Programación Web 3

UNLaM - Tecnicatura en Desarrollo Web

Trabajo Práctico de Investigación

Título: Blockchain

Integrantes

Cruz Alejandro
Guillin Víctor
Larsen Nicolas
Nuñez Evelina
Vazquez Leandro
Yucra Fabricio

Objetivo

En este trabajo de investigación, exploraremos qué es Blockchain, sus conceptos básicos y el uso más común de esta tecnología para comprender su importancia. Como punto de análisis hablaremos del Desarrollo Blockchain para luego proponer un ejemplo básico.

Situación Actual

Blockchain es una tecnología descentralizada que permite la transferencia y validación segura de datos sin la necesidad de intermediarios. Es una tecnología para registrar cambios a través del tiempo de una forma no destructiva que se hizo conocida por su uso en torno a las criptomonedas, pero su alcance va más allá de las mismas, en los últimos años las soluciones basadas en blockchain han tenido un crecimiento muy importante, siendo adoptadas por industrias como la financiera para mejorar la seguridad y eficiencia de productos y servicios existentes, así como por la industria alimenticia y la cadena de suministro para el seguimiento de productos o en la comunidad científica para la gestión de documentación. Dependiendo de las características de cada proyecto o sector, cada organización elegirá entre los distintos tipos de blockchain el que más se adapte a sus necesidades. Si bien blockchain de carácter público, como Bitcoin o Ethereum, son las más conocidas, muchas empresas se han interesado en el uso de blockchain privadas para proteger la información sensible. En este sentido, existen compañías ofreciendo blockchain como servicio (BaaS, por sus siglas en inglés), lo que permite que otras organizaciones puedan crear y utilizar aplicaciones basadas en blockchain a través de una infraestructura en la nube. Por ejemplo, la blockchain de Ethereum como servicio que ofrecen Microsoft y ConsenSys en Azure, o el proyecto Hyperledger Cello.

Desarrollo de la Investigación

Para poder seguir hablando de blockchain necesitamos definir esta tecnología, a continuación, procederemos a explicar y posteriormente ejemplificar sus conceptos para reforzar el objetivo principal de esta investigación.
Como ya adelantamos Blockchain es una tecnología descentralizada que permite la transferencia y validación segura de datos sin la necesidad de intermediarios. Consiste en una cadena de bloques enlazados que contienen transacciones verificadas y permanentemente almacenadas, pero que quiere decir que sea descentralizada, esto

significa que no hay una autoridad central, existen nodos que se conectan a una red peer-to-peer y mantiene una copia de la cadena de bloques completa, esta es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Conceptos básicos

Bloques: Cada bloque en la cadena contiene un conjunto de transacciones, información y una huella o hash único que lo identifica.

Huella o hash: cada bloque cuenta con dos huellas, una propia y la huella del bloque anterior que aporta mayor seguridad y genera la cadena, el primer bloque de la cadena es especial porque no tiene huella anterior a este se lo llama Genesis.

Cadenas: Los bloques se enlazan secuencialmente por medio de sus huellas, creando una cadena de bloques.

Nodos: Son los participantes de la red Blockchain que mantienen una copia de la cadena y participan en la validación de transacciones.

Consenso: Los nodos utilizan algoritmos de consenso para llegar a un acuerdo sobre el estado de la cadena entre todos los miembros.

Criptografía: Se emplea la criptografía para garantizar la seguridad de las transacciones y la integridad de los datos.

Arquitectura de Blockchain

La estructura de datos en Blockchain se compone de bloques que contienen información transaccional. Cada bloque está enlazado mediante hashes, lo que garantiza la integridad de la cadena.

La red Blockchain al estar descentralizada, cada nodo de la red tiene una copia completa de la cadena de bloques, lo que significa que contiene todos los registros de transacciones desde el inicio de la cadena. Los nodos se conectan y se comunican entre sí utilizando protocolos específicos de Blockchain.

La conectividad peer-to-peer en Blockchain tiene varias ventajas. Al eliminar la dependencia de una autoridad central o un servidor principal, la red se vuelve más resistente a fallos y ataques maliciosos. Si un nodo deja de funcionar o se desconecta, los demás nodos pueden continuar operando y manteniendo la integridad de la red.

Para evitar que algún participante de esta red modifique la información a su favor existe el concepto del Consenso. El consenso es de hecho un elemento fundamental en la tecnología Blockchain, ya que garantiza que todos los nodos de la red estén de acuerdo sobre el estado de la cadena de bloques. El consenso se logra a través de algoritmos específicos que determinan cómo se valida y se agregan nuevos bloques a la cadena. Algoritmos como Proof of Work o Proof of Stake se utilizan para lograr el consenso.

Como otro concepto importante de esta tecnología es la criptografía, sin duda, juega un papel crucial en la seguridad de la tecnología Blockchain. Permite garantizar la autenticidad, integridad y confidencialidad de las transacciones y los datos almacenados en la cadena de bloques.

En Blockchain, las firmas digitales se utilizan para verificar la autenticidad e integridad de las transacciones. Cada transacción se firma digitalmente utilizando la clave privada correspondiente a la dirección de envío. Los demás nodos pueden verificar la firma

utilizando la clave pública asociada, lo que garantiza que la transacción proviene del remitente correcto y no ha sido alterada. Existen técnicas para llevar a cabo esto:

1. Funciones hash: Las funciones hash criptográficas se utilizan en Blockchain para generar una representación única y fija de los datos. Cada bloque en la cadena contiene un hash que se calcula a partir de los datos del bloque anterior, lo que crea una conexión inmutable entre los bloques. Cualquier cambio en los datos de un bloque modificará su hash, lo que se detectará fácilmente en la cadena.
2. Claves públicas/privadas: En Blockchain, se utilizan pares de claves criptográficas, una clave privada y una clave pública, para cifrar y descifrar datos, así como para firmar y verificar transacciones. La clave privada se mantiene en secreto y se utiliza para firmar digitalmente las transacciones, mientras que la clave pública se comparte con otros nodos para verificar la autenticidad de las transacciones y los mensajes cifrados.

Estas técnicas criptográficas trabajan en conjunto para garantizar la seguridad en Blockchain. La utilización de firmas digitales, funciones hash y claves públicas/privadas ayuda a prevenir la falsificación, el fraude y el acceso no autorizado a los datos en la cadena de bloques.

Aplicaciones de Blockchain

La tecnología Blockchain tiene una amplia gama de aplicaciones en diferentes industrias. A continuación, exploraremos las principales aplicaciones, que incluyen criptomonedas, contratos inteligentes y sectores disruptivos.

Criptomonedas: Las criptomonedas, como Bitcoin y Ethereum, son ejemplos populares de aplicaciones basadas en Blockchain. Estas monedas digitales permiten transacciones seguras y descentralizadas sin la intervención de intermediarios. Utilizando la tecnología Blockchain, se logra un registro confiable y transparente de todas las transacciones realizadas.

Contratos inteligentes: Los contratos inteligentes son programas informáticos que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas. Estos contratos están basados en la tecnología Blockchain y permiten transacciones confiables y verificables sin la necesidad de intermediarios. Los contratos inteligentes ofrecen una forma eficiente y segura de ejecutar acuerdos y automatizar procesos comerciales.

Sectores disruptivos: Blockchain tiene el potencial de interrumpir y transformar varios sectores. En particular, sectores como finanzas, logística, salud, votación y energía pueden beneficiarse significativamente de las características de seguridad y transparencia que ofrece la tecnología Blockchain. Por ejemplo, en el ámbito financiero, Blockchain puede mejorar la eficiencia de las transacciones y reducir los costos, mientras que, en el sector de la salud, puede garantizar un registro seguro y preciso de los datos médicos.

La capacidad de Blockchain para proporcionar seguridad, descentralización y transparencia la convierte en una herramienta poderosa para revolucionar diversas industrias. A medida que la tecnología continúa evolucionando y se superan los desafíos asociados, se espera que Blockchain tenga un impacto aún mayor en la forma en que realizamos transacciones y gestionamos datos en el futuro.

Ventajas y desafíos de Blockchain

1- Seguridad y transparencia Una de las principales ventajas de Blockchain es su capacidad para proporcionar seguridad y transparencia en las transacciones. Gracias a su estructura basada en bloques inmutables y la utilización de técnicas criptográficas, Blockchain garantiza la integridad de los datos y genera confianza en las transacciones realizadas.
2- Eliminación de intermediarios Otra ventaja significativa de Blockchain es su capacidad para facilitar transacciones directas entre participantes, sin necesidad de intermediarios tradicionales como bancos o notarios. Esto agiliza los procesos comerciales, reduce costos y elimina barreras en la realización de transacciones.
3- Escalabilidad y eficiencia Uno de los desafíos que enfrenta Blockchain es la escalabilidad. A medida que la cadena de bloques crece en tamaño y número de transacciones, pueden surgir problemas de rendimiento y capacidad. Sin embargo, se están desarrollando soluciones y mejoras, como la implementación de capas de escalabilidad, para abordar este desafío y mejorar la eficiencia de la tecnología.
4- Desafíos Además de la escalabilidad, Blockchain enfrenta desafíos en otros aspectos. La privacidad es un tema importante, ya que la tecnología Blockchain se basa en un registro compartido y transparente. La gobernanza también plantea desafíos en términos de establecer estándares y reglas claras para el funcionamiento de las redes Blockchain. Por último, la adopción masiva de Blockchain es un desafío en sí mismo, ya que requiere educación, colaboración entre diferentes actores y superar barreras regulatorias y culturales.
A medida que la tecnología Blockchain sigue evolucionando, es importante abordar estos desafíos y trabajar en soluciones que permitan aprovechar plenamente el potencial de esta tecnología revolucionaria.

Casos de uso y ejemplos

En esta sección, exploraremos casos de uso y ejemplos destacados de implementaciones de Blockchain en diferentes industrias.
1- Ejemplos destacados Existen numerosos ejemplos notables de implementaciones exitosas de Blockchain en diversas industrias. Algunos de ellos incluyen:

- Ripple: Ripple es un proyecto que utiliza Blockchain para facilitar pagos internacionales de manera rápida y económica, eliminando la necesidad de intermediarios tradicionales.
- IBM Food Trust: IBM Food Trust es una plataforma basada en Blockchain que se utiliza en la industria alimentaria para rastrear y garantizar la trazabilidad de los productos, desde su origen hasta el consumidor final. Esto ayuda a mejorar la seguridad alimentaria y la transparencia en la cadena de suministro.
- Provenance: Provenance es una aplicación de Blockchain que se utiliza para rastrear y autenticar productos en la cadena de suministro. Permite a los consumidores obtener información detallada sobre la procedencia, el proceso de fabricación y otros datos relevantes de los productos que compran.

2- Casos de uso emergentes Además de los casos de uso establecidos, están surgiendo nuevas aplicaciones de Blockchain en diferentes áreas. Algunos casos de uso emergentes incluyen:

- Identidad digital: Blockchain se utiliza para crear sistemas de identidad digital seguros y descentralizados, donde los usuarios tienen el control de sus datos personales y pueden compartirlos de forma selectiva.
- Energía renovable: Blockchain se utiliza en proyectos relacionados con energía renovable para rastrear la generación, distribución y consumo de energía de fuentes renovables, facilitando la transición hacia un sistema energético más sostenible.
- Votación electrónica: Blockchain se propone como una solución para mejorar la seguridad y la transparencia en los procesos de votación electrónica, proporcionando un registro inmutable y verificable de los votos emitidos.

Estos ejemplos destacados y casos de uso emergentes demuestran el potencial de Blockchain para transformar diferentes industrias y abordar desafíos existentes. A medida que la tecnología continúa evolucionando, es probable que surjan aún más casos de uso innovadores.

Consideraciones legales y éticas

Es fundamental tener en cuenta las consideraciones legales y éticas asociadas con la tecnología Blockchain. La regulación de criptomonedas, la privacidad de los datos y la seguridad son aspectos que deben abordarse de manera adecuada y responsable.
1- Marco regulatorio El marco regulatorio para las criptomonedas y los contratos inteligentes está en constante evolución. Es esencial comprender y cumplir con las leyes y regulaciones aplicables en cada jurisdicción. Esto incluye aspectos como la licencia y registro de intercambios de criptomonedas, la prevención del lavado de dinero y la protección de los inversionistas. Mantenerse actualizado sobre los cambios regulatorios es crucial para garantizar el cumplimiento legal.
2- Privacidad y seguridad La privacidad y la seguridad de los datos son preocupaciones centrales en cualquier aplicación de Blockchain. Se deben implementar medidas adecuadas para proteger la información sensible y garantizar la confidencialidad de las transacciones. Esto implica el uso de técnicas criptográficas sólidas, la gestión adecuada de claves y la implementación de protocolos de seguridad robustos. Además, se debe tener en cuenta el cumplimiento de las regulaciones de privacidad de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea.
Es esencial mantener un enfoque ético en el desarrollo y uso de la tecnología Blockchain. Esto implica considerar las implicaciones sociales, económicas y medioambientales de las soluciones basadas en Blockchain. La transparencia, la equidad y la responsabilidad deben estar presentes en todas las etapas del diseño y la implementación de proyectos basados en Blockchain.
Al abordar estas consideraciones legales y éticas, podemos promover la adopción responsable y sostenible de la tecnología Blockchain, aprovechando su potencial para generar beneficios tanto para las organizaciones como para la sociedad en general.

Desarrollo Blockchain

En la actualidad, hay una gran cantidad de proyectos relacionados con la tecnología Blockchain, y donde hay proyectos, se necesitan desarrolladores capaces de llevar a cabo estos proyectos. Por lo general, las blockchains son proyectos abiertos, lo que significa que se puede acceder al código e incluso copiarlo para realizar modificaciones (fork) en un

desarrollo típico. De hecho, muchos de estos proyectos no tienen su propia blockchain, sino que se construyen sobre blockchains existentes.
Encontrarás numerosas propuestas de proyectos en la lista de los primeros cien en sitios como https://coinmarketcap.com/es/, que es una plataforma donde se enumeran la mayoría de los proyectos blockchain. Aunque existen miles de proyectos, los primeros diez de la lista son los más populares, como Bitcoin, Ethereum, Tether, entre otros.
Bitcoin se considera una blockchain de primera generación, cuyo propósito principal es ser una red para transferir dinero digital, es decir, su criptomoneda llamada bitcoin. Sin embargo, para el desarrollo de aplicaciones se requieren blockchains de segunda generación, es decir, blockchains que permitan la ejecución de código. Aquí es donde entra Ethereum. Esta es la red más destacada para las aplicaciones descentralizadas. Ethereum ha brindado al mundo blockchain la posibilidad de crear aplicaciones que se ejecutan en una red, a lo que se refiere como Smart Contracts. Los Smart Contracts se pueden entender como acuerdos entre dos partes sin la necesidad de un tercero, pero desde la perspectiva de un desarrollador, los Smart Contracts son simplemente código escrito en un lenguaje de programación que se sube a la blockchain para su ejecución.
El desarrollo de Blockchain se basa en muchas tecnologías web actuales. Al desarrollar Smart Contracts, la forma de interactuar con ellos es a través de programas de consola. Sin embargo, esto no es adecuado para los usuarios finales, por lo que se crea una interfaz sencilla para que los usuarios puedan interactuar de manera más amigable.
El desarrollo de smart contracts implica la creación de programas pequeños que se ejecutan en una blockchain. A diferencia de los programas típicos que encontramos en nuestro día a día, estos smart contracts suelen ser mucho más cortos, constando de cientos de líneas de código. Una vez que se suben a la blockchain, se vuelven inmutables, lo que significa que no se pueden modificar.
Sin embargo, los datos asociados a estos smart contracts sí pueden actualizarse. Es importante destacar que la actualización de un smart contract tiene un costo, ya que implica el uso de la moneda específica de la red blockchain en la que se encuentra. Por ejemplo, en el caso de Ethereum, se requieren ethers para realizar actualizaciones.
El costo de actualizar un smart contract está relacionado con el funcionamiento de la blockchain. Leer datos es gratuito, pero para guardar o actualizar un registro, la blockchain debe realizar una validación en miles de computadoras o nodos de la red. Este proceso requiere poder computacional y, por lo tanto, tiene un costo asociado en términos de ethers. Para evitar costos excesivos, los desarrolladores deben optimizar su código para reducir la cantidad de recursos necesarios.

Conclusiones

En conclusión, Blockchain es una tecnología disruptiva con el potencial de transformar numerosos sectores. Sus características de seguridad, descentralización y transparencia la convierten en una herramienta poderosa para transacciones confiables y verificables.
Sin embargo, existen desafíos técnicos, legales y de adopción que deben superarse para aprovechar todo el potencial de Blockchain. A medida que la tecnología evoluciona y se resuelven estos desafíos, se espera que su impacto y aplicación continúen expandiéndose

Referencias/Bibliografía

LibroBlockchain.com/Satoshi/ en español.
https://faztweb.com/DesarrolloBlockchain
OpenAI. GPT-3.5 (ChatGPT). Fecha de acceso: 16 de mayo de 2023. Fuente: ChatGPT (2023).