EasyChair Preprint

№ 13538

Application of Zero-Knowledge Cryptography in Blockchain Technology: Ensuring Data Privacy and Integrity.

Adiane Cueto Portuondo, Dariel González Robinson and Angel Alejandro Guerra Vilches

June 3, 2024

Aplicación de la Criptografía de Conocimiento Cero en la Tecnología Blockchain: Garantizando la Privacidad y la Integridad de los Datos.

Adiane Cueto Portuondo
Universidad de las Ciencias Informáticas
Cuba
adianecp@estudiantes.uci.cu

Dariel González Robinson
Universidad de las Ciencias Informáticas
Cuba
dgonzalezr@estudiantes.uci.cu

Angel Alejandro Guerra Vilches
Universidad de las Ciencias Informáticas
Cuba
angelagv@estudiantes.uci.cu

Resumen- **Este trabajo de investigación se centra en la criptografía de conocimiento cero y su aplicación en la tecnología blockchain. Se abordan los fundamentos teóricos de la criptografía de conocimiento cero, sus aplicaciones prácticas y limitaciones, y se exploran los protocolos existentes aplicables al blockchain. Se discuten los desafíos de privacidad y confidencialidad en el contexto del blockchain y cómo este tipo de criptografía puede mitigar esos desafíos. Se examinan varios protocolos criptográficos y se presenta un ejemplo de implementación a través del sistema zkLedger. Finalmente, se identifican varios desafíos actuales en este campo, incluyendo la eficiencia computacional, la escalabilidad y la interoperabilidad. El estudio tiene como objetivo proporcionar una visión actualizada de la criptografía de conocimiento cero aplicada al blockchain, y servir como punto de partida para futuras investigaciones en esta área.**

Palabras claves- **Criptografía de conocimiento cero, blockchain, aplicación, privacidad, confidencialidad.**

Tipo de contribución: *Investigación en desarrollo.*

I. Introducción

En los últimos años, el blockchain ha surgido como una tecnología disruptiva con amplias aplicaciones en diversas industrias. Su capacidad para proporcionar un registro inmutable y transparente de transacciones ha sido ampliamente reconocida. Sin embargo, la privacidad y la integridad de los datos en el blockchain siguen siendo desafíos significativos que requieren soluciones robustas.

En este contexto, la criptografía de conocimiento cero ha surgido como una herramienta prometedora para abordar estos desafíos en el ámbito del blockchain. La criptografía de conocimiento cero permite a las partes demostrar que se cumple una afirmación sin revelar información adicional más allá de la veracidad de la afirmación en sí misma. Esto implica que una entidad puede demostrar el conocimiento de ciertos datos sin revelar los propios datos, asegurando así la privacidad y la confidencialidad.

El objetivo de este trabajo de investigación es realizar una revisión de la criptografía de conocimiento cero empleada en el blockchain, analizando sus fundamentos teóricos, aplicaciones prácticas y limitaciones. Mediante una metodología basada en una revisión bibliográfica, se explorarán los protocolos existentes, evaluando su eficiencia y seguridad en términos de privacidad y confidencialidad de los datos, así como la integridad de los registros almacenados en el blockchain.

La estructura del trabajo se divide en los siguientes apartados: en primer lugar, se presentarán los fundamentos de la criptografía de conocimiento cero, destacando los conceptos y técnicas utilizadas. A continuación, se abordarán los desafíos de privacidad y confidencialidad en el contexto del blockchain, y se analizará cómo la criptografía de conocimiento cero puede mitigar estos desafíos. Posteriormente, se examinarán los protocolos de criptografía de conocimiento cero utilizados en el blockchain y un ejemplo de implementación. Se mencionarán otras aplicaciones de este tipo de criptografía y finalmente se discutirán los desafíos actuales en este campo.

II. Contenido

A. *Fundamentos de la criptografía de conocimiento cero*

La criptografía de conocimiento cero es un campo de estudio que permite a las partes demostrar que poseen conocimiento de cierta información sin revelar dicha información en sí misma. En otras palabras, permite demostrar la veracidad de una afirmación sin revelar datos adicionales más allá de la afirmación misma. Esta propiedad es de suma importancia en aplicaciones donde la privacidad y la confidencialidad son fundamentales.

Los sistemas de pruebas de conocimiento cero (ZKP, por sus siglas en inglés) son técnicas criptográficas que permiten a un probador demostrar conocimiento sobre un hecho o declaración específica a un verificador sin revelar información adicional más allá del propio hecho o declaración. Esto se logra mediante la generación de una prueba por parte del probador que cumple con un conjunto específico de criterios, los cuales el verificador puede utilizar para verificar la afirmación sin aprender nada más sobre la declaración. En consecuencia, los ZKP permiten minimizar y limitar el acceso a los datos en contextos distribuidos, como los servicios de Internet en general o la computación en la nube. [1]

La criptografía de conocimiento cero se basa en el concepto de "un engañador convincente", donde una entidad, llamada el verificador, puede estar convencida de que otra entidad, llamada el probador, posee cierta información sin aprender nada más sobre ella. Esto se logra mediante la interacción entre el verificador y el probador, donde se realizan una serie de desafíos y respuestas que permiten verificar la validez de la

afirmación sin revelar detalles adicionales.
Ilustrémoslo con un ejemplo: Alice y Bob se enfrentan a un desafío particular, Bob es daltónico y no puede diferenciar los colores rojo y verde. Sin embargo, Alice tiene en sus manos dos bolas idénticas que difieren solo en el color: una es roja y la otra es verde. El objetivo de Alice es demostrarle a Bob que las bolas son diferentes, sin revelar más información. El verificador es Alice y el probador es Bob.
1. Alice muestra las dos bolas a Bob y le explica que son diferentes, pero Bob no puede diferenciarlas.
2. Para comenzar la demostración, Alice le pide a Bob que se ponga ambas bolas a la espalda y le indica que muestre una de las bolas y luego la vuelva a esconder.
3. A continuación, Alice le dice a Bob que tiene la opción de volver a mostrar la misma bola que mostró inicialmente o cambiarla por la otra bola.
4. Cada vez que Bob muestra una nueva bola, Alice le indica si cambió la bola o no.
5. Alice continúa adivinando correctamente si Bob cambió o no la bola en cada turno sucesivo.
6. A medida que Alice sigue adivinando correctamente, se vuelve cada vez más probable que las bolas sean diferentes.
7. A través de esta interacción y los aciertos consecutivos de Alice, Bob se convence de que las bolas son diferentes sin que Alice tenga que revelar explícitamente por qué.

Las pruebas de conocimiento cero poseen varias características principales. En primer lugar, el verificador no puede obtener nada útil del protocolo, lo que significa que no puede adquirir información sensible a partir de este. En segundo lugar, el verificador no tiene la capacidad de suplantar al probador que ha sido verificado. Esto implica que los mensajes intercambiados durante el protocolo no pueden ser utilizados para hacerse pasar por el probador que está siendo verificado. En tercer lugar, la probabilidad de que el verificador acepte una declaración falsa como verdadera es extremadamente baja. Finalmente, la probabilidad de que el verificador sea convencido de una declaración que es verdadera es muy alta. [2]

Por lo tanto, una prueba de conocimiento cero debe cumplir con tres características básicas:
Completitud: Si la afirmación es verdadera, el verificador puede estar convencido de ello por parte del probador.
Solidez: Si lo que deseas demostrar es falso, el verificador no puede ser engañado.
Conocimiento Cero: El verificador no habrá adquirido información adicional, excepto la verdad de la afirmación.
Los dos primeros atributos son requeridos por cualquier sistema de verificación; es el conocimiento cero lo que caracteriza un método ZKP. Estos protocolos son fundamentales para garantizar la privacidad y la seguridad en contextos como las criptomonedas y la autenticación en sistemas distribuidos. [1]

Este tipo de pruebas se dividen en dos tipos: interactivas y no interactivas. Ambas implican un verificador y un probador, con el objetivo de que este último demuestre la veracidad de una afirmación.
Las pruebas no interactivas no requieren interacción entre el probador y el verificador. El probador presenta una prueba que el verificador puede analizar en cualquier momento para determinar su validez. Este proceso puede realizarse de manera offline y no requiere un canal de comunicación compartido para validar una prueba.
Las pruebas interactivas implican un intercambio de mensajes entre el probador y el verificador. En este protocolo, el probador intenta "convencer" al verificador de la veracidad de una afirmación a través de un juego interactivo. Estas pruebas son probabilísticas y requieren que el verificador esté acotado polinomialmente. El probador, que no está generalmente limitado computacionalmente, debe tener una ventaja computacional sobre el verificador. Estas pruebas permiten probar afirmaciones que no serían posibles con un método no interactivo, por lo que tienen un mayor poder expresivo.
Por lo general, los protocolos de conocimiento cero tienen una estructura formada por 3 pasos.

$$\begin{aligned} A \rightarrow B: &\quad witness \\ A \leftarrow B: &\quad challenge \\ A \rightarrow B: &\quad response \end{aligned}$$

Fig. 1. Esquema de un protocolo de conocimiento cero. [3]

En la *Fig. 1*, A tiene el rol de probador y B el de verificador. A provee un testigo (witness) a B, que computa a partir de un valor aleatorio secreto. Esto permite que cada una de las ejecuciones del protocolo sea distinta debido a la aleatorización y además establece una serie de preguntas que el probador (y sólo un probador honesto) va a ser posible de responder para "probar" su conocimiento. B luego desafía (envía un challenge) a A, seleccionando una de estas preguntas. Finalmente, A envía su respuesta al desafío y B verifica que la misma sea correcta, repitiendo el proceso completo varias veces hasta que la posibilidad de que A esté haciendo trampa sea tan baja cómo B desea. Tanto el testigo como la respuesta que envía A a B, no brindan ninguna información adicional sobre el secreto que conoce A, más allá de la aserción del conocimiento de este. [3]

En la clase de pruebas no interactivas, un concepto particularmente interesante para demostrar la integridad de los resultados de cálculos grandes es el de SNARK, es decir, argumento no interactivo y sucinto de conocimiento. Con este término, denotamos un sistema de prueba que es:

Sucinto: el tamaño de la prueba es muy pequeño en comparación con el tamaño de la declaración o el testigo, es decir, el tamaño del cálculo en sí.

No interactivo: no requiere rondas de interacción entre el demostrador y el verificador.

Argumento: lo consideramos seguro solo para demostradores que tienen recursos computacionales limitados, lo que significa que los demostradores con suficiente poder computacional pueden convencer al verificador de una declaración incorrecta.

Conocimiento sólido: no es posible que el demostrador construya una prueba sin conocer un cierto testigo llamado para la declaración; formalmente, para cualquier demostrador capaz de producir una prueba válida, hay un extractor capaz de extraer un testigo (" el conocimiento") para la declaración.

Los sistemas SNARK pueden estar equipados con una propiedad de cero conocimiento que permite que la prueba se realice sin revelar nada sobre los pasos intermedios. Estos esquemas son los zk-SNARKs. [4]

Los zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) son pruebas públicamente verificables que demuestran que el probador posee datos secretos (un testigo) que satisfacen una cierta relación NP (clase de problemas no deterministas

polinomiales) pública. La prueba no revela nada sobre los datos secretos aparte de su validez. Los zk-SNARK tienen dos fortalezas clave:

Privacidad y eficiencia: Los zk-SNARK permiten a un probador demostrar que conoce una solución válida para un problema sin revelar la solución en sí misma. Esto es útil en situaciones donde se necesita verificar la validez de una solución sin exponer detalles confidenciales. Por ejemplo, en criptomonedas como Zcash, zk-SNARK se utiliza para verificar transacciones sin revelar las direcciones de los remitentes y receptores.

Compacidad: Los zk-SNARK generan pruebas muy cortas y eficientes en términos de tamaño computacional. Esto es crucial para aplicaciones como blockchain, donde el espacio de almacenamiento y el tiempo de procesamiento son limitados. [5]

Un protocolo (zk-)SNARK (como cualquier otro sistema de prueba no interactivo) se describe mediante tres algoritmos que funcionan de la siguiente manera:

Gen es el algoritmo de configuración, genera una cadena crs necesaria utilizada más tarde en el proceso de prueba y alguna clave de verificación vrs, a veces se supone que es secreta solo para el verificador. Normalmente lo ejecuta una parte de confianza.

Prove es el algoritmo de prueba que toma como entrada el crs, la declaración u y un testigo correspondiente w y genera la prueba π.

Verify es el algoritmo que toma como entrada la clave de verificación vrs, la declaración u y la prueba π, y devuelve 1 ”aceptar” la prueba o 0, ”rechazar”. [4]

B. Desafíos de privacidad y confidencialidad en el contexto del blockchain

En el ámbito del blockchain, la privacidad y la confidencialidad son fundamentales. A pesar de que el blockchain proporciona transparencia y trazabilidad, también puede presentar desafíos para proteger la privacidad de los usuarios y la confidencialidad de la información sensible. En un blockchain público, todas las transacciones son visibles, lo que puede generar preocupaciones sobre la exposición de datos personales. Además, la dirección de billetera utilizada en una transacción puede vincularse a la identidad del usuario. Por otro lado, la confidencialidad se refiere a la protección de la información sensible. Los contratos inteligentes en el blockchain pueden contener información confidencial, y existe el riesgo de que esta información sea visible para todos los participantes en el blockchain. Estos desafíos resaltan la necesidad de soluciones que preserven la privacidad y confidencialidad en el blockchain. La criptografía de conocimiento cero puede desempeñar un papel importante en este aspecto, permitiendo que las partes demuestren la validez de cierta información sin revelar detalles adicionales.

El método principal para permitir transacciones privadas en las redes blockchain son las pruebas de conocimiento cero. El desafío con las cadenas de bloques es la naturaleza de la tecnología que se puede verificar públicamente, y el enigma es cómo se pueden registrar las transacciones en el libro mayor público en un método confiable compartido (porque no tiene confianza, es decir, confianza derivada computacionalmente) que, sin embargo, no revela los detalles específicos de la transacción. En la instanciación básica de blockchain (por ejemplo, Bitcoin), el libro mayor público rastrea la dirección del remitente, la dirección del destinatario y el monto de la transacción. Con la divulgación de direcciones y montos de transacciones, las empresas de análisis de blockchain y otras partes han podido reunir transacciones y vincular los saldos generales de propiedad de activos con identidades personales de la vida real. En los últimos años, ha habido un movimiento para implementar transacciones privadas en cadenas de bloques públicas y empresariales en las que la dirección del remitente y el destinatario, así como del monto de la transacción, estén enmascarados o protegidos en el libro mayor público y en el proceso de consenso. Las transacciones con protección de la privacidad pueden ser confidenciales (protegiendo la cantidad que se está transfiriendo), transacciones anónimas (protegiendo las direcciones que indican quién transfiere a quién) o ambas. Aunque las direcciones Blockchain brindan cierta privacidad debido a su naturaleza (las direcciones son típicamente códigos alfanuméricos de 32 caracteres), si se intercambian públicamente entre personas u otras formas de transmisión voluntaria, es posible que se puedan rastrear de ciertas maneras. [6]

C. Mitigación de los desafíos mediante la criptografía de conocimiento cero

La criptografía de conocimiento cero ha encontrado aplicación en el contexto del blockchain como una solución para mitigar los desafíos de privacidad y confidencialidad. La prueba de conocimiento cero es un concepto fundamental dentro de la criptografía de conocimiento cero que se ha implementado en transacciones que utilizan la tecnología blockchain.

En este contexto, la prueba de conocimiento cero permite que las transacciones sean validadas por un tercero ajeno que no conoce a ninguna de las partes involucradas ni la naturaleza jurídica de la transacción. En el registro de la blockchain, se registra la existencia de una transacción, pero no se revela la identidad, la naturaleza ni la causa de la transacción a aquellos que son ajenos a la cadena de bloques. [7]

Esto tiene un impacto significativo en el ámbito jurídico fuera del entorno del blockchain, especialmente en derechos como el de propiedad. Por ejemplo, en el caso de un criptocontrato para la transacción de un bien inmueble, la propiedad se puede transferir sin revelar detalles sensibles a través de la implementación de la criptografía de conocimiento cero.

En particular, al combinar la tecnología blockchain con los protocolos ZKP, es posible crear sistemas que proporcionen tanto la transparencia y seguridad de una cadena de bloques como la privacidad y confidencialidad de los ZKP. Esto se logra almacenando datos cifrados en la cadena de bloques y utilizando protocolos ZKP para demostrar la propiedad o validez de los datos sin revelar los datos reales en sí. Los ZKP ya se utilizan en criptomonedas como Zcash, que emplea zk-SNARKs para la verificación de transacciones incluso después de que estén cifradas. [1]

La criptografía de conocimiento cero ofrece varios beneficios en términos de privacidad y confidencialidad en el contexto del blockchain.

Uno de los beneficios es la protección de la identidad. Al utilizar la prueba de conocimiento cero, las transacciones pueden ser verificadas sin revelar la identidad de las partes involucradas. Esto ayuda a preservar la privacidad de los usuarios y evita la vinculación de actividades fuera del blockchain a su identidad.

Otro beneficio es la preservación de la confidencialidad. Mediante este tipo de criptografía, es posible demostrar la validez de cierta información sin revelar los detalles adicionales. Esto permite proteger la confidencialidad de información sensible, como acuerdos comerciales o datos personales, al tiempo que se verifica la integridad de la transacción.

D. Protocolos de criptografía de conocimiento cero utilizados en el blockchain

Hay diferentes protocolos de conocimiento cero que tienen en común demostrar que se conoce algo sin tener que decir exactamente qué es lo que se sabe.

Los esquemas de ZKP se pueden dividir en dos categorías: interactivos y no interactivos. En comparación con los interactivos, los no interactivos no requieren múltiples comunicaciones interactivas en el proceso de demostración, lo que evita el ataque de colusión al tiempo que garantiza una mayor seguridad. Especialmente en las aplicaciones de blockchain, los no interactivos pueden evitar las confirmaciones de transacciones causadas por interacciones repetidas en la cadena, lo que permite mejorar la privacidad de las aplicaciones sin afectar el rendimiento de la cadena.

Actualmente, zkSNARK se considera una implementación eficiente de prueba de conocimiento cero no interactiva, y se han desarrollado muchos algoritmos excelentes sucesivamente, como Groth16, PGHR13, entre otros. En comparación con otros algoritmos, Groth16 tiene un cálculo mínimo para la verificación y una prueba concisa. Por lo tanto, el ZKP basado en Groth16 se aplica ampliamente en sistemas de criptomonedas basados en blockchain como Zcash, Filecoin, y otros. [8]

Zcash es una criptodivisa basada en el código de Bitcoin, otra popular criptodivisa. Su principal característica que la diferencia de Bitcoin es la privacidad, resultado de la utilización de una forma especial de ZKP: los ya presentados zk-SNARK. De hecho, Zcash se considera una de las primeras aplicaciones generalizadas de zk-SNARK y permite que todas las transacciones públicas de la blockchain de Zcash estén encriptadas, pero a su vez puedan ser validadas bajo el consenso de la red. Monero es otra criptodivisa muy enfocada en la privacidad de las transacciones. Monero firma las transacciones con una técnica llamada multisignature, donde se necesita de varios participantes para firmar y se oculta la identidad de los firmantes. [3]

Zcash se puede describir como un protocolo criptográfico en un Blockchain gubernamental para colocar información personal. Su funcionamiento es casi igual al de Bitcoin. Los validadores de transacciones son los mineros y los nodos completos. Zcash utiliza pruebas de conocimiento cero para cifrar toda la información y solo permite que las partes aprobadas vean dicha información proporcionando claves de descifrado. Esto no se podía realizar en una cadena de bloques gubernamental hasta ahora, ya que impediría que los mineros verifiquen si las transacciones son válidas si todo ha estado cifrado en el pasado. [9]

Monero utiliza firmas de anillo para lograr confidencialidad en sus transacciones. Las firmas de anillo consisten en un anillo compuesto de un conjunto de claves públicas, en la cual una de ellas corresponde al firmante y el resto no están relacionadas, y una firma, generada con ese anillo de claves y que cualquiera que la verifica no puede determinar qué miembro de ese conjunto es el firmante. [3]

El sistema de firmas del protocolo de Monero debe cumplir con tres principales propiedades: signer ambiguity, linkability y unforgeability. La primera propiedad establece la ambigüedad de una firma, en el sentido que se pueda probar que el firmante pertenece a un grupo, pero sin revelar qué miembro de este es. Esto se utiliza para ofuscar los orígenes de los fondos en cada transacción. El segundo permite que dos mensajes diferentes que fueron firmados por la misma clave privada estén relacionados. Esto previene el double-spending, es decir, que no se pueda gastar más de una vez la misma moneda. El último establece que ningún atacante puede falsificar una firma, previniendo el robo de fondos de Monero por aquellos que no poseen la clave privada apropiada.

Monero además utiliza los conceptos de ZKP en otro aspecto crucial de su privacidad: el ocultamiento de los montos transferidos (amount hiding). La mayoría de las criptodivisas comunican esta información en texto plano. Monero en cambio utiliza commitment schemes y range proofs para ocultar esta información. [3]

La noción de commitment está en el corazón de casi cualquier construcción de los protocolos criptográficos. En este contexto, comprometerse significa simplemente que un jugador en un protocolo es capaz de elegir un valor de algún conjunto (finito) y comprometerse con su elección de tal manera que ya no pueda cambiar de opinión.

Un commitment scheme es una primitiva criptográfica que consiste en un protocolo interactivo de dos etapas entre dos partes denominadas emisor y receptor. Ambas partes son consideradas polinomialmente probabilísticas. La primera etapa corresponde al commit de un mensaje m y que sería al equivalente de cerrar una caja con un valor adentro. La segunda etapa consiste en el reveal del mensaje m al receptor, correspondiente al revelar lo que hay en la caja. Formalmente un commitment scheme tiene que cumplir con dos propiedades: hiding y binding. Hiding significa que un receptor deshonesto no puede obtener ninguna información del mensaje m, durante la etapa de commit. Binding significa que un emisor deshonesto no pueda revelar dos mensajes distintos después de la etapa de commit, es decir que no pueda seleccionar un mensaje m en la etapa de commit y luego revelar otro mensaje m’ en la etapa de reveal.

Range proofs son un tipo de pruebas de conocimiento cero que permite probar que un número está en un determinado rango sin necesidad de revelar ese número. [3]

E. Ejemplo de implementación

zkLedger, desarrollado por miembros del MIT Media Lab, es un sistema que utiliza la tecnología de contabilidad distribuida y la privacidad del cero conocimiento para permitir transacciones confidenciales y seguras en un libro de contabilidad compartido. El propósito es que sea un sistema que pueda ser fácilmente auditado, sin que merme en ningún momento la privacidad.

El sistema zkLedger se divide en tres componentes principales:

La capa de consenso: Esta capa utiliza un algoritmo de consenso distribuido, como Proof of Stake (PoS) o Proof of Work (PoW), entre otros de los disponibles, para asegurar la integridad del libro mayor compartido y validar las transacciones.

La capa de privacidad: Esta capa utiliza la criptografía de conocimiento cero para proteger la privacidad de las transacciones en el libro mayor compartido. Las transacciones

se enmascaran mediante el uso de pruebas criptográficas de conocimiento cero, lo que significa que no es necesario que ninguna de las partes revele su información privada durante la transacción.

La capa de aplicación: Esta capa se encarga de la lógica de la aplicación y los smart contrats, lo que permite que los usuarios interactúen con el libro mayor compartido y realicen transacciones en un entorno seguro y privado.

En resumen, zkLedger utiliza la criptografía de la prueba de conocimiento cero para ocultar la información privada de las transacciones mientras se mantiene la integridad y la seguridad del libro mayor compartido. Esto hace que zkLedger sea una opción atractiva para las aplicaciones de blockchain que requieren privacidad y seguridad mejoradas, como las finanzas descentralizadas y las soluciones de identidad digital. [10]

F. Otras aplicaciones

En el voto electrónico, para preservar la privacidad del votante, se puede usar una prueba de conocimiento cero. Esto permite al votante demostrar que su voto es válido ante una autoridad sin dar a conocer el valor del voto. [9] Estas pruebas tienen utilidad para implementar sistemas seguros de votos electrónicos, como se puede observar en las propuestas [10] y [11] , donde se hacen uso de esta tecnología.

En [10] se utilizan firmas grupales. En este enfoque debe existir una autoridad que emita identidades para los miembros del grupo, autorice a nuevos miembros a unirse e incluso pueda revocar miembros. La utilización de firmas grupales permite que una persona pueda demostrar que forma parte de un grupo sin necesidad de revelar su identidad. Dado que los votos son anónimos, es crucial garantizar que no se entreguen votos falsos ni que una persona vote más de una vez.

En la propuesta [11], se combina el uso de firmas digitales con pruebas de conocimiento cero.

En la autenticación remota también se utiliza este tipo de pruebas. El objetivo fundamental de la autenticación remota de entidades presenta desde sus orígenes vulnerabilidad al fraude de robo de identidad dadas las características inherentes al proceso empleado. En protocolos más simples y poco seguros como el de usuario-contraseña, si no se toman los recaudos necesarios, un espía puede capturar la contraseña y a partir de ese instante imitar al legítimo usuario. Otros protocolos mejoran la situación por asociar la contraseña con algo poseído (autenticación de dos factores) o algo inherente (autenticación biométrica). En otra categoría entran los protocolos de desafío-respuesta en los cuales se establece un diálogo interactivo entre el verificador que plantea desafíos y el pretendiente que los responde. Cualquiera sea el mecanismo, el pretendiente prueba su identidad al demostrar que posee una pieza de información secreta, ya sea exclusiva o estadísticamente asociada a su persona. Sin embargo, en la mayoría de las instancias, la prueba de identidad surge por la exposición parcial (o incluso total) de su información secreta. Aún en el caso de exponerse parcialmente la información secreta, un atacante puede capturar las partes para reconstruir suficiente información como para cometer un fraude de identidad. Esta situación se agrava porque en general la parte de información revelada es variable y el número de sesiones de autenticación progresa en el tiempo, con lo cual aumenta la eficacia de este ataque. Frente a estas limitaciones, se desarrollaron protocolos de autenticación que, a pesar de usar información secreta, no la filtran durante la prueba basados en ZKP. La propiedad de conocimiento cero implica que un pretendiente que ejecuta el protocolo (aún interactuando con un verificador malicioso) no libera ninguna información (acerca de su secreto) y que ese secreto ni siquiera es computable en tiempo polinómico a partir de la información pública que suministra durante el intercambio. Por eso, su participación no incrementa el riesgo de fraude de imitación de identidad. [3]

G. Desafíos actuales

La aplicación de la criptografía de conocimiento cero en el contexto del blockchain plantea desafíos significativos que deben abordarse para su adopción efectiva. Entre estos desafíos se encuentran la eficiencia computacional, la escalabilidad y la interoperabilidad. Los protocolos de criptografía de conocimiento cero pueden ser computacionalmente costosos, por lo que es esencial investigar métodos para mejorar la eficiencia y reducir la carga computacional. A medida que las redes blockchain crecen en tamaño y complejidad, la escalabilidad se convierte en un desafío crucial. Es fundamental explorar soluciones escalables que permitan la aplicación eficiente de la criptografía de conocimiento cero en sistemas distribuidos. Además, integrar la criptografía de conocimiento cero con otros protocolos y sistemas en el blockchain requiere una investigación cuidadosa para lograr una armonización efectiva.

III. CONCLUSIONES

Este trabajo de investigación ha proporcionado una visión actualizada de la criptografía de conocimiento cero y su aplicación en la tecnología blockchain. Se han abordado los fundamentos teóricos de la criptografía de conocimiento cero, sus aplicaciones prácticas y limitaciones, y se han explorado los protocolos existentes aplicables al blockchain.

La criptografía de conocimiento cero ha surgido como una herramienta prometedora para abordar los desafíos de privacidad y confidencialidad en el ámbito del blockchain. A través de su capacidad para permitir que las partes demuestren que se cumple una afirmación sin revelar información adicional más allá de la veracidad de la afirmación en sí misma, la criptografía de conocimiento cero puede ayudar a asegurar la privacidad y la confidencialidad en las transacciones de blockchain.

Se han examinado varios protocolos de criptografía de conocimiento cero aplicables al blockchain. Entre ellos, se incluyen los protocolos de conocimiento cero interactivo y no interactivo, haciendo énfasis en los utilizados en las criptomonedas Zcash y Monero.

Además, se ha presentado un ejemplo de implementación de la criptografía de conocimiento cero en el blockchain a través del sistema zkLedger. Este sistema utiliza la criptografía de conocimiento cero para permitir transacciones confidenciales y seguras en un libro de contabilidad compartido, proporcionando un ejemplo práctico de cómo la criptografía de conocimiento cero puede ser utilizada para mejorar la privacidad y la seguridad en las aplicaciones de blockchain.

Finalmente, se han identificado varios desafíos actuales en la aplicación de la criptografía de conocimiento cero en el blockchain, incluyendo la eficiencia computacional, la escalabilidad y la interoperabilidad. Estos desafíos subrayan la necesidad de una investigación continua en este campo para desarrollar soluciones robustas y eficientes que permitan la

adopción efectiva de la criptografía de conocimiento cero en la tecnología blockchain.

REFERENCIAS

[1] C. V. Moya, J. R. Bermejo Higuera, J. Bermejo Higuera y J. A. Sicilia Montalvo, «Implementation and Security Test of Zero-Knowledge Protocols,» 2023.

[2] D. H. Fernández, Pruebas de Conocimiento Cero, 2020.

[3] N. A. Bukovits, Zero knowledge proofs y sus aplicaciones prácticas, 2023.

[4] A. Nitulescu, zk-SNARKs: A Gentle Introduction.

[5] M. Petkus, Why and How zk-SNARK Works: Definitive Explanation, 2019.

[6] M. Swan, R. Dos Santos y F. Witte, Quantum computing: physics, blockchains, and deep learning smart networks., 2020.

[7] E. d. C. Gutiérrez, Derechos fundamentales y tecnología blockchain. Fundamental rights and blockchain technology..

[8] Z. Song, G. Wang, Y. Yu y T. Chen, «Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior,» 2022.

[9] J. Hasan, «Overview and applications of zero knowledge proof (ZKP).,» *International Journal of Computer Science and Network* , 2019.

[10] W.-B. Fajardo, Blockchain e inteligencia artificial en el sistema de información contable: la disrupción de la partida triple., 2023.

[11] D. C. Jaramillo, «El voto electrónico y retos criptográficos relacionados.,» *Revista de la Facultad de Ciencias*, 2015.

[12] G. J. A.-P. Espuelas, «Estudio y análisis de esquemas de votación electrónica mediante protocolos de firmas digitales anónimas.,» 2017.

[13] A. C. García, «Desarrollo de un sistema de votaciones electrónicas verificables basado en pruebas de conocimiento cero.,» 2021.

[14] J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol y G. Martínez Pérez, «The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends,» 2020.

.