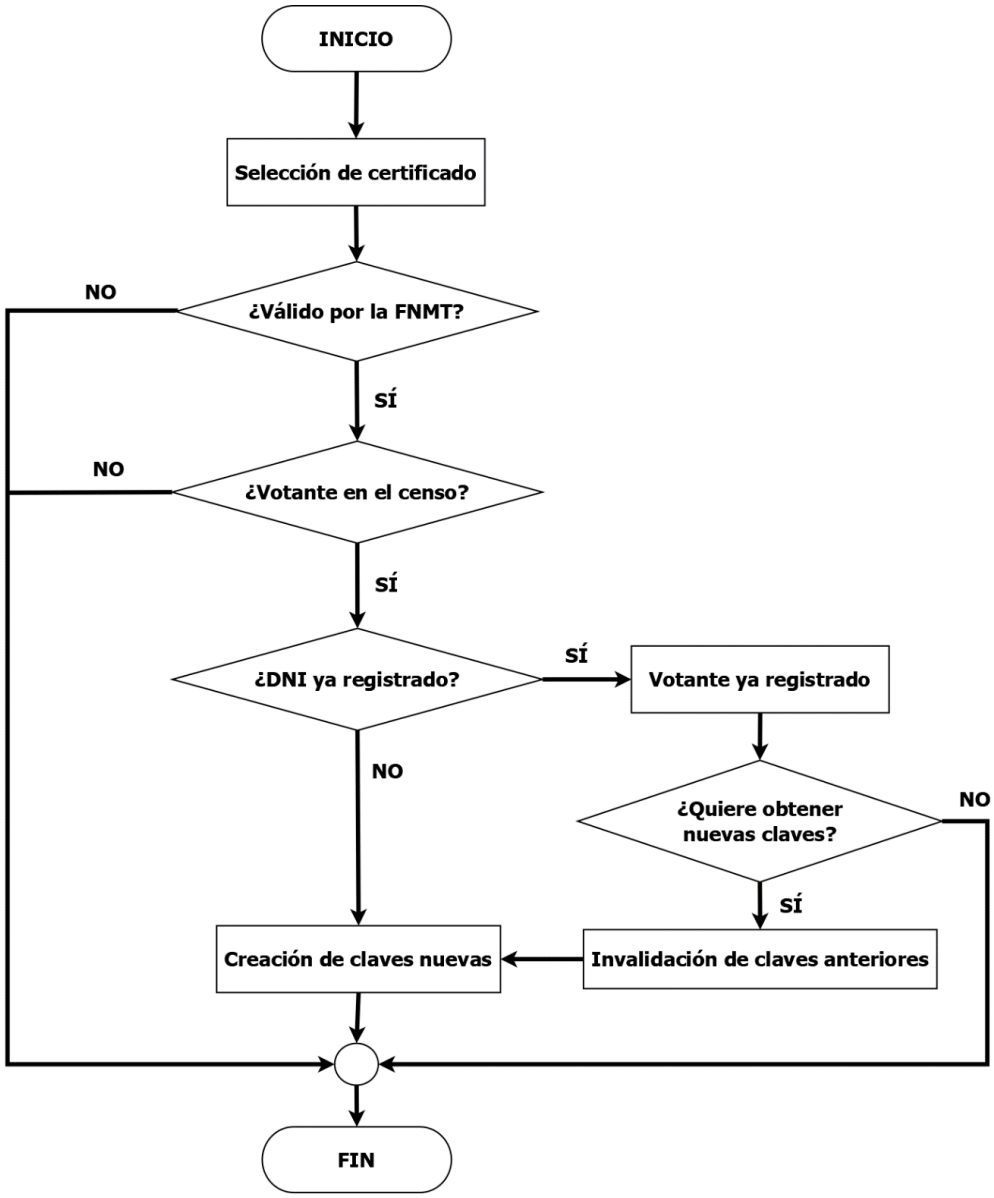


Figura 22. Diagrama de flujo del registro del votante.

En primer lugar, la aplicación solicita el certificado digital de la persona (formato .crt).

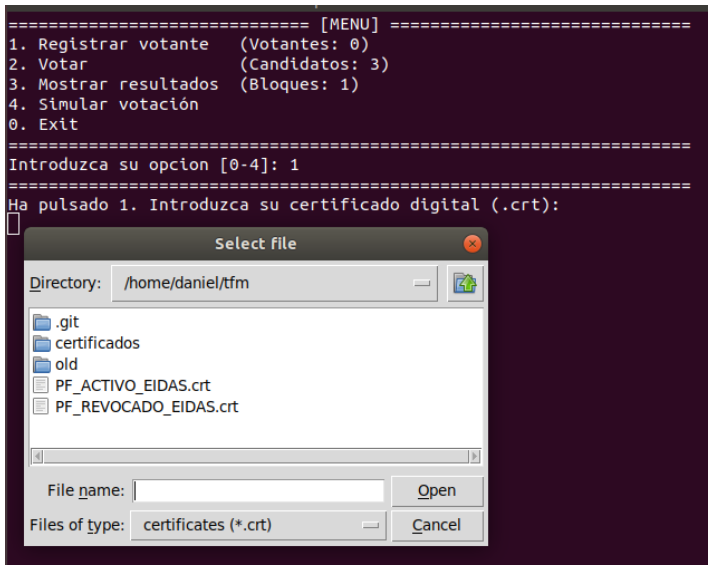


Figura 23. Introducción de certificados (extensión .crt)

Una vez se obtiene el certificado, la aplicación realiza tres comprobaciones:

1. **El certificado digital es válido**. Esta comprobación se realiza haciendo una petición al servidor OCSP oficial de la FNMT.

Comando para comprobar un certificado contra el servidor OCSP oficial de la FNMT:

```
openssl ocsp -issuer [issuer.pem] -cert [cert.pem] -url
   http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder
```

donde *issuer.pem* es el certificado del emisor (en esta ocasión la FNMT) y *cert.pem* es el certificado que se desea validar.

2. **El votante se encuentra en la base de datos del censo**. Se tiene una base de datos SQL (censo.db) en la que se encuentra el DNI, nombre y apellidos de las personas con derecho a voto, además de un número que identifica el nodo al que se debe enviar dicho voto (esto sirve para hacer conteos locales, como pudiera ser las circunscripciones que existen en las elecciones españolas).

Tabla 1. Base de datos de ejemplo de censo (censo.db).

Apellidos	Nombre	DNI	Nodo
PEREZ LORENZO	MARCOS	11111111A	1
CRUZ LOZANO	GONZALO	22222222B	4
MARTIN SANTIAGO	HELENA	33333333C	3
EIDAS CERTIFICADO	PRUEBAS	99999999R	2
FERNANDEZ MORALES	EVA	44444444D	1

3. **El votante no ha votado todavía**. Si el votante sí hubiese votado y deseara volver a votar (o hubiera perdido las claves anteriores) se le invalidará el voto y las claves anteriores, obteniendo unas nuevas.

Una vez estas tres comprobaciones resultan satisfactorias, el votante recibe un par de claves: la clave privada y la clave pública.

- **Clave privada**: solo debe ser conocida por el votante. Debido a que la clave pública es derivada de la clave privada, esta clave es la que permite al votante demostrar que la clave pública es suya.
- **Clave pública**: esta clave será visible en los resultados de la votación y permitirá al votante comprobar a quién se le ha contabilizado su voto.

En la solución se ha usado el sistema criptográfico de clave pública RSA, generando el par de claves mediante la función **new_wallet()**:

```
def new_wallet(): #Genera un par de claves(wallet) aleatoriamente
    random_gen = Crypto.Random.new().read
    private_key = RSA.generate(1024, random_gen)
    public_key = private_key.publickey()
    response = {
            'private_key': binascii.hexlify(private_key.exportKey(format =
'DER')).decode('ascii'),
            'public_key': binascii.hexlify(public_key.exportKey(format =
'DER')).decode('ascii')
}
return response
```

Las claves generadas serán guardadas en el fichero JSON correspondiente.

3.2.1.2 Opción 2: Votar

En primer lugar se le presentará al votante las posibles opciones, en este caso candidatos, que puede elegir:

```
============================== [MENU] ==============================
1. Registar votante    (Votantes: 1)
2. Votar               (Candidatos: 3)
3. Mostrar resultados  (Bloques: 1)
4. Simular votación
0. Exit
====================================================================
Introduzca su opcion [0-4]: 2
====================================================================
Ha pulsado 2. Indique el candidato al que quiere votar:
1. Candidato 1
2. Candidato 2
3. Candidato 3
0. Voto Nulo
====================================================================
Introduzca su opción [0-3]: 2
```

Figura 24. Selección de candidatos en Cliente.

Una vez que ha elegido al candidato, se le solicita al votante que introduzca sus claves, tanto la pública como la privada.

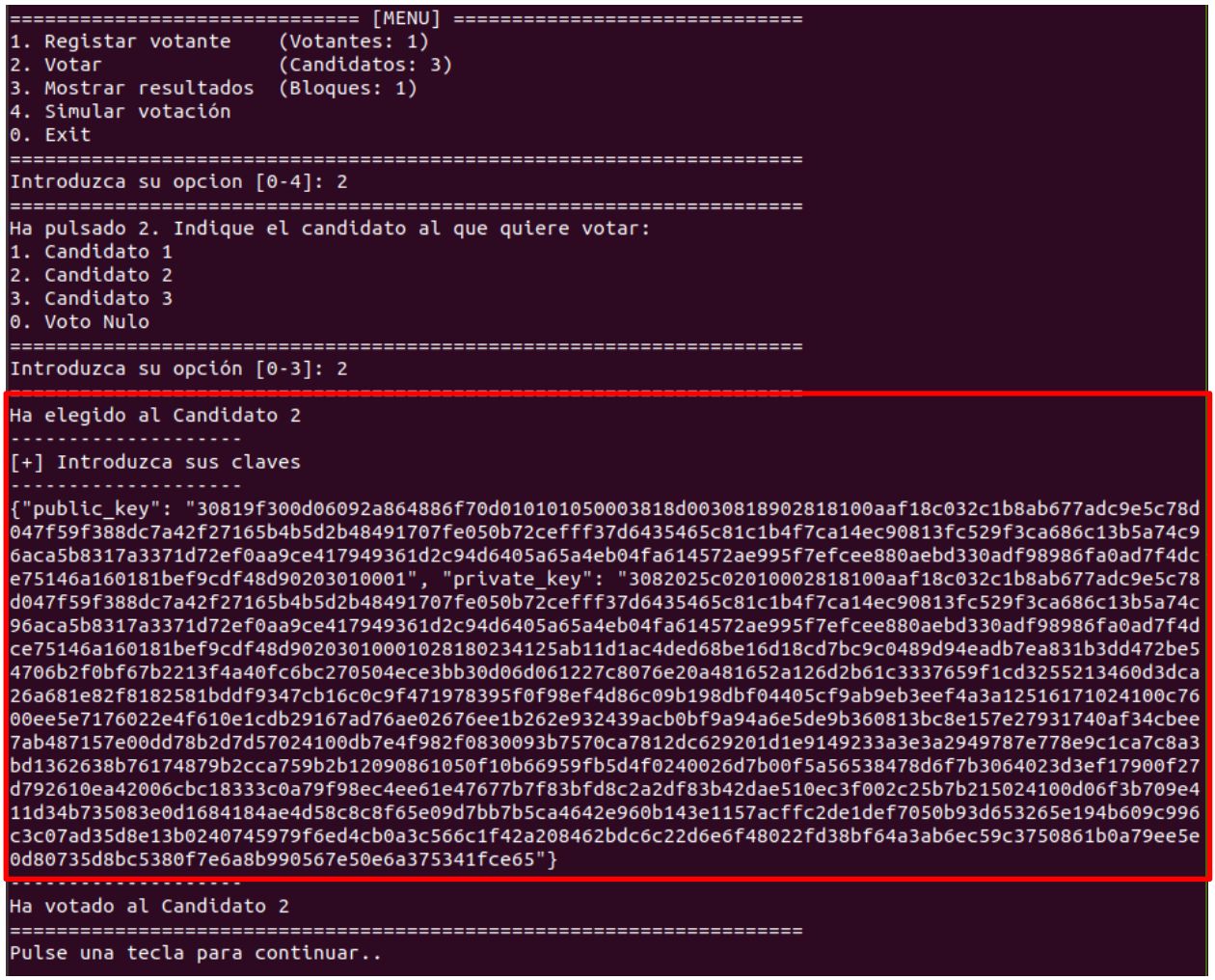


Figura 25. Elección de candidato. En esta ocasión Candidato 2.

En el caso de que dichas claves no hayan sido usadas anteriormente, la aplicación enviará al nodo correspondiente la información necesaria para contabilizar el voto:

- La **clave pública del votante**.
- La **transacción**, que consta de la clave pública del votante, la clave pública del candidato elegido y el valor a transferir (en este caso siempre será 1, debido a la regla 1 votante - 1 voto).
- La **transacción firmada** con la clave privada del votante.

Tal y como se explicó en el apartado *Verificación de transacciones*, con estos tres datos (en los cuales nunca estará explícitamente la clave privada), el nodo será capaz de verificar que el voto ha sido emitido por el votante que se registró mediante el certificado digital.

Cabe la posibilidad de que el votante introduzca unas claves con las que ya se votó anteriormente. En este caso únicamente se contabilizará el último voto que se haya realizado con dichas claves. Esta característica es necesaria para este tipo de votaciones. De este modo se asegura que el votante pueda usar sus claves tantas veces como quiera, pudiendo cambiar su voto y evitando así contabilizar un único voto que pudiera realizarse mientras está siendo coaccionado por una tercera persona.

3.2.1.3 Opción 3: Mostrar resultados

Si se elige esta opción, se abrirá el navegador con una página que mostrará tres apartados:

Chequeo de Blockchain

Este apartado se realiza mediante la función **check_blockchain()** y en ella se comprueban dos aspectos:

1. Se vuelven a calcular los hashes de todos los bloques individualmente.
2. Se comprueba que el bloque n tiene correctamente guardado el hash del bloque anterior.

Así se verifica no solo la integridad de cada bloque individualmente, sino también la integridad conjunta de toda la cadena de bloques.

Función **check_blockchain():**

```
def check_blockchain():   # Verifica que no se ha cambiado el fichero blockchain
        # Verifica los hashes de todos los bloques
        for i in range(0, len(blockchain)):

        index,timestamp,aux_transaction,aux_node,prev_hash,actual_hash=blockchain[i].s
plit("|")
                t = aux_transaction.split(",")
                aux = Transaction(t[0],t[1],t[2]).to_dict()

                aux_block = Block(index,timestamp,aux,aux_node,prev_hash)

                if aux_block.hash != actual_hash:
                        return False
                        break
        # Verifica la correspondencia de hashes entre bloques
        current_index = 0
        while current_index < len(blockchain)-1:

        index,timestamp,aux_transaction,aux_node,prev_hash,actual_hash=blockchain[curr
ent_index].split("|")

        index2,timestamp2,aux_transaction2,aux_node2,prev_hash2,actual_hash2=blockchai
n[current_index+1].split("|")
                if (actual_hash != prev_hash2):
                        return False
                        break
                current_index += 1
        return True
```

Resultados de la votación

El objetivo de esta parte es, como su propio nombre indica, mostrar los resultados de la votación, es decir, presentar la cantidad de votos que ha obtenido cada uno de los Candidatos que participan en la misma.

Este apartado se consigue leyendo, desde el principio hasta el final, todos y cada uno de los bloques que

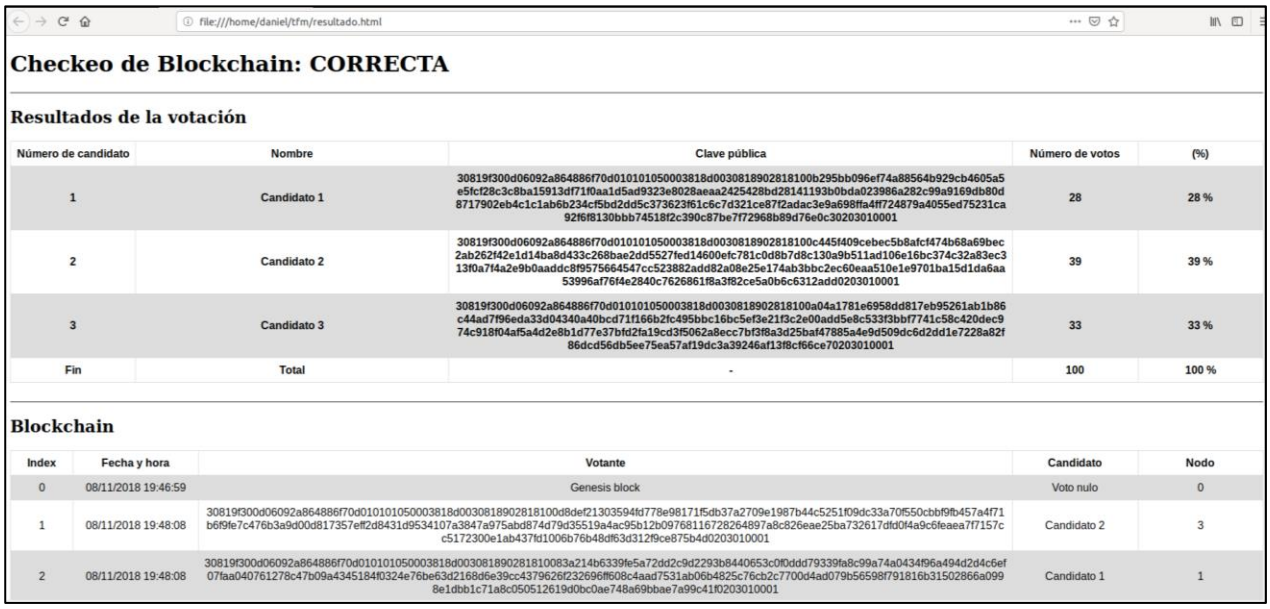
conforman la cadena, contabilizando para cada clave pública que se encuentre únicamente el último de los votos que ha realizado. Esta característica de poder votar varias veces, como ya se ha explicado en apartados anteriores, es la que garantiza que la persona pueda votar tantas veces como quiera sin desvirtuar la votación.

Además, para cada clave pública, se hace una comprobación adicional: se verifica que dicha clave pública es la última que se ha solicitado con su firma digital asociada. De este modo, si una persona perdiera sus claves -solicitando unas nuevas- únicamente se le contabilizaría el voto realizado con las últimas claves que se les proporcionó.

Nota: con éste último punto, al guardar cuáles son las últimas claves válidas de cada persona, se podría pensar que sería posible conocer la clave pública de un votante perdiendo su anonimato. Sin embargo, esto no es posible ya que la relación que se guarda es el hash de la firma digital con la clave pública asociada. Por lo tanto, debido a que a partir del hash no es posible obtener la firma digital que lo generó, se seguiría sin poder hacer la relación votante-clave pública.

Blockchain

En esta última parte de los resultados se expone la cadena de bloques completa mostrando principalmente la fecha y hora del bloque, la clave pública del votante y el Candidato al que se ha votado.



file:///home/daniel/tfm/resultado.html

Checkeo de Blockchain: CORRECTA

Resultados de la votación

Número de candidato	Nombre	Clave pública	Número de votos	(%)
1	Candidato 1	30819f300d06092a864886f70d010101050003818d00308189028181 00b295bb096ef74a88564b929cb4605a5e5fcf28c3c8ba15913df71f0aa1d5ad9323e8028aeaa2425428bd28141193b0bda023986a282c99a9169db80d8717902eb4c1c1ab6b234cf5bd2dd5c373623f61c6c7d321ce87f2adac3e9a698ffa4ff724879a4055ed75231ca92f6f8130bbb74518f2c390c87be7f72968b89d76e0c30203010001	28	28 %
2	Candidato 2	30819f300d06092a864886f70d010101050003818d00308189028181 00c445f409cebec5b8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f95756645 47cc523882add82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861f8a3f82ce5a0b6c6312add0203010001	39	39 %
3	Candidato 3	30819f300d06092a864886f70d010101050003818d00308189028181 00a04a1781e6958dd817eb95261ab1b86c44ad7f96eda33d04340a40bcd71f166b2fc495bbc16bc5ef3e21f3c2e00add5e8c533f3bbf7741c58c420dec974c918f04af5a4d2e8b1d77e37bfd2fa19cd3f5062a8ecc7bf3f8a3d25baf47885a4e9d509dc6d2dd1e7228a82f86dcd56db5ee75ea57af19dc3a39246af13f8cf66ce70203010001	33	33 %
Fin	Total	-	100	100 %

Blockchain

Index	Fecha y hora	Votante	Candidato	Nodo
0	08/11/2018 19:46:59	Genesis block	Voto nulo	0
1	08/11/2018 19:48:08	30819f300d06092a864886f70d010101050003818d00308189028181 00d8def21303594fd778e98171f5db37a2709e1987b44c5251f09dc33a70f550cbbf9fb457a4f71b6f9fe7c476b3a9d00d817357eff2d8431d9534107a3847a975abd874d79d35519a4ac95b12b097681167282648 97a8c826eae25ba732617dfd0f4a9c6feaea7f7157cc5172300e1ab437fd1006b76b48df63d312f9ce875b4d0203010001	Candidato 2	3
2	08/11/2018 19:48:08	30819f300d06092a864886f70d010101050003818d00308189028181 10083a214b6339fe5a72dd2c9d2293b8440653c0f0ddd79339fa8c99a74a0434f96a494d2d4c6ef07faa040761278c47b09a4345184f0324e76be63d2168d6e39cc4379626f232696ff608c4aad7531ab06b4825c76cb2c7700d4ad079b56598f791816b31502866a0998e1dbb1c71a8c050512619d0bc0ae748a69bbae7a99c41f0203010001	Candidato 1	1

Figura 26. Ejemplo de resultados de votación. Fichero: resultado.html

A nivel de código, esta página se construye creando el fichero `resultado.html` en tiempo de ejecución.

3.2.1.4 Opción 4: Simular votación

Esta opción simplemente pide como dato el número de votos que se quieren crear y simula todo el proceso que se ha descrito en los apartados anteriores (a excepción de la comprobación de los certificados) con votos generados aleatoriamente.

3.2.2 Nodo

La función principal del Nodo es la de ir leyendo las transacciones que se depositan en el fichero “pending”, las

verifica por orden de llegada y, en caso de resultar correcta, la añade a Blockchain.

La aplicación del Nodo se recoge en el fichero `nodo.py` y se ejecuta con el comando:

```
python nodo.py [n]
```

siendo [n] el id del nodo que se va a crear.

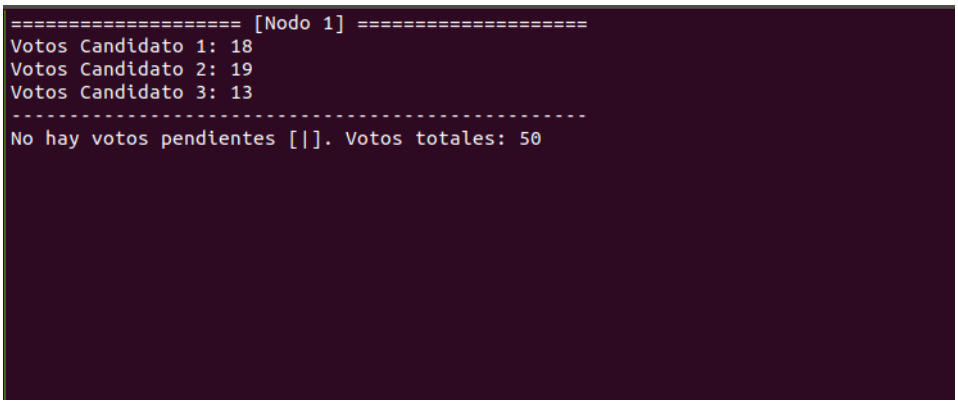


Figura 27. Aplicación del nodo. Comando: `python nodo.py 1`

3.2.2.1 Verificación de voto

La parte de verificación de transacciones se ha implementado en la Solución con la función **verify_transaction_signature**:

```
def verify_transaction_signature(sender_address, signature, transaction):
        # Check that the provided signature corresponds to transaction
        # signed by the public key (sender_address)
        this_public_key = RSA.importKey(binascii.unhexlify(sender_address))
        this_verifier = PKCS1_v1_5.new(this_public_key)
        this_h = SHA.new(str(transaction).encode('utf8'))

        return this_verifier.verify(this_h, binascii.unhexlify(signature))
```

3.2.2.2 Añadir bloque

Al contrario de lo que ocurre en Bitcoin con el sistema de Prueba de Trabajo, en este caso cualquier nodo que pertenezca a la red puede añadir bloques al registro.

Tal y como se diferenció en apartados anteriores, existen cadenas de bloques sin permisos y cadenas de bloques con permisos y en este escenario se ha pensado para que participen únicamente nodos autorizados, es decir, con permisos.

Esto podría plantear un problema, y es que varios nodos reciban votos a la vez e intentaran escribir en el registro al mismo tiempo. Esta casuística, que en Bitcoin se soluciona eligiendo siempre la cadena de mayor tamaño, se ha solucionado en esta ocasión creando un *semáforo* mediante el cual el nodo que se encuentra utilizando el registro avisa al resto para que no se sobreescriban votos.

Para añadir bloques, se ha usado la función **add_block**:

```
def add_block(blockchain,block):
        blockchain.append(block)
        fblockchain = open("blockchain.dat","a")
        fblockchain.write(block.index + "|" + block.timestamp + "|" +
block.transaction['sender_address'] + "," + block.transaction['recipient_address'] +
"," + str(block.transaction['value']) + "|" + str(block.node) + "|" +
block.previous_hash + "|" + block.hash + '\n')
        fblockchain.close()
```

En dicha función, además de añadir el bloque al fichero blockchain.dat, también se añade a la lista local que contiene cada nodo independientemente y que se guarda en la lista denominada *blockchain*.

3.2.3 Blockchain

Representa la cadena formada por los bloques que contienen todos los votos que se han realizado. Esto no significa que todos los votos que contiene son válidos, ya que cabe la posibilidad que haya varios votos realizados por la misma clave (en este caso solo se cuenta el último) o que haya votos realizados por claves que ya no son válidas (en cuyo caso no se contabilizan).

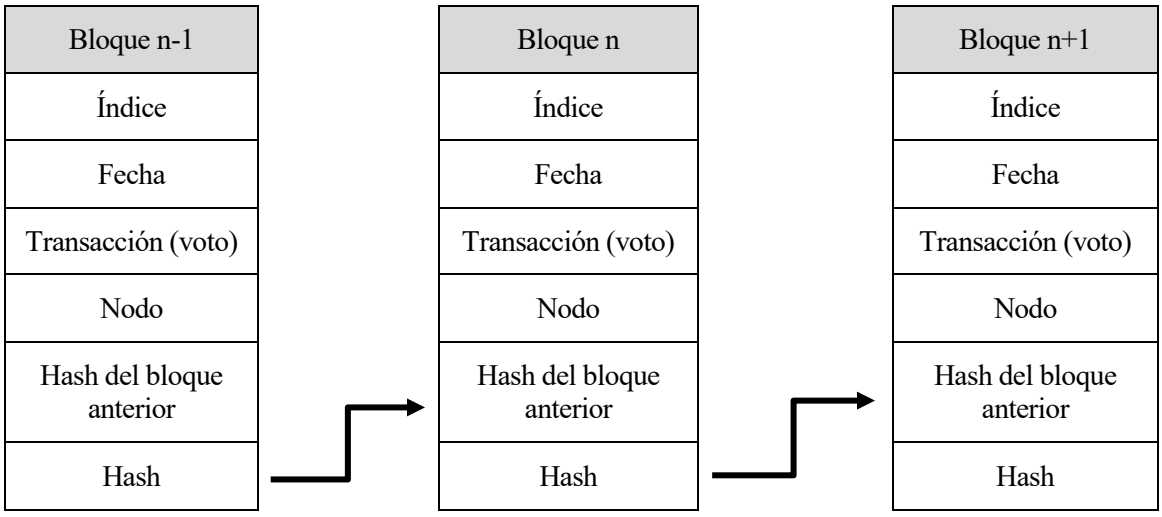


Figura 28. Descripción de la Blockchain utilizada.

Los datos de cada bloque son:

- **Índice**: número que representa la posición del bloque en la cadena de bloques.
- **Fecha**: fecha y hora en la que se ha realizado el voto.
- **Transacción**: contiene la información del votante, el candidato votado y el número de votos (en este caso siempre será 1).
- **Nodo**: nodo que ha verificado el voto.
- **Hash del bloque anterior**: función hash del bloque anterior.
- **Hash**: función hash de los datos contenidos en el bloque.

Nota: para la función hash se ha usado el algoritmo SHA-256, el cual hasta la fecha ha demostrado no presentar colisiones.

3.2.4 Relación y permisos entre entidades

Una parte importante del diseño de cualquier sistema es establecer los distintos permisos de los agentes que lo conforman.

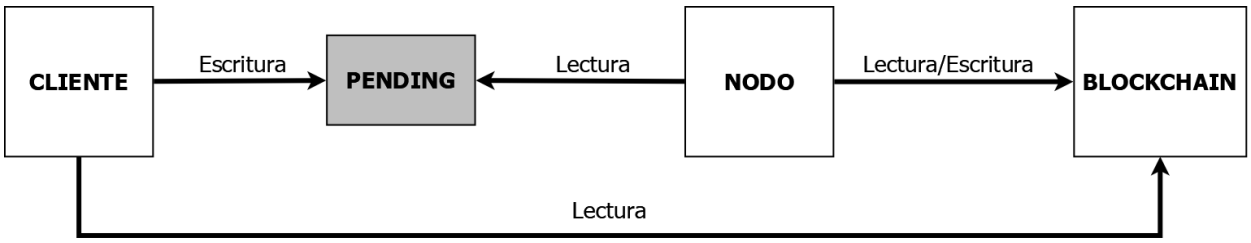


Figura 29. Relación y permisos entre entidades.

Los permisos que se detallan a continuación son los mínimos necesarios para que la votación sea lo más transparente posible además de que igualmente ninguna entidad tenga acceso a algún dato que no sea estrictamente necesario.

3.2.4.1 Cliente

Será necesario el permiso de escritura sobre el archivo pending asociado al nodo para la correcta transmisión del voto y el permiso de lectura en Blockchain para que el usuario pueda observar tanto el conteo de su voto en particular como el de toda la votación en general ya que se trata de que la votación sea lo más transparente posible.

3.2.4.2 Nodo

Al ser la parte central del Sistema será la entidad que más permisos posea, siendo por ello también la parte más crítica de la estructura y por lo tanto la entidad que más protegida debe estar.

El nodo obtiene los votos de su fichero pending asociado y por consiguiente debe tener permisos de lectura sobre él. Asimismo, debe tener permisos tanto de lectura como de escritura sobre la Blockchain; de lectura para conocer el estado en el que se encuentran los datos (por ejemplo conocer si existe el bloque génesis[11] y si no crearlo o hacer recuentos por parte de los nodos) y de escritura para añadir a la cadena los votos que han sido emitidos por los votantes.

3.2.4.3 Blockchain

Al no tener que realizar acciones sobre el resto de entidades, no es necesario que a Blockchain se le asignen permisos especiales.

3.2.5 Ficheros auxiliares

3.2.5.1 pending_n.dat

En este fichero el nodo n recibirá los datos que necesita para validar transacciones, los cuales se escriben con el siguiente formato:

[11] Se denomina Bloque Génesis al primer bloque de la cadena.

Fecha | Clave pública del votante | Transacción | Firma

Transacción = (Clave pública del votante, Clave pública del Candidato, Voto)

3.2.5.2 blockchain.dat

Fichero que contiene todos los bloques que han sido previamente validados por los nodos.

Índice | Fecha | Transacción | Nodo | Hash del bloque anterior | Hash

3.2.5.3 votantes_dni.dat

En este fichero se apuntan los DNI de los votantes que ya han realizado su voto.

3.2.5.4 votantes_publickey.dat

En este fichero se apuntan dos datos: el primero el hash del certificado digital que se ha usado para votar y el segundo la clave pública que se le ha asignado a ese hash.

Hash del certificado (SHA256), Clave pública del votante

Este fichero permite volver a votar a un votante que haya podido perder sus claves, ya que relaciona su certificado con la clave pública que tiene asignada para la votación.

En este punto se podría pensar que se puede llegar a correlar la clave pública del votante con él mismo y poder conocer el sentido de su voto. Esto en realidad no es posible debido a que a partir de la función hash no es posible determinar el certificado origen que lo ha generado.

3.2.5.5 candidatos.dat

Contiene las claves públicas de los candidatos. Cabe aclarar que para este sistema no es estrictamente necesario que los candidatos cuenten con clave pública ya que el valor a transferir (en este caso votos) no serán de uso exclusivo para el receptor como suele ocurrir por ejemplo en las criptomonedas. Sin embargo, con el propósito de guardar semejanza con los esquemas típicos de uso de Blockchain, se ha utilizado igualmente el sistema de criptografía asimétrica para los candidatos.

A continuación veremos los candidatos que se han usado para este caso:

Tabla 2. Candidatos de ejemplo usados en la Prueba de Concepto.

Candidato	Cláve pública
Cándidato 1	30819f300d06092a864886f70d010101050003818d0030818902818100b295bb096ef74a88564b929cb4605a5e5fcf28c3c8ba15913df71f0aa1d5ad9323e8028aeaa2425428bd28141193b0bda023986a282c99a9169db80d8717902eb4c1c1ab6b234cf5bd2dd5c373623f61c6c7d321ce87f2adac3e9a698ffa4ff724879a4055ed75231ca92f6f8130bbb74518f2c390c87be7f72968b89d76e0c30203010001
Cándidato 2	30819f300d06092a864886f70d010101050003818d0030818902818100c445f409cebec5b8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547cc523882add82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861f8a3f82ce5a0b6c6312add0203010001
Cándidato 3	30819f300d06092a864886f70d010101050003818d0030818902818100a04a1781e6958dd817eb95261ab1b86c44ad7f96eda33d04340a40bcd71f166b2fc495bbc16bc5ef3e21f3c2e00add5e8c533f3bbf7741c58c420dec974c918f04af5a4d2e8b1d77e37bfd2fa19cd3f5062a8ecc7bf3f8a3d25baf47885a4e9d509dc6d2dd1e7228a82f86dcd56db5ee75ea57af19dc3a39246af13f8cf66ce70203010001

3.2.5.6 Claves del votante

Las claves de los votantes se guardan en formato JSON en un fichero cuyo nombre tiene el siguiente formato "[fecha]_[hora]_[DNI].dat".

Ejemplo **20190122_16-34_99999999R.dat**:


```
{
   "public_key":"30819f300d06092a864886f70d010101050003818d003081902818100a8ad8f407b22b1bffadaa63706608abd07df
4c23c885813d37975dffd5078fa1ba7c11a8003eced3d8c7bfbcbd69d2f114d4268158cc47ffee1e8a97c3e7bb6233ee111da83d3155659
4f0831327b24bbc7b1988d067cbb46ff3a008c8d45c20a77f7ca8ce073f5edb4ccbe4100bcc4a374fae1b63d5ce7e5f54a9656decf95902
03010001",
   "private_key":"3082025d02010002818100a8ad8f407b22b1bffadaa63706608abd07df4c23c885813d37975dffd5078fa1ba7c11a
8003eced3d8c7bfbcbd69d2f114d4268158cc47ffee1e8a97c3e7bb6233ee111da83d31556594f0831327b24bbc7b1988d067cbb46ff3a0
08c8d45c20a77f7ca8ce073f5edb4ccbe4100bcc4a374fae1b63d5ce7e5f54a9656decf9590203010001028181008 4c61183dd2963274e0
bbc5885d18a83df657aa69419dab05848f2fa0532ed718dbc499da78bc8fc62a06121ed2b169b241d16ae2c3aa8d62116b35b611ed094e3
864832f263149af93159370eb992daf9e0cb8402180ae218769d87a3a9857281d82a0c724bed18687a4be776c80e5f8581aef61b0ba5a07
02272d3fb1b741d024100b671149a41ad2470bd1da80862ef5e886b8b49e54e34849fcbdb406ea801ed52213081ddadecc28ffa0423005c
f5307472b99e98d721c12de7256ce320cfa7bf024100ecafd6a0e50fb86be1c93c93c25849a8169a940f5d846f3116d824dad68fffdaf07
90332672deb2fe8a3c3a22d2875423bd1a4944a5db1006cf98d653c7a64e702406c1eb1de05240e1f7e04304be00e09d1012308050c06d5
be39bad3018131bb2a5c1efa279ce65e1ba3488651b5c55d14f5d48967fcbeb55475d2d927f58efad302405842ee1f8babc412fedca3295
aa4bfbaddcb010185d717fbcf5004d65282da5f53a35cccd3eb2cb3ede5fbd32351de0037fc628a25fd303f3f640415476b40eb02410094
311b7542d07be76a6b1c9602d9fdfbe8e7b8f2e99e06e78d85ac48be72c87aec63aa72aaf705448cbf9929b05d960e98632a42521b3a511
6d4c29299e2b7fe"
}
```


3.2.5.7 censo.db

Base de datos SQL con la información de los ciudadanos con derecho a voto, lo que comúnmente se conoce como el censo.

Tabla 3. Base de datos de ejemplo de censo (censo.db).

Apellidos	Nombre	DNI	Nodo
PEREZ LORENZO	MARCOS	11111111A	1
CRUZ LOZANO	GONZALO	22222222B	4
MARTIN SANTIAGO	HELENA	33333333C	3
EIDAS CERTIFICADO	PRUEBAS	99999999R	2
FERNANDEZ MORALES	EVA	44444444D	1

3.2.5.8 resultado.html

Código HTML con el que se muestra toda la información relativa al proceso de votación.

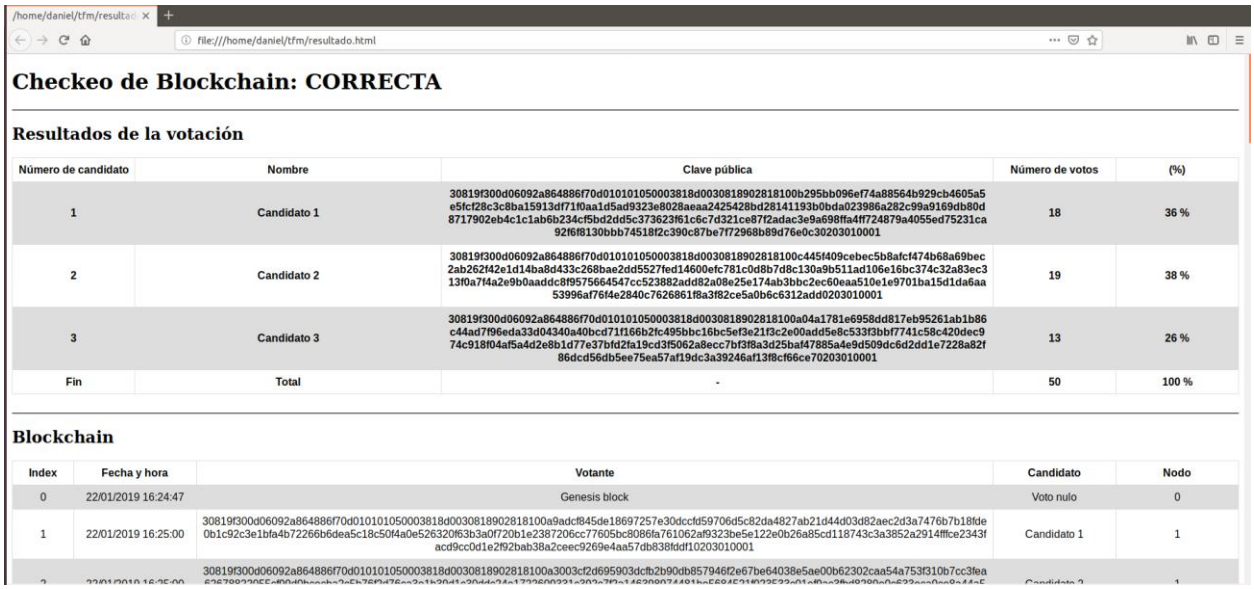


Figura 30. Página web que muestra resultados de la votación.

3.3 Escenario

En este apartado se verá cuál es el escenario que se ha montado a partir de las entidades anteriormente descritas en el apartado anterior y la relación que guardan entre ellos.

3.3.1 Esquema lógico

En la siguiente Figura se puede ver mediante un esquema lógico cuál es el el proceso que sigue un voto a través de todo el Sistema desde que es emitido por la aplicación del cliente hasta que acaba guardado en Blockchain:

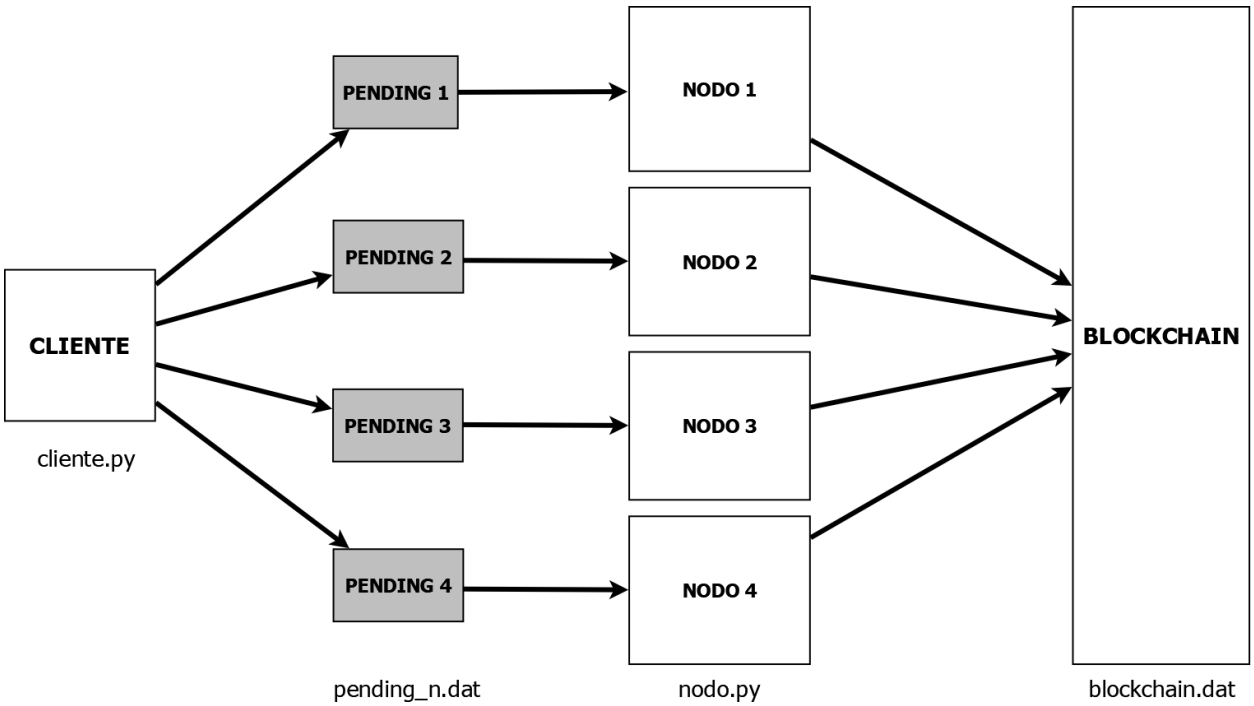


Figura 31. Principales entidades del Sistema y flujo seguido por el voto.

Cabe destacar que en dicho esquema se supone que el votante ha pasado todos los filtros ya comentados en apartados anteriores (se encuentra censado, se ha registrado correctamente, etc).

Tal y como se puede observar en la imagen anterior, la aplicación del cliente escribe los votos en el fichero pending correspondiente al nodo asociado al votante mientras que los nodos, en paralelo, leen constantemente dichos ficheros pending con el objetivo de procesar los votos que éstos contengan. Una vez el voto ha sido leído y verificado por el nodo correspondiente, éste lo escribe en la cadena de bloques.

Con el objetivo de evitar que varios nodos escriban a la vez en la cadena de bloques, se ha usado un semáforo/bandera (fichero flag.dat) el cual usan los nodos para indicar al resto que están usando la cadena de bloques y así evitar posibles conflictos.

3.3.2 Actores

A continuación se detallarán los actores que participan en la Prueba de Concepto realizada.

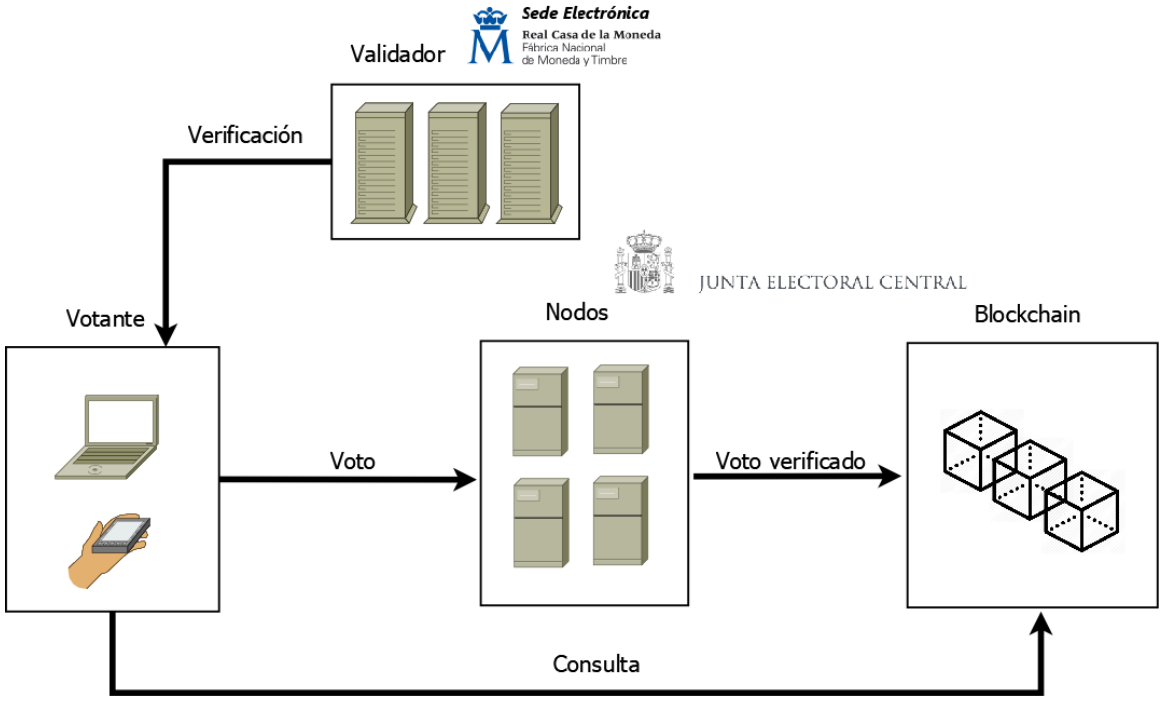


Figura 32. Representación del Sistema.

3.3.2.1 Votante

Persona que participa en el proceso de votación emitiendo el voto con su opción.

En el caso de la Prueba de Concepto que se presenta sería un **ciudadano con derecho a voto** que emite la elección del Candidato elegido.

El votante interactúa directamente con la aplicación del cliente, la cual podría ser una aplicación web a la que acceden los ciudadanos para participar en el proceso (esto por ejemplo ocurre en Estonia con la web www.valimised.ee) o también una aplicación móvil.

El votante, asimismo, mediante dicha aplicación podría además interactuar con la Blockchain, para conocer en tiempo real los resultados y otros datos que se van obteniendo en el proceso de votación.

3.3.2.2 Organizador

Son los responsables de la organización del proceso de votación, encargándose de definir las reglas que lo rigen con el objetivo de garantizar la transparencia y objetividad durante todo su desarrollo.

Las funciones podrían asemejarse a las desempeñadas por la **Junta Electoral Central** (JEC) en España, la cual además podría apoyarse en distintos organismos intermedios como las Juntas Electorales de Comunidad Autónoma, Provinciales y de Zona, aunque que la responsabilidad última siempre sería de la JEC.

3.3.2.3 Validador

Organismo que revisa la identidad de los votantes.

En este caso se ha utilizado la funcionalidad ofrecida por la sede electrónica de la **Fábrica Nacional de Moneda y Timbre** (FNMT) a través del proyecto CERES (CERtificación ESpañola) mediante la verificación de los certificados digitales que se usan para registrar al ciudadano con derecho a voto en el proceso de votación.

3.3.3 Captura del escenario

Como punto final del capítulo, y una vez se ha detallado todo el Sistema, veremos una captura de pantalla del escenario completo:

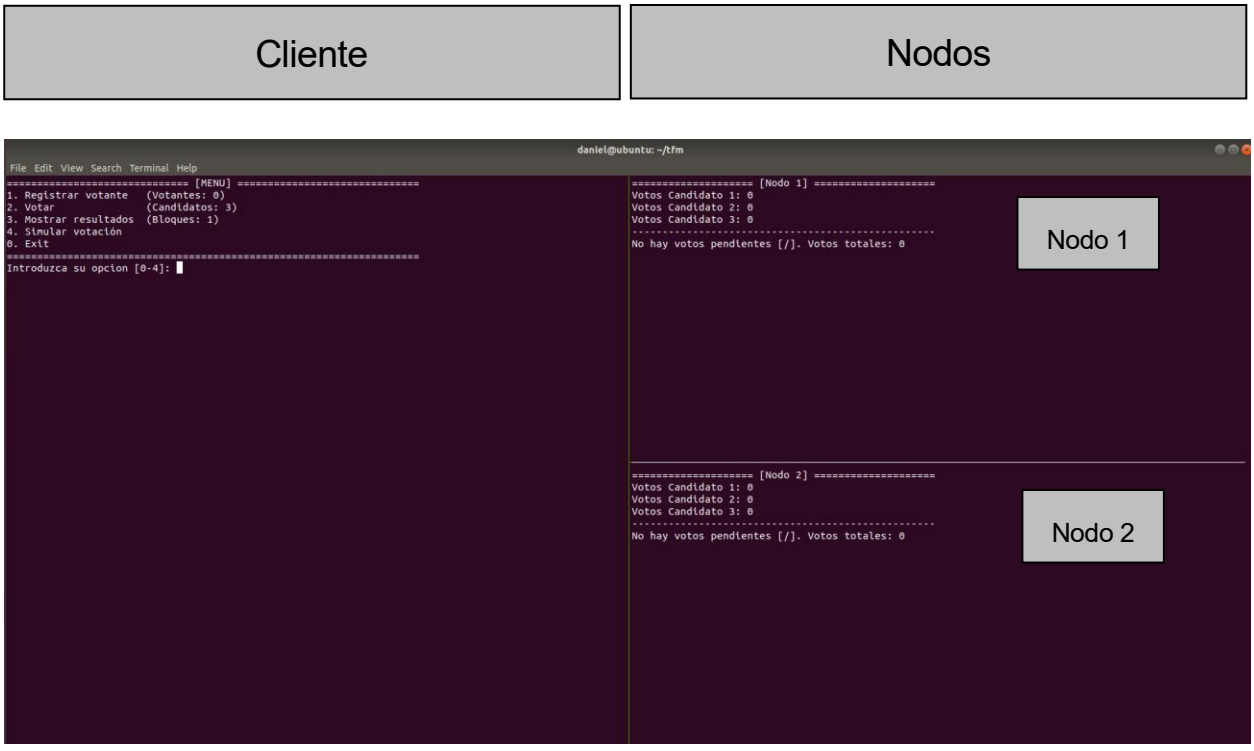


Figura 33. Escenario con dos nodos.

Tal y como se puede apreciar en la Figura anterior, en la parte izquierda se encuentra la aplicación del cliente mientras que en la parte derecha se encuentra la parte correspondiente a los nodos, que en este caso se han usado dos.

4 RESULTADOS

If you never make mistakes then you are not on the frontier of discovery, for there is where mistakes are made all the time.

- Neil deGrasse Tyson -

Con el propósito de exponer los resultados obtenidos de las diversas simulaciones realizadas, en este capítulo se mostrarán diversaas casuísticas que podrían tener lugar.

Para probar todos los posibles escenarios se van a usar 3 certificados distintos: **PF_REVOCADO_EIDAS.crt**, **PF_ACTIVO_EIDAS.crt** y **DLG.crt**. Los dos primeros me fueron proporcionados por la propia FNMT a raíz de una petición a la misma vía email, siendo uno revocado y el otro activo, respectivamente. El tercero de ellos es mi certificado digital personal.

En la siguiente tabla se muestran las características de los 3 certificados:

Tabla 4. Descripción de los certificados usados.

Certificado	Válido por FNMT	Se encuentra en el censo
PF_REVOCADO_EIDAS.crt	No	No (y es indiferente)
DLG.crt	Sí	No
PF_ACTIVO_EIDAS.crt	Sí	Sí

En los próximos apartados se describirán todas las posibles casuísticas que se podrían dar al hacer uso de la aplicación, separándolos por los apartados de **Registro del votante** y la **Acción del voto.**

4.1.1 Registro del votante

En primer lugar, las dos comprobaciones que se realizan para que una persona pueda registrarse correctamente como votante son:

1. Que tenga un certificado válido por la FNMT.
2. Que los datos de la persona (DNI, nombre y apellidos) se encuentren en el censo.

4.1.1.1 Certificado revocado por la FNMT (PF_REVOCADO_EIDAS.crt)

En este caso, en la primera comprobación ya se rechaza el registro del votante al no ser un certificado que se encuentre vigente por la FNMT.

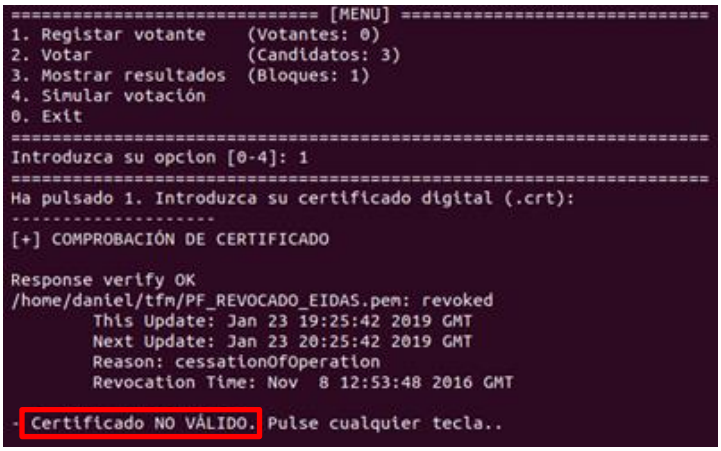


Figura 34. Votación por votante con certificado inválido.

4.1.1.2 Certificado válido por la FNMT, que no se encuentra en el censo (DLG.crt)

Con el certificado `DLG.crt` se pasa el primer filtro, pero no el segundo, ya que el DNI, nombre y apellidos no se encuentran en la base de datos del censo.

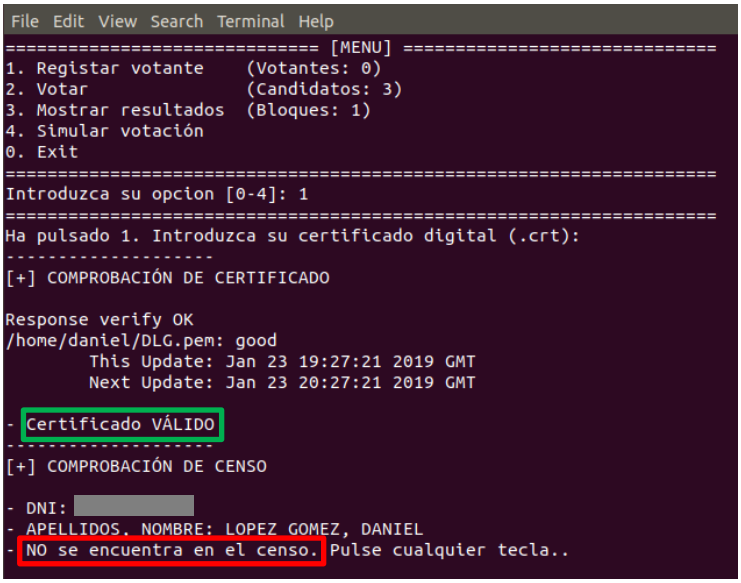


Figura 35. Votación con certificado válido que no se encuentra en el censo.

4.1.1.3 Certificado válido por FNMT y que se encuentra en el censo (PF_ACTIVO_EIDAS.crt)

Con el certificado `PF_ACTIVO_EIDAS.crt` el votante sí se puede registrar correctamente ya que es el único de los tres que cumple con todas las condiciones.

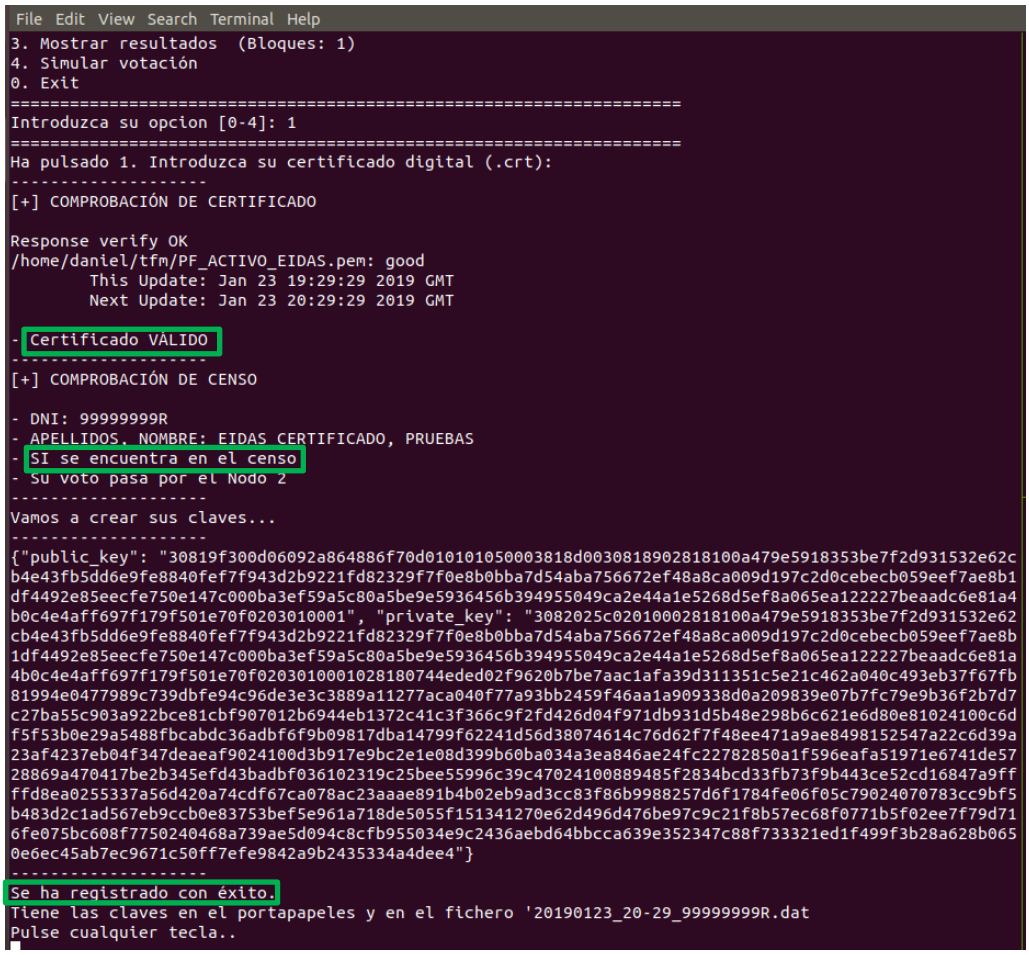


Figura 36. Votación con certificado válido y que se encuentra en el censo.

4.1.2 Acción del voto

En este apartado también pueden ocurrir distintos escenarios:

1. El votante usa sus claves para votar por primera vez.
2. El votante usa las mismas claves para votar varias veces.
3. El votante pide unas claves nuevas y vuelve a votar (por ejemplo, porque haya perdido las anteriores).

4.1.2.1 El votante usa unas claves nuevas para votar por primera vez

Este es el caso por defecto, la aplicación contabilizará el voto emitido por el votante sin mayor complicación.

```
============================== [MENU] ==============================
1. Registar votante    (Votantes: 1)
2. Votar               (Candidatos: 3)
3. Mostrar resultados  (Bloques: 1)
4. Simular votación
0. Exit
====================================================================
Introduzca su opcion [0-4]: 2
====================================================================
Ha pulsado 2. Indique el candidato al que quiere votar:
1. Candidato 1
2. Candidato 2
3. Candidato 3
0. Voto Nulo
====================================================================
Introduzca su opción [0-3]: 2
====================================================================
Ha elegido al Candidato 2
--------------------
[+] Introduzca sus claves
--------------------
{"public_key": "30819f300d06092a864886f70d010101050003818d0030818902818100aaf18c032c1b8ab677adc9e5c78d
047f59f388dc7a42f27165b4b5d2b48491707fe050b72cefff37d6435465c81c1b4f7ca14ec90813fc529f3ca686c13b5a74c9
6aca5b8317a3371d72ef0aa9ce417949361d2c94d6405a65a4eb04fa614572ae995f7efcee880aebd330adf98986fa0ad7f4dc
e75146a160181bef9cdf48d90203010001", "private_key": "3082025c02010002818100aaf18c032c1b8ab677adc9e5c78
d047f59f388dc7a42f27165b4b5d2b48491707fe050b72cefff37d6435465c81c1b4f7ca14ec90813fc529f3ca686c13b5a74c
96aca5b8317a3371d72ef0aa9ce417949361d2c94d6405a65a4eb04fa614572ae995f7efcee880aebd330adf98986fa0ad7f4d
ce75146a160181bef9cdf48d902030100010281802341 25ab11d1ac4ded68be16d18cd7bc9c0489d94eadb7ea831b3dd472be5
4706b2f0bf67b2213f4a40fc6bc270504ece3bb30d06d061227c8076e20a481652a126d2b61c3337659f1cd3255213460d3dca
26a681e82f8182581bddf9347cb16c0c9f471978395f0f98ef4d86c09b198dbf04405cf9ab9eb3eef4a3a12516171024100c76
00ee5e7176022e4f610e1cdb29167ad76ae02676ee1b262e932439acb0bf9a94a6e5de9b360813bc8e157e27931740af34cbee
7ab487157e00dd78b2d7d57024100db7e4f982f0830093b7570ca7812dc629201d1e9149233a3e3a2949787e778e9c1ca7c8a3
bd1362638b76174879b2cca759b2b12090861050f10b66959fb5d4f0240026d7b00f5a56538478d6f7b3064023d3ef17900f27
d792610ea42006cbc18333c0a79f98ec4ee61e47677b7f83bfd8c2a2df83b42dae510ec3f002c25b7b215024100d06f3b709e4
11d34b735083e0d1684184ae4d58c8c8f65e09d7bb7b5ca4642e960b143e1157acffc2de1def7050b93d653265e194b609c996
c3c07ad35d8e13b0240745979f6ed4cb0a3c566c1f42a208462bdc6c22d6e6f48022fd38bf64a3ab6ec59c3750861b0a79ee5e
0d80735d8bc5380f7e6a8b990567e50e6a375341fce65"}
--------------------
Ha votado al Candidato 2
====================================================================
Pulse una tecla para continuar..
```

Figura 37. Voto por primera vez a un Candidato.

4.1.2.2 El votante usa las mismas claves para votar varias veces

Si el cliente detecta que el certificado ya ha sido usado, preguntará si se desean utilizar las mismas claves u obtener unas nuevas:

```
--------------------
[+] COMPROBACIÓN DE CERTIFICADO

Response verify OK
/home/daniel/tfm/PF_ACTIVO_EIDAS.pem: good
        This Update: Jan 23 19:42:26 2019 GMT
        Next Update: Jan 23 20:42:26 2019 GMT

- Certificado VÁLIDO
--------------------
[+] COMPROBACIÓN DE CENSO

- DNI: 99999999R
- APELLIDOS, NOMBRE: EIDAS CERTIFICADO, PRUEBAS
- SI se encuentra en el censo
- Su voto pasa por el Nodo 2
--------------------
Este certificado ya ha sido usado. ¿Quiere obtener unas claves nuevas? [Y/N]:
```

Figura 38. Uso de certificado válido una vez ya ha votado.

Si el votante contesta que sí **(Y)**, se anularán las claves anteriores y se proporcionarán unas nuevas. En caso contrario **(N)** se volverá al menú principal.

4.1.2.3 El votante pide unas claves nuevas y vuelve a votar

Si se tratara de hacer uso de unas claves ya utilizadas anteriormente, ocurrirá lo siguiente:

Figura 39. Situación tras comprobar que se desea votar con unas claves ya utilizadas.

En el caso de que vote con distintas claves, el cliente añadirá este nuevo voto al registro, pero finalmente contabilizará solamente el último, tal y como se puede observar en la siguiente captura:

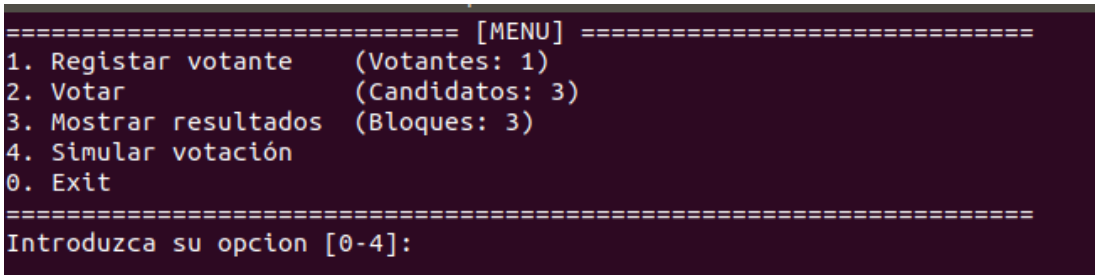
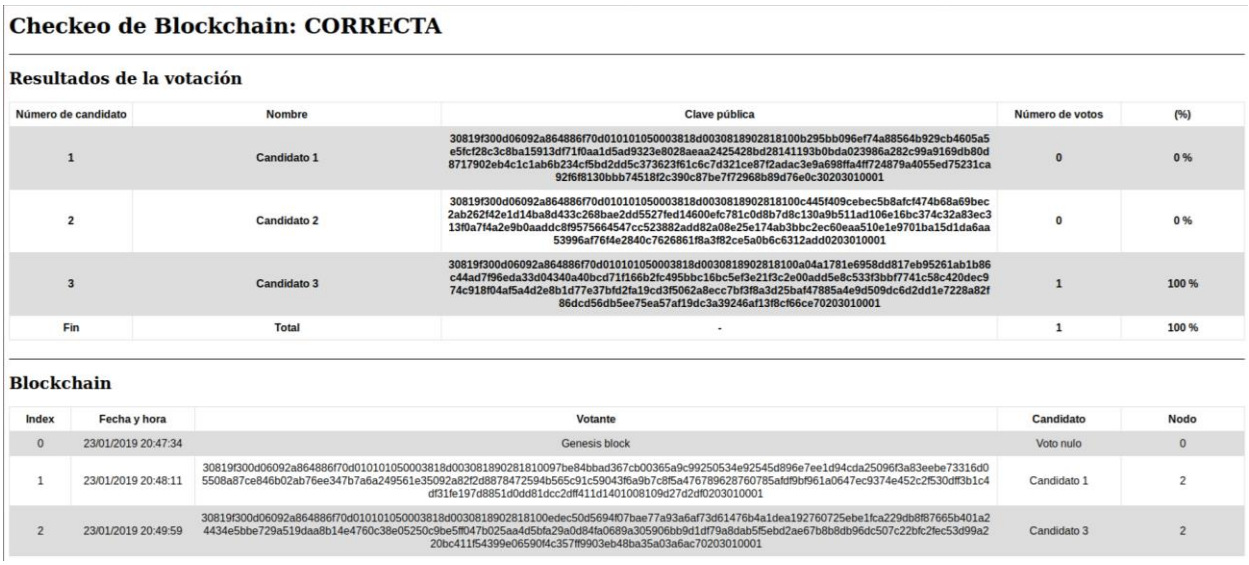


Figura 40. Situación inicial ante varios votos emitidos por un único votante.

En la imagen anterior se puede ver cómo hay un único votante **(Votantes: 1)**, pero aparecen dos votos **(Bloques: 3)**[12].

En la siguiente captura se puede constatar lo anteriormente explicado:

[12] Bloques 3: 2 votos más el Bloque Génesis.



Checkeo de Blockchain: CORRECTA

Resultados de la votación

Número de candidato	Nombre	Clave pública	Número de votos	(%)
1	Candidato 1	30819f300d06092a864886f70d010101050003818d00308189028181 00b295bb096ef74a88564b929cb4605a5e5fcf28c3c8ba15913df71f0aa1d5ad9323e8028aeaa2425428bd28141193b0bda023986a282c99a9169db80d8717902eb4c1c1ab6b234cf5bd2dd5c373623f61c6c7d321ce87f2adac3e9a698ffa4ff724879a4055ed75231ca92f6f8130bbb74518f2c390c87be7f72968b89d76e0c30203010001	0	0 %
2	Candidato 2	30819f300d06092a864886f70d010101050003818d00308189028181 00c445f409cebec5b8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547cc523882add82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861f8a3f82ce5a0b6c6312add0203010001	0	0 %
3	Candidato 3	30819f300d06092a864886f70d010101050003818d00308189028181 00a04a1781e6958dd817eb95261ab1b86c44ad7f96eda33d04340a40bcd71f166b2fc495bbc16bc5ef3e21f3c2e00add5e8c533f3bbf7741c58c420dec974c918f04af5a4d2e8b1d77e37bfd2fa19cd3f5062a8ecc7bf3f8a3d25baf47885a4e9d509dc6d2dd1e7228a82f86dcd56db5ee75ea57af19dc3a39246af13f8cf66ce70203010001	1	100 %
Fin	Total	-	1	100 %

Blockchain

Index	Fecha y hora	Votante	Candidato	Nodo
0	23/01/2019 20:47:34	Genesis block	Voto nulo	0
1	23/01/2019 20:48:11	30819f300d06092a864886f70d010101050003818d00308189028181 0097be84bbad367cb00365a9c99250534e92545d896e7ee1d94cda25096f3a83eebe73316d05508a87ce846b02ab76ee347b7a6a249561e35092a82f2d8878472594b565c91c59043f6a9b7c8f5a4767896287607 85afdf9bf961a0647ec9374e452c2f530dff3b1c4df31fe197d8851d0dd81dcc2dff411d1401008109d27d2df0203010001	Candidato 1	2
2	23/01/2019 20:49:59	30819f300d06092a864886f70d010101050003818d00308189028181 00edec50d5694f07bae77a93a6af73d61476b4a1dea192760725ebe1fca229db8f87665b401a24434e5bbe729a519daa8b14e4760c38e05250c9be5ff047b025aa4d5bfa29a0d84fa0689a305906bb9d1df79a8dab5f5ebd2ae67b8b8db96dc507c22bfc2fec53d99a220bc411f54399e06590f4c357ff9903eb48ba35a03a6ac70203010001	Candidato 3	2

Figura 41. Resultados obtenidos tras varios votos emitidos por un mismo votante.

En la parte inferior –Blockchain– se observa que se han emitido 2 votos (Candidato 1 y Candidato 3, respectivamente), pero en el apartado central –Resultados de la votación– se puede ver cómo únicamente se ha contabilizado el último de ellos (al Candidato 3).

4.1.3 Intento de modificación de Blockchain

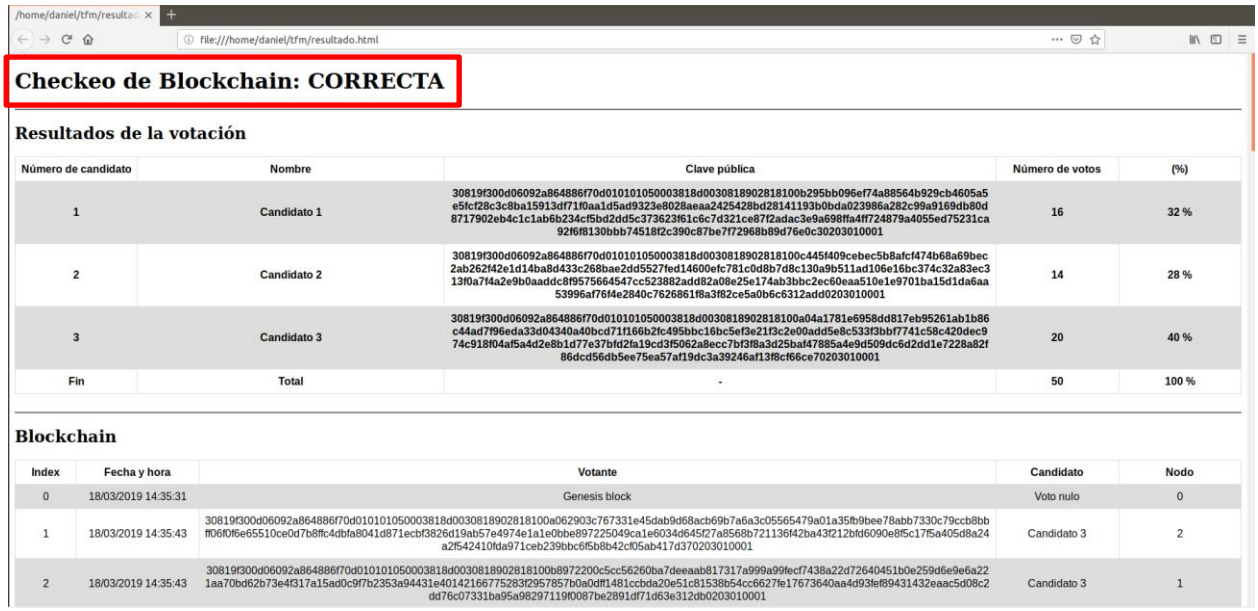
Uno de los principales objetivos del esquema que se presenta es el de proteger el registro de los votos de cualquier modificación. Es por ello que en el presente apartado se va a demostrar cómo casi (este punto se detallará al final) cualquier modificación realizada en la cadena de bloques sería detectada por cualquiera que obtenga los resultados de la votación.

Supongamos que tenemos una votación de 50 votos de 50 personas diferentes:

```
============================== [MENU] ==============================
1. Registrar votante   (Votantes: 50)
2. Votar               (Candidatos: 3)
3. Mostrar resultados  (Bloques: 51)
4. Simular votación
0. Exit
====================================================================
Introduzca su opcion [0-4]:
```

Figura 42. Simulación de 50 votos.

Si no realizamos ninguna modificación en el proceso, podremos comprobar que se muestra el resultado indicando que el chequeo de la cadena ha sido correcto:



/home/daniel/tfm/resultado.html

file:///home/daniel/tfm/resultado.html

Checkeo de Blockchain: CORRECTA

Resultados de la votación

Número de candidato	Nombre	Clave pública	Número de votos	(%)
1	Candidato 1	30819f300d06092a864886f70d0101010500003818d00308189028181 00b295bb096ef74a88564b929cb4605a5e5fcf2fc3c8ba15913df71f0aa1d5ad9323e8028aeaa2425428bd28141193b0bda023986a282c99a9169db80d8717902eb4c1c1ab6b234cf5bd2dd5c373623f61c6c7d321ce87f2adac3e9a698ffa4ff724879a4055ed75231ca92f6f8130bbb74518f2c390c87be7f72968b89d76e0c30203010001	16	32 %
2	Candidato 2	30819f300d06092a864886f70d0101010500003818d00308189028181 00c445f409cebec5b8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f89575664547cc523882add82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861f8a3f82ce5a0b6c6312add0203010001	14	28 %
3	Candidato 3	30819f300d06092a864886f70d0101010500003818d00308189028181 00a04a1781e6958dd817eb95261ab1b86c44ad7f96eda33d04340a40bcd71f166b2fc495bbc16bc5ef3e21f3c2e00add5e8c533f3bbf7741c58c420dec974c918f04af5a4d2e8b1d77e37bfd2fa19cd3f5062a8ecc7bf3f8a3d25baf47885a4e9d509dc6d2dd1e7228a82f86dcd56db5ee75ea57af19dc3a39246af13f8cf66ce70203010001	20	40 %
Fin	Total	-	50	100 %

Blockchain

Index	Fecha y hora	Votante	Candidato	Nodo
0	18/03/2019 14:35:31	Genesis block	Voto nulo	0
1	18/03/2019 14:35:43	30819f300d06092a864886f70d0101010500003818d00308189028181 00a062903c767331e45dab9d68acb69b7a6a3c05565479a01a35fb9bee78abb7330c79ccb8bbff06f0f6e65510ce0d7b8ffc4dbfa8041d871ecbf3826d19ab57e4974e1a1e0bbe897225049ca1e6034d645f27a8568b721136f42ba43f212bfd6090e8f5c17f5a405d8a24a2f542410fda971ceb239bbc6f5b8b42cf05ab417d370203010001	Candidato 3	2
2	18/03/2019 14:35:43	30819f300d06092a864886f70d0101010500003818d00308189028181 00b8972200c5cc56260ba7deeaab817317a999a99fecf7438a22d72640451b0e259d6e9e6a221aa70bd62b73e4f317a15ad0c9f7b2353a94431e40142166775283f2957857b0a0dff1481ccbda20e51c81538b54cc6627fe17673640aa4d93fef89431432eaac5d08c2dd76c07331ba95a98297119f0087be2891df71d63e312db0203010001	Candidato 3	1

Figura 43. Resultado de la simulación.

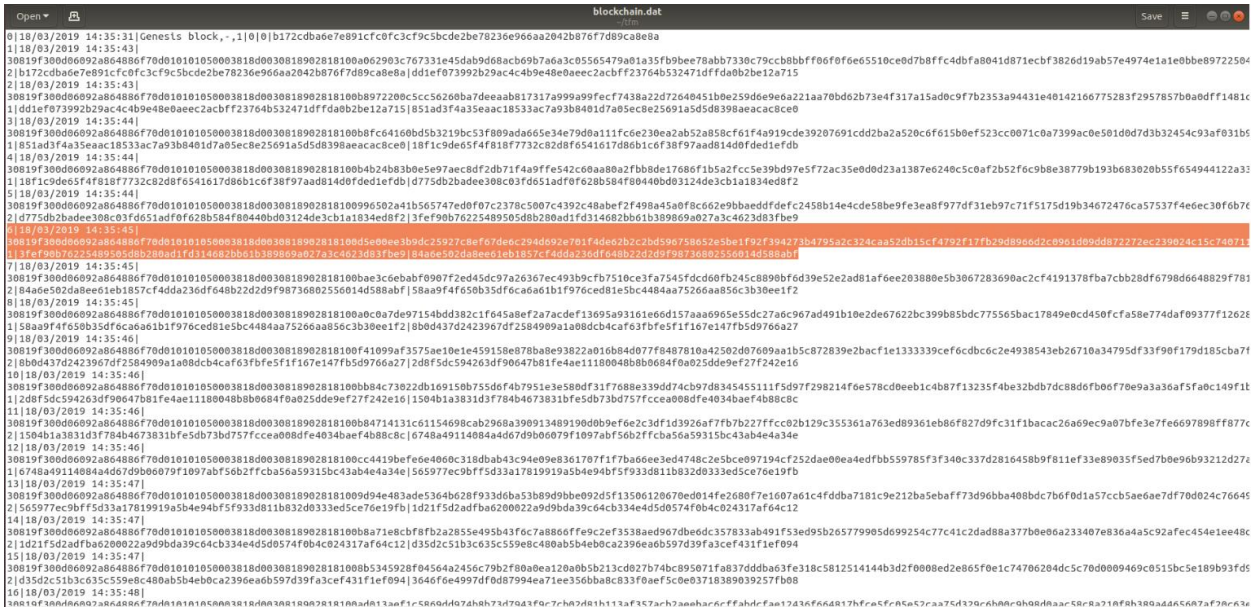
Sin embargo, ¿qué ocurriría si por algún fallo de seguridad en el sistema alguien fuese capaz de modificar cualquier mínimo dato de dicha cadena?

Por ejemplo, tenemos el siguiente archivo blockchain.dat derivado de la simulación anterior:

Nota: recordemos que la estructura de dicho archivo es

Índice | Fecha | Transacción | Nodo | Hash del bloque anterior | Hash

siendo Transacción = (Clave pública del votante, Clave pública del Candidato, Voto)



blockchain.dat

```
0|18/03/2019 14:35:31|Genesis block,-,1|0|0|b172cdba6e7e891cfc0fc3cf9c5bcde2be78236e966aa2042b876f7d89ca8e8a
1|18/03/2019 14:35:43|
30819f300d06092a864886f70d0101010500003818d00308189028181 00a062903c767331e45dab9d68acb69b7a6a3c05565479a01a35fb9bee78abb7330c79ccb8bbff06f0f6e65510ce0d7b8ffc4dbfa8041d871ecbf3826d19ab57e4974e1a1e0bbe897225042|b172cdba6e7e891cfc0fc3cf9c5bcde2be78236e966aa2042b876f7d89ca8e8a|dd1ef073992b29ac4c4b9e48e0aeec2acbff23764b532471dffda0b2be12a715
2|18/03/2019 14:35:43|
30819f300d06092a864886f70d0101010500003818d00308189028181 00b8972200c5cc56260ba7deeaab817317a999a99fecf7438a22d72640451b0e259d6e9e6a221aa70bd62b73e4f317a15ad0c9f7b2353a94431e40142166775283f2957857b0a0dff1481c|1|dd1ef073992b29ac4c4b9e48e0aeec2acbff23764b532471dffda0b2be12a715|851ad3f4a35eaac18533ac7a93b8401d7a05ec8e25691a5d5d8398aeacac8ce0|18f1c9de65f4f818f7732c82d8f6541617d86b1c6f38f97aad814d0fded1efdb
3|18/03/2019 14:35:44|
30819f300d06092a864886f70d0101010500003818d00308189028181 00b8fc64160bd5b3219bc53f809ada665e34e79d0a111fc6e230ea2ab52a858cf61f4a919cde39207691cdd2ba2a520c6f615b0ef523cc0071c0a7399ac0e501d0d7d3b32454c93af031b5|1|851ad3f4a35eaac18533ac7a93b8401d7a05ec8e25691a5d5d8398aeacac8ce0|18f1c9de65f4f818f7732c82d8f6541617d86b1c6f38f97aad814d0fded1efdb|d775db2badee308c03fd651adf0f628b584f80440bd03124de3cb1a1834ed8f2
4|18/03/2019 14:35:44|
30819f300d06092a864886f70d0101010500003818d00308189028181 00b24b83b0e5e97aec8df2db71f4a9ffe542c60aa80a2fbb8de17686f1b5a2fcc5e39bd97e5f72ac35e0d0d23a1387e6240c5c0af2b52f6c9b8e38779b193b683020b55f654944122a33|1|18f1c9de65f4f818f7732c82d8f6541617d86b1c6f38f97aad814d0fded1efdb|d775db2badee308c03fd651adf0f628b584f80440bd03124de3cb1a1834ed8f2|3fef90b76225489505d8b280ad1fd314682bb61b389869a027a3c4623d83fbe9
5|18/03/2019 14:35:44|
30819f300d06092a864886f70d0101010500003818d00308189028181 00996502a41b565747ed0f07c2378c5007c4392c48abef2f498a45a0f8c662e9bbaeddfdefc2458b14e4cde58be9fe3ea8f977df31eb97c71f5175d19b34672476ca57537f4e6ec30f6b7f|2|d775db2badee308c03fd651adf0f628b584f80440bd03124de3cb1a1834ed8f2|3fef90b76225489505d8b280ad1fd314682bb61b389869a027a3c4623d83fbe9
6|18/03/2019 14:35:45|
30819f300d06092a864886f70d0101010500003818d00308189028181 00d5e00ee3b9dc25927c8ef67de6c294d692e701f4de62b2c2bd596758652e5be1f92f394273b4795a2c324caa52db15cf4792f17fb29d8966d2c0961d09dd872272ec239024c15c740711|6|3fef90b76225489505d8b280ad1fd314682bb61b389869a027a3c4623d83fbe9|84a6e502da8ee61eb1857cf4dda236df648b22d2d9f98736802556014d588abf
7|18/03/2019 14:35:45|
30819f300d06092a864886f70d0101010500003818d00308189028181 00bae3c6ebabf0907f2ed45dc97a26367ec493b9cfb7510ce3fa7545fdcd60fb245c8890bf6d39e52e2ad81af6ee203880e5b3867283690ac2cf4191378fba7cbb28df6798d6648829f781|2|84a6e502da8ee61eb1857cf4dda236df648b22d2d9f98736802556014d588abf|58aa9f4f650b35df6ca6a61b1f976ced81e5bc4484aa75266aa856c3b30eef2
8|18/03/2019 14:35:45|
30819f300d06092a864886f70d0101010500003818d00308189028181 00a0c0a7de97154bdd382c1f645a8ef2a7acdef13695a93161e66d157aaa6965e55dc27a6c967ad491b10e2de67622bc399b85bdc775565bac17849e0cd450fcfa58e774daf09377f1262e8|1|58aa9f4f650b35df6ca6a61b1f976ced81e5bc4484aa75266aa856c3b30eef1f2|8b0d437d2423967df2584909a1a08dcb4caf63fbfe5f1f167e147fb5d9766a27
9|18/03/2019 14:35:46|
30819f300d06092a864886f70d0101010500003818d00308189028181 00f41099af3575ae10e1e459158e878ba8e93822a016b84d077f8487810a42502d07609aa1b5c872839e2bacf1e1333339cef6cdbc6c2e4938543eb26710a34795df33f90f179d185cba7f|2|8b0d437d2423967df2584909a1a08dcb4caf63fbfe5f1f167e147fb5d9766a27|2d8f5dc594263df90647b81fe4ae11180048b8b0684f0a025dde9ef27f242e16
10|18/03/2019 14:35:46|
30819f300d06092a864886f70d0101010500003818d00308189028181 00bb84c73822db169150b755def4b7951e3e580df31f7688e339dd74cb97d8345455111f5d97f298214f6e578cd0eeb1c4b87f13235f4be32bdb7dc88d6fb06f70e9a3a36af5fa0c149f1b|1|2d8f5dc594263df90647b81fe4ae11180048b8b0684f0a025dde9ef27f242e16|1504b1a3831d3f784b4673831bfe5db73bd757fccea008dfe4034baef4b88c8c
11|18/03/2019 14:35:46|
30819f300d06092a864886f70d0101010500003818d00308189028181 00b84714131c61154698cab2968a390913489190d0b9ef6e2c3df1d3926af7fb7b227ffcc02b129c355361a763ed89361eb86f827d9fc31f1bacac26a69ec9a07bfe3e7fe6697898ff877c|2|1504b1a3831d3f784b4673831bfe5db73bd757fccea008dfe4034baef4b88c8c|6748a49114084a4d67d9b06079f1097abf56b2ffcba56a59315bc43ab4e4a34e
12|18/03/2019 14:35:46|
30819f300d06092a864886f70d0101010500003818d00308189028181 00cc4419befe6e4060c318dbab43c94e09e8361707f1f7ba66ee3ed4748c2e5bce097194cf252dae00ea4edfbb559785f3f340c337d2816458b9f811ef33e89035f5ed7b0e96b93212d27a|1|6748a49114084a4d67d9b06079f1097abf56b2ffcba56a59315bc43ab4e4a34e|565977ec9bff5d33a17819919a5b4e94bf5f933d811b832d0333ed5ce76e19fb
13|18/03/2019 14:35:47|
30819f300d06092a864886f70d0101010500003818d00308189028181 0009d94e483ade5364b628f933d6ba53b89d9bbe092d5f13506120670ed014fe2680f7e1607a61c4fddba7181c9e212ba5ebaff73d96bba408bdc7b6f0d1a57ccb5ae6ae7df70d024c76649|2|565977ec9bff5d33a17819919a5b4e94bf5f933d811b832d0333ed5ce76e19fb|1d21f5d2adfba6200022a9d9bda39c64cb334e4d5d0574f0b4c024317af64c12
14|18/03/2019 14:35:47|
30819f300d06092a864886f70d0101010500003818d00308189028181 00b8a71e8cbf8fb2a2855e495b43f6c7a8866ffe9c2ef3538aed967dbe6dc357833ab491f53ed95b26577990 5d699254c77c41c2dad88a377b0e06a233407e836a4a5c92afec454e1ee48c|2|1d21f5d2adfba6200022a9d9bda39c64cb334e4d5d0574f0b4c024317af64c12|d35d2c51b3c635c559e8c480ab5b4eb0ca2396ea6b597d39fa3cef431f1ef094
15|18/03/2019 14:35:47|
30819f300d06092a864886f70d0101010500003818d00308189028181008b5345928f04564a2456c79b2f80a0ea120a0b5b213cd027b74bc895071fa837dddba63fe318c5812514144b3d2f0008ed2e865f0e1c74706284dc5c70d0009469c0515bc5e189b93fd5|2|d35d2c51b3c635c559e8c480ab5b4eb0ca2396ea6b597d39fa3cef431f1ef094|3646f6e4997df0fd87994ea71ee356bba8c833f0aef5c0e037183890392 57fb08
16|18/03/2019 14:35:48|
30819f300d06092a864886f70d0101010500003818d00308189028181 00ad813aef1c5869dd97ab8b73d7943f9c7cb02d81b113af357acb2aeebac6cffabdcfae12436f664817bfce5fc05e52caa75d329c6b00c9b98d0aac58c8a210f8b389a4465607af20c63e
```

Figura 44. Archivo blockchain.dat de la simulación.

Supongamos que modificamos el campo de la transacción del bloque número 6, el cual se ha resaltado, concretamente el dato de la clave pública del Candidato, el cual determina el Candidato al que se le contabiliza el voto.

Transacción inicial del bloque número 6:

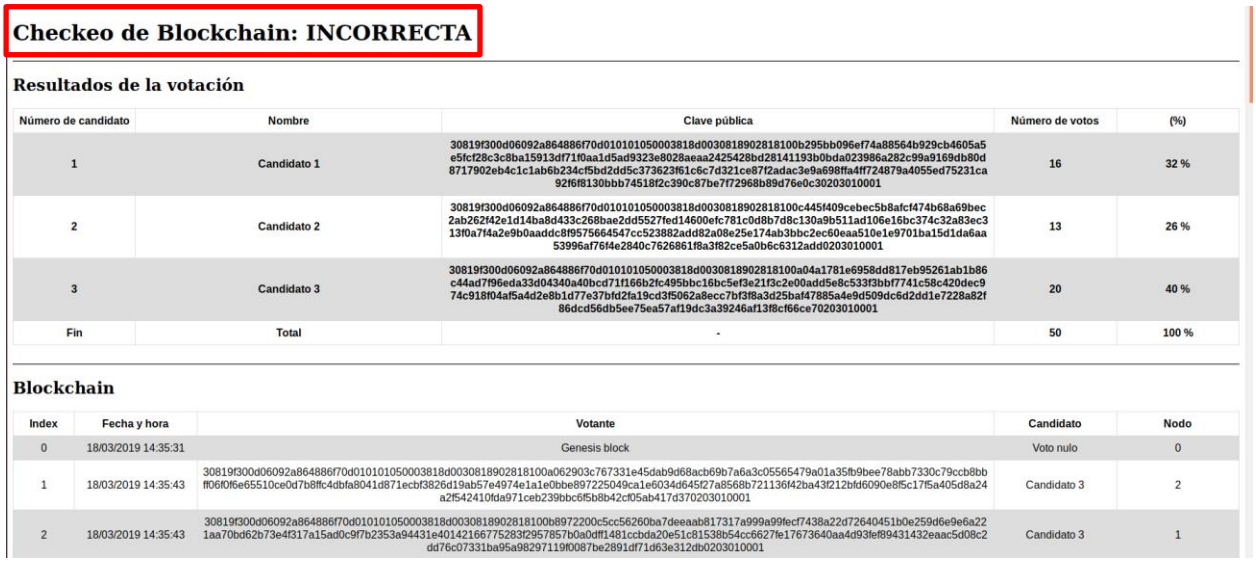
```
6|18/03/2019
14:35:45|30819f300d06092a864886f70d010101050003818d0030818902818100d
5e00ee3b9dc25927c8ef67de6c294d692e701f4de62b2c2bd596758652e5be1f92f3
94273b4795a2c324caa52db15cf4792f17fb29d8966d2c0961d09dd872272ec23902
4c15c740711b8dec28a49d0435b7d935925fd859114f9d343174d013abbabd212ef2
afdc747b8506133434e8cbf8c272c49ca66355a5cbb28011d390203010001,30819f
300d06092a864886f70d010101050003818d0030818902818100c445f409cebec5b8
afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d
8b7d8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547
cc523882add82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f
4e2840c7626861f8a3f82ce5a0b6c6312add0203010001,1|1|3fef90b7622548950
5d8b280ad1fd314682bb61b389869a027a3c4623d83fbe9|84a6e502da8ee61eb185
7cf4dda236df648b22d2d9f98736802556014d588abf
```

Al hacer la siguiente modificación:

```
30819f300d06092a864886f70d010101050003818d0030818902818100c445f409cebec5b
8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d
8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547cc523882a
dd82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861
f8a3f82ce5a0b6c6312add0203010001
```

```
30819f300d06092a864886f70d010101050003818d0030818902818100c445f409cebec5b
8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14601efc781c0d8b7d
8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547cc523882a
dd82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861
f8a3f82ce5a0b6c6312add0203010001
```

En ese caso, con esa mínima modificación realizada, al volver a comprobar los resultados se obtendría el siguiente mensaje:



Checkeo de Blockchain: INCORRECTA

Resultados de la votación

Número de candidato	Nombre	Clave pública	Número de votos	(%)
1	Candidato 1	30819f300d06092a864886f70d010101050003818d0030818902818100b295bb096ef74a88564b929cb4605a5e5fcf28c3c8ba15913df71f0aa1d5ad9323e8028aeaa2425428bd28141193b0bda023986a282c99a9169db80d8717902eb4c1c1ab6b234cf5bd2dd5c373623f61c6c7d321ce87f2adac3e9a698ffa4ff724879a4055ed75231ca92f6f8130bbb745181f2c390c87be7f72968b89d76e0c30203010001	16	32 %
2	Candidato 2	30819f300d06092a864886f70d010101050003818d0030818902818100c445f409cebec5b8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547cc523882add82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861f8a3f82ce5a0b6c6312add0203010001	13	26 %
3	Candidato 3	30819f300d06092a864886f70d010101050003818d0030818902818100a04a1781e6958dd817eb95261ab1b86c44ad7f96eda33d04340a40bcd71f166b2fc495bbc16bc5ef3e21f3c2e00add5e8c533f3bbf7741c58c420dec974c918f04af5a4d2e8b1d77e37bfd2fa19cd3f5086dcd56db5ee75ea57af19dc3a39246af13f8cf66ce70203010001	20	40 %
Fin	Total	-	50	100 %

Blockchain

Index	Fecha y hora	Votante	Candidato	Nodo
0	18/03/2019 14:35:31	Genesis block	Voto nulo	0
1	18/03/2019 14:35:43	30819f300d06092a864886f70d010101050003818d0030818902818100a062903c767331e45dab9d68acb69b7a6a3c05565479a01a35fb9bee78abb7330c79ccb8bbff06f0f6e65510ce0d7b8ffc4dbfa8041d871ecbf3826d19ab57e4974e1a1e0bbe897225049ca1e6034d645f27a8568b721136f42ba43f212bfd6090e8f5c17f5a405d8a24a2f542410fda971ceb239bbc6f5b8b42cf05ab417d370203010001	Candidato 3	2
2	18/03/2019 14:35:43	30819f300d06092a864886f70d010101050003818d0030818902818100b8972200c5cc56260ba7deeaab817317a999a99fecf7438a22d72640451b0e259d6e9e6a221aa70bd62b73e4f317a15ad0c9f7b2353a94431e40142166775283f2957857b0a0dff1481ccbda20e51c81538b54cc6627fe17673640aa4d93fef89431432eaac5d08c2dd76c07331ba95a98297119f0087be2891df71d63e312db0203010001	Candidato 3	1

Figura 45. Resultado tras modificar mínimamente la cadena de bloques.

De hecho el voto del bloque número 6 se daría como Voto Nulo:

5	18/03/2019 14:35:44	30819f300d06092a864886f70d010101050003818d0030818902818100996502a41b565747ed0f07c2378c5007c4392c48abef2f498a45a0f8c662e9bbaeddfdefc2458b14e4cde58be9fe3ea8f977df31eb97c71f5175d19b34672476ca57537f4e6ec30f6b76efbcd778bb7e92a623527f9d7e6f31af5abeca0d4c0300db5de517a6eb96c3f8612ab58f674d1908f7246a3b1d52ab75bcb3a8e2428d0203010001	Candidato 2	2
6	18/03/2019 14:35:45	30819f300d06092a864886f70d010101050003818d0030818902818100d5e00ee3b9dc25927c8ef67de6c294d692e701f4de62b2c2bd596758652e5be1f92f394273b4795a2c324caa52db15cf4792f17fb29d8966d2c0961d09dd872272ec239024c15c740711b8dec28a49d0435b7d935925fd859114f9d343174d013abbabd212ef2afdc747b8506133434e8cbf8c272c49ca66355a5cbb28011d390203010001	Voto nulo	1
7	18/03/2019 14:35:45	30819f300d06092a864886f70d010101050003818d0030818902818100bae3c6ebabf0907f2ed45dc97a26367ec493b9cfb7510ce3fa7545fdcd60fb245c8890bf6d39e52e2ad81af6ee203880e5b3067283690ac2cf4191378fba7cbb28df6798d6648829f78158add6d90cc6db56a539fd48208b232a9bd2db3f85ad25786a162efd2642d4a24d07da65656365fd3c59ca84ed8a88688be9e879fe890203010001	Candidato 2	2

Figura 46. Voto Nulo tras modificar la cadena.

4.1.4 Intento de cambiar al Candidato

Se podría pensar que el cambio anterior es detectado ya que la nueva clave pública ya no correspondería con la de ningún Candidato. Sin embargo, a continuación vamos a ver cómo aunque cambiemos la clave pública de un candidato por la de otro, se detectaría igualmente.

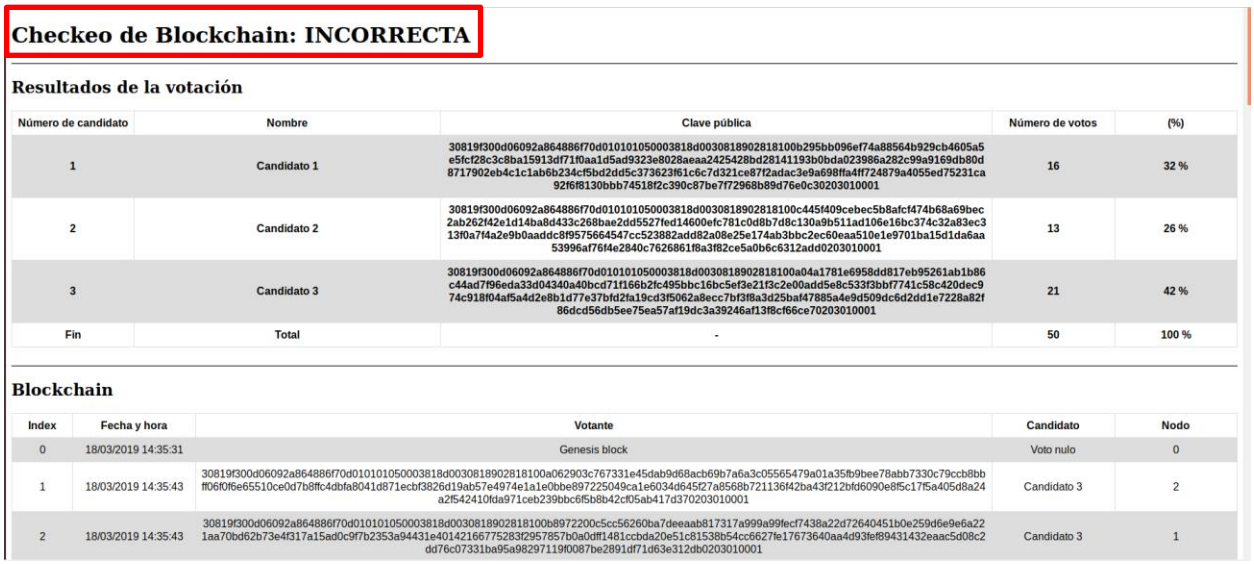
Si cambiásemos la clave pública anterior, la cual correspondía a la del Candidato 2, por la del Candidato 3

```
30819f300d06092a864886f70d010101050003818d0030818902818100c445f409cebec5b
8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d
8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547cc523882a
dd82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861
f8a3f82ce5a0b6c6312add0203010001
```

```
30819f300d06092a864886f70d010101050003818d0030818902818100a04a1781e6958dd
817eb95261ab1b86c44ad7f96eda33d04340a40bcd71f166b2fc495bbc16bc5ef3e21f3c2
e00add5e8c533f3bbf7741c58c420dec974c918f04af5a4d2e8b1d77e37bfd2fa19cd3f50
```

```
62a8ecc7bf3f8a3d25baf47885a4e9d509dc6d2dd1e7228a82f86dcd56db5ee75ea57af19
dc3a39246af13f8cf66ce70203010001
```

obtendríamos igualmente el resultado mostrando que la cadena es incorrecta:



Checkeo de Blockchain: INCORRECTA

Resultados de la votación

Número de candidato	Nombre	Clave pública	Número de votos	(%)
1	Candidato 1	30819f300d06092a864886f70d010101050003818d0030818902818100b295bb096ef74a88564b929cb4605a5e5fcf28c3c8ba15913df71f0aa1d5ad9323e8028aeaa2425428bd28141193b0bda023986a282c99a9169db80d8717902eb4c1c1ab6b234cf5bd2dd5c373623f61c6c7d321ce87f2adac3e9a698ffa4ff724879a4055ed75231ca92f6f8130bbb74518f2c390c87be7f72968b89d76e0c30203010001	16	32 %
2	Candidato 2	30819f300d06092a864886f70d010101050003818d0030818902818100c445f409cebec5b8afcf474b68a69bec2ab262f42e1d14ba8d433c268bae2dd5527fed14600efc781c0d8b7d8c130a9b511ad106e16bc374c32a83ec313f0a7f4a2e9b0aaddc8f9575664547cc523882add82a08e25e174ab3bbc2ec60eaa510e1e9701ba15d1da6aa53996af76f4e2840c7626861f8a3f82ce5a0b6c6312add0203010001	13	26 %
3	Candidato 3	30819f300d06092a864886f70d010101050003818d0030818902818100a04a1781e6958dd817eb95261ab1b86c44ad7f96eda33d04340a40bcd71f166b2fc495bbc16bc5ef3e21f3c2e00add5e8c533f3bbf7741c58c420dec974c918f04af5a4d2e8b1d77e37bfd2fa19cd3f5062a8ecc7bf3f8a3d25baf47885a4e9d509dc6d2dd1e7228a82f86dcd56db5ee75ea57af19dc3a39246af13f8cf66ce70203010001	21	42 %
Fin	Total	-	50	100 %

Blockchain

Index	Fecha y hora	Votante	Candidato	Nodo
0	18/03/2019 14:35:31	Genesis block	Voto nulo	0
1	18/03/2019 14:35:43	30819f300d06092a864886f70d010101050003818d0030818902818100a062903c767331e45dab9d68acb69b7a6a3c05565479a01a35fb9bee78abb7330c79ccb8bbff06f0f6e65510ce0d7b8ffc4dbfa8041d871ecbf3826d19ab57e4974e1a1e0bbe897225049ca1e6034d645f27a8568b721136f42ba43f212bfd6090e8f5c17f5a405d8a24a2f542410fda971ceb239bbc6f5b8b42cf05ab417d370203010001	Candidato 3	2
2	18/03/2019 14:35:43	30819f300d06092a864886f70d010101050003818d0030818902818100b8972200c5cc56260ba7deeaab817317a999a99fecf7438a22d72640451b0e259d6e9e6a2221aa70bd62b73e4f317a15ad0c9f7b2353a94431e401421667752 83f2957857b0a0dff1481ccbda20e51c81538b54cc6627fe17673640aa4d93fef89431432eaac5d08c2dd76c07331ba95a98297119f0087be2891df71d63e312db0203010001	Candidato 3	1

Figura 47. Resultado tras intentar suplantar un candidato por otro.

Estos dos casos sirven como ejemplo para demostrar que **cualquier mínima modificación de la cadena es detectada por el Sistema.**

5 CONCLUSIONES

Stay hungry, stay foolish.

- Steve Jobs -

Durante todo el trabajo se ha expuesto la situación actual existente tanto a nivel mundial como concretamente en España en cuanto a tecnologías, aspectos técnicos y burocráticos relativos a los sistemas de votaciones disponibles en la actualidad, encontrando que en España **apenas ha cambiado** a pesar de los grandes avances tecnológicos que han ido apareciendo en las últimas décadas.

Este hecho ha sido debido principalmente a dos motivos. El primero de ellos es que en todos estos años no se ha conseguido encontrar un sistema que ofreciera las mismas **garantías y seguridad** a los electores que el sistema tradicional. El segundo, y no menos importante, es la **desconfianza generalizada** en la sociedad, tanto por electores como por algunos de los expertos, de la introducción de un nuevo sistema de votación que complemente al ya existente.

Sin embargo, Bitcoin, a través de todos los **años** que lleva en funcionamiento, es un éxito constatado de cómo se puede realizar un almacenamiento de datos de manera segura gracias al protocolo Blockchain que lo hace posible.

Es por ello que ante una sociedad cada vez más tecnológicamente avanzada y global parece necesario y coherente la aparición **de sistemas alternativos** que ayuden a modernizar el sistema de voto tradicional facilitando la participación en algo tan fundamental en cualquier sociedad democrática como lo es el sufragio.

Con ese propósito, en este documento se ha analizado y demostrado, a través de una Prueba de Concepto, cómo se podría implementar una solución basada en Blockchain que **complementara** al sistema de votación que existe actualmente para las Elecciones en España. Y para ello la selección de Blockchain como base de la Prueba de Concepto no ha sido casualidad; se trata de una tecnología disruptiva que ha demostrado tener los aspectos técnicos necesarios para poder satisfacer las grandes exigencias de un sistema de votación.

Por lo tanto, aunque a buen seguro, la solución propuesta no está exenta de dificultades para llevar a cabo su implementación real, vale la pena conocer posibles sistemas alternativos y fundamentados como el que en este proyecto se ha tratado de exponer.

5.1 Línea de continuación

5.1.1 Uso de herramientas ya existentes

La construcción de la Prueba de Concepto de este trabajo se ha llevado a cabo prácticamente desde cero con fines académicos para que se pueda comprobar cómo se puede realizar un sistema Blockchain desde el inicio. Sin embargo, son varias las herramientas que han ido apareciendo en los últimos tiempos que permiten trabajar sin la complicación de tener que realizar una red de estas características desde cero.

Algunas de estas herramientas ya fueron presentadas en el apartado relativo a *Herramientas de código abierto*: Hyperledger, Corda, EWF (Energy Web Foundation), Multichain…

El uso de una de estas herramientas permitiría ahorrarse el análisis e implementación de todo lo relativo a la creación de una red **peer-to-peer**, el diseño de sus **comunicaciones**, etc.

Por lo tanto, a la hora de realizar la solución final que se deseara implementar, quizás sería conveniente utilizar una de estas herramientas, o alguna similar, ya que la construcción desde cero de una red de estas características, y además si se piensa en una red de grandes dimensiones, puede llegar a ser bastante tedioso.

5.1.2 Complementar con voto físico

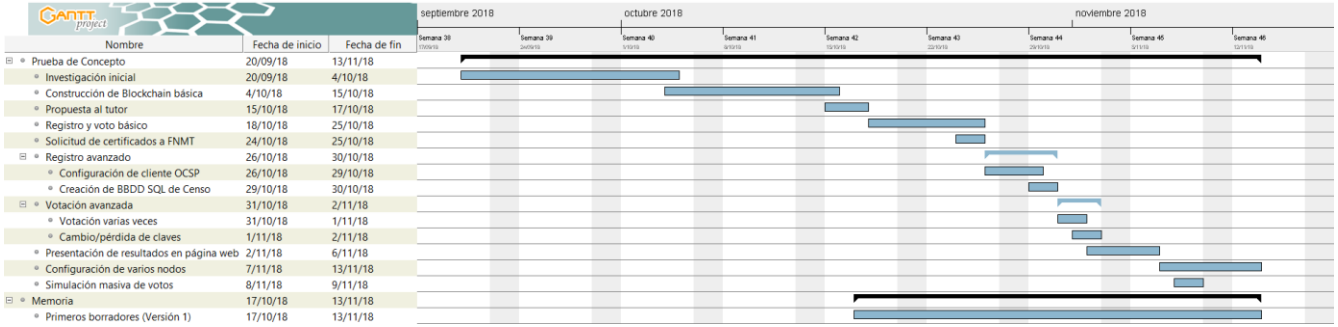
Como se ha comentado en apartados anteriores, el uso del sistema del voto electrónico no está pensado para sustituir al voto presencial, sino para **complementarlo**. Es por ello que, aunque se escapa del alcance de este Trabajo Fin de Máster, como línea futura de continuación del mismo, sería conveniente tener en cuenta el hecho de que puede existir un sistema de votación presencial que coexista con el sistema de votación electrónica. Este hecho afectaría, por ejemplo, en que sería conveniente que el sistema de votación electrónica recibiría otra fuente de información proveniente del voto presencial y viceversa

Además, y relativo a este hecho, también se podría hacer que el sistema de voto electrónico se pudiera usar de manera presencial, por lo que se podría hacer que alternativamente al uso del certificado digital se pudiera usar el DNI con el objetivo, al igual que certificado, de identificar unívocamente a los votantes.

5.2 Planificación

A continuación veremos la planificación temporal seguida durante la realización de este trabajo, la cual se ha querido representar mediante dos Diagramas de Gantt: el relativo a la Prueba de Concepto y el relativo a la Memoria y sus respectivas entregas al tutor.

En el primero de ellos se muestra la planificación seguida para la realización de la Prueba de Concepto: su investigación inicial y todo su posterior desarrollo a medida que iban surgiendo nuevas ideas y que iba manteniendo conversaciones con el tutor:

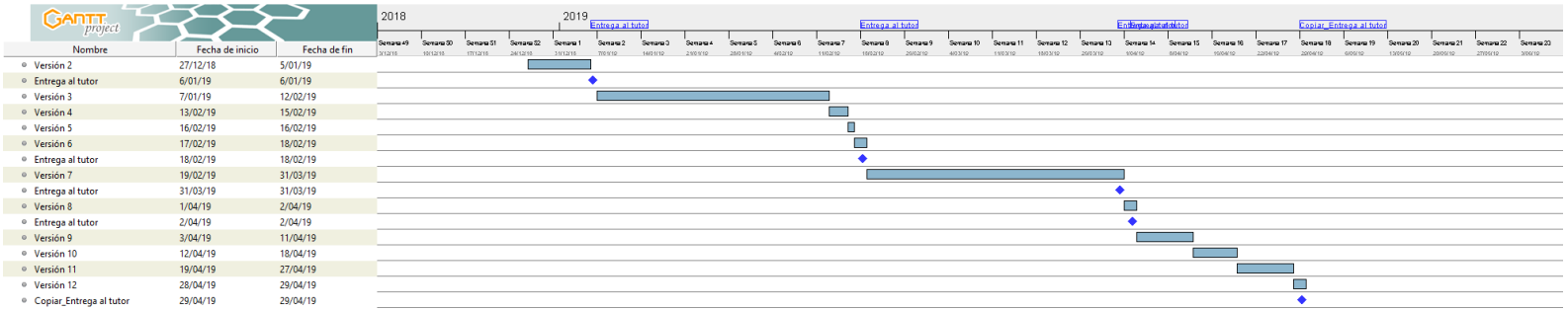


Nombre	Fecha de inicio	Fecha de fin
Prueba de Concepto	20/09/18	13/11/18
Investigación inicial	20/09/18	4/10/18
Construcción de Blockchain básica	4/10/18	15/10/18
Propuesta al tutor	15/10/18	17/10/18
Registro y voto básico	18/10/18	25/10/18
Solicitud de certificados a FNMT	24/10/18	25/10/18
Registro avanzado	26/10/18	30/10/18
Configuración de cliente OCSP	26/10/18	29/10/18
Creación de BBDD SQL de Censo	29/10/18	30/10/18
Votación avanzada	31/10/18	2/11/18
Votación varias veces	31/10/18	1/11/18
Cambio/pérdida de claves	1/11/18	2/11/18
Presentación de resultados en página web	2/11/18	6/11/18
Configuración de varios nodos	7/11/18	13/11/18
Simulación masiva de votos	8/11/18	9/11/18
Memoria	17/10/18	13/11/18
Primeros borradores (Versión 1)	17/10/18	13/11/18

Figura 48. Diagrama de Gantt de la Prueba de Concepto.

Aunque en la parte inferior del Diagrama se observa un apartado denominado “Memoria”, estos no eran más que los primeros borradores de lo que luego se fue desarrollando para la realización propiamente dicha de la Memoria ya con un mejor formato.

Una vez que la Prueba de Concepto ya estaba suficientemente desarrollada, se empezó a redactar la presente Memoria, la cual se fue enviando y consultando constantemente con el tutor.



Nombre	Fecha de inicio	Fecha de fin
Versión 2	27/12/18	5/01/19
Entrega al tutor	6/01/19	6/01/19
Versión 3	7/01/19	12/02/19
Versión 4	13/02/19	15/02/19
Versión 5	16/02/19	16/02/19
Versión 6	17/02/19	18/02/19
Entrega al tutor	18/02/19	18/02/19
Versión 7	19/02/19	31/03/19
Entrega al tutor	31/03/19	31/03/19
Versión 8	1/04/19	2/04/19
Entrega al tutor	2/04/19	2/04/19
Versión 9	3/04/19	11/04/19
Versión 10	12/04/19	18/04/19
Versión 11	19/04/19	27/04/19
Versión 12	28/04/19	29/04/19
Copiar_Entrega al tutor	29/04/19	29/04/19

Figura 49. Diagrama de Gantt de la realización de la Memoria.

REFERENCIAS

[1] El País, «Los peligros del voto online,» [En línea]. Available: https://elpais.com/politica/2016/12/09/actualidad/1481307305_335463.html.

[2] Instituto Nacional de Estadística, «Población que usa Internet,» [En línea]. Available: https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout.

[3] Ministerio del Interior, «La modernización de la gestión electoral,» [En línea]. Available: http://www.infoelectoral.mir.es/documents/10184/18279/ModernizacionGestionElectoral2011.pdf/6515f162-e51e-47c1-8389-74d86812f686.

[4] N. Goodman, «Issues guide: Internet Voting,» [En línea]. Available: https://www.edmonton.ca/city_government/documents/PDF/Internet_Voting_Issues_Guide_December_21_2012.pdf.

[5] egovernment.ch, «Electronic voting,» [En línea]. Available: https://www.egovernment.ch/en/umsetzung/schwerpunktplan/vote-electronique/.

[6] Parlamento Europeo: Oficina de España, «La comisión de Peticiones pide a España que revise el sistema de voto de los residentes en la UE,» [En línea]. Available: http://www.europarl.europa.eu/spain/es/sala_de_prensa/communicados_de_prensa/pr-2016/11-2016/101120162.html.

[7] El País, «Europa critica el voto rogado y la Junta Electoral pide al Gobierno que sea por Internet,» [En línea]. Available: https://elpais.com/politica/2016/12/08/actualidad/1481220515_503569.html#sumario_3.

[8] «Información electoral del Ministerio del Interior,» [En línea]. Available: http://www.infoelectoral.mir.es/infoelectoral/min/busquedaAvanzadaAction.html.

[9] Forbes, «Nine Companies That Want To Revolutionize Voting Technology,» [En línea]. Available: https://www.forbes.com/sites/rebeccaheilweil1/2017/12/02/eight-companies-that-want-to-revolutionize-voting-technology/#eb9bd0e12c15.

[10] El Mundo, «Las presidenciales, en manos de una empresa barcelonesa,» [En línea]. Available: https://www.elmundo.es/america/2012/11/04/estados_unidos/1352004788.html.

[11] El Mundo, «"Una persona puede cambiar todos los votos": hackean a la empresa que escrutará las elecciones Municipales y Europeas,» [En línea]. Available: https://www.elmundo.es/tecnologia/2019/03/15/5c8a582821efa060698b461d.html.

[12] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» [En línea]. Available: https://bitcoincore.org/bitcoin.pdf.

[13] «Red Lightning,» [En línea]. Available: https://es.wikipedia.org/wiki/Lightning_(red).

[14] BlockchainHub, «Blockchains & Distributed Ledger Technologies,» [En línea]. Available: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/.

[15] M. d. Castillo, «Forbes,» [En línea]. Available: https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchains-billion-dollar-babies.

[16] «Hyperledger,» [En línea]. Available: https://www.hyperledger.org/.

[17] «Corda,» [En línea]. Available: https://www.corda.net/.

[18] «Energy Web Foundation,» [En línea]. Available: http://energyweb.org/.

[19] «Multichain,» [En línea]. Available: https://www.multichain.com/.

[20] Cointelegraph, «Ataque del 51% de Ethereum Classic: La realidad del Proof-of-Work,» [En línea]. Available: https://es.cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work.

[21] «StackOverflow,» [En línea]. Available: https://stackoverflow.com/.

[22] «pyOpenSSL,» [En línea]. Available: https://pyopenssl.org/en/stable/index.html.

[23] A. Moujahid, «A Practical Introduction to Blockchain with Python,» [En línea]. Available: http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python/.

[24] G. Nash, «Let's Build the Tiniest Blockchain,» [En línea]. Available: https://medium.com/crypto-currently/lets-build-the-tiniest-blockchain-e70965a248b.

[25] Agencia EFE, «Estonia, pionera mundial en el voto por Internet,» [En línea]. Available: https://elpais.com/tecnologia/2007/03/04/actualidad/1173002462_850215.html.

[26] ACE Electoral Knowledge Network, «e-voting,» [En línea]. Available: http://aceproject.org/ace-en/focus/e-voting/default.

[27] valimised.ee, «General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia,» [En línea]. Available: https://www.valimised.ee/sites/default/files/uploads/eng/IVXV-UK-1.0-eng.pdf.

[28] Junta Electoral Central, «Información para electores,» [En línea]. Available: http://www.juntaelectoralcentral.es/cs/jec/informacion/electores.

[29] Timothy B. Lee, «Blockchain-based elections would be a disaster for democracy,» [En línea]. Available: https://arstechnica.com/tech-policy/2018/11/blockchain-based-elections-would-be-a-disaster-for-democracy/.

[30] Youtube: Crypto Español, «Cómo funciona Blockchain. Explicación sencilla visual en español,» [En línea]. Available: https://www.youtube.com/watch?v=hEoYL5j0wYU.

[31] Wikipedia, «Cryptographic Hash Function,» [En línea]. Available: https://en.wikipedia.org/wiki/Cryptographic_hash_function.

[32] bitcoin.org, «Bitcoin Developer Guide,» [En línea]. Available: https://bitcoin.org/en/developer-guide.

[33] Wikipedia, «Lightning Network,» [En línea]. Available: https://en.wikipedia.org/wiki/Lightning_Network.

[34] MiEthereum, «Blockchain,» [En línea]. Available: https://miethereum.com/blockchain/.

[35] MiEthereum, «Dapps,» [En línea]. Available: https://miethereum.com/smart-contracts/dapps/.

[36] The National Democratic Institute, «Electronic Voting and Counting Around the World,» [En línea]. Available: https://www.ndi.org/e-voting-guide/electronic-voting-and-counting-around-the-world.

[37] C. Moreno, «Criptografía asimétrica en Bitcoin.,» [En línea]. Available: https://medium.com/@cesar_m/criptograf%C3%ADa-asim%C3%A9trica-en-bitcoin-7acb484ba598.

[38] El Economista, «Criptomonedas y tokens no son el mismo criptoactivo,» [En línea]. Available: https://www.eleconomista.es/economia/noticias/8724862/11/17/La-moda-de-crear-nuevos-bitcoins-desde-Bitcoin-Cash-hasta-Bitcoin-Gold.html.

[39] Lifewire, «Which Countries Use Electronic Voting?,» [En línea]. Available: https://www.lifewire.com/which-countries-use-electronic-voting-4174877.

[40] New York Times, «It's Time for Online Voting,» [En línea]. Available: https://www.nytimes.com/2018/11/05/opinion/online-blockchain-voting.html.

[41] El Confidencial, «Cómo se hace el recuento de votos: así se lleva a cabo el escrutinio electoral,» [En línea]. Available: https://www.elconfidencial.com/elecciones-generales/2016-06-16/recuento-votos-escrutinio-electoral_1218314/.

[42] Blockchain services, «Conoce los diferentes tipos de blockchain,» [En línea]. Available: http://www.blockchainservices.es/novedades/conoce-los-diferentes-tipos-de-blockchain/.

[43] Wikipedia, «Unspent Transaction Output,» [En línea]. Available: https://en.wikipedia.org/wiki/Unspent_transaction_output.

ANEXOS

Anexo A – Puesta en funcionamiento de la PoC

El entorno que se ha usado ha sido el Sistema Operativo Ubuntu 18.04.2 LTS (64 bits) virtualizado sobre VirtualBox en su versión 5.2.26.

En el presente Anexo se detallará cómo poner en funcionamiento la Prueba de Concepto.

En un primer lugar se deben **activar los diferentes nodos** con los que se desee hacer dicha prueba. Esto se hace con el comando:

```
python nodo.py [n]
```

donde n será el id del nodo que se quiere poner en funcionamiento.

Así pues, por ejemplo, podemos poner en funcionamiento dos nodos con los comandos:

```
python nodo.py 1
```

y

```
python nodo.py 2
```

ejecutados cada uno en un terminal distinto, quedando de la siguiente manera:

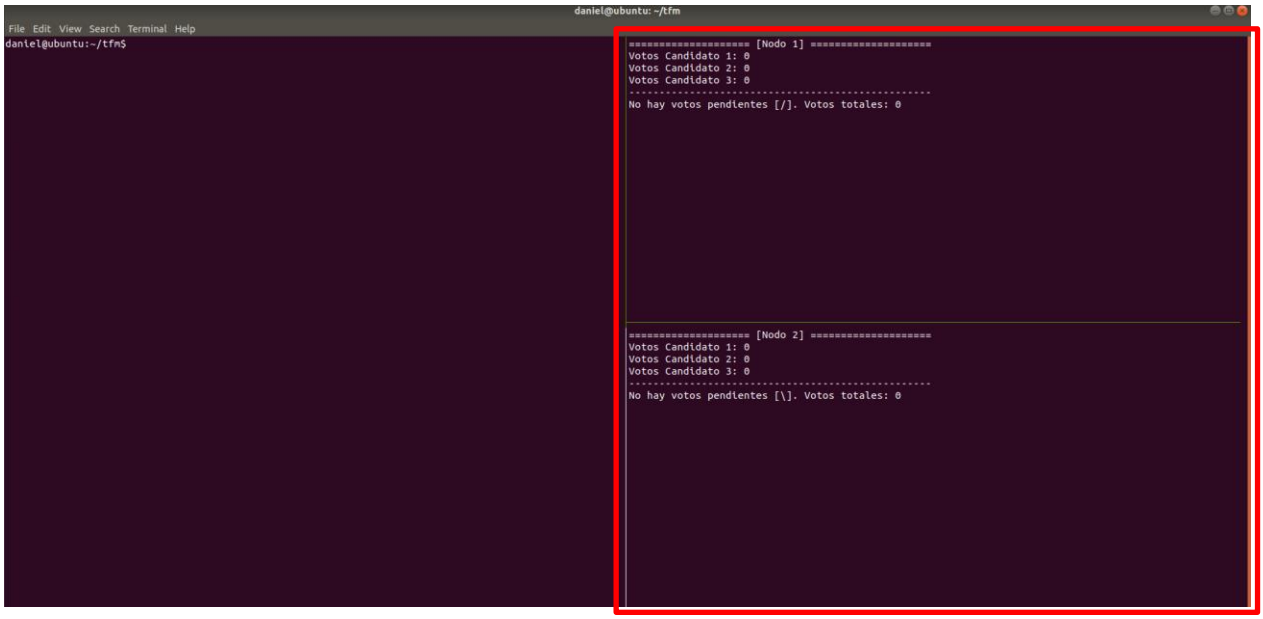


Figura 50. Puesta en funcionamiento de nodos en el sistema.

Lo siguiente sería poner en funcionamiento **la aplicación del cliente**, la cual es utilizada por el usuario para registrar su voto e interactuar con el sistema.

En este caso el comando a usar sería:

```
python cliente.py [n]
```

siendo n el número de nodos que se han puesto en funcionamiento.
Por lo tanto, para el caso anterior, en el que se han activado dos nodos, bastaría con ejecutar el comando:

```
python cliente.py 2
```

obteniendo con ello el siguiente resultado:

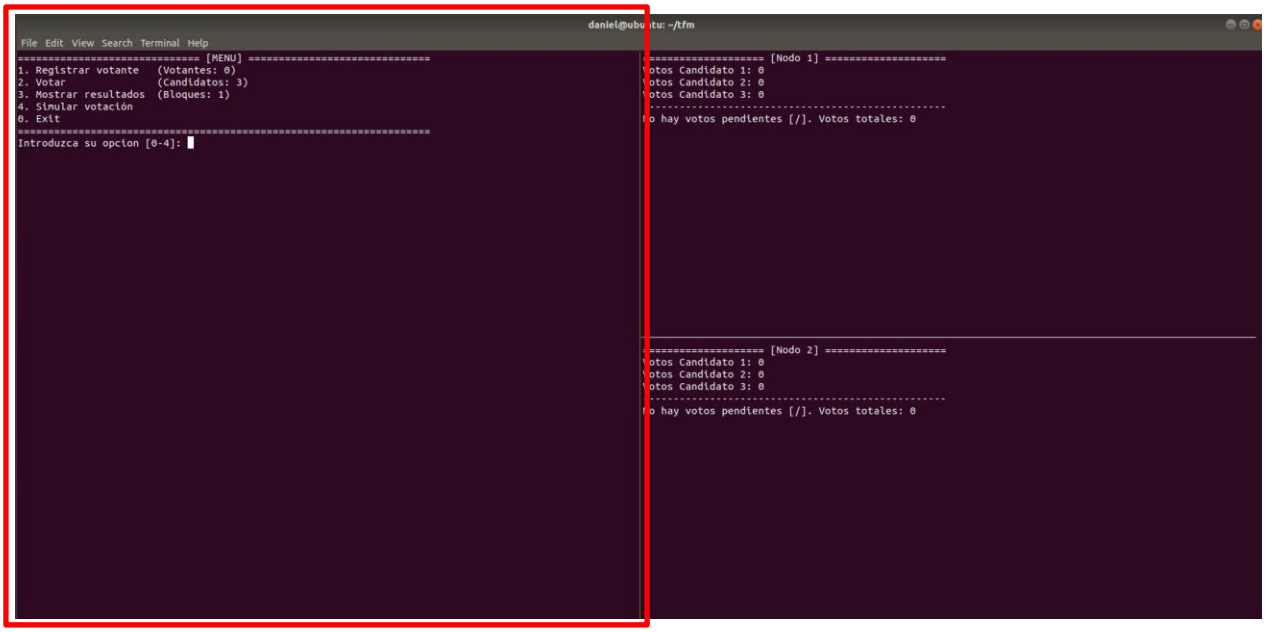


Figura 51. Puesta en funcionamiento del cliente en el sistema.

Anexo B – Código de la solución propuesta

El código íntegro se puede encontrar en el CD adjunto a esta memoria y en **https://github.com/danlopgom**