

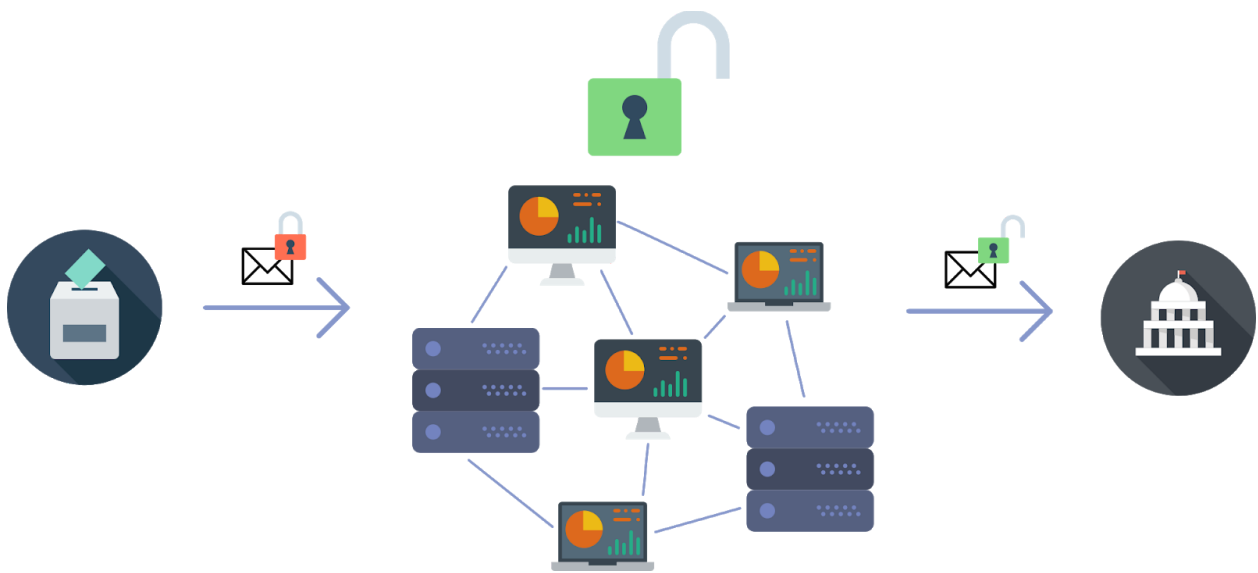


Infamous Inc.

Peer to peer democracy

Voting dApp

Adolfo Jiménez Prieto
Gonzalo Molpeceres Barrientos



Índice

Abstract	3
Objetivos	4
Modelo de negocio	6
Registro y verificación	6
Entorno de la aplicación	7
Votación	7
Enfoque corporativo	9
Pricing	9
Conceptos y tecnologías	10
¿Qué es la Blockchain?	10
Características de la Blockchain	10
Cómo funciona la Blockchain	11
Smart Contracts	12
Herramientas	12
Ethereum	13
Programa de trabajo	14
Posibilidades de futuro	16
El futuro del e-Voting	16
Futuro de nuestra dApp	17
Conclusiones	18

Abstract

Redefine your future

El sistema democrático de hoy en día consiste en la elección de un representante del pueblo que vele por sus intereses. Esto se realiza mediante la **votación individual** por el que cada persona considera al mejor individuo para llevar a cabo esa tarea. Pero este es solo un ejemplo, el acto de votar democráticamente en un grupo de personas se puede llevar hasta límites tan concretos como decisiones empresariales. Y todas y cada una de ellas tiene un problema en común: Lo **anticuado del sistema actual**, pues pese a la digitalización de la mayoría de aspectos de la vida moderna, las votaciones se suelen realizar todavía **mediante papel**, y su digitalización, además de lenta, es ineficiente, resultando en Máquinas Electrónicas de Voto (sustituyendo al voto en papel, pero requiriendo la presencia física de todas formas) y el voto mediante Internet, sistema el cual plantea varios problemas: La **falta de seguridad y privacidad**, pues con la falta de un sistema independiente confiable, los votantes han de depositar su confianza en la organización que lleva a cabo la votación, además de que es un sistema en el cual se podría llegar a acceder de forma ilegítima e insertar código malicioso. Este trabajo propone una solución en forma de **aplicación web** descentralizada y pública mediante la tecnología **Blockchain**, la cual junto a la adición de los Smart Contracts permitirá a sus usuarios realizar la votación con la seguridad de que su voto será contabilizado de forma segura y correcta sin tener que confiar en agentes externos.

“

Technology is, of course, a double edged sword.
Fire can cook our food but also burn us.

-Jason Silva

”

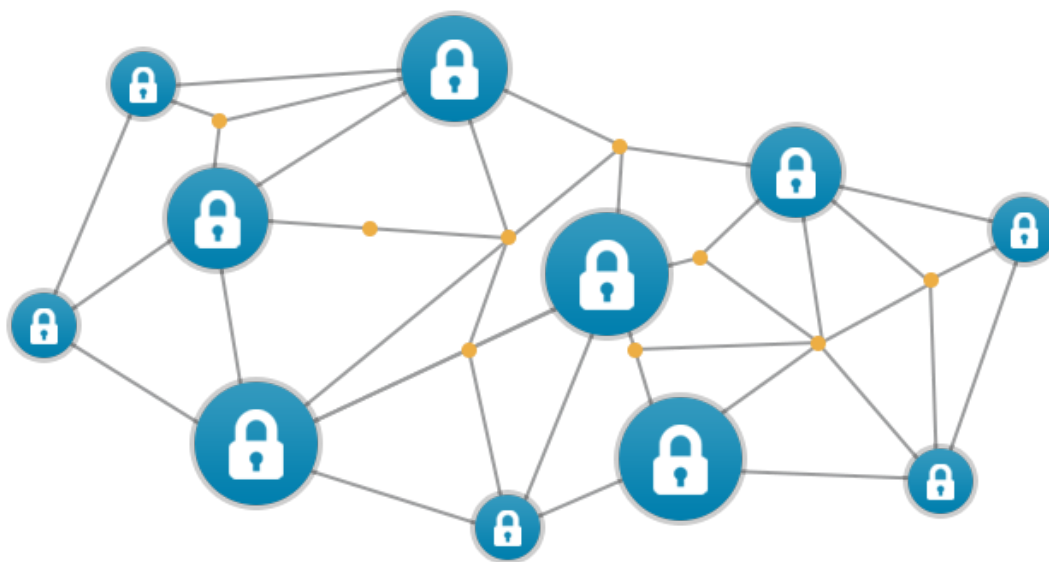
Objetivos

Strike hard and you'll strike once.

La creación de la aplicación descentralizada que tratamos tiene un objetivo muy claro: Simplemente permitir que un usuario vote.

Un objetivo primario y simple pero en el cual la magia sucede en lo que envuelve a esta acción, la cual hace este sistema el mejor para este objetivo y que buscamos que lo dote de ciertas características:

- ❑ **Seguridad:** Una característica primordial que se busca al utilizar la tecnología Blockchain es que los datos dentro de la aplicación sean completamente incorruptibles y fieles a los resultados reales.
- ❑ **Descentralización:** Una gran ventaja de la tecnología Blockchain radica en que no reside en una entidad central que tenga poder para manipular los datos y la aplicación. Al ser una tecnología peer to peer, su lógica reside en todos los nodos de la red Blockchain.



Descentralización en Blockchain

-
- ❑ **Privacidad:** Con el sistema que aquí se plantea, la contabilización de votos se realizará de tal manera que el voto y el usuario que lo ha realizado no están ligados de ninguna manera, permitiendo así el completo anonimato de los votos realizados.
 - ❑ **Integridad:** La tecnología Blockchain podrá utilizarse para garantizar la integridad del voto electrónico, ya que si un bloque es alterado de manera ilegítima los nodos que forman parte de la red Blockchain podrán percibir el cambio y actuar frente a ello.
 - ❑ **Transparencia:** Debido a la arquitectura de la tecnología Blockchain, desde cada nodo se tendrá acceso a todas las transacciones que se realicen dentro de esta y así verificar su legitimidad.
 - ❑ **Fluidez:** Nuestro objetivo es crear una forma sencilla de realizar la votación, y que después de crear tu usuario y verificar tu identidad el proceso de votar sea intuitivo y sin necesidad de saber nada relacionado con la lógica de detrás de la aplicación.
 - ❑ **Variedad:** Como se ha comentado previamente, se busca no solo realizar votaciones a nivel gubernamental y político, sino permitir a los usuarios que puedan crear grupos (de una empresa, por ejemplo) y desde ahí, trabajando con un sistema de permisos y reglas, dar la opción de crear votaciones.

Modelo de negocio

The best way to witness a change is to make your own.

Desde un primer momento, hay que dejar claro que el acceso más básico a la página no requerirá ningún tipo de contacto con la red Blockchain, estando esta ejecutándose en Background, con el usuario accediendo solamente al client-side si así lo desea.

Registro y verificación

Para poder acceder a la plataforma de votación será necesario conocer la identidad de la persona que quiere ser partícipe de una votación. El votante debe ser plenamente identificado para demostrar que está **habilitado para votar** y que no votará **más de una vez**; pero al mismo tiempo se le debe garantizar la privacidad necesaria para que su voto sea anónimo. Para esto se le otorgará una identidad digital mediante el documento nacional de identidad (DNI).

El proceso de verificación se llevará a cabo mediante la **intervención de un agente externo** (el cual podrá ser por ejemplo el gobierno o la policía), que recibirá los datos proporcionados por el usuario con el fin de verificarlos en su base de datos externa. Este agente solo tendrá acceso al DNI introducido pudiendo devolver una señal afirmativa o negativa una vez realizada la comprobación.

En caso negativo, la identidad digital no será creada dando por fallido el proceso.

En caso positivo, el usuario recibirá la posibilidad de crear un sistema de inicio de sesión con autenticación de doble factor con la cual accederá a su **identidad digital**, la cual será exclusiva y personal.

Los datos que el usuario ha de proporcionar consistirán en:

- Nombre, apellidos y número de DNI
- Foto del DNI a doble cara
- Foto de la cara para comprobar la identidad
- Correo electrónico para recibir notificaciones

Entorno de la aplicación

La aplicación web se compone de varios módulos:

- ❑ **Inicio:** Página de inicio de la aplicación web.
- ❑ **Perfil:** Permite visualizar la identidad digital del usuario registrado en ese momento.
- ❑ **Votaciones:** Módulo de la aplicación web en el que se visualizan las votaciones disponibles para un usuario. Permite al usuario ser partícipe de una votación y registrar su voto.
- ❑ **Resultados:** Una vez que la votación haya finalizado se visualizarán los resultados de las votaciones en las que el usuario a participado.
- ❑ **Grupos:** Permite crear grupos de trabajo para gestar una nueva votación. También permite unirse a grupos ya predefinidos anteriormente, así como invitar a usuarios de la plataforma a un grupo. La finalidad de este módulo es permitir a un colectivo de personas crear una votación y que los miembros de dicho grupo participen en ella votando.
- ❑ **Notificaciones:** El usuario recibe notificaciones acerca de futuras votaciones, invitaciones a grupos, disponibilidad de resultados de una votación pasada, etc.
- ❑ **Contacto:** Permite contactar con los administradores de la plataforma mediante teléfono, email o Skype.

Votación

Una vez una persona se registra correctamente (previa verificación) y posee una identidad digital está listo para votar.

El proceso en sí será tan sencillo como **entrar** en la votación deseada, **seleccionar** entre las opciones y **enviar el formulario**.

El coste de la escritura del nuevo bloque en la red Ethereum **será cargado al creador de la votación**.

A la hora de realizar dicho proceso de **crear la votación**, se necesitarán cumplir varios requisitos:

- ❑ Tener el **rol indicado** para ello: Para elecciones globales como pueden ser las elecciones generales de un país o para que el admin de un grupo cree votaciones dentro del mismo.
- ❑ Haber registrado una **cartera de Ethereum** con fondos suficientes para que todos los miembros puedan votar y los gastos de escritura corran a cargo del creador de la votación.
- ❑ Disponer del **software necesario** para poder ejecutar Ethereum dApps directamente en el navegador sin ejecutar un nodo completo de Ethereum. Se recomendará el uso de la extensión Metamask, la cual permite conectarnos a nuestra cadena de bloques Ethereum con nuestra cuenta personal.



e-Voting

Enfoque corporativo

La aplicación web no solo está orientada hacia instituciones gubernamentales sino que también está enfocada a corporaciones de cualquier tipo.

Una empresa que desee someter a votación cualquier propuesta través de nuestra plataforma sólo debe ponerse en contacto con nosotros mediante el módulo **Contacto**, consiguiendo así permisos para crear **grupos** relacionados con su empresa, **crear** votaciones dentro de ellos y a su vez **invitar** a otros usuarios.

Los administradores de la plataforma analizarán la solicitud de permisos de manera personalizada.

Pricing

Enfocándonos en el modelo de negocio aquí planteado, se proponen dos formas de cobrar por el servicio y así hacer viable tanto el desarrollo como el mantenimiento de esta aplicación:

- ❑ Pago de un **porcentaje** equivalente al 10% de lo que la votación requerirá para poder cubrir todos los gastos de escritura de bloques en la red Ethereum
- ❑ **Suscripción** mensual o anual con precios variables según la condición de la empresa (Número de empleados, número de socios, antigüedad trabajando con nosotros, etc.)

Con esto se intentará llegar a un **equilibrio** entre ofrecer un servicio accesible y a la vez rentable para los que trabajan en ella.

“

An investment in knowledge
pays the best interest

-Benjamin Franklin

”

Conceptos y tecnologías

Weird. Different. Unique. Exclusive.

Antes de entrar en detalle en tecnologías y frameworks concretos estudiaremos de manera básica qué es y cómo funciona Blockchain.

¿Qué es la Blockchain?

La cadena de bloques (**Blockchain**), es un registro único, consensuado y distribuido en varios nodos de una red. En el caso de las criptomonedas, podemos pensarlo como el libro contable donde se registra cada una de las transacciones.

La cadena de bloques se construye en base a propiedades criptográficas que buscan imposibilitar la modificación de la información que en ella se contiene.

En cada bloque se almacena:

- Una cantidad de registros o transacciones válidas,
- Información referente a ese bloque,
- Su vinculación con el bloque anterior y el bloque siguiente a través del hash de cada bloque - un código único que sería como la huella digital del bloque.

Características de la Blockchain

- ❑ **Inmutable:** El algoritmo de cálculo de las claves de las cabeceras incluye, además de la información encriptada del propio bloque, el código encriptado de la cabecera del código precedente. Al estar compuesto por estos dos elementos, cualquier cambio en un bloque de la cadena afecta a todos los que lo siguen, lo que los invalidará y así se podrían detectar manipulaciones. El coste que supone tener que modificar un bloque es elevado y cuanto más “retrasado” esté en la cadena, esta complejidad se multiplica exponencialmente porque supone tener que volver a enhebrar los bloques siguientes con los nuevos códigos calculados.

-
- ❑ **Distribuida:** Facilita que todos los nodos puedan comprobar la validez de la información que se está manejando a partir de la información encriptada, esto permite hacer esa validación de forma más ligera y rápida
 - ❑ **Consensuada:** Con la información de las cabeceras, los distintos nodos pueden comprobar si la información que ellos están manejando (y almacenando) es la misma que comparten la mayoría de los nodos, impidiendo así la alteración de nodos individualmente.

Cómo funciona la Blockchain

Cada bloque tiene un lugar específico e inamovible dentro de la cadena, ya que cada bloque contiene información del hash del bloque anterior. La cadena completa se guarda en cada nodo de la red que conforma la Blockchain, por lo que se almacena una copia exacta de la cadena en todos los participantes de la red.

A medida que **se crean nuevos registros**, estos son primeramente verificados y validados por los nodos de la red y luego añadidos a un nuevo bloque que se enlaza a la cadena.

Al ser un registro consensuado, donde todos los nodos contienen la misma información, resulta casi imposible alterar la misma, asegurando su integridad. Si un atacante quisiera modificar la información en la cadena de bloques, debería modificar la cadena completa en al menos el 51% de los nodos.

La tecnología de Blockchain nos permite almacenar información que jamás se podrá perder, modificar o eliminar. Dado que cada bloque está matemáticamente vinculado al bloque siguiente, una vez que se añade uno nuevo a la cadena, el mismo se vuelve inalterable. Si un bloque se modifica su relación con la cadena se rompe. Es decir, que toda la información registrada en los bloques es inmutable y perpetua.

En definitiva, en Blockchain los datos están distribuidos en todos los nodos de la red. Al no haber un nodo central, todos participan por igual, almacenando y validando toda la información. Se trata de una herramienta muy potente para comunicarnos y almacenar información de forma confiable; un modelo descentralizado donde la información es nuestra, ya que no dependemos de una compañía que brinde el servicio.

Smart Contracts

Dentro de la red Blockchain se desplegarán **Smart Contracts**, los cuales contienen toda la lógica empresarial de nuestra aplicación. Aquí es donde realmente modificaremos la parte descentralizada de nuestra dApp. Los contratos inteligentes se encargan de leer y escribir datos en la cadena de bloques, así como de ejecutar la lógica empresarial. Los contratos inteligentes están escritos en un lenguaje de programación llamado **Solidity**. La función de los contratos inteligentes en la cadena de bloques es muy similar a un microservicio en la web. Si el libro mayor público (Blockchain public ledger) representa la capa de base de datos de la cadena de bloques, entonces los contratos inteligentes son donde reside toda la lógica de negocios que se realiza con esos datos. Además, se llaman contratos inteligentes porque representan un **convenio o acuerdo**. En el caso de nuestro dApp de votación, es un acuerdo de que el voto del usuario contará, que otros votos solo se cuentan una vez y que el candidato con más votos ganará la elección.

Herramientas

Una vez entendido el concepto de Blockchain podemos ahondar en términos más concretos. Para implementar la aplicación descentralizada que tratamos nos serviremos de las siguientes tecnologías:

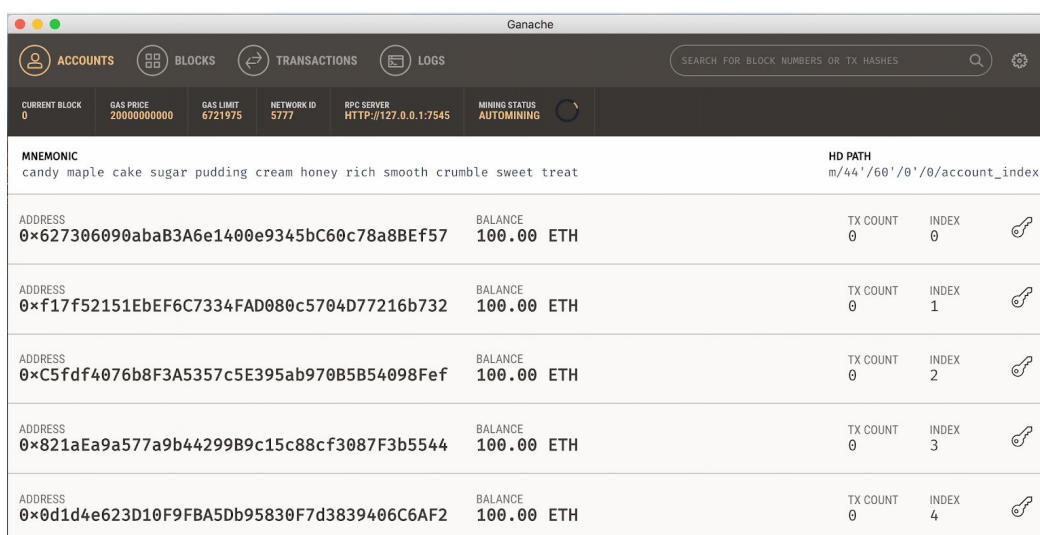
- ❑ **Truffle Framework:** Nos permite construir aplicaciones descentralizadas en la cadena de bloques Ethereum. Proporciona un conjunto de herramientas que nos permiten redactar contratos inteligentes con el lenguaje de programación Solidity. También nos permite probar nuestros contratos inteligentes y desplegarlos en la cadena de bloques. También nos da un lugar para desarrollar nuestra aplicación del lado del cliente.
- ❑ **Metamask:** Para poder utilizar la cadena de bloques, debemos conectarnos a ella (la cadena de bloques es una red). Tendremos que instalar una extensión de navegador para poder usar la cadena de bloques Ethereum. Podremos conectarnos a nuestra cadena de bloques Ethereum con nuestra cuenta personal e interactuar con nuestro contrato inteligente. Permite ejecutar Ethereum dApps directamente en el navegador sin ejecutar un nodo completo de Ethereum. Metamask incluye un almacén de identidad seguro, que proporciona una interfaz de usuario para administrar las identidades en diferentes sitios y firmar transacciones de cadena de bloques.

- ❑ **Node.js:** Entorno en tiempo de ejecución multiplataforma, de código abierto, para la capa del servidor.
- ❑ **web3.js:** Es una colección de bibliotecas de JavaScript que permite a nuestra aplicación del lado del cliente hablar con la cadena de bloques.

Ethereum

Entrando en el núcleo Blockchain del proyecto tenemos que diferenciar 2 herramientas que nos permitirán ser parte de la cadena bloques Ethereum:

- ❑ Por motivos de prueba, empezamos desarrollando nuestra aplicación descentralizada en **Ganache**, la cual consiste en una red Blockchain local alojada en memoria. Nos dará 10 cuentas externas con direcciones en nuestra cadena de bloques Ethereum local. Cada cuenta está precargada con 100 Ether falsos.



The screenshot shows the Ganache application window. At the top, there's a navigation bar with tabs for ACCOUNTS, BLOCKS, TRANSACTIONS, and LOGS. Below this is a status bar with various metrics like CURRENT BLOCK, GAS PRICE, GAS LIMIT, NETWORK ID, RPC SERVER, and MINING STATUS. The main area displays a list of accounts. Each account row includes an HD PATH, a mnemonic phrase, an address, a balance of 100.00 ETH, a transaction count, and an index. The first account's mnemonic is 'candy maple cake sugar pudding cream honey rich smooth crumble sweet treat'.

HD PATH	MNEMONIC	ADDRESS	BALANCE	TX COUNT	INDEX
m/44'/60'/0'/0/account_index	candy maple cake sugar pudding cream honey rich smooth crumble sweet treat	0x627306090abaB3A6e1400e9345bC60c78a8BEf57	100.00 ETH	0	0
		0xf17f52151EbEF6C7334FAD080c5704D77216b732	100.00 ETH	0	1
		0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef	100.00 ETH	0	2
		0x821aEa9a577a9b44299B9c15c88cf3087F3b5544	100.00 ETH	0	3
		0x0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2	100.00 ETH	0	4

Ejemplo Ganache

- ❑ Después de comprobar que todo funcionaba como esperábamos, trasladamos la aplicación descentralizada a **Geth** que nos permite formar parte de la cadena de bloques **real** de Ethereum. **Geth** es un programa que sirve como nodo para la cadena de bloques Ethereum, y mediante el cual un usuario puede minar Ether y crear un software que se ejecute en el EVM, la Máquina Virtual Ethereum.

Programa de trabajo

Commit yourself to the conquest.

El tiempo que llevará a cabo realizar la aplicación es algo muy difícil de medir, pero sí que intentaremos describir el proceso para llevar a cabo este proyecto y la dificultad de las fases subsecuentes.

Una vez preparado el entorno de trabajo con las tecnologías propuestas anteriormente, el primer paso debe ser la **instalación de Ganache** para realizar las pruebas en una red Blockchain. Esta red dispondrá de 10 cuentas con Ether falso sobre las que podremos hacer todas las pruebas. Sobre esta red prepararemos y realizaremos un “Smoke test” con el objetivo de comprobar que todo se ha llevado a cabo de forma satisfactoria.

En el siguiente paso nos centraremos en la **creación de los Smart Contract**, los cuales serán los intermediarios entre la interfaz de usuario y la red Blockchain. A medida que se van realizando es importante ir comprobando que todos funcionen de la forma esperada, pues cualquier fallo residual en el código puede ser fatal una vez el Smart Contract se despliegue definitivamente sobre la red, viéndonos obligados a eliminarlo de la red y volver a desplegar la versión corregida, eliminando de esta manera todos los datos que se hayan creado hasta el momento.



Ethereum Smart Contract

A medida que se van implementando nuevas funciones con la creación de los Smart Contract, el objetivo es ir **desarrollando paralelamente el “client-side”** que luego se le ofrecerá al usuario. La realización de una Interfaz de Usuario accesible, sencilla e intuitiva es prioridad en este paso, ya que se busca una aplicación que cualquiera pueda utilizar sin ningún tipo de complicaciones.

Mientras se trabaja en todo lo expuesto anteriormente, buscaremos encarecidamente la manera de **proveernos de un sistema de verificación 100% fiable de los usuarios**. Como se ha explicado previamente, la verificación será vía DNI, pero debido a que nosotros no disponemos de todos los datos, será necesaria la intervención de un agente externo (el cual solo tendrá acceso a verificar si el DNI es correcto, sin poder acceder a nada relacionado con las votaciones), como podría ser el gobierno o la policía.

Finalmente, todo el código desarrollado **se desplegará** sobre la auténtica red Ethereum, pasando a formar parte del conjunto de bloques, y estando ya a disposición de los usuarios para que accedan a ella.

“

The secret of success is to do
the common thing uncommonly well

-John D. Rockefeller Jr.

”

Posibilidades de futuro

Think ahead of the game.

El futuro del e-Voting

Expertos en Blockchain están discutiendo una nueva generación de "sistemas tecno-democráticos". Sin embargo, a corto plazo, el potencial más fuerte de BEV (Blockchain-enabled e-Voting) puede ser en contextos **corporativos** y no nacionales. De hecho, se han utilizado para las elecciones internas de los partidos políticos y los votos de los accionistas en Estonia. (Parlamento Europeo Research Service)

Entre los argumentos a favor de las elecciones electrónicas, destacan la valoración de la Blockchain como la **tecnología óptima para asegurar las garantías del voto** (integridad e inmutabilidad del voto) así como la expectativa de que el abstencionismo electoral decrezca dadas las facilidades que proporcionaría a los votantes su implementación (por ejemplo, no tener que desplazarse al colegio electoral).

No obstante, esta iniciativa también ha levantado críticas por parte del sector de la ciberseguridad. Y es que hay expertos que no están de acuerdo con que el Blockchain sea **suficientemente seguro** como para poder implementarlo en un área de tal relevancia. Concretamente, entienden que los dispositivos serían más sencillos de "hackear", que no sería posible garantizar que el voto sea correctamente registrado y que, al faltar un registro analógico, podrían llegar a producirse cambios indetectables en el transcurso de la votación. La integridad de unas elecciones dependerá en todo caso de la integridad de los sistemas informáticos que las soportan, sin que las tecnologías actuales (incluyendo la integración de sistemas de Blockchain) permitan garantizar sin lugar a dudas la ausencia de incidentes o ataques que puedan llegar a poner en riesgo las mencionadas condiciones de integridad.

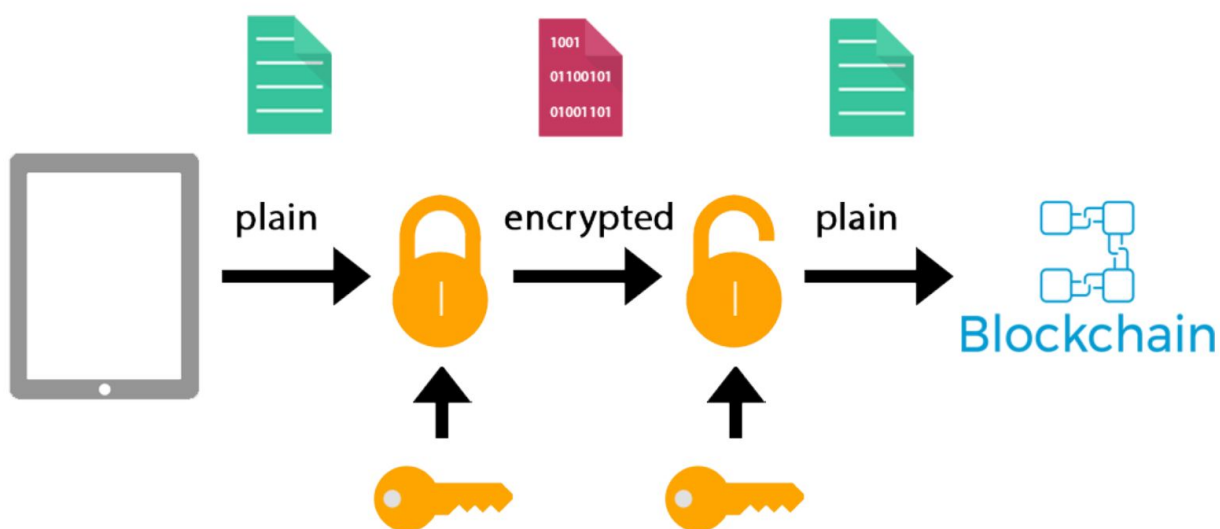
En definitiva, el futuro de las votaciones electrónicas basadas en Blockchain dependerá del **nacimiento de iniciativas** que la sepan llevar a cabo correctamente (como la que aquí se plantea) y de la **evolución del pensamiento colectivo** que sepa aprovechar la oportunidad que estas iniciativas les ofrecen en vez de rechazarlas en aras de mantener un sistema ya obsoleto a la par que inseguro.

Futuro de nuestra dApp

En el ámbito particular, un objetivo claro pero a largo plazo será desarrollar el mismo sistema que en la aplicación web pero para **dispositivos móviles**.

Contactar con empresas y organizaciones para enseñarles de lo que es capaz esta aplicación, y que así se amplíe su nivel de uso es también algo prioritario, ya que no queremos que se convierta en algo puramente gubernamental.

Otras funciones que se busca añadir en el futuro tienen como objetivo reforzar la seguridad de la aplicación mediante hacer más seguros los dispositivos con los que se accede a ella. Las funciones principales serán la **encriptación end-to-end** y la **verificación biométrica**



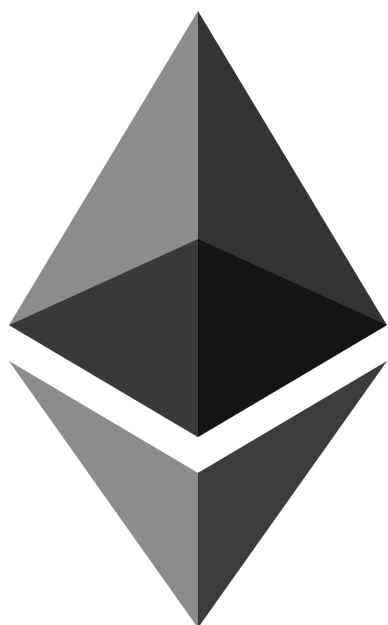
Encriptación end-to-end

Conclusiones

Welcome to blockchain: the 21st century way of voting.

Las soluciones para e-Voting son muy diversas. Sin embargo, todas ellas tienen dos problemas recurrentes: la falta de auditabilidad en el sistema, que implica el no poder verificar que este no esté guardando información adicional sobre el usuario u otras operaciones legítimas, y la centralización del sistema.

Por eso, nos planteamos la opción de proponer un **sistema propio**: descentralizado, auditable y que mantenga el voto anonimizado. Para ello, usamos **Blockchain**, una tecnología en auge que se mantiene en cambio constante.



Ethereum Logo

Hemos propuesto una dApp de votación que ha dado como resultado un prototipo que **cumple con los objetivos** propuestos al comienzo del proyecto.

De este trabajo podemos concluir que esta tecnología es **prometedora** en este campo y en otras áreas como pueden ser las ciencias IoT, las finanzas o la inteligencia artificial. Además empresas importantes como Visa, MasterCard o IBM apuestan por esta tecnología e incluso existe un consorcio multisectorial, llamado Alastria, promovido por empresas e instituciones para el establecimiento de una infraestructura semipública de Blockchain que soporte servicios con eficiencia legal en el ámbito español y acorde con la regulación europea.