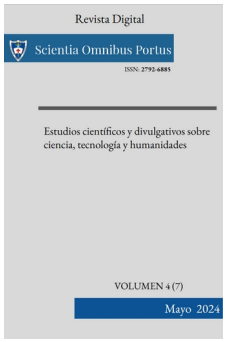
SciOP. 2024, 4(7)
Scientia Omnibus Portus
ISSN: 2792-6885
https://iescelia.org/ojs



Artículo

ATAQUE DEL 51% EN BLOCKCHAIN: GOLPE A LA DEMOCRACIA DIGITAL

Francisco José de Haro Olmo
I.E.S. Celia Viñas
fjharo@iescelia.org

Resumen: Blockchain se ha introducido en la actualidad como una de las tecnologías disruptivas que más crece en los últimos años, incorporando sus ventajas a diversos ámbitos de aplicación y sectores productivos. A pesar de contar con unas propiedades robustas en cuanto a seguridad y confianza, no está exenta de riesgos que podrían suponer un ataque a la estructura de la red de nodos que componen la cadena de bloques. El ataque del 51% puede suponer una forma democrática de corromper el sistema y llevarlo a su destrucción una vez esquilmado sus recursos mediante técnicas de invalidación de transacciones o expedición de doble gasto. La constante protección de este tipo de tecnologías debe ser motivo de preocupación y dedicación, de forma que se garantice la estructura y el buen funcionamiento del sistema.

Palabras clave: blockchain, ataque 51%, mineros, hash, democracia

Introducción

La tecnología blockchain se ha convertido en un tema de gran relevancia e interés por su aplicación en diversos ámbitos y sectores productivos. Su potencial para transformar la realidad tecnológica ha cautivado la atención de investigadores, desarrolladores y empresas, no solo las relacionadas con las criptomonedas ya que su utilidad y aplicación va más allá. En esencia, la tecnología blockchain se define como un libro mayor digital distribuido e inmutable que registra transacciones de manera segura y transparente. A diferencia de los sistemas tradicionales centralizados, donde la información reside en un único servidor, la tecnología blockchain distribuye los datos entre una red de participantes, lo que la convierte en resistente a la manipulación y el fraude. Esta característica fundamental, junto con otras como la trazabilidad, la capacidad de auditoría y la automatización, ha impulsado el auge de la tecnología blockchain en una amplia gama de aplicaciones. Desde las criptomonedas y las finanzas descentralizadas hasta la gestión de la cadena de suministro, la identidad digital y el registro de activos, la tecnología blockchain está demostrando ser un catalizador para la innovación y la eficiencia.

En el ámbito de la investigación, la tecnología blockchain abre un sinfín de posibilidades para explorar nuevos conceptos y soluciones. Entre los temas de investigación más relevantes se encuentran el desarrollo de algoritmos de consenso más eficientes, la mejora de la escalabilidad y la privacidad de las transacciones, y la exploración de aplicaciones en sectores como la salud, la energía y el gobierno. La tecnología blockchain representa un paradigma revolucionario en la era digital, con el potencial de transformar la forma en que interactuamos, transaccionamos y compartimos información.

Tecnología blockchain

Satoshi Nakamoto, en 2008, publica el libro blanco de Bitcoin [1], introduciendo el primer sistema de efectivo electrónico peer-to-peer basado en blockchain. El lanzamiento de Bitcoin en 2009 marca un punto de inflexión en la historia de la tecnología blockchain, demostrando su viabilidad práctica y atrayendo una atención significativa a su potencial.

La tecnología blockchain cuenta con una serie de elementos específicos:

- Libro mayor. Es la estructura de almacenamiento de información, un libro de contabilidad distribuido. Esto significa que todos los miembros participantes de la blockchain tienen una copia idéntica de esta base de datos distribuida.
- Protocolos de consenso. Cada vez que un nuevo bloque es introducido en la red, necesita ser validado por la mayoría de los miembros pertenecientes a la red blockchain y esto se consigue a través de los protocolos de consenso. Entre los más conocidos se encuentran Proof of Work (PoW), Proof of Stake (PoS), Delegate Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Leased Proof-of-Stake (LPoS), Proof-of-Elapsed-Time (PoET), Proof-of-Activity (PoA), Proof-of-Importance (PoI), Proof-of-Capacity (PoC), Proof-of-Burn (PoB) y Proof-of-Weight (PoW).
- Mineros. Son los nodos de la red que crean los nuevos bloques. Para ello tienen que resolver un complejo problema criptográfico que requiere mucha potencia de cálculo, el nodo que primero resuelve el reto es el responsable de crear el nuevo bloque y por tanto recibe una recompensa.
- Infraestructura de Clave Pública (PKI). Este tipo de criptografía permite no sólo identificar unívocamente los nodos participantes de la red blockchain y facilitar la comunicación entre ellos mediante claves público-privadas, sino también identificar bloques y transacciones de forma segura e irrepetible en el sistema. Se utilizan funciones hash (por ejemplo, SHA-256) para validar el contenido de cada bloque dentro de la cadena.
- Nodos. Red de nodos que componen toda la cadena de bloques.

En el aspecto de la seguridad, la tecnología blockchain tiene características muy específicas:

- ✔ Inmutabilidad. Una vez validada una transacción, se convierte en permanente y no puede modificarse.
- ✔ Disponibilidad. Estar basado en una base de datos distribuida significa alta disponibilidad.
- ✔ Integridad. La aplicación de funciones criptográficas para validar una transacción aumenta el nivel de integridad de la información y evita la inclusión de información corrupta, en cuyo caso el bloque sería rechazado al no poder verificarse su contenido con las funciones hash almacenadas. Además, cuando cada bloque mantiene una referencia a su predecesor, incluyendo el resultado de la función hash del mismo, lo que nos permite realizar la validación de toda la cadena.
- ✔ Transparencia. El hecho de que todas las transacciones se almacenen en el libro mayor y que se pueda rastrear cualquier transacción es especialmente atractivo para muchos campos de aplicación.
- ✔ Auditoría. Existe un registro de información suficiente sobre las transacciones que lleva a cualquier verificación de las mismas y de su veracidad.
- ✔ Tolerancia a fallos. Característica relacionada con el concepto de descentralización añadido a los mecanismos de consenso que validan las transacciones.

- ✔ Coherencia. El diseño descentralizado del Ledger y la aplicación de funciones criptográficas hace posible que la información almacenada en la cadena se preserve de forma permanente y sin posibilidad de modificarla sin ser detectada.
- ✔ Privacidad. La identidad de los implicados en una transacción se protege mediante funciones criptográficas, un concepto relacionado con la capacidad de anonimato en blockchain.
- ✔ Anonimato. La pseudomización o anonimización, según el caso, es proporcionada por funciones criptográficas de forma que no se conozca la verdadera identidad de los participantes en la blockchain. Esto es posible mediante el uso de criptografía de clave pública-privada.

Por otro lado, también existen los contratos inteligentes [2] (smart contracts, en inglés), término que fue acuñado por Nick Szabo en 1994, la idea de acuerdos autoejecutables mediante protocolos informáticos. Los contratos inteligentes emergen como una herramienta para la ejecución automática de acuerdos y transacciones sobre la base de la tecnología blockchain. Estos contratos se programan con términos específicos y se almacenan en la red blockchain, garantizando su cumplimiento automático una vez que se cumplen las condiciones predefinidas.

Algoritmos de consenso

Los algoritmos de consenso son componentes esenciales de las redes blockchain, garantizando la coherencia y el acuerdo entre los participantes sobre el estado actual de la cadena de bloques. Estos algoritmos resuelven el problema del doble gasto, asegurando que una unidad de valor digital no pueda gastarse más de una vez.

Prueba de Trabajo (PoW):

Los nodos compiten por resolver un complejo problema matemático, utilizando poder computacional. El primer nodo que resuelve el problema agrega un nuevo bloque a la cadena y recibe una recompensa. Como desventaja se puede resaltar que consume mucha energía y recursos computacionales. Bitcoin utiliza PoW como su algoritmo de consenso principal. La red recompensa a los mineros con bitcoins recién creados por verificar transacciones y agregar nuevos bloques a la cadena de bloques.

Prueba de Participación (PoS):

Los nodos validadores apuestan una cantidad de criptomonedas para participar en el proceso de consenso. El nodo seleccionado al azar para validar un bloque recibe una recompensa. En este caso supone la ventaja de ser mś eficiente energéticamente que PoW y permite una mayor escalabilidad. Por otro lado, como desventaja podría ser vulnerable a ataques si la mayoría de las apuestas se concentran en pocos nodos. El algoritmo, denominado Ethereum 2.0, utiliza PoS para validar transacciones y agregar bloques a la cadena.

Otros Algoritmos de Consenso:

Prueba de Autoridad (PoA): basado en la reputación de nodos preseleccionados.
Prueba de Actividad (PoA): que recompensa a los nodos por realizar actividades útiles para la red.
Prueba de Consenso Bizantino Asíncrono (ABFT): caso del algoritmo de consenso más complejo que permite mayor escalabilidad.

Los algoritmos de consenso son pilares fundamentales de las redes blockchain, garantizando la integridad y confiabilidad de las transacciones. Cada algoritmo tiene sus propias ventajas y desventajas, y la elección adecuada depende de las necesidades específicas de cada red.

Estructura de la cadena de bloques

La tecnología blockchain se compone de bloques, unidades de datos que almacenan información específica (figura 1). Cada bloque contiene:

- ✔ Registro de transacciones: se trata de un conjunto de transacciones agrupadas, como transferencias de criptomonedas o registros de datos.
- ✔ Hash del bloque anterior: conforma un identificador único que vincula el bloque actual al bloque precedente, creando una cadena cronológica.
- ✔ Marca de tiempo: un sello de tiempo o timestamp que supone un registro de la hora en que se creó el bloque.
- ✔ Datos adicionales: dependiendo de la implementación de blockchain, puede incluir información adicional como firmas digitales o metadatos.
- ✔ Hash del bloque actual: consiste en el hash del contenido de todos los campos que conforman el bloque y que sirve de firma digital para validar la información contenida y asegurar su carácter permanente e inmutable. Resaltar que entre los campos incluidos para aplicar el hash, se encuentra el hash del bloque anterior, algo que refuerza el orden de las transacciones almacenadas en la blockchain.

En el contexto de blockchain, el campo denominado NONCE ("number once" o número único) es un valor numérico aleatorio que se utiliza en el proceso de minería de bloques para encontrar un hash o clave criptográfica que cumpla con los requisitos de dificultad de la red.

Función principal del NONCE consiste en ajustar el hash. De esta forma el campo NONCE se modifica continuamente por los nodos mineros para generar diferentes valores hash para el mismo bloque de transacciones. El objetivo es encontrar un hash que comience con una cantidad específica de ceros consecutivos, lo que se conoce como la dificultad de la red.

Existe una relación entre el número NONCE y la minería en blockchain:

- Recepción de un nuevo bloque: donde los nodos de la red pertenecientes a la blockchain reciben un nuevo bloque sin un hash final válido.
- Ajuste del NONCE: cada nodo participante de la blockchain comienza a modificar el valor del NONCE dentro del bloque.
- Cálculo del hash: a cada nuevo valor de NONCE, se calcula el hash del bloque utilizando una función criptográfica.
- Verificación del hash: se verifica si el hash generado cumple con la dificultad de la red, es decir, si comienza con la cantidad requerida de ceros consecutivos.
- Envío de la solución: el nodo que encuentra un hash válido lo envía a la red con el objetivo de ser el nodo que ha conseguido "minar" el bloque y que recibirá una recompensa por haberlo conseguido.
- Validación y agregación: cuando el hash es válido, los nodos de la red verifican la solución y agregan el bloque a su propia copia de la cadena de bloques. Una característica de blockchain es que la cadena de bloques se encuentra distribuida entre todos sus nodos.

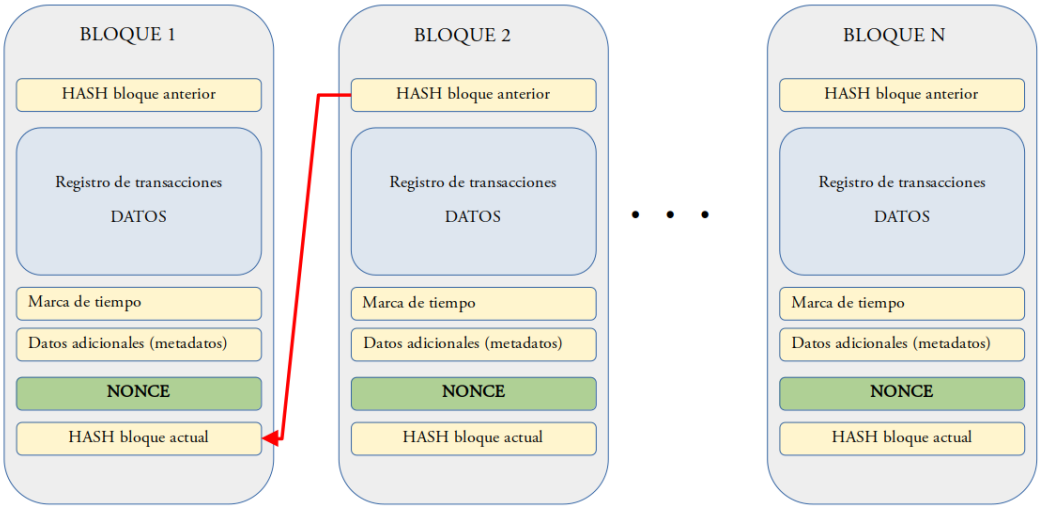


Figura 1. Estructura básica de la cadena de bloques en la tecnología blockchain.

Ataque del 51% en blockchain

Un ataque del 51% en una red blockchain [3,4]ocurre cuando una entidad o grupo de entidades obtiene el control de más del 50% del poder de hash de la red. Este control le permite al atacante realizar diversas acciones maliciosas que comprometen la integridad y el funcionamiento de la red. Este tipo de ataque puede producir consecuencias como la anulación de una transacción validada por otros mineros, algo que le estaría robando autoridad a los mineros "honestos".

Se trata de un escenario donde, al menos el 51%, de los mineros controla el poder de determinar las claves criptográficas que validan un bloque dentro de la blockchain, lo que le permite tomar el control sobre ella. Esto se puede llevar a cabo mediante la toma del control de más del 50% de la tasa de hash de mineria de la red blockchain, o bien mediante el control de más del 50% de los tokens en staking en blockchain. Un token es una unidad digital de valor que representa un activo o utilidad específica dentro de un ecosistema blockchain. Los tokens funcionan de manera similar a las unidades de cuenta tradicionales, como las monedas o los puntos de fidelización, pero con la ventaja de estar asegurados y respaldados por la tecnología blockchain.

Fases del ataque:

I. Adquisición de poder de hash: el atacante concentra una cantidad significativa de poder de hash, ya sea mediante la inversión en hardware de minería, el alquiler de servicios de minería en la nube o la toma de control de nodos existentes.
II. Reorganización de la cadena de bloques: el atacante modifica o revierte transacciones previamente confirmadas, creando una nueva cadena de bloques que refleja sus cambios.
III. Doble gasto: se consigue gastar las mismas criptomonedas en dos o más transacciones, aprovechando su control sobre la cadena de bloques para validar ambas transacciones.
IV. Negación de servicio: impedir que otros nodos validen transacciones o agreguen nuevos bloques a la cadena, interrumpiendo el funcionamiento normal de la red.

Este tipo de ataque conlleva unas consecuencias que van desde las pérdidas financieras en las que los usuarios pueden perder sus criptomonedas, un daño en la reputación de la blockchain al menoscabar la confianza y la seguridad. La centralización del poder y "asaltar" la blockchain, aproderandose de la toma de decisiones a la hora de validar las transacciones que forman parte de un bloque que se valida para formar parte de la cadena de bloques.

La importancia del impacto de este tipo de ataque es grave, ya que se consigue acabar con la descentralización y democratización de la red blockchain, unas de las principales características de esta tecnología.

Algunas recomendaciones a la hora de prevenir este tipo de ataque pasan por incrementar la dificultad computacional requerida para minar bloques, evitando que una sola entidad se apodere de la creación de los hash. Promover la descentralización fomentando la participación de una gran cantidad de nodos en la red dificulta la concentración del poder de hash. Desarrollar protocolos de consenso alternativos puede introducir elementos de seguridad al adoptar algoritmos de consenso más resistentes a ataques del 51%, como la Prueba de Participación (PoS).

Conclusiones

La democratización en la generación de claves criptográficas por parte de todas las entidades participantes en la red de nodos de blockchain puede dar lugar a un tipo de ataque si alguna entidad consigue hacerse con el 51% del poder de la toma de decisones. Si se consigue alterar el código fuente de algunos nodos participantes de forma que ya no tengan intereses alineados con el sistema en su conjunto, sino más bien tienen como objetivo la destrucción de la cadena de bloques a la vez que aprovecharse de los activos que puedan sustraer mediante el modus operandi del ataque. La tecnología debe incorporar mecanismos que detecten la "falta de honestidad" o de compromiso con los objetivos del sistema, con las reglas de funcionamiento originales que se dieron en la creación de la cadena de bloques. Sería interesante disponer de mecanismos adecuados que tras detectar conductas impropias, expulse a los nodos implicados directamente de la red de nodos de la cadena de bloques, asegurando el sistema ante este tipo de ataque democrático, que no cumple con las normas dadas inicialmente entre todos los participantes. El concepto de nodo cualificado o nodo certificado, que periódicamente se somete a controles de validación, podría suponer una forma de control sobre el buen funcionamiento del sistema en su conjunto, descartando a los nodos que no cuenten con la certificación necesaria al no haber superado las pruebas periódicas de validación y "honestidad".

Referencias bibliográficas

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf

[2] de Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. *Sensors*, *20*(24), 7171. https://doi.org/10.3390/s20247171

[3] X. Yang, Y. Chen and X. Chen, "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 261-265, doi: 10.1109/Blockchain.2019.00041.

[4] Y. Hao, "Research of the 51% attack based on blockchain," *2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA)*, Changchun, China, 2022, pp. 278-283, doi: 10.1109/CVIDLICCEA56201.2022.9824528.

Biografía.

Francisco José de Haro Olmo (Almería, 1974), es Doctor en Informática por la Universidad Almería y Máster en Criminología por la UNED. Funcionario de Carrera del Estado perteneciente al cuerpo de Profesores de Enseñanza Secundaria, especialidad de Sistemas y Aplicaciones Informáticas, con destino en I.E.S. Celia Viñas. Imparte docencia en formación profesional desde 2001, Colabora con la Universidad de Almería a través de la docencia en el Grado de Ingeniería Informática y en el Máster en Tecnologías y Aplicaciones en Ingeniería Informática. Entre 2016 y 2020 formó parte de la Red Andaluza de Formación del Profesorado como Asesor Provincial de Formación Profesional, implicándose en proyectos internacionales relacionados con la formación profesional y la transformación digital. Desde 2022 es miembro del Consejo Provincial del Instituto de Estudios Almerienses, área de Ciencias Sociales.