

Blockchain y la prevención de fraude electoral

Camilo Alexander Rodríguez Cuarán –
camiloa.rodriguezc@konradlorenz.edu.co

Fundación Universitaria Konrad Lorenz – Ingeniería de sistemas

Resumen—En una sociedad democrática los ciudadanos tienen derecho a elegir a sus gobernantes y en ella existen diversos mecanismos de elección por los cuales cada individuo podrá ejercer su acción de elegir quien los represente. Sin embargo, por situaciones como los intereses privados o de grupos políticos, en algunos casos históricos ha afectado de manera negativa dichos sistemas, coartando y afectando la expresa decisión de los ciudadanos. En el presente documento se abordará una solución por medio de una cadena de bloques para mitigar la probabilidad de ocurrencia de fraudes y entregar a los ciudadanos un sistema más confiable.

Abstract-- In a democratic society, citizens have the right to elect their rulers and in it there are various mechanisms of choice by which each one can exercise its action of choosing who it represents. However, for example, in the cases, in the cases, in the cases, in the cases, in those cases in which the systems, cooperation and affection have been negatively affected, the decision of the citizens. In this document, a solution will be addressed in the middle of a chain of blocks to mitigate the probability of occurrence of fraud and deliver a more reliable system to citizens.

I. INTRODUCCIÓN

Este documento abordará la importancia que tiene la prevención de fraude electoral [1] y el impacto que tiene en las sociedades modernas si se elige un gobernante por medio de caminos manipulados y poco democráticos, así como también se podrá dar un vistazo de las estrategias que se implementan actualmente y que se han implementado en el mundo para la prevención de fraude electoral.

Por último, se explicará en detalle la implementación propuesta por medio de Blockchain o cadena de bloques para la prevención de fraude electoral y así ofrecer mayor transparencia a los votantes.

A. Contexto

En una sociedad democrática [2] el pueblo se representa por medio de un gobernante que está en propósito y a la defensa de intereses colectivos, pero este no puede representar un poder absolutista por lo cual los sistemas democráticos han diseñado toda una estructura de segregación de poderes, cargos y

mecanismos de elección. La Constitución política colombiana de 1991 define un Estado Social de Derecho fundamentado en los principios de soberanía popular, democracia, participación y la prevalencia del interés general, entre otros. Esta misma busca garantizar y reglamentar la posibilidad de acceso de cualquier ciudadano al ejercicio del mecanismo de participación ciudadana (voto) bajo un sistema político-electoral democrático y participativo. El sistema electoral democrático se puede definir como “el conjunto de medios a través de los cuales la voluntad de los ciudadanos se transforma en órganos de gobierno o de representación política”² o como “un sistema de gobierno en el cual el pueblo puede escoger y reemplazar sus líderes en elecciones libres, justas, periódicas y con competencia real.”³, para el sistema colombiano se pueden resumir tres figuras de participación la Democracia directa o participativa que se ejerce a través de los mecanismos de participación ciudadana, en donde según el Artículo 103 de la Constitución Política Colombiana “*Son mecanismos de participación del pueblo en ejercicio de su soberanía: el voto, el plebiscito, el referendo, la consulta popular, el cabildo abierto, la iniciativa legislativa y la revocatoria del mandato. La ley los reglamentará. ...El Estado contribuirá a la organización, promoción y capacitación ..., sin detrimento de su autonomía con el objeto de que constituyan mecanismos democráticos de representación en las diferentes instancias de participación, concertación, control y vigilancia de la gestión pública que se establezcan*”, la democracia indirecta o representativa mediante la elección de representantes al senado, cámara, asamblea y concejos y la Democracia pluralista en donde se establecen garantías para la creación de partidos y movimientos políticos y se establece un estatuto de la oposición. El actual proyecto contemplará como mecanismo de participación a automatizar el voto el cual está contemplado en el artículo 258 de la Constitución Política Colombiana como “*un derecho y un deber ciudadano, que por su importancia el Estado debe velar porque se ejerza sin ningún tipo de coacción y en forma secreta por los ciudadanos en cubículos individuales instalados en cada mesa de votación sin perjuicio del uso de medios electrónicos o informáticos*”, escogiendo como escenario a replicar una elección presidencial y vicepresidencial, normada para un periodo de 4 años según lo establecido por el artículo 190 de la CPC y cuya provisión de cargo es de carácter uninominal.

Una de las mayores debilidades de los sistemas democráticos en general reside en la probabilidad de cometer diferentes tipos de fraudes electorales y la demora en la presentación de los resultados, generando pérdida de credibilidad en el sistema electoral por parte de los electores y suspicacias por parte de varios sectores en la entrega de resultados finales⁴, haciendo que en varias ocasiones se deba realizar dobles conteos (como en el caso Colombiano) aumentando los costos y tiempos incurridos en el desarrollo del escrutinio, corregir decisiones realizadas (como en el caso de las tres curules indebidamente eliminadas del partido MIRA en Colombia en el año 2014⁵) minando la credibilidad en el sistema electoral o abriendo espacios para que se den diferentes tipos de fraude.

² Según Instituto federal Electoral de México

³ Larry Diamond, El Espíritu de la Democracia. 2009

⁴ <https://www.elsalvador.com/noticias/nacional/430078/conteo-de-votos-manual-retrasara-resultados-de-elecciones-2018/>

⁵ <https://www.elespectador.com/opinion/pilas-con-el-software-de-elecciones-columna-740742>

Para solucionar las debilidades mencionadas anteriormente se han llevado a cabo diferentes aproximaciones en el contexto internacional, como es el caso de Bélgica, Brasil, EEUU (en algunos estados), Estonia, Filipinas, India, Venezuela, entre otras, países que han migrado hacia sistemas de votación electrónica y cuyos procesos no han estado exentos de polémica en aspectos como la confiabilidad de la información recopilada y generada (fraude y hacking), auditoria al funcionamiento (caso Venezuela en las elecciones presidenciales de 2017), confiabilidad en los sistemas utilizados, entre otros.⁶

Países con implantación

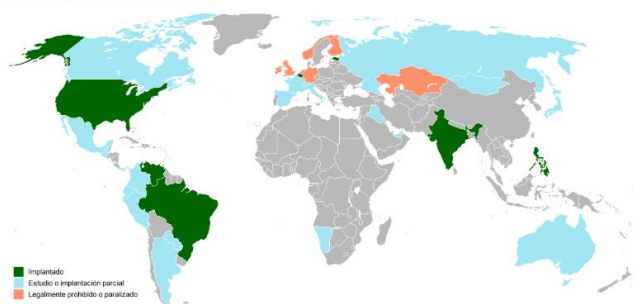


Fig. 1. Voto electrónico en el mundo⁷

Si bien, se han dado casos exitosos como el caso de Brasil⁸ en el que desde el año 2000 cuenta con un proceso totalmente automatizado, existen también otra serie de ejemplos en los que la implementación de este tipo de soluciones no generó el impacto o la confiabilidad esperada (como el caso de Venezuela).

Una de las tecnologías que puede ayudar a dar un paso adicional en la solución de los inconvenientes presentados es la tecnología Blockchain que por medio de sus fundamentos iniciales, transparencia, descentralización y robustez permite crear nuevas oportunidades en el mundo de la tecnología y democratizando nuevamente instituciones y procesos que se habían burocratizado y manipulado desde hace mucho tiempo.

Si bien esta tecnología no logrará erradicar definitivamente las dudas generadas sobre los sistemas de información que soportan las votaciones electrónicas, como bien lo presenta el artículo del MIT Technology Review titulado “Ni siquiera 'blockchain' puede garantizar el voto electrónico seguro”⁹, si constituye un paso fundamental en el avance de las tecnologías puestas al servicio del estado en temas tan fundamentales como lo son las diferentes elecciones realizadas.

B. Definiciones relevantes.

Cadena de bloques

Blockchain o DLT (Tecnología de Ledger Distribuido, por sus siglas en inglés) es una estructura de datos en que la información contenida se agrupa en grupos (bloques) virtuales y que se añade una referencia directa al bloque anterior para que se cree una impronta única e inmodificable, pero al mismo tiempo es posible auditar y acceder a la información en modo de lectura en cualquier momento.

Ethereum

“Ethereum es una plataforma descentralizada que corre contratos inteligentes sin ninguna posibilidad de tiempos de caída, censura, fraude o interferencia de alguna tercera parte”. Esta red se basa en Blockchain para poder funcionar y está distribuida a nivel global.

Contrato inteligente

“Un contrato es una colección de código y datos que residen en una dirección específica de la red de Blockchain”, en otras palabras, es una aplicación que es ejecutada en Ethereum y cuando son compilados tienen un formato binario llamado EVM (Ethereum Virtual Machine) bytecode..

Solidity

Es un lenguaje de desarrollo que permite desarrollar contratos inteligentes y permite compilar aplicaciones en EVM bytecode, este lenguaje es usado comúnmente en la comunidad de desarrollo para crear contratos inteligentes, sin embargo, no es la única opción.

API

Una interfaz de programación de aplicaciones es un conjunto de funciones y métodos que permiten interconectar dos sistemas de software entre sí para intercambiar mensajes o datos por medio de un protocolo de comunicación compartido.

Servicio Web REST

“REST es cualquier interfaz entre sistemas que use HTTP para obtener datos o generar operaciones sobre esos datos en todos los formatos posibles, como XML y JSON”

JSON

JSON (JavaScript Object Notation - Notación de Objetos de JavaScript) es un formato ligero de intercambio de datos. Leerlo y escribirlo es simple para humanos, mientras que para las máquinas es simple interpretarlo y generarlo.

C. Objetivo general

Diseñar y desarrollar un mecanismo difícil de corromper en la acción de voto apoyado en las nuevas tecnologías de la información para que al mismo tiempo ayude a que los ciudadanos puedan ejercer su derecho y obligación como integrantes de la sociedad.

II. NECESIDADES A RESOLVER

En la mayoría de sociedades democráticas modernas se implementa la elección por mayoreo, en dicha actividad se elige al representante que obtuvo la mayor cantidad de votos de los integrantes y será elegido para representar el pueblo o para desempeñar un rol significativo en la gobernación del mismo. Pero en las sociedades actuales se implementan demasiadas vías

⁶ <http://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es/>

⁷ <http://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es/>

⁸ <https://www.elespectador.com/noticias/el-mundo/el-voto-electronico-en-brasil-articulo-814081>

⁹ <https://www.technologyreview.es/s/10450/ni-siquiera-blockchain-puede-garantizar-el-voto-electronico-seguro>

de fraude electoral¹⁰, por mencionar algunas, entre ellas abarcan el intercambio de votos por especie (se le entrega un bien o recurso a cambio de algún voto), utilizar registros únicos nacionales de difuntos para hacerlos pasar como votantes válidos, manipulando las papeletas de votación para confundir y manipular a los votantes, crear distracciones o manipulación psicológica en las urnas de votación y en países más modernos, manipulando dispositivos electrónicos o sistemas de software para cambiar los votos que se han realizado por medio de estrategias de hacking, ingeniería social o robo de identidad, modificar e insertar campos en las bases de datos y entre muchos otros mecanismos, algunos más agresivos que otros pero con el único fin de atender a los intereses particulares de entes privados o personas fomentando así la corrupción.

Las sociedades actuales están viviendo cambios de paradigmas por el uso de nuevas tecnologías, y la elección de representantes en los sistemas democráticos no es ajena a esta, así que podemos ver nuevos canales de comunicación, de expresión, de protesta, de elección y un sinnúmero de intercambios culturales, sin embargo, esta tecnificación moderna ha conllevado nuevos problemas que en algunos casos afecta a la población mundial directamente y de manera muy eficaz como son la propagación de nuevas enfermedades, robos de identidad masivos, espionaje a escala mundial y manipulación de ideologías y pensamientos colectivos. Por estas razones y más es importante reconocer que la seguridad informática es un ítem mucho más complejo e importante que cada día toma más fuerza para prevenir desastres.

El caso relacionado más influyente que ha sucedido en la última década es el escándalo que ocasionó la compañía Cambridge Analytica, en el que esta fue capaz de obtener datos privados de usuarios de la red social más grande en el momento del escándalo (Facebook) para manipular psicológicamente a los residentes de Estados Unidos de América en las elecciones de 2016 en el que el resultado de dicha actividad fuera que Donald Trump haya sido seleccionado como presidente de la nación durante el período electo.

La estrategia en sí fue muy bien elaborada y diseñada, ya que por medio de formularios de personalidad las víctimas permitían entregar su información personal, lista de amigos, entre otros datos a los atacantes y así ir construyendo una red de manipulación, para que la víctima cuando navegue en internet, lea los Feed de Facebook vaya viendo noticias falsas que aparentemente son reales e ir desestabilizando la credibilidad a las instituciones, así también iban “conociendo” cómo es que la persona debía ser tratada y con qué tono.

El problema radica principalmente en que la red social (Facebook) no presentaba fallas de seguridad ni fue vulnerada su infraestructura para obtener la información de las personas, por el contrario, fue usada una estrategia de ingeniería social para poder manipular al votante. Sin embargo, esta controversial campaña política se vio envuelta en otros escándalos más directos en el que se llevaron a cabo ataques cibernéticos para poder hacer fraudes electorales.

Por lo tanto, allí es donde es primordial identificar riesgos electorales a partir de la generación de alertas tempranas, proveer información a las autoridades competentes, prevenir prácticas y acciones que afectan de manera negativa el proceso electoral y la identificación de posibles fraudes electorales.

III. SOLUCIÓN PROPUESTA

Por los temas ya vistos, se conoce el potencial riesgo que representa el no usar distintas vías de certificación y auditoría en un sistema de votación.

Así que se plantea desarrollar un sistema de votación completo en el que se usará un Smart Contract de Ethereum, aprovechar su cadena de bloques para que sea más fácil mitigar técnicas de hacking conocidas en las cadenas de bloque si se usa una pública en vez de una privada; un ejemplo claro es el que representa Bitcoin con su vulnerabilidad del ataque de 51%, en el que consiste que si un actor tiene la potencia de la mitad más uno este será capaz de modificar la cadena y sus registros.

Sin embargo, tener solo el contrato inteligente no basta para crear un sistema de votación efectivo y cercano a la realidad ya que en la red de Ethereum crear una “aplicación” de estas no permite tener un control detallado, escalable, gráfico o tener módulos avanzados de autenticación o autorización de una manera nativa, porque si bien existen las Dapp que son las mismas aplicaciones para Ethereum pero que al mismo tiempo permiten visualizar archivos HTML y manipular archivos JS por medio de un navegador especial; sin embargo, en una aplicación de este tipo se requiere tener una arquitectura y un diseño mucho más robusto, por ejemplo, para demostrar que un votante es realmente quien dice ser se requieren reconocimientos biométricos, escaneo del documento o un medio más sencillo como un sistema de autorización; teniendo en cuenta esa necesidad se requiere crear un Servicio Web o API REST que permita interconectar entre el contrato inteligente, las bases de datos necesarias y una aplicación web de ejemplo que servirá como portal para que los participantes puedan ejercer el voto.

Así también, al contar con un Servicio Web tipo REST será posible extender la funcionalidad a distintos tipos de clientes que se requieran en un futuro, bien sea una aplicación web mucho más robusta, en una aplicación móvil, por medio de servicio de mensajes cortos (SMS, por sus siglas en inglés) o algún otro medio efectivo que sea capaz de conectarse a una red de Internet.

IV. DESARROLLO

Para iniciar el desarrollo de la solución se separaron cuatro componentes principales, el contrato inteligente para Ethereum, el Servicio Web, la base de datos y un cliente de ejemplo que en este caso será Web. A continuación, un detalle de cada módulo que compone la solución.

A. Servicio Web

Para que este proyecto sea escalable se debe implementar un patrón de diseño robusto, pero al mismo tiempo versátil en el

que se puedan integrar distintos clientes y componentes. Por lo tanto, se decide escoger un patrón API Gateway, para poder romper la arquitectura monolítica tradicional y no centrar todos los servicios en un solo punto con el fin de evitar cuellos de botella o ataques centrales. Se puede definir que este patrón (API Gateway) es un servicio que cumple con el objetivo de punto de entrada a la aplicación desde Internet e internamente es el responsable de hacer la capa de ruteo, definición de componentes de API y otras funciones como la autenticación y autorización en una capa superior para proteger las funcionalidades principales; también es posible partir desde este patrón hacia otros mucho más complejos como el Service Mesh Pattern With Side Car o Micro-Gateway que se enfoca en microservicios para distribuir la carga, el despliegue y el mantenimiento, así como también permite desarrollar servicios más escalables, por lo cual es posible aislar componentes de alta frecuencia como la consulta de los votantes vs otros componentes que no tiene tanta concurrencia.

El patrón API Gateway tiene similitudes con el patrón de diseño Fachada (Facade) en programación orientada objetos porque este encapsula la arquitectura de la aplicación internamente para proveer un API hacia los clientes; por lo que conlleva a crear responsabilidades como tener límite de peticiones, autenticación, filtro de peticiones y prevención de fallos para que sea una implementación exitosa, de lo contrario puede ser un cuello de botella o un vector de ataque cibernético para la denegación de servicios como se había mencionado anteriormente. También es deseable anteponer un sistema de Firewall y proteger los servicios que están detrás del API Gateway.

El desarrollo de este API será llevado a cabo en Node.js y usando una plantilla de proyecto llamada Beat en el que permite implementar de una manera muy granular el ruteo, validaciones y definición de componentes antes de acceder a los módulos, se usará JSON como formato de intercambio de datos y se diseñó un protocolo de mensajes para manipular distintos tipos de canales de petición y respuesta.

- a. API REST: El formato de respuesta se compone de tres elementos; la verificación que informa si la operación fue exitosa o no, el mensaje que contiene información detallada para humanos de la operación y el resultado que puede ser cualquier tipo de dato soportado por JSON.

Definición:

```
{
  success: boolean,
  message: string,
  result: object
}
```

Ejemplo:

```
{
  success: true,
  message: "La operación se completó exitosamente",
  result: {id: "biz-0af12"}
}
```

- b. Sockets: El formato de petición y respuesta se compone cuatro elementos; el identificador nativo que informa el localizador único e irremplazable del nodo en el sistema, el contexto que provee información de la comunicación, el comando que define qué se va a ejecutar o responder en el nodo y los valores de resultado.

Definición:

```
{
  nativeId: string
  context: {
    channel: string
    sender: object,
    receiver: object,
    type: string
  },
  command: string
  values: object
}
```

Ejemplo:

```
{
  nativeId: 'node-as23' // Identificador único del nodo
  context: {
    channel: 'ws', // Puede ser Socket o WebSocket
    sender: {
      socketId: socket.id // Identificador del emisor
    },
    receiver: {
      socketId: socket.id // Identificador del receptor
    },
    type: 'gatewayMessage', // Existe un directMessage o un gatewayMessage
  },
  command: 'getAllNodes#request', // Es un comando para conocer qué ejecutar
  values: {} // Cualquier parámetro que quiera recibir o retornar
}
```

B. Base de datos

En este proyecto se usará una base de datos no relacional Google Firebase Real Time con fines ilustrativos, pero internamente la plantilla de proyecto Beat combina dos patrones de diseño llamados Abstract Factory y Bridge para poder desacoplar el motor de base de datos y sus operandos porque se entiende que en sectores de gobierno se usan bases de datos relacionales y se desconoce a nivel de este proyecto qué motor de base de datos se podría específicamente en una implementación real, sin embargo el esquema de los datos será normalizado para que el tratamiento de los datos siga siendo transversal al tipo de base de datos.

A continuación, la definición de las entidades que se usarán.

A continuación, la definición del esquema de los datos.

C. Aplicación Web

La aplicación Web de prueba también estará con un motor de Back-end basado en V8 y JavaScript (Node.js), así como también su tecnología de Front-end será Vue.js para administrar

correctamente los datos que serán recopilados desde el Front-End y así mismo la manera en cómo serán entregados hacia el API.

Se cuenta con dos secciones importantes, la del votante y la del conteo de votos.

La primera tendrá un formulario web para ingresar el documento de identidad del votante que estará previamente registrado en la base de datos para que el API pueda corroborar que es un votante habilitado. Aquí por fines ilustrativos solamente se buscará la existencia del registro.

La segunda es un control de visualización para poder determinar qué candidato es el que tiene mayor cantidad de votos al momento de la consulta.

D. Contrato inteligente

Esta aplicación será desarrollada con Solidity, el lenguaje de programación oficial de Ethereum para poder crear EVM bytecode y poder distribuirla en la red. Sin embargo, para poder prevenir fraudes electorales se implementará un concepto llamado DAO (Decentralized Autonomous Organizations, por sus siglas en inglés) en donde los estatutos de la organización están incrustados en el código del contrato y se pueden crear reglas complejas de gobernanza, por lo tanto en este punto podemos comenzar a ver al Estado como una organización o “empresa” que tiene una jerarquía para poder funcionar y que para tomar decisiones se debe llegar a un consenso entre todos involucrados. En Blockchain existe este concepto de votación desde sus fundamentos para que todos los entes puedan elegir un representante, en el caso de Bitcoin (que fue la primera tecnología en implementar Blockchain) sería quien se gana la recompensa y almacena los registros durante un tiempo determinado; en este caso, usaremos un consenso para determinar qué candidatos serán los que tienen mayor cantidad de votos y solo unos cuantos podrán ser candidatos, no todos.

Para aclarar, DAO nos permite tener reglas complejas internas para que podemos crear validaciones de conteo en un solo voto, rangos de tiempo de votación, verificación de ubicación geográfica, entre otras que no aplican a este proyecto.

Finalmente, este contrato será divulgado en la red de Ethereum para poder ejecutarse asíncronamente y de manera segura previniendo múltiples ataques cibernéticos.

V. CONCLUSIÓN

Si bien tener herramientas tan robustas, buenas prácticas de programación, buena arquitectura y hasta una solución basada en Blockchain que permite mitigar muchos casos de fraude como la falsificación de registros, robos de identidad, modificación de votos en las bases de datos, ataques de denegación de servicio, entre otros, no se puede proveer una solución absoluta a todos los casos de corrupción y fraude que se pueden presentar épocas de elecciones como fue el caso de Cambridge Analytica. Por eso, determinar qué vectores de ataque o vulnerabilidades incluso humanas se pueden explotar para realizar actos ilegítimos e ilegales son de vital

importancia en un mundo interconectado y en constante evolución.

Como en todo, riesgos significa oportunidades. Conocer los desafíos que presenta esta tecnología disruptiva puede convertirse en una ventaja competitiva para la democracia de nuestra sociedad. Ignorar los riesgos que conlleva a que personas y grupos inescrupulosos manipulen la real voluntad de los ciudadanos puede acabar convirtiendo el futuro de un país en un lastre.

Aunque en el corto plazo no se estén considerando mecanismos para formalizar este tipo de medios electrónicos como canales formales de elección popular, el país está cada día preparándose para hacer frente a estos nuevos retos, aunque pueda parecer que mecanismos como el propuesto sea costoso de implementar, el efecto a largo plazo para combatir la corrupción traerá muchos más beneficios alineados a los reales intereses del pueblo, por lo tanto, este proyecto abre la posibilidad a nuevas investigaciones de tipo económico, social y político acerca de los impactos reales que tendría la misma.

VI. REFERENCIAS

- [1] <http://www.scielo.org.mx/pdf/rms/v69n1/v69n1a1.pdf> [¿Qué es el fraude electoral? Su naturaleza, sus causas y consecuencias]
- [2] <http://web.stanford.edu/~ldiamond/iraq/WhatsDemocracy012004.htm> [What is Democracy?]
- [3] <http://perfilesia.flasco.edu.mx/index.php/perfilesia/article/view/307/260> [El ejercicio de las instituciones electorales en la manipulación del voto en México*]
- [4] <https://poseidon01.ssrn.com/delivery.php?ID=881031104121115078064104029026121088037017063054033022103118072092013119096070070066122030022042108012118124116107067095075092016071069044035003087028092083092109011038062012025001115065105122126113123004007087122116003004107120113125099084004085091096&EXT=pdf> [Blockchain Technology: What is it good for?]
- [5] <https://www.cs.cmu.edu/afs/cs.cmu.edu/Web/People/NatProg/papers/Ellis2007FactoryUsability.pdf> [The Factory Pattern in API Design: A Usability Evaluation]
- [6] <https://github.com/ethereum/wiki/wiki/White-Paper> [A Next-Generation Smart Contract and Decentralized Application Platform]
- [7] <https://arxiv.org/pdf/1703.06322.pdf> [An empirical analysis of smart contracts: platforms, applications, and design patterns]
- [9] <https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/> [Bootstrapping A Decentralized Autonomous Corporation: Part I]
- [10]
- [11] <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/> [DAOs, DACs, DAs and More: An Incomplete Terminology Guide]
- [12] <https://solidity.readthedocs.io/en/v0.4.24/> [What is Solidity]
- [13] <https://bbvaopen4u.com/es/actualidad/api-rest-que-es-y-cuales-son-sus-ventajas-en-el-desarrollo-de-proyectos> [API REST: qué es y cuáles son sus ventajas en el desarrollo de proyectos]
- [14] REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces, Mark Masse
- [15] <https://patents.google.com/patent/US8621598B2/en> [Method and apparatus for securely invoking a rest API]
- [16] <https://bbvaopen4u.com/es/actualidad/que-es-una-api-y-que-puede-hacer-por-mi-negocio> [Qué es una API y qué puede hacer por mi negocio]
- [17] <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.675.7497&rep=rep1&type=pdf> [What Makes APIs Hard to Learn? Answers from Developers]
- [18] <https://www.redhat.com/es/resources/3scale-what-is-an-api-ebook> [What is an API? Your guide to the internet business (r)evolution]

- [19] <https://www.json.org/json-es.html> [Introducción a JSON]
- [20] <http://ethdocs.org/en/latest/contracts-and-transactions/contracts.html> [Contracts]
- [21] www.forrester.com/report/Predictions+2019+Distributed+Ledger+Technology/-/E-RES144635 [Predictions 2019: Distributed Ledger Technology]
- [22] <https://es.cointelegraph.com/news/report-companies-dropping-the-term-blockchain-due-to-hype-around-technology> [Informe: Compañías abandonan el término 'Blockchain' debido al hype en torno a la tecnología]
- [23] <https://blockchainhub.net/dao-decentralized-autonomous-organization/> [What is a DAO?]
- [24] <https://www.ethereum.org/dao> [Decentralized Autonomous Organization]
- [25] <https://www.forbes.com/sites/forbesfinancecouncil/2018/07/30/The-economics-of-decentralized-organizations-the-end-of-for-profit-corporations/#6dad1c1d3966> [The Economics Of Decentralized Organizations: The End Of For-Profit Corporations?]
- [26] <https://highlyscalable.wordpress.com/2012/03/01/nosql-data-modeling-techniques/> [NoSQL data modeling techniques]
- [27] <https://smartbear.com/learn/api-design/what-are-microservices/> [What is Microservices Architecture?]
- [28] <https://dzone.com/articles/api-management-design-patterns-for-digital-transfo> [API Management Design Patterns for Digital Transformation]
- [29] <https://freecontent.manning.com/the-api-gateway-pattern/> [The API Gateway Pattern]
- [30] Microservices Patterns With examples in Java, Chris Richardson
- [31] <http://www.cs.yale.edu/homes/jf/Gonzalez.pdf> [Hacking the citizenry?]
- [32] <https://www.bbc.com/mundo/noticias-43472797> [5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US\$37.000 millones en un día]
- [33] https://www.abc.es/internacional/abci-hackers-rusos-ceban-grupos-republicanos-contrarios-idilio-entre-trump-y-putin-201808220149_noticia.html [Los «hackers» rusos se ceban con grupos republicanos contrarios al «idilio» entre Trump y Putin]