Universidad Nacional del Sur

Tesis de Licenciatura
en Ciencias de la Computación

Sistemas de votación electrónica seguros utilizando Blockchain y Smart-Contracts

Razuc Gonzalo

Directores: Stankevicius Alejandro - de Matteis Leonardo

Bahía Blanca – Argentina

2024

Índice general

0.1. Introducción

En la era digital, la evolución de la tecnología ha transformado múltiples aspectos de la vida cotidiana, incluyendo la forma en que se realizan las votaciones. Los sistemas de votación tradicionales presentan varios desafíos, como la manipulación de votos, la falta de transparencia y la logística compleja para garantizar la seguridad, correctitud e integridad del proceso.

Estos desafíos se agravan en nuestro país, donde en cada votación surgen conflictos entre las diferentes facciones políticas, con frecuentes acusaciones de fraude y manipulación. Estas tensiones y desconfianzas afectan la legitimidad de los resultados electorales y a su vez erosionan la confianza del público en el sistema democrático.

El sistema de votación argentino,en particular, ha sido objeto de controversias a lo largo de los años, con reportes de presuntos casos de fraude electoral reportados. Estas acusaciones han generado un debate público sobre la necesidad de modernizar y reforzar los procesos de votación para garantizar su transparencia y confiabilidad.

Entre las prácticas fraudulentas más comunes se encuentran el voto cadena y la manipulación de boletas, dos problemas que reflejan las vulnerabilidades inherentes del sistema actual y la urgencia de adoptar soluciones tecnológicas. Es por ello que ambos problemas serán abordados en una sección posterior, donde se analizarán en detalle para proporcionar una comprensión más profunda de su funcionamiento y cómo afectan la integridad del proceso electoral, con el objetivo de explicar cómo pueden ser mitigados mediante la implementación de tecnologías adecuadas.

En este contexto, los sistemas de votación electrónica han surgido como una alternativa potencialmente viable para abordar estos desafíos. Sin embargo, su adopción no ha estado exenta de críticas, ya que los riesgos asociados a la seguridad digital, tales como los ataques informáticos y la manipulación remota, han generado dudas sobre su fiabilidad. A pesar de estas preocupaciones, el desarrollo de tecnologías emergentes como *Blockchain* y *Smart Contracts* promete aportar nuevas soluciones a estos problemas.

Blockchain, una tecnología de registro distribuido, ofrece una plataforma segura, transparente e inmutable, ideal para la gestión de votos. Cada voto se registra como un bloque en la cadena, y una vez registrado, no puede ser alterado, lo que garantiza la integridad del proceso electoral y proporciona un sistema auditable en el que cada

voto es trazable sin comprometer el anonimato del votante. La descentralización de *Blockchain* también reduce la posibilidad de manipulación, ya que no hay una única entidad que controle todo el sistema.

Por otro lado, los *Smart Contracts* son programas autoejecutables que se almacenan en la *Blockchain* y se activan automáticamente cuando se cumplen ciertas condiciones predefinidas. Estos contratos inteligentes pueden automatizar y asegurar diversas partes del proceso de votación, desde la verificación de la identidad del votante hasta el conteo de votos y la publicación de resultados, reduciendo la intervención humana y minimizando el riesgo de errores o fraudes.

A nivel internacional, algunos países han comenzado a explorar el uso de tecnologías basadas en *Blockchain* para mejorar sus sistemas de votación. Por ejemplo, Estonia ha implementado un sistema de votación electrónica que permite a los ciudadanos votar de forma remota de manera segura [7]. Asimismo, se han realizado pruebas de votación electrónica basada en *Blockchain* en la ciudad de Zug, Suiza [3]. Estos ejemplos internacionales proporcionan una base sólida para investigar la implementación de estas tecnologías en el contexto argentino, adaptando las soluciones tecnológicas a las particularidades de nuestro sistema electoral y marco regulatorio.

La integración de estas tecnologías no solo mejora la seguridad y la transparencia, sino que también puede simplificar el proceso de votación, reducir costos y aumentar la confianza de los votantes en el sistema electoral. No obstante, la implementación de dichos sistemas plantea desafíos significativos, incluyendo la infraestructura tecnológica necesaria, los marcos legales y regulatorios que deben adaptarse, así como la aceptación por parte del público. Todos estos factores deben ser abordados cuidadosamente para garantizar que el sistema propuesto sea práctico y viable.

Esta tesis se enmarca en el contexto de la búsqueda de sistemas de votación más seguros y confiables, explorando específicamente el uso de *Blockchain* y *Smart Contracts* para desarrollar un sistema de votación electrónica seguro que mitigue los riesgos de fraude y manipulación, asegurando al mismo tiempo la transparencia y la eficiencia del proceso electoral en Argentina.

0.2. Sistema de votación Argentino actual

El sistema de votación en Argentina sigue un proceso detallado y riguroso, diseñado para garantizar la participación democrática de la ciudadanía y mantener la integridad del voto. A lo largo del día electoral, el procedimiento se inicia cuando el votante se presenta en la mesa electoral correspondiente, la cual está compuesta por un presidente de mesa y fiscales de los diferentes partidos políticos. Los fiscales tienen la función de observar y garantizar la transparencia del proceso en representación de sus respectivos partidos o alianzas.

Al llegar el votante presenta su documento de identidad (DNI), el cual es verificado por el presidente de mesa para confirmar que se encuentra en el padrón electoral. Una vez verificada su identidad el votante es marcado como presente en el padrón, su DNI queda retenido hasta que complete el proceso de votación y se le entrega un sobre vacío firmado por el presidente de mesa. Este sobre es un elemento **clave** del proceso, ya que su firma garantiza que es legítimo y que podrá ser introducido en la urna sin inconvenientes.

Con el sobre firmado el votante se dirige al "cuarto oscuro", un espacio privado donde se encuentran dispuestas las boletas de todos los partidos y listas electorales. Estas boletas están ordenadas y disponibles para que el votante elija libremente su preferencia. El cuarto oscuro asegura la privacidad y el secreto del sufragio, permitiendo que su selección sea completamente confidencial.

El votante puede optar por cortar boleta, una práctica común en elecciones donde se votan múltiples cargos. Esto significa que puede seleccionar una boleta de un partido para un cargo y otra boleta de un partido diferente para otro cargo. Para hacer esto, el votante corta físicamente las boletas y combina sus secciones preferidas antes de introducirlas en el sobre. Una vez que el votante ha seleccionado la o las boletas, las coloca dentro del sobre firmado y lo cierra.

Tras salir del cuarto oscuro el votante regresa a la mesa electoral con el sobre cerrado y lo deposita en la urna bajo la supervisión del presidente de mesa y los fiscales, quienes verifican que todo el procedimiento se realice conforme a la normativa vigente. Luego de depositar el sobre en la urna el votante firma el padrón electoral, certificando así que ha ejercido su derecho al voto. Esta firma constituye un registro fundamental para el control de la participación electoral.

A continuación, los fiscales le devuelven su DNI junto con un certificado firmado por el presidente de mesa, que acredita su presencia y participación en el proceso electoral. Con este paso el votante concluye el proceso y puede retirarse.

Al finalizar la jornada de votación las urnas son abiertas por el presidente de mesa en presencia de los fiscales de los partidos. Los votos son contados manualmente, uno por uno, y los resultados de cada mesa son consignados en actas oficiales. Estas actas son firmadas tanto por el presidente de mesa como por los fiscales presentes y luego son enviadas a los centros de escrutinio, donde se consolidan los resultados a nivel regional y nacional.

Este proceso, aunque estructurado para garantizar la transparencia y seguridad, presenta varias vulnerabilidades que han sido objeto de fraude a lo largo de los años. Entre las prácticas fraudulentas más comunes están el voto cadena, el robo de boletas y las urnas embarazadas.. Estos fraudes serán explicados en detalle en la siguiente sección, donde se analizarán sus mecanismos y cómo comprometen la seguridad del sistema electoral.

0.2.1. Vulnerabilidades

A pesar de los esfuerzos por garantizar la integridad del voto, el sistema de votación argentino se enfrenta a una serie de fraudes que ponen en riesgo la transparencia del proceso electoral. Estos fraudes han persistido durante décadas y han sido objeto de críticas y debates tanto a nivel político como social. A continuación se explican los fraudes más comunes que afectan al sistema electoral:

1. **Robo de Boletas**

   El robo de boletas es una técnica de manipulación electoral que se basa en la sustracción deliberada de las boletas correspondientes a uno o más partidos políticos en los lugares de votación, con el fin de limitar las opciones disponibles para el votante y alterar los resultados electorales. Seguidamente, se describe el proceso de su ejecución y sus implicancias de forma detallada.

   1.1 Sustracción de boletas

   El proceso comienza cuando individuos vinculados a un partido político ingresan al cuarto oscuro, el lugar donde los votantes seleccionan la boleta de su

preferencia. Estos individuos retiran sistemáticamente las boletas de los partidos rivales de las mesas, dejándolas fuera del alcance de los electores. Esta acción suele repetirse a lo largo de la jornada electoral, lo que asegura que en la mayor parte del tiempo los votantes no puedan acceder a las boletas afectadas.

1.2 Impacto en la elección del votante

Cuando un votante ingresa al cuarto oscuro y no encuentra la boleta de su partido preferido, se enfrenta a un dilema:

- Emitir un voto en blanco: Si el votante decide no apoyar otra opción y no solicita asistencia, su voto será contabilizado como "en blanco", lo que puede impactar en la distribución de escaños y favorecer a los partidos que no han sido afectados por el robo.

- Votar por otro partido: Ante la ausencia de la boleta deseada algunos votantes optan por votar a otro partido, aunque esta no sea su primera opción, lo que altera las preferencias originales del electorado.

- Salir a solicitar más boletas: Aunque la legislación permite que los votantes soliciten boletas adicionales al presidente de mesa, esto no siempre ocurre, ya sea por desconocimiento, incomodidad o presiones sociales. Como resultado, muchos votantes se ven forzados a emitir su voto de manera distinta a lo planeado.

1.3 Limitaciones en la reposición de boletas

Aunque la ley establece que los fiscales de cada partido tienen el derecho y la responsabilidad de reponer boletas cuando estas faltan, la efectividad de esta medida depende en gran medida de la capacidad organizativa y del tamaño del partido afectado. En algunos casos los fiscales no cuentan con la cantidad de boletas necesarias o no están presentes durante toda la jornada, lo que permite que las mesas queden sin boletas de forma prolongada e, incluso, durante toda la jornada.

2. **Voto cadena**

   El "Voto cadena" es una técnica de manipulación electoral utilizada para influir en los resultados de una elección. En el sistema electoral argentino, esta

práctica fraudulenta explota la logística del proceso de votación, específicamente el manejo de sobres oficiales y boletas de papel, para controlar el voto de ciertos electores. A continuación, se describe detalladamente el mecanismo de ejecución y sus implicancias.

2.1 Obtención de un sobre oficial

El proceso comienza con la obtención de un sobre oficial de votación fuera del centro electoral. Los organizadores del fraude, conocidos como "punteros" introducen en este sobre una boleta del partido o candidato que desean favorecer y lo sellan cuidadosamente. Este sobre oficial es indistinguible de los entregados en las mesas electorales, lo que dificulta su detección.

2.2 Primer votante cómplice

Un votante inicial, que colabora voluntariamente con los organizadores del fraude, recibe el sobre sellado antes de ingresar al lugar de votación. Este votante sigue estos pasos:

- Se presenta ante la mesa electoral y recibe un sobre oficial vacío, como es el procedimiento estándar.

- Ingresa al cuarto oscuro con el sobre oficial vacío y el sobre sellado que le dio el puntero.

- Una vez dentro guarda el sobre oficial vacío.

- Sale del cuarto oscuro sin tomar ninguna boleta ni utilizar el sobre que le fue entregado en la mesa.

- Deposita en la urna el sobre sellado que traía consigo.

- Al salir entrega el sobre oficial vacío a los organizadores del fraude.

2.3 Continuación de la cadena

El sobre oficial vacío recuperado es utilizado para continuar el fraude con votantes subsiguientes, que pueden ser coaccionados o sobornados. Cada nuevo votante sigue el mismo procedimiento:

- Antes de ingresar al centro de votación recibe de los organizadores un sobre sellado con una boleta dentro.

- En la mesa electoral recibe un sobre oficial vacío.

- En el cuarto oscuro oculta el sobre oficial vacío.

- En la urna deposita el sobre sellado que recibió previamente.

- Al salir entrega el sobre oficial vacío a los organizadores para repetir el ciclo.

Este ciclo se repite con cada votante involucrado, creando una cadena continua que permite a los organizadores controlar cada voto emitido mediante este mecanismo fraudulento. El "voto cadena" es uno de los fraudes **más difíciles de detectar una vez iniciado**, debido a su discreción y al hecho de que simula el comportamiento normal de votación.

3. **Urnas embarazadas**
   El fraude conocido como "Urnas embarazadas" es una práctica ilícita que implica la manipulación de urnas electorales para alterar los resultados de una elección. Este fraude se refiere a la práctica de introducir boletas fraudulentas en las urnas antes de que comience la jornada electoral. Al introducir boletas a favor de un candidato o partido específico dentro de las urnas antes de que se haya depositado ningún voto real se alteran los resultados desde el inicio. Esta manipulación requiere acceso previo a las urnas, lo que implica la complicidad de autoridades electorales corruptas o la falta de supervisión en momentos claves del proceso. Se presenta a continuación una descripción detallada del mecanismo de ejecución y sus implicaciones.

   3.1 Introducción previa de boletas:

   Antes de la apertura de las mesas de votación, se introducen boletas fraudulentas en las urnas de forma clandestina. Este paso requiere acceso indebido a las urnas, generalmente facilitado por personal electoral corrupto o fallas en los controles de seguridad.

   3.2 Manipulación durante el traslado:

   Las urnas pueden ser manipuladas durante su transporte desde los centros de distribución hasta las mesas de votación. El personal encargado del traslado, si está involucrado en el fraude, puede introducir boletas fraudulentas en las

urnas o alterar los sellos de seguridad. Esta etapa es crítica, ya que la falta de supervisión efectiva facilita la manipulación.

3.3 Sustitución de urnas:

En situaciones atípicas y complejas las urnas originales pueden ser directamente reemplazadas por otras que ya contienen boletas fraudulentas. Este método requiere una logística compleja y coordinación entre varios individuos, incluyendo personal de seguridad y autoridades electorales corruptas.

3.4 Complicidad de autoridades electorales:

La colaboración de autoridades de mesa, fiscales o personal electoral es esencial para ejecutar este fraude sin levantar sospechas. La ausencia de supervisión rigurosa o la falta de presencia de fiscales de partidos opositores facilita considerablemente su implementación.

Las urnas embarazadas son especialmente difíciles de detectar porque, una vez que se han introducido boletas fraudulentas en la urna, éstas se mezclaran con las boletas legítimas. Por ende, esto complica la verificación posterior, ya que durante el escrutinio es prácticamente imposible distinguir entre las boletas fraudulentas y las legítimas. Además, si el número de boletas fraudulentas no excede significativamente el número esperado de votantes, las discrepancias pueden pasar desapercibidas.

4. **Manipulación de votos durante el conteo**
   El conteo manual de votos al cierre de la jornada electoral es una etapa crítica y una de las más vulnerables a fraudes. Aunque los errores involuntarios pueden surgir por el agotamiento o la presión, también es posible que se cometan manipulaciones deliberadas para alterar los resultados finales. A continuación, se detallan las principales formas de manipulación durante esta fase.

   4.1 Alteración de las actas de resultados Una de las prácticas más comunes es la modificación directa de las cifras en las actas de escrutinio, alterando el conteo para beneficiar a un candidato o partido. Este tipo de manipulación busca que las discrepancias pasen desapercibidas durante la consolidación final.

   4.2 Sustracción o eliminación de votos Otra forma de manipulación consiste en la desaparición de boletas legítimas, especialmente de aquellos candi-

datos opositores, con el fin de reducir su conteo total. Asimismo, se pueden dañar o manipular boletas para que sean consideradas inválidas durante el escrutinio, anulando votos que deberían ser válidos.

4.3 Inclusión de votos fraudulentos El agregado de boletas falsas es una táctica utilizada para inflar artificialmente los resultados de un candidato específico. En paralelo, votos que deberían ser anulados pueden ser deliberadamente validados si benefician al candidato deseado, lo que altera aún más la legitimidad del conteo.

4.4 Intimidación y restricciones a la observación La intimidación de fiscales y observadores es otra estrategia utilizada para evitar la denuncia de irregularidades. Esto puede incluir amenazas o coacción directa hacia los representantes de otros partidos. Además, en algunos casos se restringe el acceso de fiscales y observadores durante el proceso de conteo, limitando la transparencia y facilitando la ejecución de fraudes sin ser detectados.

5. **Compra de votos**

   La compra de votos es una práctica fraudulenta que implica coaccionar o sobornar a los votantes para que emitan su voto a favor de un candidato o partido específico. Esta práctica es especialmente común en áreas vulnerables, donde factores como la pobreza o la dependencia económica facilitan la manipulación electoral.

   Este tipo de fraude puede manifestarse de varias formas:

   5.1 Sobornos monetarios: Consiste en ofrecer dinero a los votantes a cambio de su compromiso de votar por un determinado candidato. El monto puede variar según el contexto y la situación económica de los votantes.

   5.2 Beneficios en especie: En lugar de dinero, se ofrecen bienes materiales como alimentos, ropa, medicinas o incluso promesas de empleo o acceso a servicios públicos.

   5.3 Coacción y presión: En algunos casos los votantes son amenazados con perder beneficios sociales, empleos o sufrir represalias si no votan por el candidato indicado.

5.4 Traslado de votantes: En Argentina, se han documentado numerosos casos en los que partidos políticos transportan a los votantes en autobuses hacia las mesas de votación. Esta estrategia, comúnmente conocida como "acarreo", permite a los partidos ejercer mayor control sobre los votantes y presionarlos para que elijan al candidato del partido que financió el traslado.

6. **Suplantación de identidad**

   La suplantación de identidad es una práctica de fraude electoral en la que una persona vota en nombre de otra, ya sea un votante fallecido o alguien que por distintos motivos no se presenta a votar. Este tipo de fraude puede ocurrir mediante diversas tácticas y en distintos escenarios, frecuentemente en áreas con baja supervisión o donde los mecanismos de verificación de identidad son débiles.

   Este fraude puede ser llevado a cabo de diversas formas:

   6.1 Uso de documentos falsificados y/o manipulación de registros electorales:

   Este método puede manifestarse de dos maneras: mediante la falsificación de documentos de identidad utilizando los datos de votantes ausentes, lo que permite a terceros hacerse pasar por ellos; o a través de la manipulación de los padrones electorales, agregando personas ficticias o alterando la información de votantes reales, facilitando así la emisión de votos fraudulentos.

   6.2 Complicidad de autoridades electorales:

   La complicidad de las autoridades electorales puede manifestarse tanto por negligencia como por acciones deliberadas. En algunos casos las autoridades de mesa no verifican correctamente la identidad de los votantes, permitiendo irregularidades por descuido o falta de supervisión adecuada. En otros, su participación activa facilita de forma consciente la suplantación de identidad.

   6.3 Aprovechamiento de ausencia de votantes:

   Esta forma de fraude se basa en la utilización ilícita de los datos de votantes que no participarán en la elección. Esto incluye tanto a personas fallecidas cuyos nombres aún figuran en el padrón electoral como a votantes ausentes

que por diversas razones no acudirán a las urnas. En ambos casos, se realiza una suplantación de identidad para emitir votos fraudulentos.

0.3. Blockchain

0.3.1. Introducción

En las últimas décadas, el avance exponencial de la tecnología ha impulsado innovaciones que han transformado sectores clave. Entre estas, el ***Blockchain*** destaca como una tecnología disruptiva, redefiniendo paradigmas en áreas como la seguridad informática, las finanzas y la gestión de datos. Su capacidad para ofrecer una plataforma descentralizada, segura y transparente lo convierte en un pilar fundamental en la construcción de sistemas confiables en un mundo digital.

El *Blockchain* surgió con la creación de **Bitcoin**, una criptomoneda diseñada como respuesta a la necesidad de un sistema financiero descentralizado y resistente a la censura. Aunque inicialmente concebido para las criptomonedas, el *Blockchain* ha demostrado su versatilidad con aplicaciones que abarcan desde la trazabilidad de productos y los contratos inteligentes hasta el registro de propiedades y la identidad digital.

La esencia de esta tecnología radica en su estructura de datos: bloques enlazados criptográficamente, que almacenan registros inmutables de transacciones. Gracias a su diseño distribuido, múltiples partes pueden confiar en un sistema compartido sin depender de intermediarios, resolviendo problemas como la vulnerabilidad ante fallos, la falta de transparencia y la dependencia de entidades centralizadas.

Para comprender a fondo el *Blockchain*, es crucial analizar el **whitepaper de Bitcoin**, titulado *Bitcoin: A Peer-to-Peer Electronic Cash System*, publicado en 2008 por Satoshi Nakamoto [6]. Este documento no solo describe el sistema Bitcoin, sino que establece conceptos fundamentales del *Blockchain*, como la descentralización, la criptografía y el consenso distribuido.

El whitepaper presenta una solución innovadora al problema del doble gasto, una limitación clave en los sistemas de pago electrónicos descentralizados. Mediante una estructura distribuida y sin necesidad de una autoridad central, Bitcoin mantiene un registro confiable de transacciones, apoyado en la **prueba de trabajo** (Proof of Work) y un **sistema de consenso** que garantiza la validez e inmutabilidad de los datos.

En esta sección se desarrollarán los principales mecanismos técnicos descritos en el whitepaper, incluyendo:

1. **Modelo Peer-to-Peer**: Cómo la red descentralizada elimina la necesidad de intermediarios y permite la transferencia directa de valor entre pares.

2. **Estructura de Bloques y Cadenas**: El método mediante el cual se agrupan y encadenan las transacciones para formar un registro inmutable.

3. **Prueba de Trabajo (Proof of Work)**: El mecanismo que asegura la integridad y seguridad de la red, y cómo se resuelve la competencia entre nodos para añadir nuevos bloques.

4. **Sistema de Consenso Distribuido**: Cómo los nodos acuerdan sobre el estado de la cadena y se evita la manipulación de datos.

Cada uno de estos elementos será analizado en detalle, desglosando las ideas originales del whitepaper y su relevancia en el contexto del *Blockchain* como tecnología base.

0.3.2. Transacciones

0.3.2.1. Introducción

Las transacciones son el núcleo funcional de Bitcoin. En términos simples, una transacción representa el intercambio de valor entre dos partes. Este sistema, basado en criptografía de clave pública, permite que cada participante en la red transfiera fondos de manera segura y directa.

En Bitcoin, cada moneda (o fracción de moneda) se representa como una **cadena de firmas digitales**. El funcionamiento básico de una transacción incluye los siguientes pasos:

1. **Firmas Digitales:**
    - El propietario actual de una moneda genera un *hash* de la transacción previa y la clave pública del receptor.
    - Luego, este *hash* se firma digitalmente con la clave privada del propietario actual.
2. **Encadenamiento de Transacciones:**
    - La firma resultante se añade a la transacción, formando un eslabón en una cadena.
    - El receptor puede verificar la firma utilizando la clave pública del propietario anterior, confirmando así la legitimidad de la transacción.

Este encadenamiento garantiza que la propiedad de la moneda pueda ser trazada de manera verificable hasta su origen, sin ambigüedades.

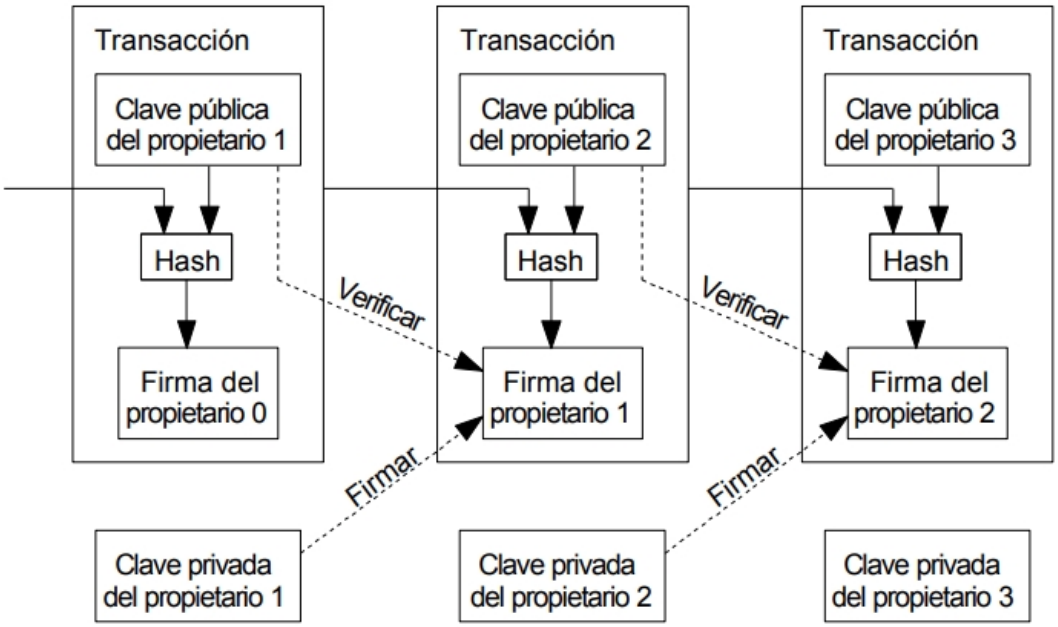

Figura 1: Flujo de firmas en una transacción

0.3.2.2. El Problema del Doble Gasto

En los sistemas digitales tradicionales, los datos pueden ser fácilmente duplicados, lo que presenta un desafío único para las monedas electrónicas: **¿Cómo prevenir que el mismo activo digital sea gastado más de una vez?**

Primero, expliquemos que es el problema del Doble Gasto:

El doble gasto ocurre cuando un propietario intenta usar la misma moneda en múltiples transacciones. Este problema se resuelve fácilmente en sistemas centralizados, donde una entidad confiable (como un banco) mantiene un registro maestro de todas las transacciones. Sin embargo, en un sistema descentralizado como Bitcoin, no existe tal entidad central.

En sistemas tradicionales, el problema se aborda mediante un intermediario que:

- Verifica cada transacción.
- Actualiza un registro centralizado, asegurando que las monedas no sean reutilizadas.

Bitcoin, al rechazar la necesidad de intermediarios, requiere un mecanismo que

permita a los participantes de la red acordar de manera autónoma y descentralizada qué transacciones son válidas.

0.3.2.3. Necesidad de un Registro Público Compartido

Para evitar el doble gasto sin un intermediario, es crucial que todos los nodos de la red mantengan un **registro único y compartido de transacciones**. Esto introduce un nuevo desafío: **¿Cómo garantizar que todos los nodos acuerden sobre el orden de las transacciones?** Bitcoin propone una solución innovadora: cada transacción debe ser anunciada públicamente. Esto permite que cualquier participante valide las transacciones y que todos los nodos trabajen con la misma información. Sin embargo, anunciar transacciones es una condición necesaria pero no suficiente. Necesitamos un mecanismo que:

- 1. Asegure que las transacciones se registren en un orden cronológico inmutable.
- 2. Proporcione una prueba de que un conjunto de transacciones existía en un momento específico.

0.3.3. Servidor de Sellado de Tiempo

0.3.3.1. Introducción

Para abordar la necesidad de un registro público compartido, Bitcoin introduce el concepto de un **servidor de sellado de tiempo**, una pieza fundamental en su diseño. Este mecanismo descentralizado garantiza que todas las transacciones se registren en un orden cronológico inmutable, evitando conflictos como el doble gasto y proporcionando un historial confiable y verificable.

0.3.3.2. Funcionamiento

El servidor de sellado de tiempo funciona tomando un conjunto de transacciones, agrupándolas en un bloque y calculando un **hash** de ese bloque. Este hash actúa como una huella digital única del contenido del bloque.

El proceso es el siguiente:

1. Se recopilan todas las transacciones pendientes en un bloque.
2. Se genera un **hash** del bloque, que sirve como identificador único.
3. El **hash** se publica públicamente, asegurando que cualquier alteración del bloque posterior sería evidente.

Para reforzar la seguridad, cada bloque incluye el **hash** del bloque anterior. Esto forma una **cadena de bloques** (*Blockchain*), donde cada bloque depende criptográficamente del anterior.

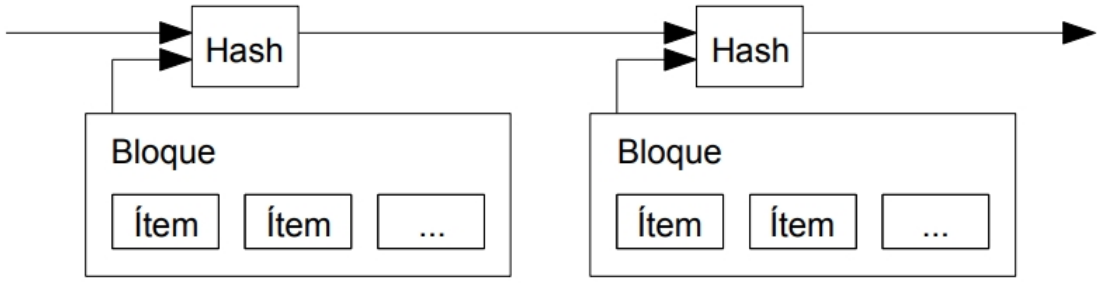

Figura 2: Ejemplo del funcionamiento del servidor de sellado de tiempo. Cada bloque contiene el hash del bloque anterior, formando una cadena inmutable.

0.3.3.3. Importancia del Encadenamiento

El encadenamiento de bloques asegura que cualquier intento de modificar una transacción pasada requeriría recalcular los **hashes** de todos los bloques subsiguientes. Esto haría computacionalmente inviable alterar el historial de transacciones.

Este mecanismo proporciona dos beneficios clave:

- **Inmutabilidad**: Una vez que una transacción se ha registrado y confirmado, no puede ser modificada.

- **Integridad**: La integridad del historial completo de transacciones puede ser verificada por cualquier nodo en la red.

0.3.3.4. Descentralización y Seguridad

En sistemas tradicionales, el servidor de sellado de tiempo podría ser centralizado, lo que lo haría vulnerable a ataques y fallos. Sin embargo, en Bitcoin, este servidor está distribuido entre todos los nodos de la red.

Para que este modelo distribuido funcione, se requiere un mecanismo que permita que todos los nodos acuerden sobre el orden de las transacciones sin necesidad de confianza mutua. Este mecanismo es la **prueba de trabajo** (*Proof of Work*), que se explicará en la siguiente sección.

0.3.4. Proof of Work

0.3.4.1. Introducción a la Prueba de Trabajo

La prueba de trabajo (*Proof of Work, PoW*) es un mecanismo clave que permite a Bitcoin mantener la integridad de su red descentralizada. Este sistema asegura que las transacciones y bloques sean válidos, resolviendo así uno de los mayores desafíos en la gestión de registros distribuidos: la necesidad de consenso sin intermediarios confiables.

0.3.4.2. Funcionamiento

El proceso de prueba de trabajo implica que los nodos de la red, también conocidos como *mineros*, deben resolver un problema matemático complejo para validar un bloque de transacciones. Este problema consiste en encontrar un valor (*nonce*) que, al ser combinado con el contenido del bloque y sometido a un algoritmo de hash (SHA-256), produzca un hash que cumpla con ciertos requisitos de dificultad (por ejemplo, que comience con un número específico de ceros).

El proceso puede ser resumido en los siguientes pasos:

1. El minero toma un bloque con un conjunto de transacciones.
2. Incrementa el valor del *nonce* y calcula el hash del bloque.
3. Verifica si el hash cumple con los requisitos de dificultad.
4. Si no cumple, repite el proceso con un nuevo *nonce*.
5. Cuando se encuentra un hash válido, el bloque se considera resuelto y es transmitido a la red.

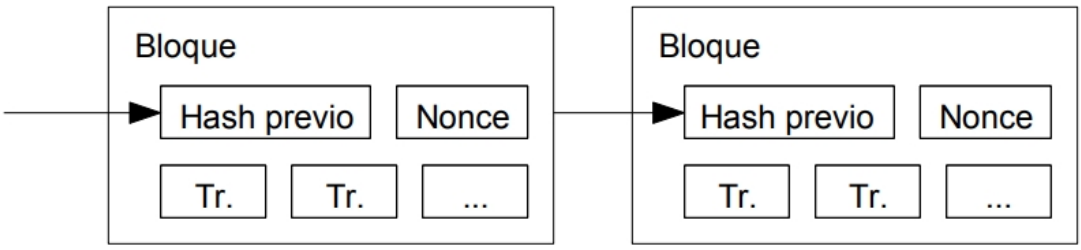

Figura 3: Ejemplo del proceso de Prueba de Trabajo. El objetivo es encontrar un hash que cumpla con los requisitos de dificultad.

0.3.4.3. Beneficios

La prueba de trabajo proporciona varios beneficios esenciales para la red Bitcoin:

- **Seguridad**: Cambiar un bloque requiere rehacer la prueba de trabajo no solo de ese bloque, sino también de todos los bloques posteriores, lo que es computacionalmente inviable.
- **Consenso Distribuido**: Los nodos de la red aceptan como válida la **cadena más larga**, es decir, la cadena con mayor acumulación de trabajo.
- **Prevención de Ataques Sybil**: Al basar el consenso en potencia computacional y no en la identidad de los nodos, se evita que un atacante controle la red mediante la creación de múltiples identidades falsas.

0.3.4.4. Ajuste de la Dificultad

Para mantener un tiempo promedio constante entre bloques (aproximadamente 10 minutos), Bitcoin ajusta automáticamente la dificultad del problema de hash cada 2016 bloques (aproximadamente cada dos semanas). Si los bloques se generan demasiado rápido o demasiado lento, la dificultad aumenta o disminuye, respectivamente.

La prueba de trabajo es el mecanismo que permite a Bitcoin descentralizar la toma de decisiones. Sin embargo, para que funcione eficientemente en una red distribuida, los nodos deben ser capaces de coordinarse y aceptar bloques válidos. En la siguiente sección se analizará cómo la red peer-to-peer de Bitcoin se organiza para

garantizar un consenso efectivo, permitiendo que todos los nodos trabajen de forma independiente pero coordinada.

0.3.5. Red Peer-to-Peer

0.3.5.1. Introducción

La red peer-to-peer es el componente fundamental que permite a Bitcoin operar de manera descentralizada. A diferencia de los sistemas tradicionales, donde una autoridad central coordina todas las transacciones, en Bitcoin todos los nodos de la red participan en la validación y propagación de las transacciones y bloques. Esto asegura que la red pueda operar sin un único punto de falla.

0.3.5.2. Funcionamiento

El proceso de coordinación en la red peer-to-peer de Bitcoin se puede resumir en los siguientes pasos:

1. **Transmisión de Transacciones**: Cuando un usuario genera una nueva transacción, esta se transmite a todos los nodos de la red.

2. **Recolección de Transacciones en Bloques**: Los nodos recopilan las transacciones no confirmadas en un bloque.

3. **Resolución de la Prueba de Trabajo**: Los nodos trabajan en resolver el problema de prueba de trabajo para validar el bloque.

4. **Propagación de Bloques Validados**: Una vez que un nodo resuelve la prueba de trabajo, transmite el bloque a la red.

5. **Validación por otros Nodos**: Los nodos verifican que el bloque y las transacciones contenidas en él sean válidas antes de aceptarlo.

6. **Extensión de la Cadena**: Los nodos aceptan el bloque válido y comienzan a trabajar en el siguiente bloque, utilizando el hash del bloque recién aceptado como referencia.

0.3.5.3. Manejo de Bifurcaciones

Dado que la red es distribuida, es posible que diferentes nodos reciban versiones conflictivas del próximo bloque al mismo tiempo, lo que crea una bifurcación en la cadena. Bitcoin resuelve este problema mediante el principio de la **cadena más larga**, que se define como la cadena con la mayor acumulación de trabajo computacional.

- **Detección de Bifurcaciones**: Los nodos pueden trabajar temporalmente en diferentes cadenas.
- **Resolución Automática**: Cuando se encuentra un nuevo bloque que extiende una de las cadenas, los nodos se alinean automáticamente con la cadena más larga.
- **Consistencia Eventual**: Este proceso asegura que la red converge hacia un único historial válido de transacciones.

0.3.5.4. Tolerancia a Fallos y Pérdida de Conexión

La red peer-to-peer es robusta frente a fallos. Los nodos pueden desconectarse y reconectarse en cualquier momento, aceptando la cadena más larga como el estado actual de la red. Además, no es necesario que todas las transacciones lleguen a todos los nodos inmediatamente, basta con que alcancen a la mayoría de los nodos para ser incluidas en un bloque y propagadas de manera eficiente.

0.3.6. Incentivos

0.3.6.1. Introducción

La participación activa de los nodos es esencial para que Bitcoin funcione de manera eficiente y la red se mantenga operativa. Dado que no existe un sistema centralizado, se requiere un modelo de incentivos que motive a los participantes a dedicar recursos computacionales a la validación de transacciones y la creación de bloques. Bitcoin logra esto mediante un sistema de recompensas y comisiones, asegurando así la contribución continua de los nodos a la red.

0.3.6.2. Recompensa por Bloque

Cada vez que un nodo (o minero) resuelve un bloque, recibe una recompensa en forma de nuevas monedas. Esta recompensa es conocida como **recompensa por bloque** y sirve como el mecanismo principal para introducir nuevas monedas en circulación.

- **Naturaleza Deflacionaria**: La recompensa por bloque disminuye aproximadamente cada cuatro años, en un proceso conocido como **halving**, hasta que se alcance el límite máximo de 21 millones de bitcoins.
- **Analogía con la Minería de Oro**: Así como los mineros de oro consumen recursos para extraer oro, los mineros de Bitcoin consumen tiempo de CPU y electricidad para generar nuevas monedas.

0.3.6.3. Comisiones por Transacción

Además de la recompensa por bloque, los mineros también reciben **comisiones por transacción**. Estas comisiones se derivan de la diferencia entre la cantidad de entrada y salida de una transacción, y se incluyen en el bloque que valida el minero.

- **Sostenibilidad a Largo Plazo**: A medida que la recompensa por bloque disminuya con el tiempo, las comisiones por transacción se convertirán en la principal fuente de ingresos para los mineros.
- **Incentivo a la Prioridad**: Las transacciones con comisiones más altas suelen ser procesadas con mayor rapidez, ya que los mineros prefieren incluirlas en sus bloques.

0.3.6.4. Seguridad y Honestidad de la Red

El sistema de incentivos no solo asegura la participación de los mineros, sino que también refuerza la seguridad y la honestidad de la red:

- **Dificultad de Ataques**: Un atacante que quiera desestabilizar la red necesitaría controlar la mayoría de la potencia computacional, lo que sería extremadamente costoso.

- **Equilibrio Económico**: Para un atacante, seguir las reglas y participar honestamente en la red es más rentable que intentar subvertir el sistema.

Si bien el sistema de incentivos asegura la participación y seguridad de la red, el crecimiento continuo de la *Blockchain* plantea desafíos de almacenamiento. Bitcoin aborda este problema mediante técnicas de optimización como la **recuperación de espacio de disco**.

0.3.7. Recuperación de Espacio de Disco

0.3.7.1. Introducción

A medida que Bitcoin crece, la cadena de bloques (*Blockchain*) acumula un historial completo de todas las transacciones realizadas. Aunque esto garantiza la transparencia y la inmutabilidad, también plantea un desafío: el tamaño de la *Blockchain* puede llegar a ser considerable, aumentando la carga de almacenamiento para los nodos participantes.

Para abordar este problema, Bitcoin implementa técnicas que permiten la recuperación de espacio de disco, asegurando que los nodos puedan operar de manera eficiente sin sacrificar la integridad del sistema.

0.3.7.2. Uso del Árbol de Merkle

La clave para optimizar el almacenamiento radica en el uso de una estructura de datos conocida como **Árbol de Merkle**. Esta estructura permite compactar los datos de transacciones en cada bloque mientras se mantiene la capacidad de verificar la integridad de las transacciones.

- **Raíz de Merkle**: Cada bloque almacena solo la raíz del Árbol de Merkle, lo que permite a los nodos verificar si una transacción pertenece al bloque sin necesidad de almacenar todas las transacciones.

- **Podado de Ramas**: Una vez que una transacción ha sido enterrada bajo suficientes bloques (es decir, ha sido ampliamente confirmada), las transacciones individuales y sus nodos intermedios en el Árbol de Merkle pueden ser eliminados, dejando solo la raíz.

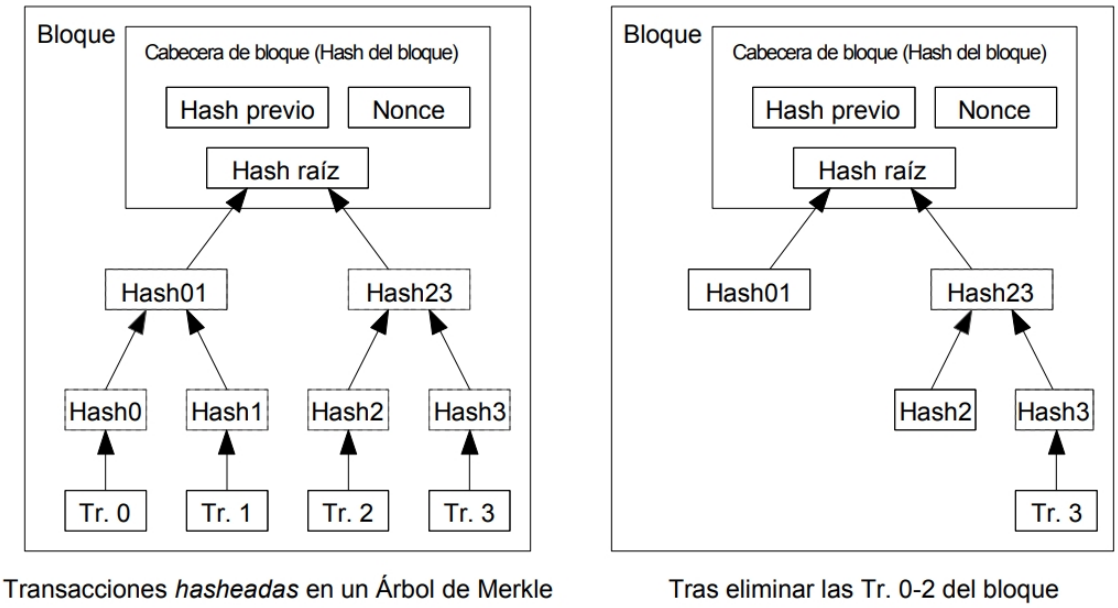

Figura 4: Estructura de un Árbol de Merkle utilizado para compactar transacciones en un bloque.

0.3.7.3. Compactación de Bloques Antiguos

Bitcoin permite que los nodos compacten bloques antiguos mediante un proceso conocido como **pruning** (podado). En este proceso, se eliminan las transacciones individuales de los bloques más antiguos, conservando únicamente las cabeceras de bloque y la raíz del Árbol de Merkle.

- **Reducción de Requisitos de Almacenamiento**: Las cabeceras de bloque son significativamente más pequeñas que los bloques completos, lo que reduce drásticamente la carga de almacenamiento.
- **Conservación de la Integridad**: A pesar de la compactación, la estructura de la *Blockchain* sigue siendo verificable gracias a la inclusión de las raíces de Merkle en las cabeceras.

0.3.7.4. Escalabilidad y Sostenibilidad

Estas optimizaciones aseguran que la *Blockchain* de Bitcoin pueda seguir creciendo sin que los requisitos de almacenamiento se vuelvan prohibitivos. Además, permiten que incluso dispositivos con recursos limitados puedan participar como nodos en la red, contribuyendo a la descentralización y la resistencia del sistema.

0.3.8. Verificación Simplificada de Pagos

0.3.8.1. Introducción

En Bitcoin, no todos los usuarios necesitan operar un nodo completo que almacene la totalidad de la *Blockchain*. Para aquellos con recursos limitados o necesidades más simples, el protocolo permite una forma de **verificación simplificada de pagos** (*Simplified Payment Verification*, SPV). Este método permite verificar transacciones sin necesidad de descargar y almacenar la cadena completa, manteniendo un equilibrio entre eficiencia y seguridad.

0.3.8.2. Funcionamiento

El proceso de SPV se basa en la capacidad de verificar que una transacción específica ha sido incluida en un bloque de la *Blockchain*. Esto se logra utilizando únicamente las **cabeceras de bloque** y las **ramas de Merkle**.

1. El usuario descarga solo las cabeceras de los bloques, que contienen el hash del bloque anterior, la raíz del Árbol de Merkle y la información de la prueba de trabajo.

2. Para verificar una transacción, el usuario solicita la rama de Merkle correspondiente, que conecta la transacción con la raíz del Árbol de Merkle almacenada en la cabecera del bloque.

3. Si la transacción está correctamente conectada a la raíz de Merkle y la cabecera del bloque está en la cadena más larga validada por la red, la transacción es considerada válida.

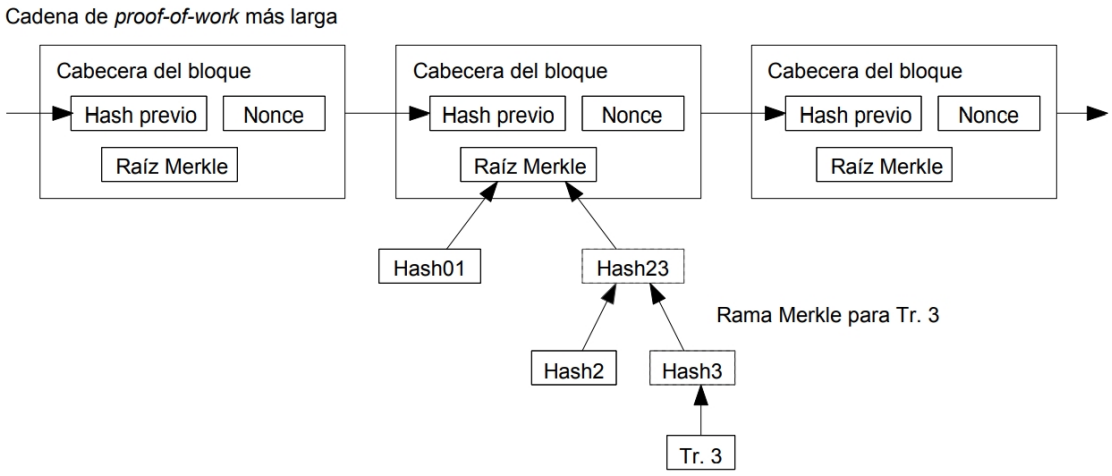

Figura 5: Esquema de Verificación Simplificada de Pagos (SPV). El usuario utiliza cabeceras de bloque y ramas de Merkle para verificar transacciones.

0.3.8.3. Ventajas

El método SPV ofrece varias ventajas para los usuarios:

- **Eficiencia**: Los usuarios no necesitan almacenar la *Blockchain* completa, lo que reduce significativamente los requisitos de almacenamiento y ancho de banda.
- **Accesibilidad**: Dispositivos con recursos limitados, como teléfonos móviles, pueden participar en la red Bitcoin.
- **Seguridad Suficiente**: Aunque no proporciona la misma seguridad que un nodo completo, SPV es lo suficientemente seguro para la mayoría de los casos de uso cotidianos.

0.3.8.4. Limitaciones

A pesar de sus beneficios, SPV tiene ciertas limitaciones:

- **Dependencia de Nodos Completos**: SPV requiere confiar en nodos completos para obtener las cabeceras de bloque y las ramas de Merkle.
- **Mayor Vulnerabilidad a Ataques**: Si un atacante controla la mayoría de la red, podría engañar a los clientes SPV al proporcionar información falsa.

0.3.9. Privacidad

0.3.9.1. Introducción

En sistemas financieros tradicionales, la privacidad se garantiza limitando el acceso a la información sobre las transacciones a las partes involucradas y a un intermediario de confianza, como un banco. Sin embargo, en Bitcoin, todas las transacciones son públicas y están registradas en la *Blockchain*. Esto plantea un desafío: **¿cómo proteger la identidad de los usuarios en un sistema transparente?**

0.3.9.2. Privacidad mediante Claves Públicas Anónimas

Bitcoin aborda el problema de la privacidad utilizando un sistema de **claves públicas anónimas**. Cada usuario opera con una clave pública, que no está directamente vinculada a su identidad personal.

- **Anonimato Relativo**: El público puede ver que una dirección específica está enviando fondos a otra dirección, pero no puede identificar fácilmente a las personas detrás de esas direcciones.

- **Uso de Nuevas Direcciones**: Para aumentar la privacidad, se recomienda que los usuarios generen un nuevo par de claves (nueva dirección) para cada transacción, dificultando la correlación entre transacciones.

0.3.9.3. Vulnerabilidades y Vinculación de Transacciones

A pesar de estas medidas, la privacidad en Bitcoin no es absoluta. Existen vulnerabilidades que pueden comprometer el anonimato:

- **Análisis de Cadena**: Al observar el flujo de transacciones en la *Blockchain*, un atacante podría vincular múltiples direcciones a un mismo usuario.

- **Transacciones Multientrada**: Cuando un usuario combina múltiples entradas en una sola transacción, revela que esas entradas pertenecen al mismo propietario, facilitando la vinculación.

0.3.9.4. Comparación con la Privacidad Tradicional

En comparación con los sistemas financieros tradicionales, Bitcoin ofrece una privacidad basada en el anonimato de las claves públicas, pero carece de confidencialidad total debido a la transparencia de la *Blockchain*.

0.3.10. Cálculos y Seguridad Matemática

0.3.10.1. Introducción

La seguridad de Bitcoin se basa en principios matemáticos y criptográficos que garantizan la integridad de la red y la invulnerabilidad frente a ciertos tipos de ataques. Uno de los principales desafíos es prevenir que un atacante pueda sobrescribir la *Blockchain* con una cadena alternativa, conocida como el **problema del doble gasto**.

0.3.10.2. El Problema del Doble Gasto y la Cadena Honesta

En Bitcoin, un atacante podría intentar generar una cadena alternativa con el objetivo de sobrescribir una transacción ya confirmada. Esto implicaría crear bloques que contengan transacciones fraudulentas y hacer que esta cadena supere en longitud a la cadena honesta.

Para evitar esto, Bitcoin emplea la **prueba de trabajo** (Proof of Work), que hace computacionalmente difícil construir una cadena falsa. Mientras la mayoría de la potencia computacional esté en manos de nodos honestos, la cadena honesta siempre crecerá más rápido que la cadena de un atacante.

0.3.10.3. Modelo Matemático de Seguridad

La probabilidad de que un atacante logre superar a la cadena honesta se puede modelar como un *paseo aleatorio* binomial. Este problema es matemáticamente equivalente al problema de la **ruina del jugador**.

- **Definición de Variables**:
  - p: Probabilidad de que un nodo honesto encuentre el siguiente bloque.

- q: Probabilidad de que el atacante encuentre el siguiente bloque, donde $q < p$.
- z: Número de bloques que el atacante está detrás de la cadena honesta.

- **Fórmula de Éxito del Atacante**:

$$q_z = \begin{cases} 1 & \text{si } q \geq p, \\ \left(\frac{q}{p}\right)^z & \text{si } q < p. \end{cases}$$

  Esta fórmula muestra que la probabilidad de que un atacante supere a la cadena honesta disminuye exponencialmente con el número de bloques que el atacante está detrás.

0.3.10.4. Implicaciones Prácticas

- **Confirmaciones de Bloques**: Cuantos más bloques se añaden tras una transacción, menor es la probabilidad de que pueda ser revertida. Por convención, se considera que una transacción es segura después de 6 confirmaciones de bloque.

- **Coste de Ataques**: Para un atacante, intentar sobrescribir una transacción sería extremadamente costoso, ya que requeriría controlar más del 50 % de la potencia computacional de la red.

0.3.10.5. Resiliencia Frente a Ataques

Bitcoin es resistente no solo a ataques individuales, sino también a escenarios más complejos como:

- **Ataques de Reorganización de Cadena**: Donde se intenta alterar bloques confirmados.

- **Ataques del 51 %**: Un atacante necesitaría controlar la mayoría de la potencia computacional, algo económicamente inviable en una red suficientemente descentralizada.

La robustez matemática de Bitcoin garantiza que incluso con recursos limitados, los nodos honestos pueden mantener la integridad de la red frente a atacantes poderosos.

0.3.11. Conclusión

0.3.11.1. Resumen de Problemas y Soluciones Propuestas

A lo largo de esta tesis, hemos identificado y analizado los principales problemas del sistema de votación argentino actual, incluyendo fraudes como el robo de boletas, el voto cadena, las urnas embarazadas y la manipulación de votos durante el conteo.

Por otro lado, también se destacaron las fortalezas de la tecnología *Blockchain*, cuyo diseño resuelve problemas similares en el ámbito de las criptomonedas. A continuación, se sintetiza cómo cada desafío electoral puede ser mitigado mediante *Blockchain*:

- **Integridad e Inmutabilidad del Voto**: *Blockchain* asegura que cada voto, una vez registrado, no pueda ser alterado o eliminado. Esto evita problemas como la manipulación de boletas o la adulteración de urnas, garantizando que cada voto cuente tal como fue emitido.

- **Prevención del Voto Doble o Cadena**: Utilizando el modelo de transacciones de Bitcoin, cada voto se registra como una transacción única en la *Blockchain*. La estructura descentralizada y el uso de un sistema de consenso (como prueba de trabajo) garantizan que ningún voto pueda ser emitido más de una vez.

- **Transparencia y Auditabilidad**: La *Blockchain* proporciona un registro público y auditable, donde cualquier ciudadano o entidad puede verificar el conteo de votos sin comprometer la privacidad de los votantes. Esto resuelve la falta de transparencia en el escrutinio.

- **Privacidad del Votante**: Mediante el uso de claves públicas anónimas, se asegura que la identidad del votante no pueda ser asociada directamente con su voto, preservando el secreto del sufragio.

- **Descentralización y Resiliencia**: Al no depender de una autoridad central, el sistema es resistente a ataques o manipulaciones que suelen aprovechar las vulnerabilidades de una infraestructura centralizada. Esto reduce significativamente la posibilidad de fraudes organizados, como el voto cadena o la suplantación de identidad.

0.3.11.2. Limitaciones de *Blockchain* en el Contexto Electoral

A pesar de las soluciones que *Blockchain* ofrece a varios problemas del sistema electoral, aún persisten desafíos que esta tecnología por sí sola no puede resolver. Uno de estos problemas es el **fraude durante el conteo de votos**. Aunque *Blockchain* garantiza que los votos registrados no puedan ser alterados, no aborda el riesgo de manipulación en el proceso de consolidación y conteo final de los votos.

El conteo de votos es una etapa crítica donde se pueden cometer errores, ya sean accidentales o intencionales. Para superar este desafío, es necesario incorporar tecnologías complementarias que automaticen y aseguren esta fase del proceso electoral.

Para abordar las limitaciones mencionadas, proponemos el uso de ***Smart Contracts***. Estos contratos inteligentes permiten la automatización del conteo de votos, asegurando que el proceso se realice de manera transparente, precisa y sin intervención humana.

Los *Smart Contracts*, al ser programas autoejecutables almacenados en la *Blockchain*, pueden:

- **Automatizar el Conteo de Votos**: Garantizando un cálculo preciso y verificable de los resultados.
- **Reducir la Intervención Humana**: Minimizar el riesgo de errores o manipulaciones deliberadas durante el escrutinio.
- **Publicar Resultados en Tiempo Real**: Proporcionando mayor transparencia al proceso electoral.

En el próximo capítulo, exploraremos cómo los *Smart Contracts* pueden integrarse en el sistema propuesto para abordar los problemas del conteo de votos y completar un sistema de votación electrónica seguro y confiable.

0.4. Smart Contracts

0.4.1. Definición y Principios Fundamentales

Un *Smart Contract*, o contrato inteligente, es un programa almacenado en una *Blockchain* que se ejecuta automáticamente al cumplirse ciertas condiciones predefinidas. Estos contratos permiten la transferencia de activos digitales o la realización de operaciones complejas de manera descentralizada, sin necesidad de intermediarios, garantizando transparencia, seguridad e inmutabilidad [1].

Ethereum revolucionó este concepto al introducir una *Blockchain* con capacidad de ejecutar programas **Turing-Completos**, permitiendo la implementación de sistemas complejos de transición de estados que pueden representar desde contratos financieros hasta organizaciones autónomas descentralizadas (DAO, por sus siglas en inglés).

0.4.2. Características Principales

Los *Smart Contracts* en Ethereum presentan características que los diferencian de otros sistemas de contratos digitales:

- **Turing-completitud**: Los contratos en Ethereum pueden ejecutar cualquier operación computacional concebible, habilitando funciones avanzadas como bucles y recursión.

- **Inmutabilidad**: Una vez desplegado en la *Blockchain*, el contrato no puede ser alterado, asegurando que las reglas iniciales del acuerdo se mantengan intactas.

- **Autoejecución**: Se ejecutan automáticamente al cumplirse las condiciones establecidas en el código.

- **Transparencia y Auditabilidad**: Todos los contratos son visibles en la *Blockchain*, permitiendo la verificación pública de sus operaciones.

0.4.3. Estructura y Funcionamiento

En Ethereum, los contratos inteligentes son ejecutados por la Ethereum Virtual Machine (EVM), una máquina virtual que procesa instrucciones de bajo nivel almacenadas en la *Blockchain*. Cada contrato cuenta con:

- Una dirección única.
- Un código asociado que define su comportamiento.
- Un estado almacenado que puede modificarse durante la ejecución.

Los usuarios interactúan con los contratos mediante transacciones, que pueden activar funciones específicas del contrato, enviar datos o transferir activos como *ether*.

0.4.4. Aplicaciones

Los *Smart Contracts* permiten la implementación de aplicaciones descentralizadas (dApps), abarcando sectores diversos:

- **Finanzas Descentralizadas (DeFi)**: Incluyen préstamos, intercambios y derivados financieros.
- **Organizaciones Autónomas Descentralizadas (DAO)**: Gestión automatizada de fondos y toma de decisiones basada en contratos inteligentes.
- **Sistemas de Votación Electrónica**: Automatizan el registro, conteo y auditoría de votos, asegurando transparencia y eficiencia.

0.4.5. Ventajas y Limitaciones

0.4.5.1. Ventajas

- Reducción de costos y tiempos al eliminar intermediarios.
- Mayor seguridad al operar sobre *Blockchain*.
- Posibilidad de auditar todas las operaciones realizadas.

0.4.5.2. Limitaciones

- **Errores en el código**: Un contrato mal programado puede ser explotado, como ocurrió en el incidente de *The DAO* [5].
- **Costo de ejecución**: Cada operación tiene un costo asociado en gas, lo que puede limitar su uso en sistemas complejos.
- **Dependencia de oráculos**: Para interactuar con datos externos, los contratos requieren oráculos que actúan como intermediarios, introduciendo posibles vulnerabilidades.

0.5. Conclusiones Finales

0.5.1. Resumen de Soluciones Propuestas

A lo largo de esta tesis, hemos explorado cómo la tecnología *Blockchain*, complementada con *Smart Contracts*, puede transformar el sistema de votación electrónica, abordando vulnerabilidades presentes en el sistema electoral tradicional. En especifico, el uso de *Smart Contracts* en un sistema de votación electrónica tiene el potencial de abordar problemas pendientes, como la transparencia en el conteo de votos y la automatización de procesos críticos.

0.5.1.1. Problemas Resueltos por *Blockchain*

Blockchain, como se describió en capítulos anteriores, resuelve problemas clave relacionados con la integridad, transparencia y descentralización:

- Garantiza la **inmutabilidad** de los votos, eliminando riesgos de manipulación.
- Previene el **voto doble** mediante un registro único y descentralizado.
- Proporciona **transparencia y auditabilidad**, permitiendo que los ciudadanos verifiquen los resultados sin comprometer su privacidad.
- Asegura la **privacidad del votante** mediante claves públicas anónimas.

Sin embargo, como se destacó, *Blockchain* por sí sola no resuelve el problema del conteo de votos y la automatización del escrutinio, etapas críticas donde pueden ocurrir errores o manipulaciones. Este desafío requiere la integración de *Smart Contracts*.

0.5.1.2. Contribución de los *Smart Contracts*

Los *Smart Contracts* complementan las capacidades de la *Blockchain* al automatizar procesos clave, como el conteo de votos, la validación y la publicación de resultados. Esto permite abordar problemas específicos que *Blockchain* no resuelve completamente:

- **Automatización del Conteo de Votos**: Los *Smart Contracts* realizan cálculos precisos en tiempo real, minimizando errores humanos y manipulaciones deliberadas.
- **Reducción de la Intervención Humana**: Al eliminar la necesidad de contar votos manualmente, se garantiza un escrutinio objetivo e imparcial.
- **Publicación de Resultados en Tiempo Real**: Los resultados se registran directamente en la *Blockchain*, haciendo que sean accesibles de forma inmediata y verificable para todas las partes interesadas.

0.5.2. Modelo Propuesto para un Sistema de Votación Electrónica

Integrando *Blockchain* y *Smart Contracts*, el modelo propuesto para un sistema de votación electrónica incluye las siguientes características:

- **Registro de Votantes**: Cada votante recibe una clave privada única, asociada a una clave pública anónima, que garantiza su autenticidad y privacidad.
- **Emisión de Votos**: Los votos se registran como transacciones en la *Blockchain*, asegurando que cada voto sea único y verificable.

- **Conteo Automatizado con *Smart Contracts***: Un *Smart Contract* se encarga de sumar los votos en tiempo real y publicar los resultados en la *Blockchain*.
- **Auditabilidad Transparente**: Cualquier ciudadano puede verificar el conteo accediendo al registro público, sin comprometer el secreto del voto.

0.5.3. Ventajas del Modelo Propuesto

- **Seguridad y Confianza**: La combinación de *Blockchain* y *Smart Contracts* garantiza un sistema resistente a manipulaciones y ciberataques.
- **Transparencia Total**: Cada etapa del proceso electoral es auditable por las partes interesadas, mejorando la confianza del público en los resultados.
- **Reducción de Costos y Eficiencia Operativa**: Al no necesitar boletas de papel, se disminuyen los costos asociados a la impresión masiva de las mismas. Además, al automatizar procesos como el conteo de votos se disminuyen los costos asociados al personal y se optimiza la logística electoral.

0.5.4. Desafíos y Trabajo Futuro

A pesar de sus ventajas, implementar este modelo en el contexto argentino presenta desafíos significativos:

- **Infraestructura Tecnológica**: Es necesario garantizar acceso a tecnologías modernas para todos los votantes, especialmente en zonas rurales.
- **Adaptación del Marco Legal**: Las leyes electorales deben modificarse para aceptar y regular el uso de *Blockchain* y *Smart Contracts* en elecciones.
- **Educación Pública y Confianza**: Es crucial educar al público y a las autoridades sobre los beneficios y limitaciones de la tecnología, asegurando su aceptación.

El trabajo futuro debe enfocarse en pruebas piloto que validen la viabilidad técnica y operativa del modelo propuesto, así como en la creación de un marco legal que permita su implementación.

0.5.5. Conclusión Final

A lo largo de esta tesis, hemos analizado profundamente las vulnerabilidades inherentes al sistema de votación argentino y las posibilidades que ofrecen las tecnologías emergentes, específicamente la *Blockchain* y los *Smart Contracts*, para mitigar estas problemáticas. Este estudio ha puesto en evidencia que, aunque el sistema actual tiene mecanismos destinados a garantizar la transparencia, la seguridad y la equidad, sigue siendo vulnerable a fraudes como el voto cadena, el robo de boletas y las urnas embarazadas, entre otros.

La integración de tecnologías como la *Blockchain* en sistemas de votación electrónica presenta una oportunidad sin precedentes para transformar el sistema electoral. Su capacidad para garantizar la inmutabilidad de los datos registrados, prevenir el doble voto y ofrecer transparencia sin comprometer la privacidad del votante, la posiciona como una herramienta crucial para fortalecer la confianza pública en los procesos democráticos.

Por otro lado, los *Smart Contracts* complementan esta tecnología al permitir la automatización de procesos críticos como el conteo de votos, la validación de resultados y la publicación transparente de los mismos. Al eliminar la intervención humana en estas etapas, se reducen significativamente los riesgos de errores o manipulaciones intencionales. La implementación conjunta de *Blockchain* y *Smart Contracts* permite no solo resolver los problemas actuales, sino también ofrecer una solución escalable y adaptable a diferentes contextos electorales.

Sin embargo, también es importante destacar las limitaciones y desafíos que estas tecnologías conllevan. La implementación de un sistema basado en *Blockchain* requiere infraestructura tecnológica avanzada, la cual no siempre está disponible en contextos de países en desarrollo. Asimismo, la aceptación social de un cambio tan radical en la manera de votar dependerá de la claridad con la que se explique el nuevo sistema y de la confianza que se genere en el mismo, asegurando que todos los votantes comprendan su funcionamiento y los beneficios que ofrece. Los costos asociados con la implementación inicial y el mantenimiento del sistema también deben ser considerados, aunque se espera que a largo plazo estos sean menores que los de los sistemas tradicionales.

En esta tesis, hemos explorado cómo estas tecnologías pueden aplicarse en el

contexto argentino, considerando tanto sus fortalezas como sus limitaciones. Los ejemplos internacionales, como los sistemas implementados en Estonia y Suiza, proporcionan una base sólida para demostrar la viabilidad de estas soluciones, siempre y cuando sean adaptadas a las particularidades culturales, legales y logísticas del entorno local.

Finalmente, esta investigación no solo propone un modelo de sistema de votación electrónica seguro y confiable, sino que también abre la puerta a futuras investigaciones y desarrollos en el ámbito de las tecnologías aplicadas a la democracia. Entre los desafíos a abordar se encuentran la interoperabilidad con sistemas existentes, la regulación específica para sistemas *Blockchain* y el diseño de interfaces accesibles que permitan la inclusión de todos los ciudadanos, independientemente de su nivel tecnológico.

En conclusión, la adopción de *Blockchain* y *Smart Contracts* en sistemas de votación electrónica representa una evolución necesaria para responder a los desafíos del siglo XXI en materia electoral. Aunque el camino hacia su implementación está lleno de retos, los beneficios potenciales en términos de transparencia, seguridad y confianza pública justifican plenamente su exploración y desarrollo. Esta tesis constituye un aporte inicial para ese proceso, proporcionando una base teórica y práctica para futuros trabajos en este campo.

Bibliografía

[1] Buterin, V. Ethereum whitepaper, 2014.

[2] Coinbase. ¿Qué es un contrato inteligente?, 2023.

[3] DiarioBitcoin. Zug prueba con éxito sistema de votación diseñado con tecnología blockchain, 2024.

[4] Ethereum Foundation. Introduction to smart contracts, 2023.

[5] Gemini. The dao hack: Understanding decentralized finance (defi), 2024.

[6] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system, 2008.

[7] Smartmatic. Estonia: La solución de votación en línea más avanzada y confiable, 2024.

[8] Solana Foundation. Programs, 2023.