Oráculos - Caso particular ChainLink

Autor: Alejandro Becerra Acevedo (alejandro.becerraa@udea.edu.co)

RESUMEN

Este artículo examina el rol cada vez más relevante de Chainlink como una solución de oráculo descentralizado, clave para mejorar la funcionalidad de las blockchains al conectar de forma segura datos del mundo real con contratos inteligentes. Se sintetizan hallazgos de investigaciones académicas y artículos técnicos, que incluyen estudios sobre arquitecturas de oráculos, modelos de confianza y los retos específicos enfrentados en el ámbito de las finanzas descentralizadas (DeFi), particularmente con los feeds de precios. Se destaca la hoja de ruta de Chainlink 2.0, la cual pretende mejorar la escalabilidad y la seguridad. Los hallazgos subrayan el papel crucial de Chainlink en el avance de redes de oráculos descentralizados y en la resolución de casos de uso en el mundo real.

PALABRAS CLAVE: Blockchain, descentralización, oráculo, contratos inteligentes, Chainlink, feeds, cripto-economía.

I. INTRODUCCIÓN

La tecnología blockchain, aunque ha mejorado la automatización a través de contratos inteligentes, presenta limitaciones cuando se trata de interactuar con datos externos de manera segura y confiable. Para abordar este desafío, los oráculos se han convertido en un componente crucial, permitiendo la conexión de blockchains con información del mundo real. Chainlink ha surgido como uno de los líderes en este ámbito, ofreciendo una solución descentralizada que garantiza la seguridad y precisión de los datos transferidos a los contratos inteligentes [1]. La propuesta de Chainlink mejora la fiabilidad de los datos externos mediante la descentralización, lo que reduce significativamente los riesgos de manipulación y puntos únicos de falla.

Una de las principales ventajas de Chainlink en comparación con otros oráculos es su arquitectura basada en múltiples nodos independientes, lo que refuerza la confiabilidad de los datos suministrados [2]. Este enfoque descentralizado podría validar la información de manera distribuida, asegurando que los contratos inteligentes reciban datos exactos y verificables. Sin embargo, como en toda tecnología, existen desafíos. Entre ellos, destacan los costos operativos de los nodos y la posible latencia en la transmisión de datos [4].

Chainlink ha seguido evolucionando para abordar estos desafíos, tal como se destaca en la propuesta de Chainlink 2.0. Esta nueva versión introduce mejoras significativas, como mayor escalabilidad y seguridad, además de nuevas funcionalidades para mejorar el rendimiento de los oráculos [3]. Estas mejoras posicionan a Chainlink como una solución robusta y escalable, capaz de continuar resolviendo los problemas asociados a la integración de datos externos en blockchains.

II. DEFINICIÓN DE ORACLE

Un oráculo en blockchain es un servicio intermediario que proporciona datos externos a un contrato inteligente, permitiendo la integración de información del "mundo real" dentro de un entorno blockchain. Dado que los contratos inteligentes no pueden acceder de forma nativa a datos externos a la red blockchain (off-chain), los oráculos actúan como puentes entre el blockchain y el mundo exterior. Este vínculo es esencial para ejecutar la lógica de los contratos en función de eventos o datos externos, como precios de mercado, clima, o resultados de sensores de IoT [1]. Los oráculos son los encargados de gestionar y determinar el comportamiento del mercado para los Blockchain con sus respectivos intercambios de valor, ya sea en moneda digital o papel moneda.

Se puede ver los oráculos como una parte fundamental del comportamiento financiero y de transferencia de datos que requieren las diferentes Blokchains con sus respectivos valores dentro del mercado que constantemente están siendo estimulados por la oferta y la demanda de la moneda virtual.

III. ORÁCULOS CENTRALIZADOS Y DESCENTRALIZADOS

Oráculos Centralizados: Un oráculo centralizado está controlado por una única entidad que es el único proveedor de información para el contrato inteligente [1]. Se entiende que toda la información que recibe el contrato inteligente proviene de esta única fuente, lo que centraliza el control y permite agilizar la transmisión de datos. Sin embargo, esta centralización presenta riesgos significativos, ya que una manipulación o fallo en el oráculo centralizado puede afectar directamente el funcionamiento del contrato inteligente.

Oráculos Descentralizados: Comparten algunos de los mismos objetivos que los blockchains públicos, como evitar el riesgo de contraparte [1]. Los oráculos descentralizados distribuyen la responsabilidad de proporcionar información entre varios nodos o fuentes de

datos. En lugar de depender de un solo proveedor, estos oráculos combinan datos de varias fuentes y utilizan un sistema de consenso para validar la información antes de entregarla al contrato inteligente. Este enfoque busca mitigar los riesgos de manipulación y aumentar la fiabilidad y seguridad de los datos al eliminar el "punto único de fallo".

La principal diferencia entre los oráculos centralizados y los descentralizados radica en la estructura de confianza y control [2]. Los oráculos centralizados son rápidos y directos, ya que dependen de una sola entidad para transmitir datos, lo que permite un procesamiento de datos más veloz. Sin embargo, este enfoque centralizado implica que el sistema depende completamente de la integridad de esa única entidad, lo que puede generar vulnerabilidades y hacer que el contrato inteligente sea más susceptible a manipulaciones o fallos técnicos.

Por el contrario, los oráculos descentralizados aumentan la seguridad y fiabilidad al distribuir la responsabilidad entre varios nodos. Al utilizar un consenso, estos oráculos aseguran que los datos presentados sean precisos y representen la información de múltiples fuentes. Aunque el modelo descentralizado incrementa la confianza en la integridad de los datos, puede ser más complejo y lento, ya que involucra la validación de información por parte de múltiples participantes antes de llegar a un consenso.

Debilidades y Fortalezas

Oráculos Centralizados:

Fortalezas: Velocidad y simplicidad en la transmisión de datos. Al depender de una única fuente, los oráculos centralizados pueden proporcionar información de manera más rápida y con menor uso de recursos.
Debilidades: Riesgo de un "punto único de fallo" y vulnerabilidad frente a manipulaciones. Cualquier error o ataque a la entidad centralizada afecta directamente al contrato inteligente.

Oráculos Descentralizados:

Fortalezas: Mayor seguridad y resistencia a manipulaciones. La descentralización reduce los riesgos de corrupción de datos, ya que los nodos deben llegar a un consenso. Además, este modelo se alinea mejor con la filosofía de transparencia y seguridad de las blockchains.

Debilidades: Procesamiento más lento y mayor complejidad técnica, ya que requiere la colaboración de múltiples nodos y el uso de recursos adicionales para alcanzar un consenso.

IV. ARQUITECTURA

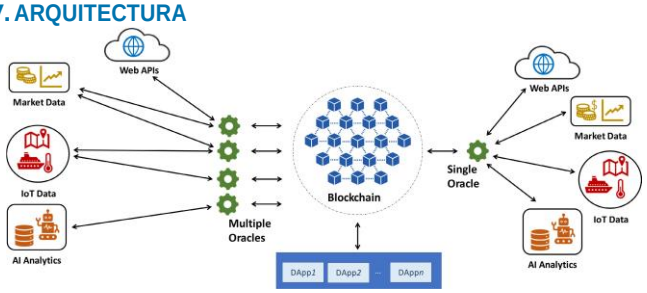


Figura 1. Rol de lo Oráculos en el sistema blockchain [2].

En la figura anterior, se puede apreciar el comportamiento de los oráculos dentro del sistema de cadenas en la blockchain. Estos oráculos actúan como intermediarios cruciales que permiten la transferencia de información entre el entorno externo y la blockchain. Al comparar los oráculos centralizados con los descentralizados, se observa que los oráculos centralizados dependen de una única fuente de datos, lo que puede generar problemas de confiabilidad y vulnerabilidad. Esta dependencia puede comprometer la seguridad de los contratos inteligentes y el ecosistema blockchain en su conjunto.

Además, los oráculos desempeñan un papel fundamental en la obtención de datos fuera de la cadena (off-chain), lo que permite que los contratos inteligentes respondan a eventos del mundo real. Por ejemplo, pueden proporcionar información sobre precios de activos, resultados de eventos deportivos o condiciones meteorológicas, entre otros. Este flujo de información es vital para la funcionalidad de muchas aplicaciones descentralizadas, ya que, sin una conexión confiable con el mundo exterior, los contratos inteligentes perderían gran parte de su utilidad. La implementación efectiva de oráculos asegura que la blockchain pueda interactuar con datos externos de manera precisa y segura.

V. ORACLES TAXONOMY

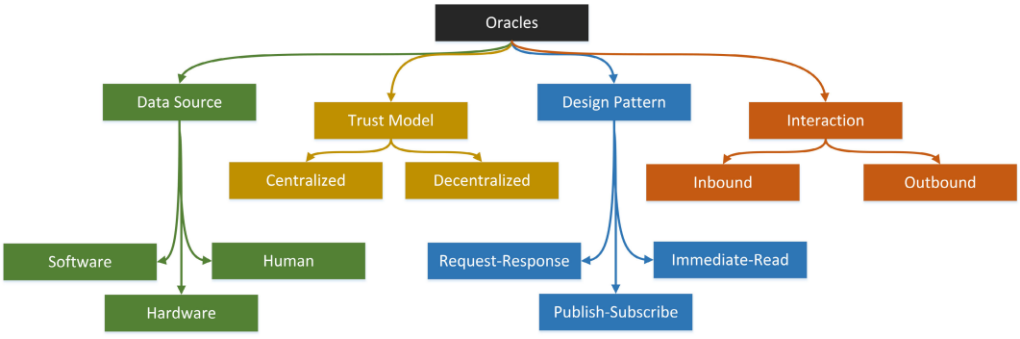


Figura 1. Taxonomía de los oráculos [2]

La taxonomía de los oráculos en blockchain se clasifica según sus fuentes de datos, modelos de confianza, patrones de diseño e interacciones, lo que facilita la comprensión de su funcionamiento en este ecosistema. Existen tres tipos principales de oráculos según la fuente de datos: los oráculos de software, que extraen información de fuentes en línea como precios de activos y tasas de cambio; los oráculos de hardware, que obtienen datos del mundo físico a través de sensores y dispositivos, como sensores RFID y de temperatura; y los oráculos humanos, que dependen de la acción de las personas para proporcionar información a los contratos inteligentes. Los modelos de confianza se dividen en centralizados, que dependen de una única fuente de datos, y descentralizados, que mitigan el riesgo de un punto de fallo único, aunque a costa de una mayor latencia en el procesamiento de datos.

En cuanto a los patrones de diseño, se pueden clasificar en tres formas: el patrón de solicitud-respuesta, ideal para conjuntos de datos grandes donde solo se requiere una parte en un momento dado; el patrón de publicar-suscribir, que permite la difusión de datos cambiantes como feeds de precios y meteorológicos; y el patrón de lectura inmediata, que proporciona datos necesarios para decisiones rápidas, como certificados. Los oráculos también se diferencian por su interacción con el mundo externo: los oráculos inbound insertan datos del exterior en la blockchain, mientras que los oráculos outbound permiten que los contratos inteligentes entreguen información al mundo físico. Esta clasificación subraya la importancia de los oráculos en la conexión entre los mundos digital y físico, permitiendo que los contratos inteligentes interactúen con eventos del mundo real de manera confiable y eficiente.

VI. SEGURIDAD

La seguridad en los oráculos es un aspecto crítico para garantizar la integridad y confiabilidad de la información que se transfiere entre el mundo externo y la blockchain. Los oráculos actúan como intermediarios, y su diseño y operación pueden afectar significativamente la seguridad del sistema en el que operan [2]. A continuación, se describen varios componentes clave de la seguridad en los oráculos:

Integridad de los Datos: La seguridad de un oráculo comienza con la calidad y la veracidad de los datos que proporciona. Los oráculos deben obtener información de fuentes confiables y verificables para evitar que datos incorrectos o manipulados comprometan el funcionamiento de los contratos inteligentes. Esto puede incluir la implementación de mecanismos de validación que aseguren que los datos sean precisos antes de ser transmitidos a la blockchain.

Descentralización: Los oráculos centralizados presentan un único punto de falla, lo que los hace más vulnerables a ataques y manipulaciones. Por lo tanto, se están desarrollando oráculos descentralizados que utilizan múltiples fuentes de datos y consenso entre diferentes nodos. Este enfoque reduce el riesgo de fraude, ya que los datos se verifican a través de múltiples oráculos independientes antes de ser introducidos en la blockchain.

Cifrado y Autenticación: La comunicación entre el oráculo y la blockchain debe estar protegida mediante cifrado para evitar intercepciones y manipulaciones. Además, los mecanismos de autenticación son esenciales para garantizar que solo fuentes autorizadas puedan enviar datos al oráculo, lo que ayuda a prevenir ataques de suplantación o entrada de datos falsos.

Auditoría y Transparencia: La capacidad de auditar las operaciones del oráculo es vital para mantener la confianza. Los oráculos pueden implementar registros de auditoría para rastrear el origen de los datos y cualquier modificación realizada. La transparencia en el proceso de adquisición y transmisión de datos permite a los usuarios verificar la fiabilidad del oráculo y sus fuentes.

Mecanismos de Penalización: Para mitigar el riesgo de comportamientos maliciosos, se pueden establecer mecanismos de penalización para los oráculos que proporcionen información incorrecta. Esto puede incluir la pérdida de recompensas o la inhabilitación para operar en la red, lo que incentiva a los oráculos a actuar de manera honesta y responsable.

La combinación de estos elementos contribuye a la seguridad general de los oráculos y, por ende, al funcionamiento seguro y eficaz de las aplicaciones basadas en blockchain. La implementación cuidadosa de estos mecanismos es crucial para proteger los ecosistemas descentralizados y asegurar que los contratos inteligentes puedan interactuar con el mundo real de manera confiable.

A continuación, se explica uno de los Oráculos existentes y sus características de falencias o faltantes.

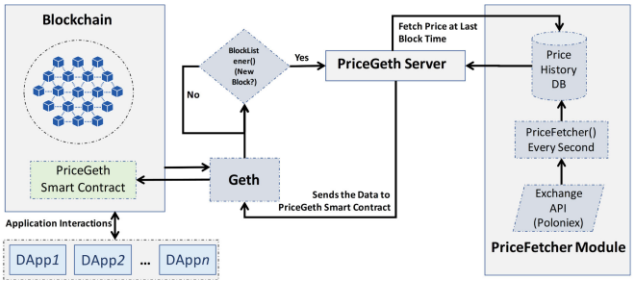


Figura 3. PriceGhet Diagrama de flujo [2].

PriceGeth se implementó como una prueba de concepto para permitir que una entidad de confianza publique pares de precios en la blockchain. PriceGeth fue implementado como un contrato inteligente para publicar pares de precios en tiempo real en la blockchain de Ethereum y mantiene todos los precios históricos en la cadena, por lo que no se requerirá gas para acceder a los precios. El flujo de trabajo de PriceGeth, como se muestra en la Fig. 3, implica interacciones entre contratos inteligentes de Ethereum, el servidor PriceGeth y el módulo PriceFetcher (que obtiene precios de acciones cada segundo de una API web externa).

Los autores de PriceGeth afirmaron que su diseño tiene un punto de fallo central y argumentaron que para que las fuentes de precios descentralizadas puedan generar confianza en la blockchain, es necesario contar con una infraestructura de intercambio descentralizada. También han destacado otro desafío en su diseño, donde no se ofrece ningún incentivo a los oráculos de precios por publicar y almacenar pares de precios, lo que incurre en costos de gas para estos oráculos [2].

VII. ORACLE CHAINLINK

Se prevé un papel cada vez más expansivo para las redes de oráculos, donde complementan y mejoran las blockchains existentes y nuevas al proporcionar conectividad universal rápida, confiable y que preserve la confidencialidad, así como computación off-chain para contratos inteligentes. Esta evolución implica un enfoque hacia una infraestructura más robusta y versátil que puede adaptarse a las demandas cambiantes del ecosistema blockchain.

La base del plan se centra en lo que se denomina Redes de Oráculos Descentralizados (DONs, por sus siglas en inglés). Una DON es una red mantenida por un comité de nodos de Chainlink y soporta una gama ilimitada de funciones de oráculos elegidas para su implementación [3]. De este modo, una DON actúa como una poderosa capa de abstracción, ofreciendo interfaces para contratos inteligentes que conectan recursos off-chain extensos y recursos de computación off-chain altamente eficientes y descentralizados dentro de la propia DON. Este enfoque permitirá una mejor integración y utilización de recursos tanto en la blockchain como fuera de ella, facilitando el desarrollo de soluciones más complejas y efectivas.

Con las DONs como punto de partida, Chainlink se enfocará en avances en siete áreas clave. Estas áreas incluyen contratos inteligentes híbridos que combinan recursos on-chain y off-chain; la simplificación de la funcionalidad para desarrolladores y usuarios, eliminando la necesidad de familiaridad con protocolos complejos; y la escalabilidad para asegurar que los servicios de oráculos cumplan con las exigencias de latencia y rendimiento de los sistemas descentralizados de alto rendimiento. Además, se abordarán la confidencialidad de los datos sensibles, la equidad en la secuenciación de transacciones, la minimización de la confianza mediante técnicas criptográficas y garantías cripto-económicas, y la seguridad basada en incentivos que motive a los nodos a comportarse de manera confiable. Estas innovaciones representan una ampliación y un fortalecimiento de las capacidades previstas para la red Chainlink, con el objetivo de convertirla en un pilar fundamental en el ecosistema blockchain [3].

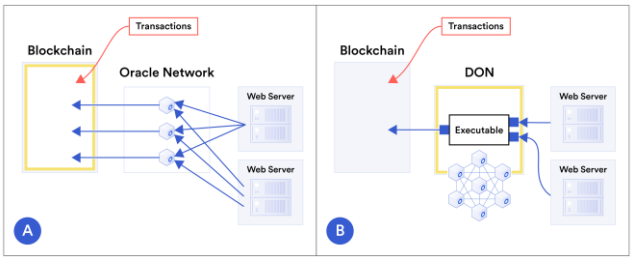


Figura 4. Figura conceptual que muestra cómo las Redes de Oráculos Descentralizadas (DON, por sus siglas en inglés) [3].

De la figura anterior se pude decir que las DONs mejoran la escalabilidad de los contratos inteligentes habilitados en blockchain. La Figura A muestra una arquitectura de oráculo convencional. Las transacciones se envían directamente a la blockchain, al igual que los informes de oráculo. De este modo, la blockchain, resaltada en amarillo, es el principal centro de procesamiento de transacciones.

La Figura B muestra el uso de una DON para respaldar contratos en la blockchain. Un ejecutable de la DON procesa transacciones junto con datos de sistemas externos y envía los resultados —por ejemplo, transacciones agrupadas o cambios de estado de contrato resultantes de los efectos de las transacciones— a la blockchain [3]. Así, la DON, resaltada en amarillo, se convierte en el principal centro de procesamiento de transacciones.

Evaluación de seguridad

La arquitectura descentralizada de Chainlink representa una ventaja crucial en términos de seguridad frente a sistemas de oráculos centralizados, los cuales dependen de una única fuente de datos, incrementando el riesgo de manipulaciones o errores en la información. Chainlink distribuye la verificación de los datos a través de múltiples nodos independientes, lo cual significa que, incluso si algún nodo fuera comprometido o presentara errores, el sistema podría rechazar esos datos falsos basándose en la mayoría de los nodos confiables. Esta verificación en múltiples puntos establece una red de confianza distribuida, crucial para la seguridad en contratos inteligentes que dependen de datos precisos, como los de precios en el ámbito de las finanzas descentralizadas (DeFi).

Además, Chainlink ha implementado mecanismos de recompensa y sanción que incentivan a los operadores de nodos a mantener altos niveles de seguridad y precisión. Estos incentivos crean un sistema de autorregulación que refuerza la integridad de la red al asegurar que solo los nodos de confianza permanezcan activos y sean utilizados en contratos inteligentes sensibles.

Solution	On/Off Chain	Trust Model	Native Token
Provable	Off-chain	Centralized - Authenticity Proofs (TLSNotary)	None
TownCrier	Off-chain	Centralized – TEE (SGX)	None
PriceGeth	Off-chain	Centralized -Single Price Feed	None
Witnet	On-chain	Decentralized - Reputation-Based	Wit
Augur	On-chain	Decentralized - Reputation-Based	REP
ChainLink	Off-chain / On-chain	Decentralized - Reputation-Based	LINK
ASTRAEA	On-chain	Decentralized - Voting-Based	None
Aeternity	On-chain	Decentralized - Consensus-based	Aeon

Tabla 1. Comparación de soluciones Oracle existentes basadas en modelos de confianza [2].

ChainLink propone un modelo de confianza descentralizado y distribuido que abarca componentes tanto on-chain como off-chain, facilitando la transferencia segura de datos entre contratos inteligentes y APIs web para crear contratos inteligentes externos e inmunes a manipulaciones [2]. Este modelo de confianza asegura que los componentes de ChainLink mantengan la integridad, confidencialidad y autenticidad de los datos utilizados en contratos inteligentes. Además, garantiza una selección adecuada de oráculos externos, supervisa las sesiones de reporte de datos entre contratos inteligentes y nodos de ChainLink, y agrega los resultados de consultas provenientes de múltiples fuentes de datos, lo que mejora la confiabilidad de la información en la blockchain.

El modelo de confianza de ChainLink también incorpora contratos inteligentes de reputación para incentivar y penalizar a los oráculos que reportan datos, promoviendo así la equidad entre ellos. Esta función de reputación se basa en parámetros como el número total de tareas asignadas y completadas, el tiempo de respuesta promedio, y el total de penalizaciones pagadas por los oráculos. Las transacciones financieras en la plataforma ChainLink se realizan a través del token LINK, desarrollado sobre los estándares ERC20 y ERC223 de Ethereum. Adicionalmente, ChainLink ofrece un sistema de validación, un sistema de certificación y un servicio de actualización de contratos para asegurar el cumplimiento estricto del diseño descentralizado del protocolo ChainLink.

Comparación de rendimiento

La estructura de Chainlink, basada en múltiples nodos, permite un proceso de validación de datos más confiable y robusto en comparación con los oráculos centralizados. En un sistema de oráculo centralizado, cualquier fallo o manipulación en el nodo central puede llevar a la transmisión de datos incorrectos, impactando negativamente en las decisiones automáticas de los contratos inteligentes. Chainlink, al requerir consenso entre múltiples nodos independientes, reduce significativamente este riesgo y, en consecuencia, mejora la precisión y confiabilidad de los datos que proporciona.

Este enfoque distribuido también permite a Chainlink soportar una mayor variedad de aplicaciones que necesitan datos en tiempo real y de alta precisión, tales como mercados financieros y plataformas de seguros. La comparación entre el rendimiento de Chainlink y el de otros oráculos centralizados es fundamental para evaluar cómo este sistema descentralizado no solo aumenta la seguridad, sino que también eleva la fiabilidad operativa, especialmente en aplicaciones donde se requiere precisión para la toma de decisiones críticas.

Mejora en escalabilidad

Chainlink 2.0 introduce un diseño mejorado en cuanto a la escalabilidad y la seguridad de la red, con funcionalidades avanzadas para optimizar su rendimiento. Entre los cambios más relevantes se encuentra la implementación de "Chainlink Off-Chain Reporting" (OCR), un mecanismo que permite a los nodos recopilar y acordar datos off-chain antes de transmitirlos a la blockchain [3]. Esta tecnología reduce significativamente la cantidad de datos que deben ser procesados en la cadena, minimizando los costos de transacción y mejorando la velocidad del sistema.

Gracias a OCR y a otras innovaciones de Chainlink 2.0, el sistema puede ahora manejar un volumen mayor de solicitudes de datos, permitiendo que múltiples contratos inteligentes consulten datos sin saturar la red [3]. Esta escalabilidad es esencial para soportar la adopción masiva de aplicaciones de DeFi y otros servicios que dependen de datos externos, contribuyendo así a una integración más eficiente entre el mundo real y los contratos inteligentes.

Identificación de desafíos

Aunque Chainlink ha avanzado significativamente, todavía enfrenta varios desafíos que deben ser abordados para maximizar su eficiencia y adopción. Algunos de los principales retos incluyen:

Costos operativos: Los operadores de nodos en la red Chainlink asumen gastos considerables debido al procesamiento de datos y la energía que estos requieren. En un sistema descentralizado como este, la dependencia de múltiples nodos implica que cada consulta realizada por un contrato inteligente puede generar múltiples costos de transacción. Estos costos operativos deben ser mitigados para lograr que el sistema sea viable a gran escala y accesible para una gama más amplia de aplicaciones y usuarios.

Latencia en la red: La transmisión y validación de datos a través de varios nodos pueden resultar en una latencia en el tiempo de respuesta. Aunque el sistema de Chainlink es robusto, la necesidad de consenso entre múltiples nodos puede ralentizar el proceso en comparación con oráculos centralizados. Chainlink 2.0 ha implementado mejoras para reducir esta latencia, pero es necesario continuar investigando y desarrollando nuevas técnicas para mejorar el tiempo de respuesta, especialmente en aplicaciones en las que la velocidad de procesamiento es crítica.

VIII. CONFIANZA

Chainlink emplea un sistema de oráculos descentralizados para garantizar la confianza y precisión de los datos que suministra a los contratos inteligentes. En lugar de depender de un único oráculo centralizado, que podría introducir vulnerabilidades o manipulaciones, Chainlink utiliza múltiples nodos para recopilar y verificar la información de fuentes externas. Este enfoque descentralizado permite reducir los riesgos asociados con un único punto de fallo, pues los datos son validados

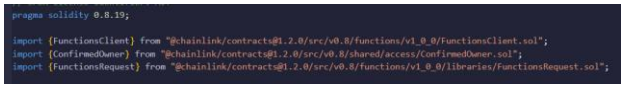
mediante un proceso de consenso. Cada nodo dentro de la red aporta datos que luego son comparados y agregados para asegurar que los contratos inteligentes reciban información verificada y confiable.

Para determinar la confianza en su red, Chainlink también implementa un sistema de reputación y mecanismos cripto-económicos. Cada nodo es evaluado en función de su desempeño, historial y confiabilidad en la entrega de datos precisos y a tiempo. Los operadores de nodos que cumplen consistentemente con estos criterios reciben incentivos en forma de recompensas, mientras que aquellos que entregan datos incorrectos o actúan de manera maliciosa son penalizados económicamente o pierden su reputación en la red. Esta combinación de incentivos y penalizaciones cripto-económicas fomenta que los nodos actúen de manera honesta, asegurando así que la red de Chainlink mantenga altos estándares de calidad en los datos que transmite a los contratos inteligentes en blockchain.

IX. EJEMPLO BASE

En la página oficial de Chainlink, es posible acceder a un ejemplo práctico que permite ejecutar y comprender mejor el funcionamiento del oráculo de Chainlink y su correcta aplicación. Este recurso está diseñado para ayudar a los desarrolladores a familiarizarse con la integración de datos externos en contratos inteligentes, utilizando la tecnología de Chainlink para obtener datos fiables y seguros desde el mundo real hacia la blockchain. A través de este ejemplo, los usuarios pueden entender cómo configurar y utilizar el oráculo, así como observar su comportamiento en un entorno de prueba, lo cual es fundamental para aprovechar todo el potencial que esta herramienta ofrece en el desarrollo de aplicaciones descentralizadas a continuación de procederá a hacer una explicación del código utilizado.

El siguiente contrato inteligente escrito en Solidity utiliza la tecnología de Chainlink Functions para hacer solicitudes HTTP desde un contrato en la blockchain [6]. En este caso, se hace una solicitud HTTP a la API de Star Wars para obtener el nombre de un personaje, dado su ID.



Estos importan contratos necesarios para trabajar con Chainlink Functions, el cual permite realizar llamadas HTTP desde Solidity, y el contrato ConfirmedOwner, que establece controles de acceso solo para el propietario.

```
contract GettingStartedFunctionsConsumer is FunctionsClient, ConfirmedOwner {
    using FunctionsRequest for FunctionsRequest.Request;
```

Aquí se define el contrato GettingStartedFunctionsConsumer, que hereda de FunctionsClient (para manejar solicitudes HTTP) y de ConfirmedOwner (para limitar ciertas funciones solo al propietario del contrato).

```
// State variables to store the last re
bytes32 public s_lastRequestId;
bytes public s_lastResponse;
bytes public s_lastError;
```

s_lastRequestId: Almacena el ID de la última solicitud enviada.
s_lastResponse: Almacena la respuesta de la solicitud HTTP.
s_lastError: Almacena cualquier error que ocurra durante la solicitud.

```
// Custom error type
error UnexpectedRequestID(bytes32 requestId);

// Event to log responses
event Response(
    bytes32 indexed requestId,
    string character,
    bytes response,
    bytes err
);
```

UnexpectedRequestID: Error personalizado que se usa si el requestId de la solicitud recibida no coincide con el último ID de solicitud.
Response: Evento que emite los resultados de la solicitud (respuesta y errores).

```
address router = 0xb83E47C2bC239B3bf370bc41e1459A34b41238D0;

// JavaScript source code
// Fetch character name from the Star Wars API.
// Documentation: https://swapi.info/people
string source =
    "const characterId = args[0];"
    "const apiResponse = await Functions.makeHttpRequest({"
    "url: `https://swapi.info/api/people/${characterId}/`"
    "});"
    "if (apiResponse.error) {"
    "throw Error('Request failed');"
    "}"
    "const { data } = apiResponse;"
    "return Functions.encodeString(data.name);";
```

router: La dirección del router de Chainlink para la red de pruebas Sepolia.

source: Contiene el código JavaScript que se ejecutará en la solicitud HTTP. Este código obtiene el nombre de un personaje desde la API de Star Wars usando el characterId.

```
uint32 gasLimit = 300000;

bytes32 donID =
    0x66756e2d65746865726d2d7365706f6c69612d3100000000000000000000;
```

gasLimit: Límite de gas para ejecutar el código de devolución de llamada (callback) cuando se recibe una respuesta.
donID: ID de red de Oráculos Descentralizados (DON) de Chainlink, también específico para Sepolia.

```
constructor() FunctionsClient(router) ConfirmedOwner(msg.sender) {}
```

Este constructor inicializa el contrato con la dirección del router y establece al despliegue del contrato como el propietario.

```
function sendRequest(    infinite gas
    uint64 subscriptionId,
    string[] calldata args
) external onlyOwner returns (bytes32 requestId) {
    FunctionsRequest.Request memory req;
    req.initializeRequestForInlineJavaScript(source);
    if (args.length > 0) req.setArgs(args); // Set the

    // Send the request and store the request ID
    s_lastRequestId = _sendRequest(
        req.encodeCBOR(),
        subscriptionId,
        gasLimit,
        donID
    );

    return s_lastRequestId;
}
```

Esta función envía una solicitud HTTP a la API. Se pasan dos parámetros:

- subscriptionId: ID de la suscripción de Chainlink.
- args: Array con argumentos necesarios para la solicitud HTTP.

Pasos en la función:

- Crea una solicitud req usando FunctionsRequest.Request.
- Inicializa la solicitud con el código JavaScript (source) y establece los argumentos (args).
- Almacena el requestId retornado para el seguimiento.

```
function fulfillRequest(    undefined gas
    bytes32 requestId,
    bytes memory response,
    bytes memory err
) internal override {
    if (s_lastRequestId != requestId) {
        revert UnexpectedRequestID(requestId); // Check if request IDs match
    }
    // Update the contract's state variables with the response and any errors
    s_lastResponse = response;
    character = string(response);
    s_lastError = err;

    // Emit an event to log the response
    emit Response(requestId, character, s_lastResponse, s_lastError);
}
```

Esta función es la devolución de llamada que recibe la respuesta de la solicitud Chainlink.

Pasos en la función:

- Verifica que el requestId recibido coincida con s_lastRequestId. Si no, lanza un error.
- Si todo está correcto, actualiza las variables de estado (s_lastResponse, character, s_lastError) con la respuesta y el error.
- Emite el evento Response, registrando el ID de la solicitud, la respuesta (character) y cualquier error que haya ocurrido.

Para utilizar Chainlink Functions, es necesario crear una suscripción en Chainlink que permita realizar solicitudes de datos externos hacia la blockchain. La suscripción garantiza que el contrato pueda interactuar con los nodos de Chainlink y acceder a recursos necesarios para el funcionamiento de las funciones externas. La documentación de Chainlink proporciona una guía detallada sobre cómo configurar y ejecutar este proceso, incluyendo los pasos para crear la suscripción y establecer la conexión entre el contrato inteligente y los oráculos de Chainlink. Esta configuración es esencial para garantizar una integración adecuada de Chainlink en el contrato y se puede consultar en la guía oficial [6].

X. DESAFÍOS DE INVESTIGACIÓN

El desafío de equilibrar descentralización y eficiencia en los oráculos de blockchain surge porque, aunque la descentralización ofrece una mayor seguridad al distribuir la confianza entre múltiples nodos, esta misma característica también complica el proceso de consenso y aumenta los costos de operación. En una red de oráculos completamente descentralizada, los datos externos deben ser recopilados, verificados y comparados entre múltiples nodos antes de llegar a un consenso, lo cual garantiza que la información sea confiable y resistente a manipulaciones. Sin embargo, este proceso de consenso lleva tiempo y consume recursos significativos, lo que puede provocar latencias en la transmisión de datos y aumentar los costos operativos, especialmente en aplicaciones que requieren respuestas en tiempo real o tienen un gran volumen de consultas.

Para abordar este desafío, los investigadores están explorando el desarrollo de algoritmos de consenso optimizados, como el consenso federado o basado en grupos de nodos seleccionados, que permiten llegar a un acuerdo en menos tiempo y con menor consumo de recursos. Este tipo de consenso puede configurarse para que solo una selección de nodos altamente confiables participe en la verificación de datos para aplicaciones menos críticas, mientras que en aplicaciones sensibles se puede optar por un mayor número de nodos para incrementar la seguridad, aunque implique un mayor costo y tiempo de procesamiento. Además, se están implementando sistemas avanzados de reputación que evalúan y clasifican a los nodos según su desempeño, historial de precisión y disponibilidad, lo que facilita la selección de nodos óptimos para cada tipo de consulta o

contrato inteligente.

Otra línea de investigación es la adaptación dinámica de la descentralización en función del tipo de datos y las necesidades de cada aplicación. Esto implica ajustar el nivel de descentralización en tiempo real, de acuerdo con factores como la sensibilidad de la información, el tiempo de respuesta requerido y el valor económico en riesgo. Por ejemplo, en aplicaciones financieras de alta criticidad, donde la seguridad es primordial, puede optarse por una configuración altamente descentralizada. En cambio, en aplicaciones menos sensibles, un modelo con menos nodos podría proporcionar un equilibrio aceptable entre seguridad y eficiencia. Esta flexibilidad permitiría que la red de oráculos sea escalable y capaz de adaptarse a diferentes contextos en el ecosistema blockchain, optimizando así el rendimiento y la efectividad de los oráculos descentralizados sin sacrificar su confiabilidad.

XI. CONCLUSIONES

Los oráculos son fundamentales para la expansión de las aplicaciones blockchain, ya que conectan contratos inteligentes con datos externos del mundo real, habilitando un rango más amplio de aplicaciones, especialmente en sectores como finanzas, seguros y logística. Sin los oráculos, los contratos inteligentes estarían limitados a operar solo con datos internos, reduciendo significativamente su utilidad.

La descentralización aumenta la seguridad y la resistencia de los oráculos frente a manipulaciones al distribuir la confianza entre múltiples nodos. Sin embargo, también introduce desafíos en términos de eficiencia y costos operativos, ya que el proceso de consenso puede ralentizar la validación de datos y elevar los recursos necesarios.

Para optimizar el balance entre seguridad y eficiencia, se están desarrollando algoritmos de consenso más eficientes y sistemas de reputación avanzados que permiten clasificar los nodos según su desempeño. Estas innovaciones son cruciales para mejorar la velocidad y precisión de los oráculos descentralizados sin comprometer su integridad.

La capacidad de ajustar dinámicamente el nivel de descentralización según el tipo de aplicación y los requisitos específicos de cada caso de uso permite que los oráculos descentralizados sean más eficientes y adaptables. Esto permite un mejor equilibrio entre seguridad y costo, especialmente en aplicaciones que varían en sensibilidad y requisitos de respuesta.

A pesar de los avances, los oráculos descentralizados aún enfrentan desafíos en cuanto a la verificación y autenticación de datos. Es necesario seguir investigando para mejorar los protocolos de seguridad y establecer marcos de confianza más sólidos que permitan a los contratos inteligentes recibir información confiable en cualquier circunstancia.

REFERENCES

1. A. Beniiche, "A Study of Blockchain Oracles," *IEEE Access*, vol. 8, pp. 85675-85685, May 2020, doi: 10.1109/ACCESS.2020.2992698.
2. H. Al-Breiki, M. H. Ur Rehman, K. Salah, and D. Svetinovic, "Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges," *IEEE Access*, vol. 8, pp. 85686-85706, May 2020.
3. L. Breidenbach et al., "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks," Apr. 2021, v1.0.
4. K. M. Khan, R. Taufique, and M. A. Rauf, "Investigation on a Price Oracle Problem," *Mehran University Research Journal of Engineering and Technology*, vol. 41, no. 4, pp. 138-145, 2022, doi: 10.22581/muet1982.2204.14.
5. Chainlink. “Blockchains and Oracles: Similarities, Differences, and Synergies.” *Chainlink Education Hub*, 25 de julio de 2023. https://chain.link/education-hub/blockchain-vs-oracles
6. Chainlink Labs, "Getting Started: Configure Your Resources," Chainlink Documentation. Available: https://docs.chain.link/chainlink-functions/getting-started#configure-your-resources. Accessed: Nov. 8, 2024.