INSTITUTO TECNOLÓGICO SUPERIOR DE SANTIAGO PAPASQUIARO

ING. SISTEMAS COMPUTACIONALES

“Blockchain Aplicada a la Transparencia Electoral”

TALLER DE INVESTIGACIÓN 2

Autores:

Marvin Meza Hurtado [19010104]

Jesús Alfredo Saravia Díaz [19010111]

Hendrik Alberto Villarreal Sarmiento [19010115]

Asesor:

M.C. Rudy Ramírez Gamboa

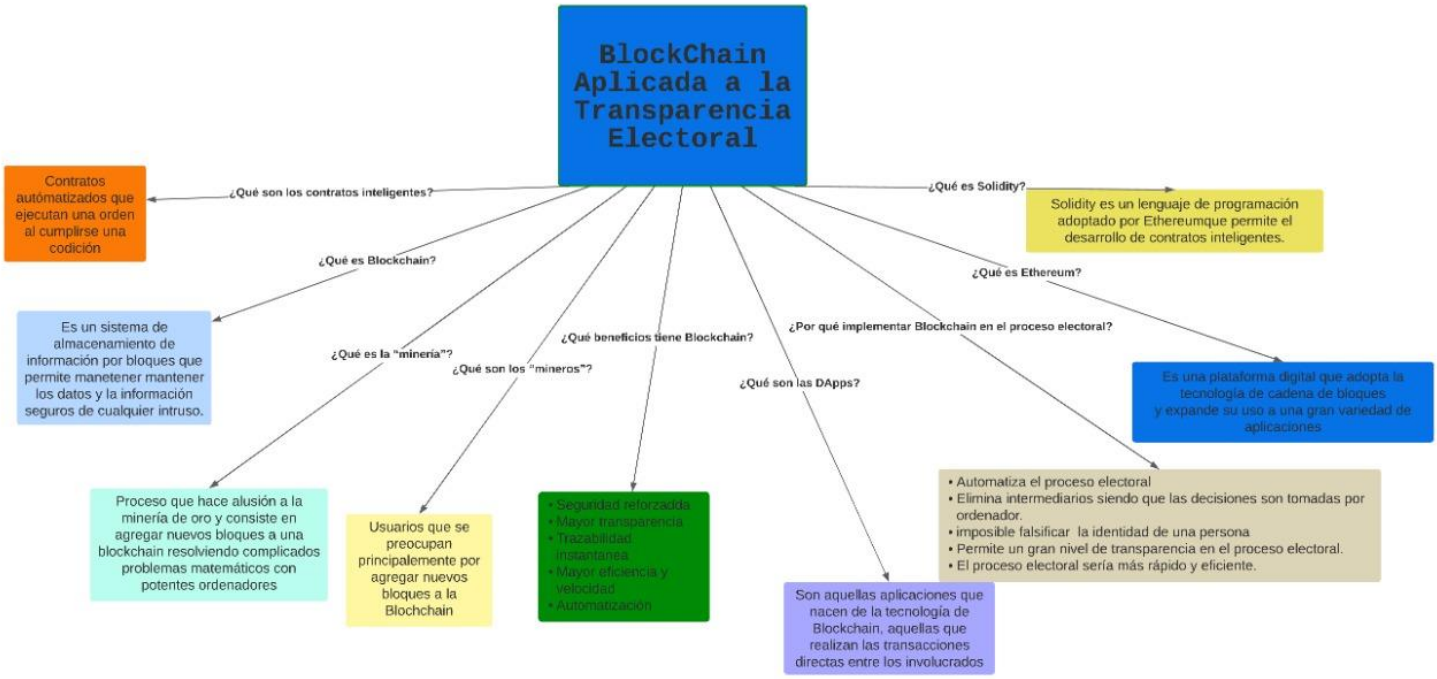
Santiago Papasquiaro, Dgo. Febrero 2023

Contenido

Lugar de Investigación

El área de estudio que tomaremos para nuestra investigación son los estudiantes que asisten a la carrera de Ingeniería en Sistemas Computacionales en el grupo de 7°C del Instituto Tecnológico Superior de Santiago Papasquiaro, ubicado en la capital del municipio de Santiago Papasquiaro en el estado de Durango de los Estados Unidos Mexicanos.

Mapa Conceptual



Preguntas de la investigación

¿Qué es Blockchain?, ¿Cómo está compuesto el Blockchain?, ¿Quién creó el Blockchain?, ¿Quién usó Blockchain por primera vez?, ¿Para qué se usó el Blockchain?, ¿En qué se usa el Blockchain actualmente?, ¿Qué es la "minería"?, ¿Qué son los "mineros"?, ¿Qué son las DApps?, ¿Ha habido problemas o errores al usar Blockchain?, ¿Qué beneficios tiene Blockchain?, ¿Blockchain de verdad es tan seguro?, ¿Qué es un voto electrónico?, ¿Qué beneficios tiene Blockchain en los procesos electorales?, ¿Cómo se puede usar Blockchain en los procesos electorales?, ¿Por qué implementar Blockchain

en el proceso electoral?, ¿Qué son los contratos inteligentes?, ¿Qué es Ethereum?, ¿Qué tienen de importante los contratos inteligentes?

Hipótesis

El Blockchain al ser un sistema que puede proteger datos e información, actualmente se usa más en la criptomoneda, tal es el caso de bitcoin. Pero Blockchain es más que solo eso, al ser un sistema que asegura la información que ingresa en él, haría más sencillo algunos aspectos de la vida cotidiana, por ejemplo, podría dificultar o evitar por completo la falsificación de información y documentos importantes.

Utilizar las características del Blockchain, como la seguridad y la confianza de la imparcialidad de las decisiones que se toman, se visualiza la opción de ser usado en la elección democrática de cualquier tipo, eliminando los problemas que las elecciones a grande escala han sufrido.

La tecnología Blockchain abre la oportunidad a elecciones más honestas permitiendo que la voz de la gente sea realmente escuchada como es debido, todo esto con la seguridad de la protección que ofrece Blockchain y la confianza de ser totalmente imparcial en las decisiones tomadas.

Variables Hipótesis

- Independiente

  Dentro de las variables independientes tenemos la tecnología Blockchain, los procesos electorales y los participantes de la Blockchain, estos no dependen de ninguna acción del investigador, por lo cual son consideradas variables independientes

- Dependiente

  Usar Blockchain en los procesos electorales mejorando el proceso y eliminando las fallas de la forma anterior de llevar el proceso, depende del uso dado a la tecnología Blockchain y como esta es aplicada en el tema de procesos electorales con el objetivo de mejorar dicho proceso.

Hipótesis alterna

Dada la transparencia que permite la Blockchain, es posible identificar rápidamente algún intento de fraude o algún intento no permitido de modificar los datos de la Blockchain, lo es parte de la seguridad de la misma, también permite dar un seguimiento a la transacción con el fin de encontrar el origen de dicho movimiento prohibido.

Esto permite no solo tener más seguridad sino más confianza ya que la información general de los movimientos de la Blockchain es compartida por todos los usuarios, por lo que si se intenta hacer un movimiento indebido todos los participantes lo sabrán, lo que quiere decir que en una Blockchain usada para el proceso electoral, todos los votantes tendrán acceso a dicha información.

Variables Hipótesis Alterna

- Independiente

  La tecnología Blockchain y los participantes de una cadena de bloques es un elemento independiente, ya que no tiene dependencia de algún elemento manipulable por el investigador.

- Dependiente

  Realizar la trazabilidad depende de la Blockchain, así como de los participantes de la Blockchain, por lo que es un elemento dependiente.

Objetivo General

Demostrar la efectividad de la tecnología Blockchain en la realización de un proceso electoral transparente implementando un sistema de votaciones simple basado en Blockchain para la elección de jefe de grupo en el grupo de 7°C de la carrera de Ingeniería en Sistemas Computacionales del Instituto Tecnológico Superior de Santiago Papasquiaro.

Objetivos Específicos

- Investigar los puntos más importantes sobre la tecnología de Blockchain en la actualidad.
- Analizar las formas más comunes de implementar sistemas de elecciones en la actualidad.
- Evaluar los distintos casos de procesos electorales en los que se haya implementado la tecnología Blockchain.
- Desarrollar una solución basada en Blockchain sobre un sistema de elecciones simple.
- Probar el sistema de elecciones basado en Blockchain realizando diferentes casos de uso.

Justificación

Nuestra investigación se justifica por la necesidad de comprobar que el Blockchain es un método viable para implementar un sistema de elecciones transparente para el grupo de 7°C de la Ingeniería en Sistemas Computacionales del Instituto Tecnológico Superior de Santiago Papasquiaro. A continuación, se describen los diferentes puntos de vista de los posibles afectados.

- Los alumnos podrán darse cuenta de lo seguro y efectivo que sería implementar un sistema de elecciones a base de la tecnología Blockchain, ya que, al ser descentralizado, los votos de los alumnos son respetados sin temor a alteraciones o fallos.
- Los directivos tendrán una solución para aplicar a los ámbitos en los que se requieran votaciones por parte de los alumnos o del personal del Instituto Tecnológico Superior de Santiago Papasquiaro en general, ya que al tratarse de un sistema que está comprobado que es seguro, dará mayor confianza a los votantes a participar en la toma de decisiones de la institución asegurando que su elección será tomada en cuenta.
- Las demás instituciones educativas se darán cuenta de la efectividad y la seguridad que proporciona el Blockchain en la toma de decisiones transparentes, por lo que

considerarían implementar un sistema basado en esta tecnología en los eventos en donde se requiera de la votación del personal.

- Al darse cuenta los demás habitantes del municipio del sistema de elecciones basado en la tecnología de Blockchain, podrían proponer un sistema de elecciones, pero llevado a cabo a una escala mayor, como para las elecciones de algún representante municipal.
- En un futuro, el INE municipal podrían basarse del sistema de elecciones basado en Blockchain llevado a cabo en el Instituto Tecnológico de Santiago Papasquiaro para implementar un sistema de elecciones para la elección de los representantes del municipio de Santiago Papasquiaro.
- En dado caso de que se implementara un sistema de elecciones basado en la tecnología de Blockchain para la elección de los representantes del municipio de Santiago Papasquiaro, los representantes de los distintos partidos políticos podrán tener la confianza de que las elecciones se harán de la manera más transparente posible.
- Las personas que vienen a votar desde otros poblados cercanos mostrarán mayor interés al participar en las elecciones del municipio, además de que tendrán una mayor confianza de que su voto será respetado y validado para la elección de los representantes de la cabecera municipal.
- Al haber varios casos de éxito y satisfacción en la implementación de la tecnología de Blockchain en los sistemas electorales, esta solución podría extenderse por todo el estado de Durango e inclusive por todo el país en los distintos ámbitos que requieran de la implementación de un sistema de elecciones seguro y viable.
- Gracias a la demanda que puede tener el implementar la tecnología de Blockchain en los procesos electorales, muchos investigadores con mayor experiencia podrían ahondar más en el tema con el objetivo de encontrar mejoras de la tecnología de Blockchain aplicables a los sistemas de elecciones, esto con el propósito de mejorar de forma constante esta solución, disminuyendo la posibilidad de que surja alguna vulnerabilidad. Además, a raíz de esta solución, se podrían generar otras investigaciones sobre otros casos o ámbitos en donde se pueda implementar la tecnología de Blockchain.

- Desde el punto de vista económico, esta solución ahorra los costos, ya que se omitiría el uso de material físico y se ahorraría el tener que contratar personal para las distintas fases del proceso de las elecciones.
- Desde el punto de vista medioambiental, el hecho de implementar este sistema basado en una tecnología digital, se evitaría el uso de papel, por lo que estaríamos generando un impacto positivo en el medio ambiente.

Marco Teórico

CAPÍTULO I. ASPECTOS GENERALES DE BLOCKCHAIN

1.1 ¿Qué es Blockchain?

Blockchain en español significa “Cadena de Bloques”, es un sistema de almacenamiento de información que permite mantener los datos y la información seguros de cualquier intrusión o intento de manipulación (Universidad Politécnica de Catalunya).

Desde hace mucho tiempo la información ha sido administrada por humanos, esos seres lentos, corruptibles, perezosos y hedonistas que siempre habrá la incertidumbre de si la información está en buenas manos. Blockchain busca asignarle esta tarea a otro tipo de seres, más confiables, eficaces, sacrificados y cada día más veloces… los ordenadores.

Pero todos saben la gran debilidad que tiene un sistema informático, que es hackeable. Entonces ¿cómo evita este problema Blockchain?

1.1.1 Funcionamiento de Blockchain

Blockchain no funciona con un poderoso antivirus o por un vigoroso firewall, Blockchain se autoprotege gracias a su propia estructura, su propia arquitectura.

Como ya se vio anteriormente, Blockchain significa “Cadena de Bloques”, viéndolo de forma gráfica se puede decir que son cajas que están unidas entre sí y esas cajas se componen de tres partes principales:

1.1.1.1 Partes de Blockchain

Una de las partes que conforman a Blockchain es la Información que son los datos que contendrá el bloque, en el caso de Bitcoin puede entrar lo que sería el emisor, receptor, fecha, cantidad, etc.

Otra parte que lo conforma es el Hash. El Hash es el número identificador del bloque, es una serie de dígitos que es único e irrepetible y cada bloque tiene el suyo propio.

Y finalmente, el Hash del bloque anterior, haciendo que cada bloque quede conectado con el bloque que le sigue formando una cadena, he aquí la razón de su nombre.

Viéndolo de una forma visual sería como en la *Ilustración 1*, donde dentro del bloque se encuentra la información y a los costados los Hash.

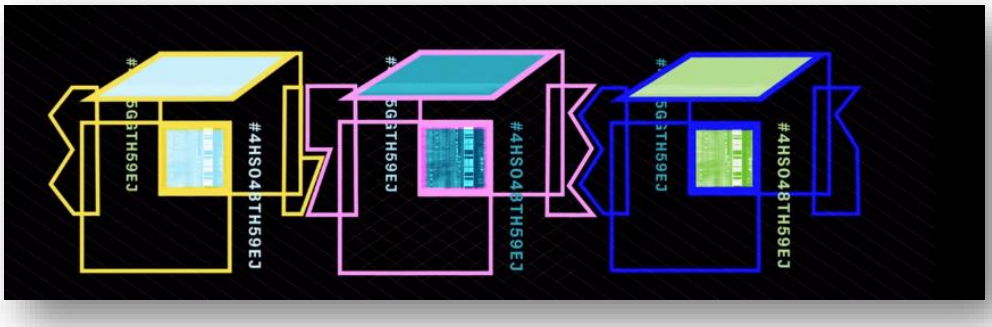


Ilustración 1 Cadena de bloques creado por canal de YouTube "PlayGround"

1.2 ¿Qué hace a Blockchain inhackeable?

Esto es gracias a principalmente 2 cosas, una de ellas es el Hash, y otra es que hay muchos ojos mirando todo el rato. Como ya se vio anteriormente, el Hash es el número único e irrepetible de cada bloque, pero este tiene la peculiaridad de que cambia según la información que tenga dentro. Esto quiere decir que si alguien trata de cambiar la información automáticamente cambiará también el Hash, lo que hará que ya no quede unido con su predecesor, haciendo que la cadena quede inválida. (*Ilustración 2*)

Ilustración 2 Incompatibilidad por modificación de la información

Y no es que haya solo una base de datos, cada usuario tiene una copia de ella y dado a que hay muchos ojos mirando si un usuario modifica la información la comunidad lo sabe, haciendo que su versión de la base de datos sea anulada. (*Ilustración 3*)

Ilustración 3 Anulación por manipulación de información

Eso es lo que hace Blockchain confiable, ya que la seguridad se la dan los mismos usuarios, no una empresa, ni una organización ni un banco, sino usuarios por igual, pero muchos.

Gracias a esta forma de trabajo, los programas o aplicaciones que utilizan como base a Blockchain se les dice que son apps descentralizadas.

1.3 ¿Cómo hace Blockchain para captar a sus usuarios?

Las personas pueden usar Blockchain por dos cosas, una es simplemente usar el sistema, otra es con un fin un poco más goloso, crear nuevos bloques para la cadena, aquí entran los llamados “Mineros”.

1.3.1 ¿Qué son los “Mineros” de Bitcoin?

Muchos usuarios de Blockchain no están ahí para usar el sistema, se concentran solamente en crear nuevos bloques. A medida que se va necesitando almacenar más información se requieren de nuevos bloques a la cadena.

1.3.2 ¿Cómo agregar nuevos bloques a la cadena?

Para añadir un nuevo bloque a la cadena se requiere resolver un problema matemático muy complejo que requiere de un gran poder de computación, aquí entra el PoW, así que los mineros ponen a toda máquina sus ordenadores para resolver el problema. Normalmente cada problema es resuelto en 10 min (Universidad de Buenos Aires. Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería, 2017). *(Ilustración 4, se puede observar de forma visual el añadir un nuevo bloque a la cadena).*

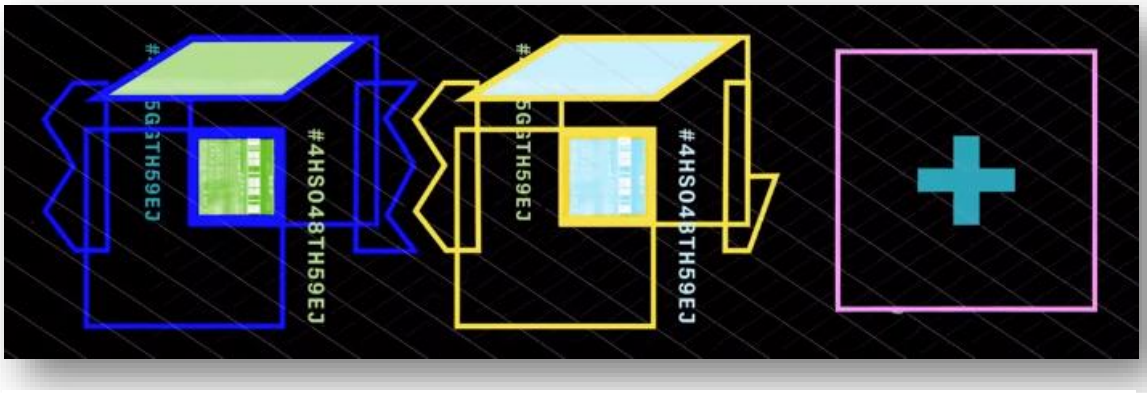


Ilustración 4 Agregar nuevo bloque a la cadena

Una vez que creen haber resuelto el problema, la comunidad se encarga de revisar el resultado obtenido, si es el correcto el nuevo bloque es agregado a la cadena, la información es consolidada y el acuerdo se lleva a cabo, y lo más importante, el usuario que resolvió el problema recibe una remuneración que es de aproximadamente 12.5 Bitcoins, lo que no está nada mal, dado que en estos días (26/Octubre/2022) un solo bitcoin vale aprox. $415,513.14 pesos mexicanos o poco más de $20,700 dólares estadounidenses (Coinbase, s.f.).

1.4 Ejemplos de aplicaciones de Blockchain

1.4.1 Sector médico

Una problemática que se ha presentado desde hace tiempo es en el apartado con respecto a los datos clínicos de las personas que, si bien están catalogadas como

confidenciales, ha habido ciertos conflictos por el acceso y el uso de esta información (Arellano Mejía & Sánchez Morales, 2017).

Solo el personal con una autorización puede obtener acceso a la información clínica de los pacientes, pero también se le puede dar autorización a otras personas para ingresar la información, y nada promete que alguien pueda modificar los datos que se encuentran ahí.

Blockchain puede guardar la información del expediente, que es la prueba de la relación médico-paciente que hay, al ingresar los datos se puede tener la seguridad que éstos ya no serán modificados.

1.4.2 Documentaciones

Al realizar el guardado de una documentación ya sea importante o no, se quedará seguro con Blockchain. Se podrán realizar respaldos de registros como firmas, registros de tiendas o supermercados, registrar compras realizadas, etc. En el tema del comercio además de que las transacciones o pagos serán seguros también lo será el registro de la compra.

Cualquier información que requiera una documentación será difícil que pueda ser falsificado.

1.4.3 Votaciones políticas

Después de las elecciones presidenciales de un país, tal vez los ciudadanos no estén satisfechos con la elección que se ha realizado, y no es para más, ya que probablemente la mayoría de las personas duden de sus gobernantes políticos, puesto que el humano es muy tentado por obtener un beneficio extra, aunque no sea de una forma éticamente correcta (Universidad Politécnica de Valéncia, 2017-2018).

Con Blockchain se podrá tener la seguridad de que las votaciones no han sido manipuladas, puesto que se tendrá la información del registro dentro de la cadena por lo tanto una vez ingresado no podrá ser modificado o eliminado, de esa forma el pueblo podrá estar más seguro de que el ganador de la candidatura fue de forma democrática.

1.4.4 Alimentos

Con Blockchain será difícil por no decir imposible la falsificación de la procedencia de alimentos, pues la información de los mismos estará en constante vigilancia y será fácil mantenerlos rastreados, para de esa forma, evitar el desvió del producto y verificar que todo esté en orden.

1.4.5 Firmas de contratos

Todos los días se necesitan realizar firmas de contratos, ya sea para contratar un servicio o en el caso de las empresas llegar a un acuerdo con otra organización, pero a veces pueden llegar a ocurrir ciertas situaciones por la falsificación de una firma, el riesgo que pueda haber confusiones o incluso acciones que puedan llegar a perjudicar a la empresa o al individuo que ofrece su firma para documentos.

Al aplicar Blockchain a este campo las firmas de contratos estarán seguras. La información resguardada y la seguridad del cliente intacta.

1.4.6 Educación

Así es, Blockchain también se puede aplicar en el sector educativo, esto gracias a que podría ampliar el historial académico de un alumno. Según Abraham Vázquez del Observatorio de Innovación Educativa del Tecnológico de Monterrey, señala que Blockchain podría romper barreras entre instituciones, esto quiere decir que ahora en lugar de que un título tuviera que ser validado de país en país, ahora simplemente se podría tener un único certificado digital (EDUTEC. Revista Electrónica de Tecnología Educativa., 2017).

1.5 ¿Qué es una aplicación descentralizada (DApps)?

Se le llama a la(s) aplicación(es) descentralizada(s) o DApps (Moto, 2018) a todas las aplicaciones que nacen basándose en Blockchain, quiere decir, que remueven la necesidad de un tercero cuando hablamos de intercambios entre una persona y un proveedor. En la Ilustración 5 se puede observar la diferencia entre el funcionamiento de una app en la cual se tiene un intermediario y al lado una forma visual de ver una app descentralizada

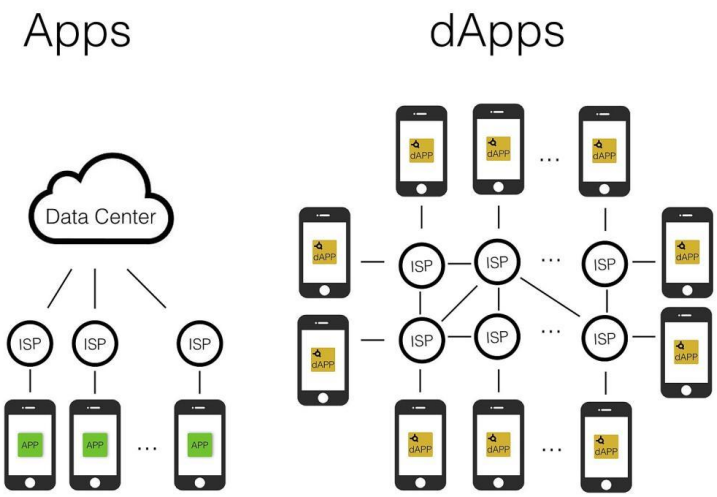


Ilustración 5 Ejemplo Apps Descentralizadas

1.5.1 ¿Qué es el protocolo Peer to Peer (P2P)?

El protocolo peer to peer (en español se le conoce como **red entre pares** o **red de igual a igual**) es un protocolo de red de comunicación que permite tener una relación directa entre usuario y servidor (Plata, 2019).

Permite una conexión entre nodos (ordenadores) que se comportan como iguales entre sí, esto quiere decir que pueden hacer función de cliente y servidor. Se conectan de forma directa sin la necesidad de intermediarios como servidores o controladores fijos, es decir, que se pueden compartir ficheros entre los demás usuarios que estén dentro de la red de forma directa, un ejemplo de ellos sería el Skype o el BitTorrent. En la *Ilustración 6* se puede observar de forma visual la diferencia que tiene una estructura P2P y una de cliente-servidor que es la que se utiliza normalmente.

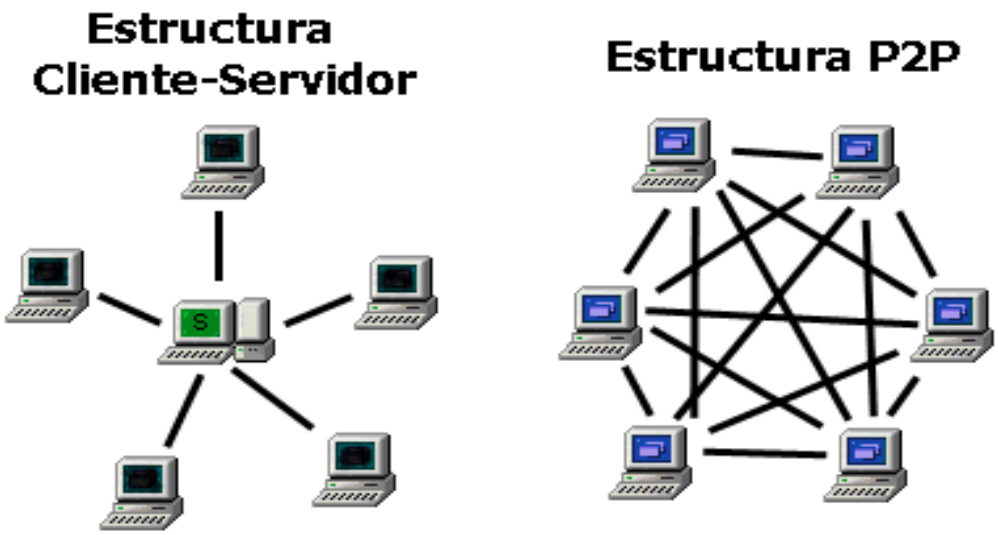


Ilustración 6 Comparación Estructura Cliente-Servidor y Estructura P2P

Aunque este protocolo no es muy seguro, ya que cada persona o usuario debe encargarse que no entre ningún tipo de virus a la red, puesto que al tener acceso de conectividad con otras computadoras éste puede infectar fácilmente a otra. Además, si otros ordenadores o nodos están conectándose a una para bajar o descargar algún archivo que se haya compartido, pueden bajar el rendimiento de ese ordenador de forma considerable (Sanz Romero, 2019).

Además de que esto ha traído problemas legales con las industrias del entretenimiento por la muy llamada piratería o la violación por derechos de autor, los usuarios pueden compartir el contenido de forma libre. Es el doble filo que tiene esta red, ya que dependiendo el uso que se le dé tendrá cierto efecto a un individuo.

Pero no todo es malo con este protocolo, por ejemplo, Spotify utilizó por un tiempo esta red, pero por el gran crecimiento que tuvo logró hacerse con suficientes servidores para abastecer a todos sus usuarios. Es una ventaja de P2P, si no se cuenta con demasiado dinero como para rentar un servidor ésta es una buena forma de empezar.

De hecho, actualmente las marcas de *Xiaomi, Oppo* y *Vivo* están utilizando este protocolo para crear una aplicación que permita compartir archivos entre dispositivos sin importar de que marca sean.

Por ejemplo, si una persona tiene un video normalmente para compartirlo lo subiría a YouTube, pero en la red P2P si otra persona quiere tener ese video se lo pediría directamente al creador de ese contenido. Al mismo tiempo, esa persona al ya tener ese video lo puede compartir con otra que se lo pida, y ahora todo aquel que tenga ese video también lo puede compartir con otras personas.

1.5.2 ¿Qué es el protocolo PoW (Proof of Work)?

El protocolo de prueba de trabajo o PoW por sus siglas en ingles es un protocolo que consiste en que partes de una red realicen de forma exitosa un trabajo que requiera de mucha potencia computacional para poder tener acceso a los recursos de dicha red. *(En la Ilustración 7 se muestra una imagen ilustrativa de PoW).*

Ilustración 7 Imagen ilustrativa de Proof of Work

Este protocolo funciona a que le asignan una tarea a un usuario que luego es verificado por la red. Normalmente las tareas son problemas matemáticos complejos para que realice la computadora. Podemos poner de ejemplo a la famosa *Captcha,* la cual para poder ingresar al servicio de la red se debe pasar por una serie de pruebas en este caso sencillas para que sean resueltas, de esta manera se evita que un atacante pueda crear millones de registros y de esa manera colapsar la página web (Bit2Me, Academy by Bit2me, s.f.).

Pero cuando es comunicación entre ordenadores el problema no debe ser tan complejo, debe poder resolverse, pero con una dificultad relativa.

Lo peculiar de PoW es que su sistema es asimétrico, es decir, que por la parte del cliente el problema a resolver será algo complicado de realizar, pero la verificación por parte de la red será sencilla. Esto quiere decir que el problema lleva mucho tiempo en resolverse y es costoso hablando de recursos, pero al generarse el problema, también genera una serie de patrones que facilitan la verificación.

1.5.3 ¿Qué es el HashCash?

El HashCash es una solución que se propuso contra los mensajes basura o también conocidos como Spam. Se basa en el protocolo PoW para verificar si un correo es basura o no (Bit2Me, Academy by Bit2me, s.f.).

El objetivo de HashCash es requerir un trabajo de computación para que este sea verificado, una vez verificado, al usuario se le da luz verde para utilizar dicho servicio. El usuario ingresa un encabezado al correo mediante HashCash, de esta forma se crea como una especie de “sello” que asegura que el correo ha pasado por una prueba de trabajo.

El sello es un identificador que demuestra o comprueba que el procesador ha utilizado el procesador por una pequeña cantidad de tiempo, pues es lo que genera un sello genuino para cada correo que se va a enviar.

Y, ¿cómo ayuda esto a evitar al spammer?

Como se mencionó anteriormente, se necesita un pequeño consumo extra en el procesador para crear el “sello”. Para un usuario que manda unos cuantos correos no será

ningún problema, ya que el consumo energético del procesador no será tan exagerado como para incrementar demasiado la factura de luz.

Pero para el spammer no es así, dado que al enviar tantos correos hace que el procesador tenga que trabajar más para poder enviar esos correos, lo que conlleva a que se necesite de más energía, por lo que la factura del spammer le llegará más elevado por el alto consumo energético del procesador.

Esto es lo que hace que disminuya la probabilidad de que el spammer envíe sus correos basura a las bandejas de entrada de los usuarios.

1.5.4 ¿Qué es un token?

Un token es un objeto que solo tiene valor dentro de cierto contexto. Por ejemplo, una moneda de casino, esos pedazos de plásticos que fuera del establecimiento no tienen ningún valor aparente, pero dentro del casino representan cierta cantidad de dinero para facilitar el conteo o la manipulación al momento de jugar (Ripio Blog, 2018).

Y esta es la función principal de los tokens, representar algo más. En el mundo de las criptomonedas se intercambia hacen transferencias con tokens que representarían en este caso la moneda de dicho sistema de transacción.

Pero los tokens se pueden usar para otras cosas, ya que además de representar algo económico, también pueden representar alguna recompensa o ser simplemente objetos coleccionables. Las empresas pueden emplear los tokens para representar las acciones que tiene dicha empresa.

1.5.5 ¿Qué es hedonismo?

El hedonismo o ser hedonista se refiere a que se busca un placer o un bien, enfocado más a uno mismo, es decir, que se busca un beneficio propio (Wikipedia, s.f.).

CAPÍTULO II. TRANSPARENCIA ELECTORAL

2.1 El proceso electoral

El proceso electoral es un proceso democrático donde se busca escuchar la voz de los ciudadanos, así como su opinión respecto a los temas gubernamentales, siendo más específicos en el proceso de elección de los integrantes que representan los poderes legislativos y ejecutivos del país.

La democracia busca dar al país soberanía por, sobre todo, donde el pueblo tengo el derecho a elegir a sus representantes, así como participar activamente en los procesos gubernamentales donde la elección de representantes esté presente.

2.1.1 ¿Qué es un proceso electoral?

El proceso electoral se refiere al conjunto de acciones realizadas por partes en el que la Ley General de las Instituciones y Procedimientos Electorales y la Constitución mandan a los partidos políticos, las autoridades electorales y los ciudadanos votantes para renovar a los representantes de los poderes legislativos y ejecutivo federal, así como de las entidades federativas. (*Ilustración 8*)

Ilustración 8 Conteo de votos de una elección electoral.

El proceso electoral está organizado por un conjunto de reglas que dictan el procedimiento a seguir para llevar a cabo la elección, dicho proceso consta de la participación de los ciudadanos para realizar su voto, una vez terminado el periodo de votación, los votos se contabilizan y en base a los resultados arrojados por el proceso electoral se selecciona a los escaños (Integrante de la cámara de diputados o la cámara de senadores) en caso de los miembros del poder legislativo o a los cargos de gobierno en caso del poder ejecutivo.

2.2 Etapas del proceso electoral

El proceso electoral ordinario se compone de las siguientes etapas:

1. **Preparación de la elección.**

Inicia con la primera sesión que el Consejo General del INE celebre durante la primera semana de septiembre del año previo en que deban realizarse las elecciones federales ordinarias y concluye al iniciarse la jornada electoral. (UNAM, 2018)

2. **Jornada Electoral.**

Inicia a las 8:00 horas del primer domingo de junio y concluye con la clausura de casilla, excepto en 2018, cuando las elecciones tendrán verificativo el primer domingo de julio. (UNAM, 2018)

3. **Resultados y declaraciones de validez de las elecciones**

Inicia con la remisión de la documentación y expedientes electorales a los consejos distritales y concluye con los cómputos y declaraciones que realicen los consejos del Instituto, o las resoluciones que, en su caso, emita en última instancia el Tribunal Electoral. (UNAM, 2018)

4. **Dictamen y declaraciones de validez de la elección**

Inicia al resolverse el último de los medios de impugnación que se hubiesen interpuesto en contra de esta elección o cuando se tenga constancia de que no se presentó ninguno y concluye al aprobar la Sala Superior del Tribunal Electoral el dictamen que contenga el cómputo final y las declaraciones de validez de la elección y de presidente electo. (UNAM, 2018)

Ilustración 9 Proceso electoral

Durante el tiempo de duración del proceso electoral, tienen participación varios actores, cada uno desarrolla su papel como es debido para intentar llevar a cabo un proceso electoral sin ningún percance o algún insulto hacía la patria al manipular dicho proceso:

- Autoridades Selectorales.

  Dentro de las autoridades electorales participantes en el proceso electoral tenemos al Instituto Nacional Electoral (INE), Organismos Públicos Locales Electorales, Fiscalía Especializada para la Atención de Delitos Electorales (FEPADE), Tribunal Electoral del Poder Judicial de la Federación, Autoridades Electorales jurisdiccionales locales.
- Partidos políticos
- Los Ciudadanos y las Ciudadanas

  Tanto partidos políticos nacionales como partidos políticos Locales.
- Los Ciudadanos y las Ciudadanas

  Se refiere a los ciudadanos electores, funcionarios de mesa directiva de casilla, observadores electorales y candidatos independientes.

2.3 El Sistema Electoral en México

El sistema electoral de México, donde se elige a los representantes del país, a los lideres que cargarán con el nombre del país.

El sistema electoral de México se basa en un sistema democrático donde la voz de la gente es la que dicta quien será quien tome las riendas de este país. México divide su gobierno en 3 ramas principales, también llamados poderes, el poder Legislativo, el poder Ejecutivo y el poder Judicial.

- Poder Legislativo

  Este poder es depositado en el Congreso de la Unión, este se divide en 2 Cámaras, la Cámara de Diputados y la Cámara de Senadores, estos se encargan de expedir las leyes que regulan la estructura y el funcionamiento internos de la República Mexicana.

  La Cámara de Diputados está conformada por 500 Diputados, de los cuales 300 de sus miembros son elegidos por medio de la elección por mayoría relativa, es decir por los votos de los ciudadanos, mientras los restante 200 se eligen por la representación proporcional, es decir que aunque no hayan alcanzado la cifra de votos para ganar la elección, es posible entrar a la cámara de diputados, esto se hace con el fin de que las minorías políticas no sean relegadas y todos tengas voz dentro de la Cámara de Diputados

  La Cámara de Senadores está conformada por 128 miembros de los cuales cada estado que conforma la República Mexicana elige 2 por medio de la elección por mayoría relativa y uno por representación proporcional, este último se elige en base a quien quedó en segundo lugar en cantidad de votos, los restantes 32 miembros son elegidos mediante el principio de representación proporcional mediante el sistema de listas votadas en una sola circunscripción plurinominal nacional.

  Con esto se refiere que es un “Área geográfica integrada por un grupo de entidades federativas, que sirve de base para la elección de los 200 diputados y 32 senadores electos por el principio de representación proporcional.” (Secretaría de Relaciones Exteriores, 2021)

- Poder Ejecutivo

El poder Ejecutivo gobierna en conformidad con lo establecido en la legislación, su representante, el Presidente Constitucional de los Estados Unidos Mexicanos, es elegido por medio de la elección directa, este gobierna durante un periodo de 6 años sin posibilidad a reelección.

Para ejecutar sus labores, el presidente tiene el poder para nombrar a sus colaboradores más cercanos, los Secretarios de Estado y el Procurador General de la República.

- Poder Judicial

El poder Judicial de la federación se encarga de vigilar el cumplimiento de la Constitución y las Leyes, preserva que la Constitución sea la Ley Suprema y que no haya ninguna Ley o norma que la contradiga.

La suprema Corte de Justicia de la Nación es el máximo tribunal de México y se encarga de resolver las controversias entre la Federación y las entidades federativas. El poder Judicial está conformado por:

- La Suprema Corte de Justicia de la Nación
- El Tribunal Electoral
- Los Tribunales Colegiados y Unitarios, y los Juzgados de Distrito.

2.3.1 Una definición de Sistemas electorales

Un sistema Electoral, un conjunto de medio por el cuál la voluntad de aquellos que residen en el país se transforma en órganos de gobierno o de representación política, el sistema electoral recibe los votos de los ciudadanos y por medio del conteo de dichos votos, da a conocer la voluntad de la gente, dicha voluntad dicta quien estará representando al país.

En resumen, se puede decir que el sistema electoral se puede definir como el conjunto de reglas y normas que regulan las elecciones de un país, su propósito es definir las reglas mediante las cuales los electores pueden hacer valer su voto en favor de determinados partidos o candidato.

De acuerdo con Dieter Nohlen, los Sistemas Electorales se refiere “Al principio de representación, que subyace al procedimiento técnico de elección, y al procedimiento

mismo por medio del cual los electores expresan su voluntad política en votos que a su vez se convierten en escaños o poder público".

2.3.2 Efectos de los Sistemas Electorales

- Los sistemas electorales son importantes en la vida democrática del país, ya que por medio de estos se coloca al lector frente a la posibilidad de elegir entre las diversas opciones de candidatos y de partidos políticos.
- El Sistema Electora se encarga de traducir la voluntad del pueblo transmitida por medio de votos a favor de quien consideren mejor para el trabajo y transformarlo en puestos legislativos y ejecutivos.

El sistema electoral permite que el pueblo tenga cierto control sobre el país, ya que deja que los mismos ciudadanos sean los que eligen el rumbo que el país tomará dando la libertad de elección a aquellos que conforman la parte más importante de un país, la gente.

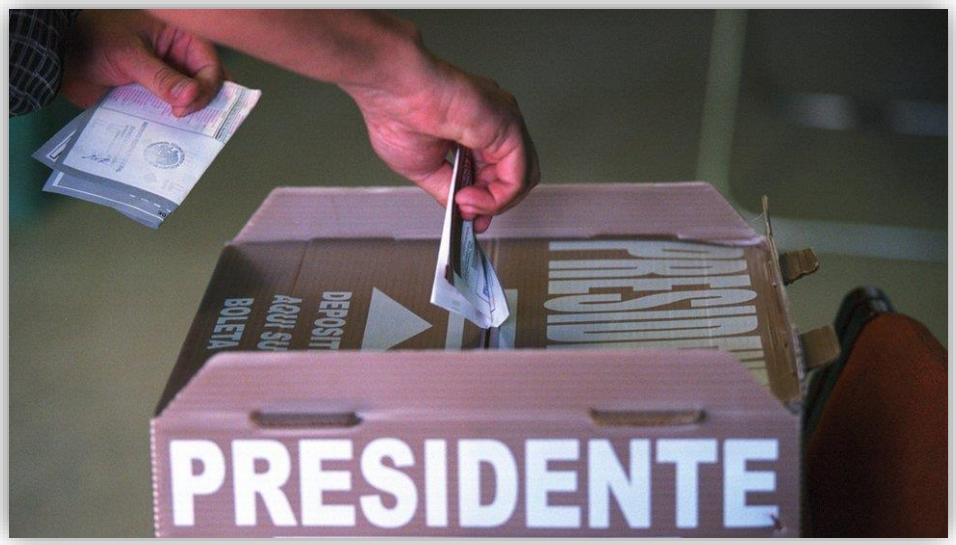


Ilustración 10 Elecciones presidenciales

2.3.3 El Sistema Electoral perfecto… ¿existe?

Existen algunos sistemas electorales, cada uno surge como intento de obtener el sistema electoral perfecto.

- **Sistema Electoral por Mayoría**
  - Eligen a una mayoría gobernante.

    Este argumento está severamente condicionado, pues no siempre se cuenta con un sistema bipartidista.
  - Reduce la fragmentación de partidos.

    Regido por la premisa “El ganador se queda con todo” no reduce por completo al formato bipartidista, pero si lo comprime y lo mantiene su número en niveles relativamente bajos.
  - Crea una relación directa entre electores y representantes.

    Una afirmación un tanto dudosa dado a que cualquier afirmación de una relación directa debe de tomar en cuenta el número de votantes.
  - Mejora la calidad de los funcionarios elegidos.

    La calidad es algo difícil de medir, lo que se toma como punto negativo. El tener personas buenas en el gobierno no es, por completo, la cura a un mal gobierno.

- **Sistema de Representación Proporcional**

  Este sistema tiene un mérito indiscutible, la equidad de la representación, mas, sin embargo, así como su mérito indiscutible, también tiene una crítica severa.

  No evita o disminuye la fragmentación de los partidos políticos, esto derivando en una fragmentación extrema dando como resultado una gobernatura muy pobre donde los gobiernos heterogéneos dificultan la toma de decisiones.

- **La Segunda Ronda Electoral**

  Este tercer modelo, contempla una segunda ronda de votación, su funcionalidad se basa en que la primera votación el ciudadano vote por su candidato favorito, esto es llamado “Voto Emocional”. En la segunda votación, donde se elige a un candidato de forma racional y donde se elige de manera efectiva quien desea que lo gobierne.

Dadas las diferencias entre los países, tanto culturales, sociales, históricos, etc. No hay forma de establecer un sistema electoral “perfecto” que funcione en todas las situaciones.

Así como cada país tiene diferentes necesidades, esto conlleva a una reflexión lógica sobre que podría mejorar el sistema electoral de cada país, y como todo en el mundo, los

modelos de sistemas electorales tiene fallas, por lo que siempre será posible aprovecharse de dichas fallas y esto puede llegar a tener grandes consecuencias, dado a esto, es imposible establecer un solo sistema electoral para todo el mundo, ya que cada uno tiene que aplicar y moldear el sistema electoral que más ventajas tenga dada las condiciones a las que se está sometiendo.

Los sistemas electorales son una forma de mantener a la gente en contacto con las grandes decisiones que están por llevar al país por lo grande o en caso contrario, llevarlo, ya sea lentamente o de manera súbita, a su perdición, dado a que no es un sistema perfecto, es posible aprovecharse de sus fallas con el objetivo del bien común, esto a conllevado a que los propios ciudadanos desconfíen sobre si el proceso electoral es llevado como es debido.

2.4 El Voto Electrónico

Con la globalización de la tecnología, se ha marcado un cambio en la evolución económica, política, social y cultural de la sociedad. Con esta expansión tecnológica se comienza a implementar la tecnología en muchos campos, en el campo político se implementa la idea del voto electrónico, sin embargo, este no es una idea que haya surgido de manera relativamente reciente, se tienen antecedentes que se remontan a tiempo mucho antes de la expansión tecnológica, dichos antecedentes se remontan a 1869, año en el que se registró la patente para la primera máquina diseñada para recibir algún tipo de votación.

En México, los antecedentes datan de 1911 y 1918 con la “Ley Madero” y la “Ley Carranza” respectivamente, en donde se preveía el uso de máquinas para sufragar, sin embargo, dicho pensamiento desapareció con el tiempo, pero gracias a globalización tecnológica dicha idea resurgió no solo como forma de evitar situaciones maliciosas durante las elecciones, sino como una forma de mejorar dicho sistema.

La implementación de voto, según el doctor Julio Téllez Valdés, exige 3 condiciones que son necesarias aplicar si se quiere hacer funcionar este nuevo método de votación:

- Un nivel adecuado de aceptación social frente a las nuevas tecnologías aplicadas en el ámbito electoral.

- Una factibilidad técnica que colme los requisitos constitucionales y legales en el ejercicio del sufragio público.
- Un atractivo político para los diversos actores en un contexto democrático.

Si bien realizar un cambio ante una costumbre tan arraigada y que “ha funcionado bien” será una tarea difícil, principalmente porque los humanos somo seres de costumbres, buscamos una estabilidad donde conocemos el resultado y si este no parece tan malo, estaremos más predispuestos a volverlo a elegir por encima de la incertidumbre de elegir algo nuevo sin saber cómo este irá a resultar.

Después de todo el ser humano teme al fracaso más que cualquier otro ser, pero aun con todo eso es necesario seguir avanzando y probar cosas nuevas, si bien parece que el país está dispuesto a buscar este cambio, todavía falta que las personas acepten dicho cambio y los vuelvan una nueva costumbre para poder confiar en el nuevo sistema plenamente.

2.4.1 Concepto de voto electrónico

Voto electrónico es una de las denominaciones dadas a este concepto, hay más de 15 denominaciones que están aceptadas dentro del concepto, entre ellas destacan:

- Voto Electrónico
- Voto Informático
- Voto Informatizado
- Voto Telemático
- Tecnovoto
- E-vote
- E-poll
- Voto automatizado
- Etc.

Sin embargo, la denominación de Voto Electrónico es la que está mayormente aceptada y empleada a la hora de referirnos a este concepto, se podría definir al voto electrónico de las siguientes maneras:

- “El voto electrónico en sentido amplio, es todo mecanismo de elección en el que se utilicen los medios electrónicos, o cualquier tecnología, en las distintas etapas del proceso electoral, teniendo como presupuesto básico que el acto efectivo de votar se realice mediante cualquier instrumento electrónico de captación del sufragio”. (Télles Valdés, 2010)
- “En sentido estricto, el voto electrónico es el acto preciso en el cual el emitente del voto deposita o expresa su voluntad a través de medios electrónicos (urnas electrónicas) o cualquier otra tecnología de recepción del sufragio”. (Télles Valdés, 2010)

Estos conceptos encierran la idea de que la voluntad del elector sea manifestada mediante la emisión del voto por medios electrónicos, según la recopilación de María de la Luz Domínguez Campos, otro concepto sería:

- “Todos los actos electorales factibles deben ser llevados a cabo apelando a la tecnología de la información”. (Télles Valdés, 2010)

2.4.2 Características del Voto Electrónico

Según la recopilación Domínguez Campos el voto electrónico debe tener las siguientes características:

1. **Autentico.** Solo los votantes autorizados pueden votar.
2. **Accesibilidad.** Permite que personas con diversidad funcional o discapacitadas puedan ejercer el voto sin problema alguno.
3. **Anónimo.** No se puede relacionar al votante con el voto que este ha emitido, este es un requisito especialmente importante, ya que puede aparecer en todos los escenarios posibles. Para este requisito es importante tener en cuenta que, al usar un equipo tecnológico capaz de realizar votaciones, se debe validar la identidad de la persona para admitir un voto, lo que conlleva a que se deje un rastro que puede ser rastreado y dar con el votante que emitió dicho voto, una forma de eliminar la posibilidad de rastreo por parte de algún tercero, es por medio de mecanismos criptográficos avanzados basados en firmas ciegas, secreto dividido, etc.

4. **Certificable o Auditable.** Las soluciones tecnológicas, así como el hardware y software usado deben ser abiertas e íntegramente auditables, es decir que sea capaz de darle una revisión cuidadosa ante, durante y después del proceso electoral.
5. **Comprobable.** Se debe ser capaz de comprobar los sistemas por parte de las autoridades electorales, con el objetivo de constatar que cumple con los criterios establecidos.
6. **Código abierto.** Para que tanto las autoridades como los ciudadanos generales puedan obtener los detalles del funcionamiento del sistema.
7. **Costo reducido.** Al utilizar las TICs se espera reducir los costos de realizar el proceso electoral, ya que este es caro de realizar de la manera tradicional.
8. **Confiabilidad.** Debe tener la seguridad de que el sistema no tendrá pérdida de votos y que trabaje de manera segura incluso durante una situación extrema.
9. **El sistema debe de ser robusto.** Sin pérdida de votos, sin fallas en el sistema, tanto en máquinas servidores como en la comunicación a través de internet.
10. **Compatibilidad con mecanismos de votación convencionales.** Que sea compatible con la tradición electoral, que tenga el mayor parecido con la urna convencional en aspecto y uso.
11. **Comprensible para el votante.** Que el votante no tenga ningún problema a la hora de realizar la votación. El sistema debe ser los más intuitivo posible, ya que no todos los ciudadanos generales tienen conocimientos en el campo de la informática.
12. **Fácil uso.** Si bien no es necesario que tengan conocimientos informáticos avanzados, tampoco queremos agobiarlos con un sistema tediosos de usar, mantener el sistema lo más simple posible es la mejor opción.
13. **Fiabilidad.** El principal objetivo del cambio del proceso electoral tradicional por el voto electrónico es evitar la alteración fraudulenta de los resultados de la votación, por lo que este es un punto a tener en cuenta, ya que buscamos mitigar y de ser posible eliminar completamente los intentos de alteración fraudulenta.
14. **Veracidad de la votación.** Si se descubre algún defecto en los resultados, el sistema debe tener mecanismos para probar el fraude.
15. **Imposibilidad de Coacción.** Ningún votante debe ser capaz de demostrar que voto a emitido. De esta forma se impide la compra masiva de votos y la presión sobre los votantes.

16. **Imparcialidad.** El voto emitido deberá permanecer en secreto, así la decisión de los votantes no se verá influenciada por la “filtración” de resultados parciales
17. **Movilidad de los votantes.** Permite que los ciudadanos con los requisitos y la facultad para sufragar, puedan hacerlo desde cualquier lugar del mundo con sus respectivas claves de seguridad.
18. **Verificación Individual.** Cada votante deberá tener la seguridad de que su voto será tomado en cuenta, para esto se debe dar prueba del voto, pero esto puede llegar a contradecir la **Imposibilidad de Coacción** al revelar que se ha emitido un voto, por lo que se debe buscar una forma de constatar que se ha votado sin hacerlo demasiado explicito.
19. **Voto Rápido.** El proceso electoral por medio de voto electrónico debe ser más rápido y ágil que el método tradicional.
20. **Unicidad del Voto.** Asegurarse que solo se pueda votar una vez y que dicho voto no pueda modificarse.

2.5 Cómo ‘Blockchain’ puede cambiar la forma en que votamos

La transformación digital es imparable. Procesos de todo tipo están migrando a ecosistemas digitales para ser más efectivos. Los procesos electorales ya se han fijado en nuevas tecnologías como el 'Blockchain' para hacer más transparente la forma en la que votamos. (Fernández Espinosa, 2019)

Las votaciones han evolucionado mucho, en el pasado lejano, las votaciones solían ser en grupos pequeños y se hacían en base a alguna señal, como alzar la mano, con el tiempo esto ha ido evolucionando, se ha requerido que una gran cantidad de personas tengan participación en una votación, para ellos se han creado distintos tipos de técnicas para llevar a cabo dicho proceso lo más neutral e imparcial posible.

La evolución de las técnicas de votación nos ha llevado a donde estamos hoy en día, las votaciones tradicionales fueron el pináculo de las técnicas de votación por un tiempo, pero esto está llegando a su fin, la era tecnológica está apoderándose de cada vez más sectores y el sector político está cada vez más automatizado.

La automatización de las votaciones se ha tenido en la mira desde hace bastante tiempo, pero existía el problema de que la tecnología existente no podía cumplir con los

requisitos para llevar a cabo de manera exitosa una votación con voto electrónico (*Ilustración 11*), por esa razón no se había implementado, al menos no de manera extendida, eso es hasta que llegó Blockchain.

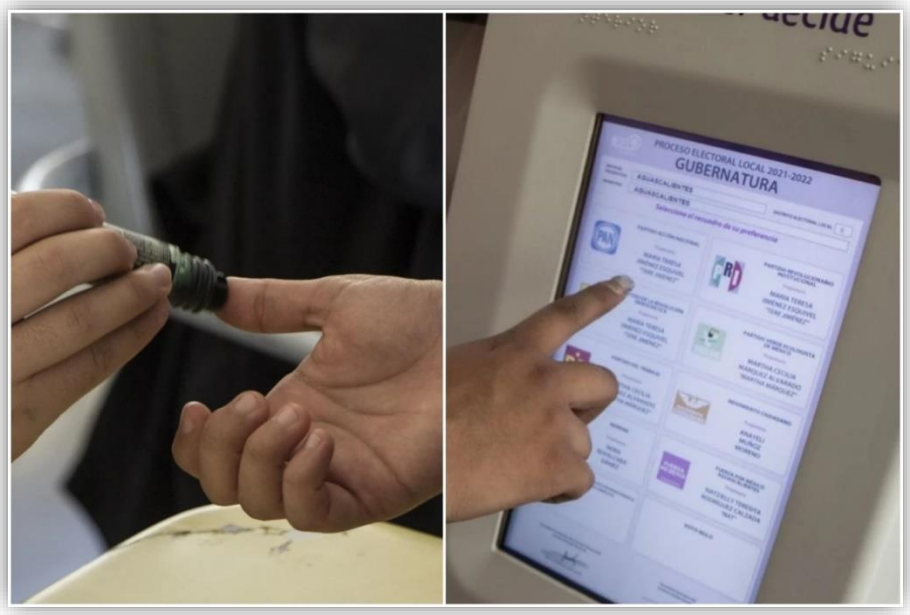


Ilustración 11 Votaciones electrónicas

Gracias a la tecnología de la cadena de bloques se pueden mejorar procesos públicos en los que la intervención humana es decisiva. “Al usar ‘Blockchain’, cualquier documento queda registrado y es inmutable. Es ideal a la hora de realizar contratación pública, registro de propiedad de tierras o seguimiento de recursos públicos. También en los procesos electorales, porque ayudaría a generar confianza entre los ciudadanos”, señala Mauricio Tovar, director de la Fundación Blockchain Colombia y responsable de un proyecto piloto de elecciones estudiantiles en Bogotá con ‘Blockchain’. (Fernández Espinosa, 2019)

Dado a que la tecnología de Blockchain utiliza herramientas criptográficas para asegurar la seguridad de los datos que maneja, solo el destinatario y el remitente conocen el contenido de la operación en una red totalmente descentralizada.

Algunos de los beneficios que Blockchain provee son:

- **La validez de los resultados.** Los resultados de la votación no pueden ser falsificados, en cualquier momento se puede verificar cuántos votos se emitieron al comienzo de la votación y cuantos se contabilizan en el recuento. Todos los votos, ya sean válidos o en blanco, se conocen al momento de hacer el recuento.
- **Transparencia en el proceso.** Blockchain brinda la oportunidad de controlar el proceso e incluso permite saber cuándo el voto ha sido emitido y contabilizado, ingresando a la plataforma habilitada con sus claves.
- **Privacidad y Anonimato.** Dado a que la votación con Blockchain contaría como una herramienta descentralizada, nadie salvo el propio ciudadano sabrá que ha votado, desde dónde o cuando lo ha hecho.
- **Velocidad en el recuento.** El conteo de votos se hará de manera automática gracias a la descentralización de Blockchain, esto sin tomar en cuenta si los votos se emitieron de manera nacional, provincial o por ciudad.
- **Ahorro de costes y personal.** Como todo cambio hacia la automatización esto ahorrará en costes y dado a que el proceso se principalmente automático, el personal necesario para llevar a cabo las votaciones será mucho menor.

La tecnología de Blockchain en el tema del proceso electoral ha permitido reunir los requisitos necesarios para implementar un sistema automatizado funcional de las votaciones, agilizando el proceso y ahorrando en gastos, la tecnología de Blockchain tiene todo lo que se necesita, el voto será anónimo ya que la descentralización de Blockchain no permite que terceros conozcan ni un detalle sobre la operación en cuestión, dado a la naturaleza de esta tecnología es imposible suplantar tu identidad.

2.6 Desafíos estratégicos de la tecnología Blockchain en procesos electorales

Si bien la tecnología Blockchain puede ser un gran coste de implementación, esto puede contar como una inversión, donde a largo plazo llegará a ser beneficiosa tanto en materia económica como en otros sectores, si se sigue adelante con el desarrollo de la

Blockchain, es posible ayudar a la trasparencia no solo de las votaciones sino de las transacciones gubernamentales.

En tema de los procesos electorales, la tecnología Blockchain supondría un gran salto de los procesos electorales actuales, siendo que los procesos actuales, tanto tradicionales como aquellos que se han automatizado con métodos tecnológicos convencionales han fallado en arreglar los errores básicos de los procesos electorales físicos, siendo un gran ejemplo los hackeos que sufrieron tanto Rusia como Colombia, ambos usando un sistema de voto electrónico convencional

Sufrieron un gran ataque de hackeos, la cantidad de hackeos podía ser contada en miles, lo que supuso un gran problema, ya que se pudo perforar los sistemas de seguridad de un proceso tan importante como lo es una votación de este calibre, la tecnología de Blockchain supone una solución a este problema, no solo se ha probado inhackeable hasta el momento, sino que supone algunas otras ventajas.

Con Blockchain la identidad de los votantes está protegida al mismo nivel que las operaciones realizadas en la misma, lo que hace casi imposible rastrear tanto una transacción como los involucrados en dicha transacción, aunado a esto, imposibilita la falsificación de la identidad, así como la identidad está protegida para no ser rastreada, esta es igualmente infalsificable, asegurando que la votaciones sean lo más honestas posibles, una vez hecha la votación, esta será completamente inamovible.

La Blockchain ha introducido un nuevo mundo al sistema electoral, siendo que sus beneficios no se limitan simplemente a este sector, esta tecnología podría ser la llave que lleve la democracia a un nuevo nivel, un nivel más objetivo y con menos posibilidad de errores, esto supondría un punto que hasta ahora era inalcanzable e inaudito en el mundo físico.

2.7 Transparencia electoral. La receta para la credibilidad

Con el pasar de los años, los procesos electorales han perdido mucha credibilidad principalmente debido a la vulnerabilidad de los métodos de votación existentes hasta la fecha, siendo que la votación física sufría de falsificaciones de papel, suplantaciones de

identidad, compra de votos, etc. Lo que hacía que fuera muy poco fiable y dado a todos los casos que se han vistos de esto pasando.

Los votos electrónicos tampoco eran la excepción, dado a que la implementación del voto electrónico se realizó con tecnología convencional, por llamarla de algún modo, esta pecó de ingenua ante la vulnerabilidad de los ataques de hacking, siendo que en durante su implementación en el año 2018 en las elecciones tanto de Colombia como de Rusia los ataques cibernéticos que sufrieron ambos países fueron tan masivo que los ataque se contabilizaban por miles

Dichos ataques lograron penetrar los sistemas de seguridad, atrasando el proceso de voto y conteo, así como borrando datos del proceso electoral, esto aunado a que no se había encontrado una forma de evitar las vulnerabilidades naturales de cada sistema electoral, ha provocado que la confianza en los procesos electorales vaya en decremento.

La transparencia se ha vuelto fundamental para el buen desarrollo del proceso electoral, este permite una gestión eficiente y abona a la credibilidad del proceso y a la legitimidad del resultado. Dada la falta de transparencia, ha habido casos donde el proceso electoral terminó en crisis política e incluso en violencia, solo porque el proceso electoral no tuvo plena transparencia.

Un gran ejemplo de lo importante que es la transparencia, las elecciones generales de Kenia en 2007, problemas y retrasos con el conteo de votos y la transmisión de resultados provocaron protestas y violencias que culminaron en la desafortunada muerte de 1,000 personas, así como el desplazamiento de aproximadamente 500,000 personas.

Gracias a la transparencia, se puede identificar irregularidades en los procesos electorales, informar sobre la mala conducta de funcionarios y evidenciar posibles prácticas fraudulentas. La transparencia no solo sirve para evidenciar las fallas de los organismos gubernamentales, sino que también funge como mecanismo para justificar, fundamentar y defender a dichos organismos gubernamentales, así como su personal y sus actividades de acusaciones sin fundamentos y percepciones de fraudes.

Así mismo, la transparencia se convierte en un pilar que ayuda a mejorar la percepción de la ciudadanía sobre la integridad de los procesos electorales, dando como resultado que la ciudadanía tenga más confianza en las elecciones.

La transparencia puede sonar un tanto ambiguo, y si no conoces el concepto puede sonar muy abstracto, la transparencia basa su utilidad en 2 condiciones clave, para que un proceso sea transparente, los datos que este genere deben ser visibles e inferibles, es decir, que la información pueda traducirse y expresarse en mecanismos que le den visibilidad y claridad o que la hagan inferible o entendible.

Ahora, como podemos aplicar la transparencia en el proceso electoral sin poner en riesgo la información de los votantes, para eso hay que tomar en cuenta las divisiones del proceso electoral: el periodo preelectoral, periodo electoral y el periodo post-electoral. Cada una de esas divisiones cuenta con fases, para poder aplicar la transparencia en el proceso electoral hay que ver que partes no comprometen información delicada, por ejemplo: diseño y planeación del presupuesto, calendario electoral, capacitación del personal y la actualización del registro de votación. Esto en el periodo preelectoral.

En el periodo electoral podemos transparentar las actividades: fases de campaña, nominación, votación, resultados, postulación de candidatos, desarrollo de la votación, acreditación de observadores electorales, escrutinio de los votos, declaración y publicación de los resultados.

CAPITULO III: CONTRATOS INTELIGENTES

3.1 Definición

Un contrato inteligente es un programa que se almacena en una cadena de bloques, dicho programa se ejecuta automáticamente al momento de cumplirse con alguna de las condiciones con las cuales fue programada, los contratos inteligentes se utilizan con el objetivo de automatizar un acuerdo previamente acordado, de esta forma los participantes puedan estar seguros de que una vez se cumplan las condiciones estipuladas en el contrato este se ejecutara y dará un resultado sin la participación de ningún intermediario así como tener que esperar a que se haga deliberación del resultado, ya que este será de inmediato y solamente entre los participantes del contrato.

El criptólogo Nick Szabo fue el primero en hablar sobre la idea de los contratos inteligentes, dando su primer vistazo a este concepto en una página web llamada Smart Contract Glossary en 1995, un año después profundizaría sobre este concepto en su trabajo Smart Contracts for Digital Marketing donde comenzó a ver la posibilidad de aplicar los contratos inteligentes en las transacciones económicas eliminando los intermediarios, aunque no sería hasta el año 2013 donde su idea finalmente se concretaría.

Con la creación de Etherium, los contratos inteligentes finalmente tendrían un uso concreto, comenzando a volverse más famosos y así llegando a ser lo que Nick Szabo había pensado 18 años antes.

En un contrato inteligente los ordenadores juegan un importante rol, no se trata de simplemente guardar un documento digital o admitir la firma electrónica, los contratos inteligentes van más allá, según explica Javier Sebastian, responsable de Regulación Digital de DLT de BBVA research, “estos programas realizan análisis y ejecutan alguna de las partes de su lógica interna” (Fernández Espinosa, 2019), Dando a entender que el ordenador será el encargado de ejecutar aquellos estipulado en el contrato, y por la propia naturaleza del ordenador, está será hecha desde el punto más objetivo posible.

3.2 Funcionalidad

La funcionalidad de un contrato inteligente es relativamente simple, se trata de un “si/cuando… entonces…” básicamente una condición para que se active alguna acción, un tema muy común cuando se trata de programación, ya que este es el pan de cada día para los programadores, estas declaraciones están escritas en código en una cadena de bloques.

Dada la naturaleza del Blockchain, es en una red de computadoras donde se ejecutan las acciones. Cuando se cumpla la condición y se compruebe su veracidad la red de computadoras ejecutará aquellos que esté estipulado en el contrato inteligente, esto puede ir desde liberar fondos a las partes apropiadas, registrar un vehículo, enviar notificaciones, etc.

Cuando la acción se ha efectuado, la cadena de bloques se actualiza, lo que quiere decir que la transacción no se puede cambiar.

Como se ve en la *Ilustración 12*, un contrato inteligente es una transacción entre dos partes sin la intervención de un intermediario, así mismo, cuando un contrato se efectúa y la Blockchain se actualiza, hace irrevocable la transacción y solo las partes involucradas pueden ver el resultado de dicha transacción, asegurando un nivel de privacidad bastante alto, ya que no es posible ver una transacción en la que no se participe.

Ilustración 12 Transacción entre dos partes por contrato inteligente.

Dentro del contrato, no hay límite al número de estipulaciones que puede contener, por lo que se pueden especificar tantas como sea necesario para que ambas partes estén satisfechas con lo estipulado en el contrato, así mismo, permite limitar tanto como sea posible el número de malentendidos, asegurando que los participantes estén satisfechos con el resultado.

Si bien, el contrato por si solo no garantiza que la transacción sea exactamente como se espera, esto recae en las manos de aquellos que especifican las condiciones y acciones que el contrato debe tener y llevar a cabo, así como explorar todas las posibilidades y excepciones y definir lo más detalladamente posible que es lo que el contrato hará.

3.3 Beneficios

Un contrato inteligente conlleva algunos beneficios a tomar mucho en cuenta, muchos de ellos vienen dados por la tecnología que usa para funcionar, que es la Blockchain.

- **Velocidad, eficiencia y precisión.**

Una vez que la condición estipulada se cumple, el contrato se ejecuta inmediatamente, por lo que no hay que esperar.

Ya que los contratos son digitales y automatizados, no hay papeleo en espera de ser procesado ni reconciliaciones que a menudo acaban en documentos que hay que llenar, lo que hace que el proceso se tarde aún más

- **Confianza y transparencia.**

Dado a que no hay un intermediario involucrado y dado a que los registros de la transacción se comparten con los participantes, no hay necesidad de cuestionar el resultado, ya que no es posible que la información se altere para beneficio personal sin que dicho cambio sea percibido por los participantes de la transacción.

- **Seguridad.**

Por la naturaleza de la tecnología Blockchain, las transacciones están encriptadas, lo que hace que sea muy difícil de piratear, y no solo la encriptación es difícil, sino que dado a que los registros de la Blockchain están conectados entre sí, será necesario que el atacante modifique la cadena entera para poder modificar un solo registro, esto solamente aumenta de dificultad cuando la cadena es muy grande, y como con cada transacción está cadena va creciendo, va siendo cada vez más difícil atacar una cadena de bloques existente.

- **Ahorros**

Al eliminar la presencia de un intermediario, ya no hay necesidad de que estos manejen las transacciones, y por tanto los retrasos y las tarifas asociados, lo que hace que la transacción se lleve a cabo sin mayores gastos más que los especificados en el contrato.

3.4 Desventajas

La desventaja más común y probablemente la más peligrosa sería el riesgo que puede llegar a tener un contrato inteligente mal programado. Un contrato inteligente es capaz de gestionar activos digitales, que a final de cuentas es dinero.

El hecho de mover dinero ya es razón suficiente para poner especial atención en la programación y buscar que haya la menor cantidad de incertidumbre y de ser posible nulificar la posibilidad de un malfuncionamiento, perolos contratos inteligentes pueden llegar a mover cantidades exageradamente grandes de dinero por lo que el detallismo que se requiere es especialmente grande.

Dado a que los contratos inteligentes pueden mover una enorme cantidad de dinero el riesgo de perderlo por una mala programación siempre está presente, lo que presiona a que los usuarios exijan a los desarrolladores la menor cantidad de riesgo posible, ya que, si bien el dinero no lo es todo en esta vida, puede llegar a significar un gran cambio, desde mejorar considerablemente la calidad de vida, hasta llegar al punto de terminar en la ruina por perder una gran cantidad de dinero.

3.5 Usos y Aplicaciones

Actualmente ya existen varias empresas que hacen uso de los contratos inteligentes y de sus beneficios para resolver problemas, entre ellas tenemos a una impresa de nivel internacional como lo es IBM en conjunto con Sonoco.

“Desarrollado por IBM Blockchain Transparent Supply, Pharma Portal es una plataforma basada en blockchain que rastrea productos farmacéuticos con control

de temperatura a través de la cadena de suministro para proporcionar datos confiables y precisos en múltiples partes." (IBM, s.f.)

Demostrando que la blockchain no solo tiene uso en transacciones puramente monetarias, sino que su uso puede ser expandido a muchas otras áreas expandiendo así el abanico de posibilidades y llegando a más público que al mismo tiempo puede ser el que estos le den un uso diferente logrando así tener un círculo de expansión.

Otra empresa que se suma a la entrada al mundo de Blockchain es The Home Depot, implementando el uso de contratos inteligentes como forma de solución a las disputas con los proveedores.

"A través de la comunicación en tiempo real y una mayor visibilidad de la cadena de suministro, están construyendo relaciones más sólidas con los proveedores, lo que da como resultado más tiempo para el trabajo fundamental y la innovación." (IBM, s.f.).

Con los contratos inteligentes es más fácil crear relaciones de confianza dado a la transparencia de los datos y a la seguridad que viene implícita al momento de usar Blockchain, por ello cada vez más empresas comienzan a usar blockchain, como se puede observar en la *Ilustración 13* y los contratos inteligentes como formas de solución a algunos problemas con los que lidian o para impulsar algún proyecto en el que estén trabajando.

Ilustración 13 Empresas que usan Blockchain.

3.6 Ethereum

"Ethereum es una plataforma digital que adopta la tecnología de cadena de bloques (blockchain) y expande su uso a una gran variedad de aplicaciones" (IG, 2022) Como se menciona anteriormente, la tecnología Blockchain ya se tenía en mente desde hace mucho tiempo y Ethereum llegó a expandir su variedad, principalmente entre la aplicaciones descentralizadas y colaborativas.

3.6.1 Ether

Ether (ETH) es la moneda nativa usada por Ethereum, esta es el token usado en las transacciones de contratos inteligentes en Ethereum, al igual que la Bitcoin, la criptomoneda con mayor valor y la más conocida, el ether existe como un sistema financiero autónomo de pares, está libre de las intervenciones gubernamentales.

Durante su tiempo de vida ha tenido altibajos al igual que Bitcoin, llegando a un gran pico en los años 2018-2019 y rebajando su valor a finales del año 2020 y nuevamente

subiendo su valor de manera explosiva en el año 2021 llegando a un pico mucho mayor que el que tuvo en 2018 y nuevamente dando bajada en el año 2022, como se muestra en la *Ilustración 14* dada la naturaleza de las criptomonedas estás tienen un valor muy volátil y a pesar del gran mercado de criptomonedas que hay actualmente siendo una de miles, es una de las pocas criptomonedas que tienen capitalización de mercado significativa, otro ejemplo de esta capitalización sería la Bitcoin.

Ilustración 14 Fluctuación del Ether durante su historia.

3.6.2 Cuentas

Hay 2 tipos de cuentas en Ethereum que comparten el mismo espacio de dirección: las **cuentas externas** que son las usadas por las personas, aquella que están controladas por medio de claves públicas-privadas y las **cuentas contrato** que son controladas por el código almacenado conjuntamente en la cuenta.

La dirección de una cuenta externa se define por la clave pública de esta misma, mientras la cuenta contrato define su dirección al momento de la creación de dicho contrato, la dirección de la cuenta contrato se deriva de la dirección del creador del contrato y el número de transacciones enviadas desde la dirección del creador, también llamado "Nonce".

3.6.3 Transacciones

Una transacción hace referencia a una acción iniciada por una cuenta de propiedad externa, es decir una cuenta controlada por otra persona y no un contrato.

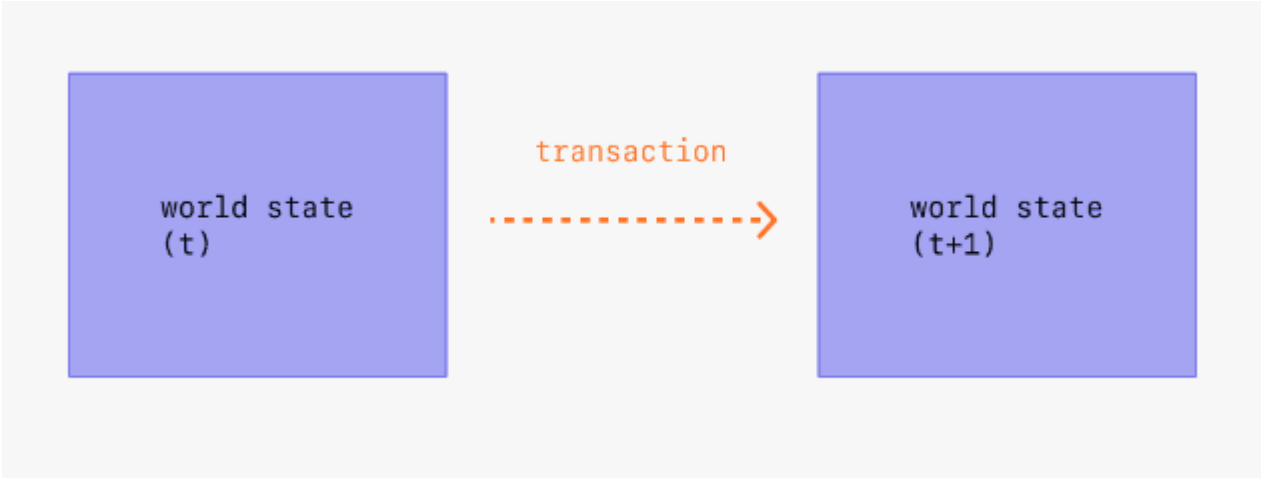


Ilustración 15 Representación de una transacción.

Como se puede observar en la *Ilustración 15*, las transacciones modifican el estado de la Máquina Virtual de Ethereum, esta acción se debe transmitir a toda la red.
Las transacciones enviadas incluyen la siguiente información:

- **Destinatario:** La transacción destinataria, si es de una cuenta externa la transacción transferirá valor, en caso de ser una cuenta contrato ejecutará el código del contrato.
- **Firma:** Identificador del remitente, esta se genera mediante la clave privada y es prueba de que el remitente a autorizado la transacción.
- **Valor:** Cantidad de ETH que se está transfiriendo, en WEI que es una denominación de ETH.

- **Datos:** Este es un campo opcional en el que se pueden indicar algunos datos, tales como el objetivo de la transacción o cosas así.
- **Límite de Gas:** La cantidad máxima de unidades de Gas que la transacción puede usar, siendo que la unidad de gas representa los pasos computacionales.
- **MaxPriorityFeePerGas:** La cantidad máxima de gas que se incluirá como recompensa para el minero.
- **maxFeePerGas:** es la cantidad mínima de Gas que se quiere pagar por la transacción.

3.6.4 Gas

El Gas hace referencia al esfuerzo computacional necesario para realizar operaciones específicas en la red de Ethereum.

Dado a que cada transacción realizada en Ethereum requiere un cierto grado de esfuerzo computacional para que este se pueda ejecutar, cada transacción requiere una comisión, esta comisión es el Gas.

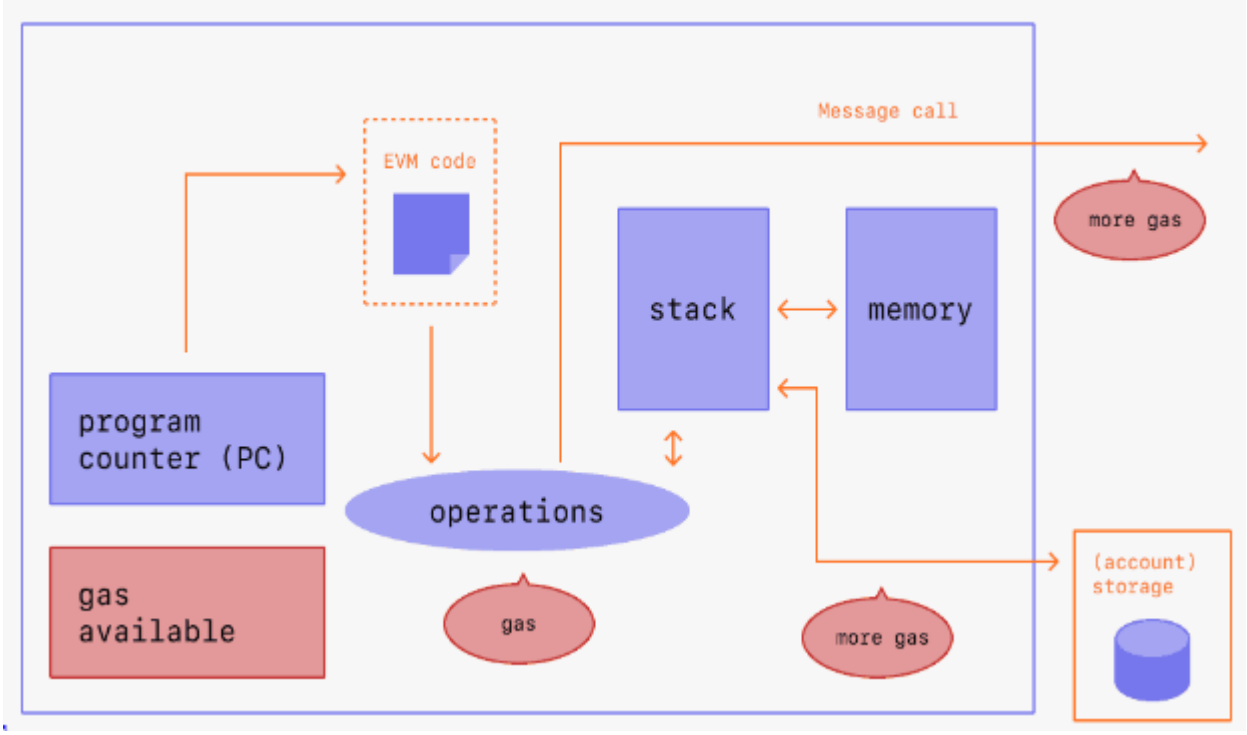


Ilustración 16 Gas consumido en una transacción sencilla.

En la *Ilustración 16* se puede observar cuales son las operaciones computacionales que hacen uso de Gas para poder funcionar.

3.6.5 Almacenamiento, Memoria y la Pila

Cada cuenta tiene un área de memoria llamada almacenamiento, este es un almacén clave valor difícil de leer y más un de modificar, dicho almacén mapea palabras de 256 bits con palabra de 256 bits, los contratos no pueden leer ni escribir en un almacenamiento que no sea el suyo.

La segunda área de memoria se llama memoria, de esta se obtiene de manera ágil una instancia clara de cada Message Call.

La EVM no es una máquina de registro, es una máquina de pila por lo que todas las operaciones se realizan en la tercera área de memoria, llamada la pila, esta tiene un límite de 1024 elementos y contiene palabra de 256 bits, los registros se apilan por lo que hay que limitar los registros que haya en la cima, esta pila funciona con el modelo FILA (First In, Last Out) es decir aquellos que estén en la cima de la pila tienen prioridad.

3.6.6 Conjunto de instrucciones

El conjunto de instrucciones se mantiene en mínimo con el fin de evitar implementaciones incorrectas que puedan causar problemas de consenso. Todas las instrucciones se operan con el tipo de dato básico, palabra de 256 bits. Tiene presente las operaciones de aritmética habitual, de bit, de lógica y de comparación. Se permite los saltos condicionales y los no condicionales. Se puede acceder a datos relevantes del bloque tales como el número del bloque y el timestamp.

3.6.7 Message Call

Los Message Calls son similares a las transacciones, ambos tienen origen, destino, datos, Ether, Gas y datos de retorno, de hecho, las transacciones consisten en un Message Call de alto nivel que es capaz que de forma consecutiva pueda crear Message Calls posteriores.

"Los contratos pueden llamar a otros contratos o enviar Ether a cuentas que no sean de contratos usando message calls." (Solidity, 2017). Mostrando el uso de los message calls en un contrato.

Cuando un contrato hace una llamada, el contrato llamado recibirá una instancia de memoria vacía y tendrá acceso a los datos de la llamada, estos datos se le proveerán en un área separada llamada calldata, cuando se termine la ejecución este devolverá los datos y estos serán almacenados en una localización de la memoria del que hace la llamada, dicha localización de la memoria ya había sido previamente reservada para los datos devueltos de la llamada.

3.6.8 Delegatecall / Callcode y librerías

Delegatecall o Callcode son una variación del Message call, estos son idénticos al Mesasage call con la única excepción de que el código en la dirección destino se ejecuta en el contexto del que hace la llamada y que el remitente y el valor no cambian.

Esto significa que un contrato puede cargar código dinámicamente desde una dirección diferente. Datos como el almacenamiento, la dirección actual y el balance siguen siendo del contrato que hace la llamada, solo se toma el código de la dirección llamada.

Esta función hace posible la implementación de librerías en Solidity, el código de librería se puede aplicar a un almacenamiento de contrato, y se puede, por ejemplo, implementar estructuras de código más complejas.

3.6.9 Logs

Esta es una función que se implementa en Solidity, permite implementar eventos, los contratos no pueden acceder a los datos del log una vez que este se haya creado, aunque estos datos pueden ser leídos desde fuera de la blockchain de forma eficiente, estos datos son accesibles incluso si los participantes de la red no se han descargado la cadena de bloques completa.

3.6.10 Creación

Es posible que un contrato cree otro contrato usando un opcode especial, esta es Create Call, la diferencia con el Message call es que los datos son ejecutados y el resultado almacenado en el código, y aquel que hace la llamada reciben la dirección del nuevo contrato en la pila.

3.6.11 Auto-destrucción

La única forma de borrar el código de la blockchain es cuando un contrato, en esa dirección de bloque realiza la operación de selfdestruct. Cuando se activa la operación de auto-destrucción, los ETH restantes que estaban almacenados en esa dirección son enviados al destinatario, una vez se lleva a cabo esta acción, se procede a borrar el almacenamiento y el código del estado.

El contrato no debe necesariamente llevar la operación de selfdestruct, este todavía puede ser ejecutado mediante la operación de delegatecall o callcode.

3.7 Solidity

Solidity es un lenguaje de programación, pero a diferencia de los más comunes como son Java, C o Python, Solidity no está diseñado para crear programas normales, este está diseñado enteramente para crear contratos inteligentes. La sintaxis de solidity está basada en ECMAScrip, por lo que tiene similitudes a JavaScrip, lenguaje que se usó de base para ECMAScrip, así mismo tiene características propias del lenguaje C, pero solidity implementa el tipado fuerte en la declaración de variable y argumentos, esto con el objetivo de que el contrato se ejecute lo más estable posible.

Solidity fue creado por un equipo de desarrolladores que colaboraron en la creación de Ethereum, por lo que concretamente podemos decir que Solidity es un lenguaje de programación creado para ser ejecutado en la EVM (Ethereum Virtual Machine) que funcionan sobre la Blockchain de Ethereum.

Los contratos de Solidity pueden almacenarse de distintas maneras, siendo que puede ser local, es decir directamente en tu ordenador, o también se puede desplegar en la red Ethereum, esto hará que el contrato se aloje de manera descentralizada, es decir que se mantiene replicándose en la red de ordenadores de la Blockchain, eso da como resultado que nadie esté en control directo sobre el contrato.

En el tema de compatibilidad, es normal pensar que el contrato no se podría ejecutar en otras Blockchains fuera de la de Ethereum, pero siempre que haya cierto nivel de compatibilidad o similitud entre las Blockchains, no debería haber ningún problema, por ejemplo, las redes de Ethereum, Polygon y Binance son lo suficientemente similares como para que se pueda implementar un contrato en la 3 y que su funcionamiento sea predecible.

3.7.1 Estructura de un contrato

Si bien el fin de solidity es totalmente diferente de los lenguajes de programación convencionales, eso no quiere decir que su estructura sea completamente diferente, de hecho, dado a su parecido con algunos de estos lenguajes convencionales, la estructura de solidity es bastante similar.

Cualquier contrato puede contener declaraciones del tipo variables de estado, funciones, modificadores de función, eventos, struct y enums, así mismo, los contratos pueden heredar de otros contratos.

- **Variables de estado:** Son valores que están permanentemente almacenadas en una parte del contrato conocida como storage del contrato.
- **Funciones:** Son las unidades ejecutables del código dentro de un contrato.
- **Modificadores de función:** Se usan para corregir la semántica de las funciones.
- **Eventos:** Los eventos permiten el uso de la capacidad de registro del EVM, que a su vez puede “llamar” a los callbacks de JavaScrip en la interfaz de usuario de una Dapp que escucha a esos eventos.
- **Structs:** Un Struct permite crear estructuras de código más complejas al agrupar datos relacionados, estas pueden crearse fuera de un contrato e importarse a otro.
- **Enums:** Permite la agrupación de datos bajo un mismo tipo, simplificando el código.

3.8 Oráculos (Oracles)

Los oráculos son la forma de conectar la Ethereum con el mundo real, es decir externa a la Blockchain (off-chain), esto con el fin de que se pueda consultar datos en los contratos inteligentes, por ejemplo, una Dapp de compras usará los oráculos para consultar los datos de venta, tales como el precio, vendedor, ofertas, etc.

Bibliografía

Arellano Mejía, J., & Sánchez Morales, C. A. (Abril-Junio de 2017). *SciElo*. Obtenido de ¿El expediente clínico debe ser clasificado como confidencial y reservado?: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0028-37462017000200111

Binance Academy. (18 de Noviembre de 2019). *Binance Academy*. Obtenido de La Historia de Blockchain: https://www.binance.vision/es/blockchain/history-of-blockchain

Bit2Me. (30 de Enero de 2021). *bit2me Academy*. Obtenido de Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?: https://academy.bit2me.com/que-son-los-smart-contracts/

Bit2Me. (s.f.). *Academy by Bit2me*. Obtenido de Qué es Prueba de trabajo / Proof of Work (PoW): https://academy.bit2me.com/que-es-proof-of-work-pow/

Bit2Me. (s.f.). *Academy by Bit2me*. Obtenido de Qué es el HashChash: https://academy.bit2me.com/que-es-hashcash/

Brandom, R. (9 de Enero de 2019). *The Verge*. Obtenido de Why the Ethereum Classic hack is a bad omen for the blockchain: https://www.theverge.com/2019/1/9/18174407/ethereum-classic-hack-51-percent-attack-double-spend-crypto

Centro de Capacitación Judicial Electoral. (Junio de 2010). *Trinubal Electoral.* Obtenido de Sistemas Electorales y de Partidos: https://www.te.gob.mx/ccje/Archivos/manual_sistemas.pdf

Coinbase. (s.f.). *Coinbase*. Obtenido de Precio Bitcoin: https://www.coinbase.com/price/bitcoin

Cuentas, R. (2019). *Rendir Cuentas*. Obtenido de ÍNDICE DE PERCEPCIÓN DE LA CORRUPCIÓN 2019: http://www.rendircuentas.org/noticia/indice-percepcion-la-corrupcion-2019/

Dr. Duarte, M., & Arboledas, H. (06 de Agosto de 2018). *Comunas del Litoral.* Obtenido de Desafíos Estratégicos de la Tecnología Blockchain en Procesos Electorales: https://comunaslitoral.com.ar/nota/6583/desafios-estrategicos-de-la-tecnologia-blockchain-en-procesos-electorales

EDUTEC. Revista Electrónica de Tecnología Educativa. (2017). En *BLOCKCHAIN EN EDUCACIÓN* (pág. 4).

Ethereum. (14 de Noviembre de 2022). *Ethereum*. Obtenido de ORÁCULOS: https://ethereum.org/es/developers/docs/oracles/

Ethereum. (14 de Noviembre de 2022). *Ethereum*. Obtenido de TRANSACCIONES: https://ethereum.org/es/developers/docs/transactions/#:~:text=Una%20transacción%20de%20Ethereum%20hace,en%20la%20cuenta%20de%20Alice

Fernández Espinosa, L. (10 de Septiembre de 2019). *BBVA*. Obtenido de ¿Qué son los "smart contracts" o contratos inteligentes basados en Blockchain?: https://www.bbva.com/es/smart-contracts-contratos-basados-blockchain/

Fernández, Y. (12 de Abril de 2022). *Xataka*. Obtenido de Solidity: qué es y para qué sirve este lenguaje de programación: https://www.xataka.com/basics/solidity-que-sirve-este-lenguaje-programacion

Gusson, C. (14 de Noviembre de 2019). *Cointelegraph*. Obtenido de ¿Por qué los gobiernos y las corporaciones necesitan blockchain?: https://es.cointelegraph.com/news/why-do-governments-and-corporations-need-blockchain

Harán, J. M. (Abril de 2019). *Welive Security*. Obtenido de Blockchain: problemas de seguridad que giran alrededor de esta tecnología: https://www.welivesecurity.com/la-es/2019/04/02/blockchain-problemas-seguridad-alrededor-tecnologia/

IBM. (s.f.). *IBM*. Obtenido de ¿Qué son los contratos inteligentes en blockchain?: https://www.ibm.com/mx-es/topics/smart-contracts

IG. (2022). *IG*. Obtenido de ¿Qué es Ethereum y cómo funciona?: https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona

INE. (2022). *INE.* Obtenido de Información Básica Sistema Electoral Mexicano: https://portalanterior.ine.mx/archivos3/portal/historico/contenido/Sistema_Politico_Electoral_Mexicano/

kjchints. (21 de Diciembre de 2021). *YouTube*. Obtenido de Solidity Explicado Fácilmente ft. @Filosofía Código: https://www.youtube.com/watch?v=PebL9RuWwTg

Macario, C. A. (s.f.). *Campus Virtual TEV.* Obtenido de El Sistema Electoral en México: http://www.campus-virtual-tev.gob.mx/files/DIAPOSITIVAS-DE-SITEMA-ELECTORAL-EN-MEXICO.pdf

Mario. (6 de Octubre de 2019). *Dirigentes Digital*. Obtenido de Los diez países que más usan criptomonedas: https://dirigentesdigital.com/economia/los-diez-paises-que-mas-usan-criptomonedas-GA1233686

Martínez Silva, M., & Salcedo Aquino, R. (2006). *Gobernación.* Obtenido de Proceso electoral: http://sil.gobernacion.gob.mx/Glosario/definicionpop.php?ID=193

Moto, E. (20 de Junio de 2018). *Qore*. Obtenido de ¿Qué es una aplicación descentralizada?: https://www.qore.com/noticias/65116/Que-es-una-aplicacion-descentralizada

Plata, U. N. (2019). Facultad de Informática. En I. M. Gallardo Urbini, *Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada* (pág. 101). La Plata, Argentina.

Ripio Blog. (19 de Julio de 2018). Obtenido de ¿Qué es un token y cómo funciona: https://www.ripio.com/ar/blog/que-es-un-token-y-como-funciona/

Sanz Romero, M. (14 de Septiembre de 2019). *Computer Hoy*. Obtenido de ¿Qué es P2P y en qué consiste?: https://computerhoy.com/reportajes/tecnologia/p2p-que-es-489221

Secretaría de Relaciones Exteriores. (27 de Mayo de 2021). *Relaciones Exteriores*. Obtenido de https://embamex.sre.gob.mx/nuevazelandia/index.php/sobremexico/gobiernoyestructura#:~:text=El%20Supremo%20Poder%20de%20la,Poderes%20Legislativo%2C%20Ejecutivo%20y%20Judicial

Solidity. (2017). *Solidity*. Obtenido de Introducción a los Contratos Inteligentes: https://solidity-es.readthedocs.io/es/latest/introduction-to-smart-contracts.html#un-contrato-inteligente-simple

Solidity. (2017). *Solidity*. Obtenido de Estructura de un contrato: https://solidity-es.readthedocs.io/es/latest/solidity-by-example.html#votacion

Solidity. (2017). *Solidity*. Obtenido de Contratos: https://solidity-es.readthedocs.io/es/latest/contracts.html

Télles Valdés, J. (2010). *Temas selectos de Derecho Electoral.* Obtenido de El voto electrónico: https://www.te.gob.mx/publicaciones/sites/default/files/archivos_libros/14_voto.pdf

UNAM. (2018). Obtenido de EL PROCESO ELECTORAL: https://archivos.juridicas.unam.mx/www/bjv/libros/12/5660/14.pdf

Universidad de Buenos Aires. Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería. (2017). Carrera de Esepecialización en Seguridad Informática. En J. A. Aguirre Regato, *Cadena de bloques: potencial aplicación a Historias Clínicas Electrónicas* (pág. 16). Buenos Aires.

Universidad Politécnica de Catalunya. (s.f.). En C. Dolader Retamal, J. Bel Roig, & J. L. Muñoz Tapia, *LA BLOCKCHAIN: FUNDAMENTOS, APLICACIONES Y RELACIÓN CON OTRAS TECNOLOGÍAS DISRUPTIVAS* (pág. 34). Cataluña.

Universidad Politécnica de Valéncia. (2017-2018). En P. García Mateo, *Blockchain aplicado al sector púnlico* (pág. 59). Valéncia.

Universidad Politécnica de Valéncia. (2017-2018). En P. García Mateo, *Blockchain aplicado al sector público* (pág. 26). Valéncia.

Wikipedia. (s.f.). Obtenido de Hedonismo: https://es.wikipedia.org/wiki/Hedonismo