Criptografía Aplicada a la Blockchain

Jeison Eduardo Mena Marín
Estudiante de Maestría en Ciberseguridad
Escuela de Ingeniería en Sistemas
Universidad Internacional San Isidro Labrador
Pérez Zeledón, San José, Costa Ricas

***Abstract* — Cryptography is the foundational pillar that supports the security and integrity of blockchain technologies and cryptocurrencies. This paper explores the application of cryptographic principles within blockchain, focusing on how they secure transactions and operations in major cryptocurrencies such as Bitcoin (BTC), Ethereum (ETH), and Binance Coin (BNB), as well as stablecoins. Through a detailed analysis, the paper explains basic cryptographic concepts, the mining process, the use of hashing algorithms, and the significance of these elements in creating and verifying transactions. The paper emphasizes the importance of understanding cryptography for the secure development of blockchain-based applications, making the topic accessible to readers without prior knowledge.**

Keywords* — *Cryptography, Blockchain, Cryptocurrencies, Mining, Hashing, Bitcoin, Ethereum, Binance Coin, Stablecoins.

***Resumen* —** La criptografía es el pilar fundamental que sostiene la seguridad e integridad de las tecnologías blockchain y las criptomonedas. Este artículo explora la aplicación de los principios criptográficos en la blockchain, centrándose en cómo aseguran las transacciones y operaciones en las principales criptomonedas como Bitcoin (BTC), Ethereum (ETH) y Binance Coin (BNB), así como en las stablecoins. A través de un análisis detallado, el artículo explica conceptos criptográficos básicos, el proceso de minería, el uso de algoritmos de hashing y la importancia de estos elementos en la creación y verificación de transacciones. Se enfatiza la importancia de comprender la criptografía para el desarrollo seguro de aplicaciones basadas en blockchain, haciendo el tema accesible para lectores sin conocimientos previos.

Palabras clave* — *Criptografía, Blockchain, Criptomonedas, Minería, Hashing, Bitcoin, Ethereum, Binance Coin, Stablecoins.

I. INTRODUCCIÓN

La criptografía, desde sus inicios en la antigüedad como técnica para proteger la comunicación mediante la codificación de mensajes, ha recorrido un largo camino para convertirse en una de las tecnologías más esenciales y sofisticadas del mundo moderno, especialmente en el ámbito de la seguridad digital. Con el advenimiento de la era digital, la criptografía ha evolucionado significativamente, adaptándose a las nuevas necesidades y desafíos que surgen en un mundo cada vez más conectado y dependiente de la información.

En el contexto de blockchain y criptomonedas, la criptografía se erige como la piedra angular que garantiza la seguridad, privacidad e integridad de las transacciones y datos. Estas tecnologías disruptivas, que permiten la creación de sistemas descentralizados y sin intermediarios, dependen en gran medida de los principios criptográficos para funcionar de manera segura y eficiente. La capacidad de realizar transacciones en un entorno donde la confianza no se delega en una autoridad central, sino que se distribuye a través de una red de nodos, es posible gracias a la aplicación rigurosa de técnicas criptográficas.

Este artículo tiene como objetivo desmitificar los conceptos fundamentales de la criptografía en el contexto de blockchain y criptomonedas, brindando una explicación detallada y accesible de cómo estas técnicas se implementan en la práctica y por qué son tan cruciales para el funcionamiento seguro del ecosistema criptográfico. A lo largo del documento, se abordarán temas clave como la minería, el proceso de hashing, y la importancia de

los algoritmos criptográficos en la creación y verificación de transacciones, con el fin de proporcionar una comprensión profunda y clara que sea accesible incluso para aquellos que no tienen conocimientos previos en el tema.

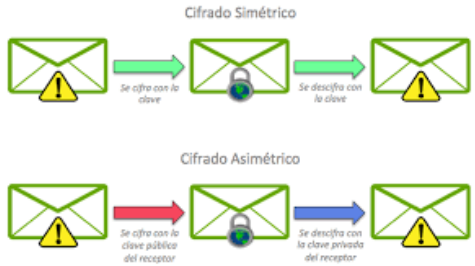
II. FUNDAMENTOS DE CRIPTOGRAFIA

La criptografía, en términos simples, es el arte de escribir o resolver códigos. En el ámbito digital, se refiere a las técnicas utilizadas para proteger la información mediante la transformación de datos legibles en un formato que solo puede ser descifrado por aquellos que poseen la clave correcta. Hay dos tipos principales de criptografía utilizados en blockchain: criptografía simétrica y criptografía asimétrica.

Criptografía Simétrica: Utiliza una sola clave para cifrar y descifrar la información. Es rápida y eficiente, pero su seguridad depende de mantener la clave secreta.

Criptografía Asimétrica: Utiliza un par de claves, una pública y otra privada. La clave pública se usa para cifrar los datos, y solo la clave privada correspondiente puede descifrarlos. Este método es fundamental en la blockchain, donde permite la creación de firmas digitales y la protección de transacciones.

Figura 1: Ilustración sencilla de cómo funciona los tipos de cifrados.



Fuente: ***https://informaticatutoriales.com/encriptacion-asimetrica-simetrica/***

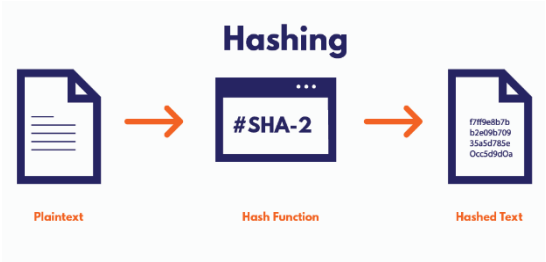
En la Figura 1, se presentan una de paso de como se diferencian los tipos de cifrados, donde en la simétrica necesita solamente una sola clave, mientras en la asimétrica es compuesta de 2 tipos de claves, pública y privada.

III. BLOCKCHAIN: ARQUITECTURA Y SEGURIDAD

Una blockchain es esencialmente una base de datos distribuida que registra todas las transacciones que han tenido lugar en la red. Está compuesta por bloques, y cada bloque contiene un conjunto de transacciones. La seguridad de la blockchain se basa en la criptografía, que garantiza que una vez que se ha agregado un bloque a la cadena, no se puede modificar sin alterar todos los bloques posteriores, lo cual es prácticamente imposible.

El Rol del Hashing: El hash es una función criptográfica que convierte una entrada en una cadena de caracteres de longitud fija, lo que facilita la verificación de la integridad de los datos. En la blockchain, cada bloque contiene el hash del bloque anterior, creando una cadena de bloques interconectados y asegurando que cualquier alteración sea evidente.

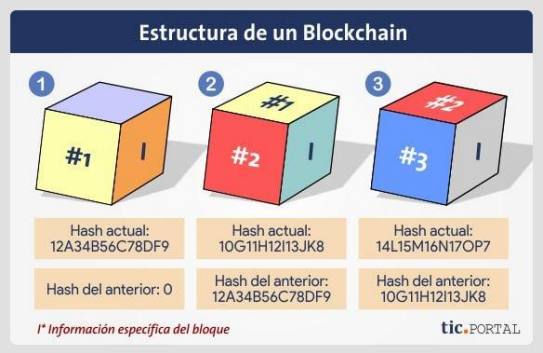
Figura 2: Ilustración del funcionamiento del hashing



Fuente: ***https://www.linkedin.com/pulse/blockchain-hash-function-kumar-singh/***

En la Figura 2, se presentan un ejemplo sencillo de como es aplicado el hashing a un texto, y este mismo una vez procesado el resultado es una serie de caracteres alfanuméricos que no podrá ser reconocido.

Figura 3: Explicación de los bloques en blockchain bajo su idea de cadena segura.



Fuente: https://www.ticportal.es/glosario-tic/blockchain

Figura 3: En la imagen se puede observar cómo cada bloque en la cadena contiene tanto su propio hash como el hash del bloque anterior. Este mecanismo crea un vínculo entre los bloques, formando una cadena en la que cada uno está conectado al siguiente. De esta manera, se garantiza la integridad de la información y se mantiene un control riguroso sobre la secuencia de bloques, haciendo que cualquier intento de alterar un bloque afecte a todos los subsiguientes.

IV. MINERÍA DE CRIPTOMONEDAS: BITCOIN, ETHEREUM Y BINANCE COIN

La minería es el proceso mediante el cual se validan y registran las transacciones en la blockchain. Los mineros compiten para resolver problemas criptográficos complejos, y el primer minero en resolver el problema puede agregar un nuevo bloque a la cadena y recibir una recompensa en criptomonedas.

A. Bitcoin (BTC): Bitcoin es la primera y más conocida criptomoneda, y utiliza el algoritmo SHA-256 para la minería. Los mineros resuelven problemas matemáticos utilizando grandes cantidades de poder computacional, lo que asegura que las transacciones sean válidas y evita el doble gasto.

B. Ethereum (ETH): Ethereum, a diferencia de Bitcoin, permite la creación de contratos inteligentes, que son programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Ethereum utiliza el algoritmo Ethash para la minería, que está diseñado para ser resistente a los ASIC (circuitos integrados de aplicación específica), promoviendo una minería más descentralizada.

C. Binance Coin (BNB): Binance Coin se originó como un token en la blockchain de Ethereum, pero posteriormente se trasladó a su propia blockchain, Binance Chain. Aunque BNB no se mina en el sentido tradicional como BTC y ETH, juega un papel crucial en el ecosistema de Binance, incluyendo la reducción de tarifas de transacción y la participación en las Ofertas Iniciales de Monedas (ICO) en Binance Launchpad.

Figura 4: Ejemplo de máquinas mineras.

En la Figura 4, se presentan las máquinas mineras con tarjetas de video, conocidas como rigs de minería GPU, son sistemas que utilizan tarjetas gráficas para minar criptomonedas, aprovechando su capacidad para realizar cálculos paralelos. Estas GPUs, inicialmente diseñadas para gráficos, fueron muy demandadas en la minería, lo que disparó sus precios hasta tres veces más. Sin embargo, con la bajada de precio en las criptos y la aparición de máquinas especializadas llamadas ASIC, mucho más eficientes, las GPUs perdieron protagonismo en la minería de criptomonedas populares como Bitcoin, aunque siguen siendo usadas en otras monedas y proyectos.

V. STABLECOINS: SEGURIDAD Y ESTABILIDAD EN CRIPTOMONEDAS

Las stablecoins son un tipo especial de criptomoneda diseñada para mantener un valor estable en relación con un activo subyacente, como el dólar estadounidense. Estas monedas utilizan varios mecanismos para mantener su valor estable,

como la reserva de activos físicos o la implementación de algoritmos de estabilización.

Criptografía en Stablecoins: Aunque las stablecoins están diseñadas para ser menos volátiles que otras criptomonedas, siguen utilizando criptografía para garantizar la seguridad de las transacciones y la integridad de la cadena de bloques. Algunos ejemplos de stablecoins incluyen Tether (USDT) y USD Coin (USDC), que están respaldadas por reservas en dólares estadounidenses

VI. VULNERABILIDADES Y AMENAZAS EN BLOCKCHAIN Y CRIPTOMONEDAS

A pesar de su robustez, la criptografía no es completamente infalible. Existen varias amenazas y vulnerabilidades que podrían comprometer la seguridad de las blockchain y criptomonedas, como los ataques del 51%, donde un solo actor controla más del 50% de la potencia de hash de la red, y la aparición de computadoras cuánticas, que podrían romper los algoritmos criptográficos actuales.

Figura 5: Ilustración del ataque del 51%

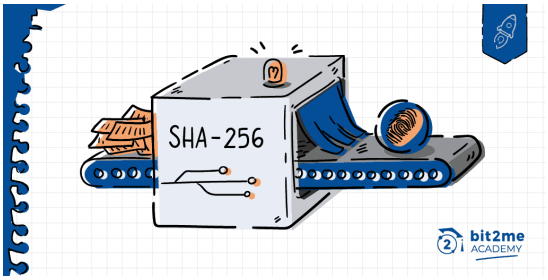
Fuente: https://www.bitcoin.com.mx/que-es-un-51-attack-y-como-podria-afectar-a-bitcoin/

En la Figura 5, la ilustración muestra lo que sucede cuando un solo actor o grupo adquiere más del 50% de la potencia de cómputo en una red blockchain. Esta situación les permite manipular la red, revertir transacciones ya confirmadas o bloquear nuevas transacciones, lo que compromete gravemente la integridad y la seguridad de la blockchain.

VIII. DESARROLLO DE APLICACIONES SEGURAS EN BLOCKCHAIN

El desarrollo seguro de aplicaciones basadas en blockchain requiere una comprensión profunda de la criptografía y las mejores prácticas en su implementación. Esto incluye la gestión segura de claves, el uso de algoritmos criptográficos robustos y la protección contra ataques comunes, como el phishing y la inyección de código malicioso.

Figura 6: Ilustración del procesamiento de información para obtener un resultado



Fuente: ***https://academy.bit2me.com/sha256-algoritmo-bitcoin/***

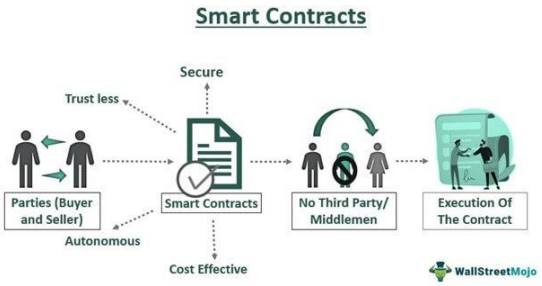
IX. CRIPTOGRAFÍA EN SMART CONTRACTS

Los Smart Contracts o contratos inteligentes son programas informáticos autoejecutables que se almacenan y se ejecutan en una blockchain. La particularidad de estos contratos es que sus términos y condiciones están escritos en código, y se ejecutan automáticamente cuando se cumplen las condiciones predefinidas. Esto elimina la necesidad de intermediarios, ya que las reglas y consecuencias de los acuerdos se codifican directamente en el software.

Desde el punto de vista criptográfico, los contratos inteligentes se apoyan en algoritmos criptográficos para asegurar que solo las partes autorizadas puedan ejecutar y verificar las condiciones del contrato. Por ejemplo, utilizan *ECDSA (Elliptic Curve Digital Signature Algorithm)* para crear firmas digitales que autentican la identidad de los participantes y aseguran que la información transmitida no haya sido alterada. Además, la criptografía asimétrica y los algoritmos de hashing garantizan que las transacciones dentro de un smart contract sean inmutables y verificables, lo que aumenta la confianza en que el contrato se ejecutará

tal como fue programado, sin posibilidad de fraude o manipulación.

Figura 6: Ilustración del funcionamiento de un Smart contracts.



Fuente:https://imagenz.net/imagen-blogs/cybersecurity-of-smart-contract/

Figura 6: La ilustración muestra cómo un smart contract se ejecuta automáticamente en una blockchain al cumplirse ciertas condiciones. Este mecanismo permite la realización de transacciones y acuerdos peer-to-peer (P2P) entre dos partes, sin la intervención de intermediarios, garantizando que los términos del contrato se cumplan de forma automática y transparente.

X. CONCLUSIONES

La criptografía desempeña un papel crucial en la seguridad y funcionalidad de las tecnologías blockchain y las criptomonedas. Es el cimiento sobre el cual se construyen transacciones seguras, contratos inteligentes, y sistemas descentralizados, asegurando la integridad y la confianza en un entorno sin intermediarios. Desde la minería hasta los algoritmos de hashing, los principios criptográficos garantizan la inviolabilidad y el correcto funcionamiento de las blockchain. Sin embargo, con el avance de la computación cuántica, surge un nuevo desafío que podría poner en riesgo estos sistemas. Por ello, es imperativo que los desarrolladores y las organizaciones permanezcan a la vanguardia de la investigación en criptografía post-cuántica, para asegurar que las tecnologías blockchain continúen siendo seguras y resistentes frente a las amenazas del futuro.

XI. REFERENCIAS

[1] A. M. Antonopoulos, *Internet del Dinero*. Alamut, 2017..

[2] S. Nakamoto, "Bitcoin: Un sistema de dinero electrónico entre iguales," 2008. [En línea]. Disponible en: https://bitcoin.org/bitcoin.pdf. [Accedido: 11-ago-2024]..

[3] M. A. Bravo y J. A. Rodríguez, "Criptografía aplicada a blockchain y criptomonedas: Un enfoque práctico," *Revista Española de Ciberseguridad*, vol. 3, no. 1, pp. 45-67, 2019.

[4] J. R. Molina, "La seguridad de las criptomonedas: Vulnerabilidades y mecanismos de protección," en *Ciberseguridad y Criptoeconomía*, Universidad Autónoma de Barcelona, pp. 89-104, 2020.

[5] P. A. Sánchez, "Computación cuántica y su impacto en la criptografía moderna," *Revista Iberoamericana de Tecnología*, vol. 12, no. 3, pp. 23-36, 2021.