ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.
Volume 3, Issue no. 2, DOI 10.18502/espoch.v4i1.15795
Production and Hosting by Knowledge E

Research Article

Blockchain Algorithm Literature Review

Revisión Bibliográfica de Algoritmo De Blockchain

Ruiz L, Chito F, Jaramillo J, Iguago M, Chango W

Escuela Superior Politécnica de Chimborazo, Morona Santiago, Ecuador

ORCID
Wilson Chango: https://orcid.org/0000-0003-3231-0153

INDEXACIÓN II CONGRESO INTERNACIONAL DE CIENCIA Y TECNOLOGIA MORONA SANTIAGO CICTMS 2021

Corresponding Author:
Chango W

Published: 18 April 2024

Production and Hosting by Knowledge E

Abstract

Within the last decade, blockchain has become a security technology used to protect the integrity of the information contained in a database, especially in collaborative and open systems. One of its main advantages is that it allows consensus to be reached on the new blocks of data that are added to the chain. There are several other techniques in the literature that claim to be popular new mechanisms. Despite this, the number of these technologies has grown too quickly to separate all the possibilities. This work reviews the types of algorithms that can be implemented to have a network supervised by the participants that integrate it.

Keywords: *blockchain, integrity, consensus, algorithm.*

Resumen

En la última década, blockchain se ha convertido en una tecnología de seguridad utilizada para proteger la integridad de la información contenida en una base de datos, especialmente en sistemas colaborativos y abiertos. Una de sus principales ventajas es que permite alcanzar un consenso sobre los nuevos bloques de datos que se añaden a la cadena. Existen muchas otras técnicas en la literatura que pretenden ser nuevos mecanismos populares. a pesar de ello, el número de estas tecnologías ha crecido demasiado rápido como para separar realmente todas las posibilidades. Este trabajo propone revisar los tipos de algoritmos que se pueden implementar para que una red sea supervisada por los participantes que la integran.

Palabras Clave: *Blockchain, Integridad, Consenso, algoritmo.*

1. Introducción

La tecnología Blockchain es una nueva opción y oportunidad de crear una nueva serie de variedad de soluciones a los problemas sociales actuales, Así como Internet reinventó la comunicación, Blockchain puede redefinir las transacciones, los contratos y la confianza que sustentan las empresas, el gobierno y la sociedad. Olson y Wessel explican la cadena de bloques como un registro constantemente actualizado de transacciones mantenidas de forma independiente por los usuarios de Internet; en otras palabras, pueden decir que es un libro mayor distribuido inmutable [1].

La función central de Blockchain o también conocida como cadena de bloques es la gestión segura de un libro mayor compartido donde las transacciones se verifican y almacenan en la red sin una autoridad central, pero gestionadas por los participantes [2].

Las cadenas de bloques pueden ser públicas o privadas, y puede establecer permisos de lectura o escritura en ellas. Los algoritmos, los cálculos y las matemáticas (como las funciones hash criptográficas) unen las cadenas de bloques, lo que permite no solo transacciones sino también proteger la integridad y el anonimato de la cadena de bloques.

Blockchain, al igual que otras tecnologías, ofrece soluciones a diversos problemas, pero también tiene aspectos que se pueden mejorar. Además, tiene muchas ventajas. Sin embargo, se debe considerar la cuestión de los requisitos computacionales para ejecutar algoritmos de consenso de blockchain, por ejemplo, como la potencia informática, ya que algunos de estos algoritmos consumen mucho tiempo y recursos informáticos y computacionales [3]. En este caso encontramos algoritmos basados en prueba de trabajo.

2. Desarrollo y Discusión

2.1. Algoritmo De Consenso

El algoritmo de concenso aplicado en Blockchain conocida como cadena de bloques, es necesario para proporcionar una mayor verificación de los procesos de datos [4]. Teniendo en cuenta a los usuarios que la conforman como los responsables de mantener íntegros estos datos con el fin de evitar la modificación en los bloques que se crean a partir de los nuevos registros donde por votación se encargan de validar si los nuevos cambios realizados son correctos [5]. Los cambios realizados tienen efecto alrededor de todas las bases de datos que conforman el sistema donde esta tecnologías está implementada, es por ello que los usuarios tienen un motivo para cuidar que ninguno de los demás participantes generen un cambio en beneficio de ellos mismos porque esto afectaría negativamente a los demás usuarios, esta tecnología Blockchain esta principalmente en las criptomonedas las cuales proveen de un costo monetario en el caso de generar malas transacciones [6], es por ello que cuidar las bases de datos donde se registran y almacenan son necesarios como propio incentivo para proteger sus fondos.

2.2. Algoritmo Pow en consenso

Es un algoritmo integrado en el método de concenso que tiene como objetivo comprobar que no se realicen ”dobles pagos” a la hora de ejecutar transacciones en las bases de datos con el fin de evitar datos duplicados a la hora de llegar a un concenso

y ejecutar una transacción exitosa, ejemplo al ser datos estos se los pueden duplicar generando un doble valor de transacción al que se tenía.

Entre las diferencias que encontramos de Pow y PoS es determinar quién puede aprobar un bloque de transacciones [7]. La prueba de participación es la alternativa más popular a la prueba de trabajo. Es un mecanismo de consenso diseñado para mejorar algunas de las limitaciones de PoW, como problemas de escalabilidad y consumo de energía.

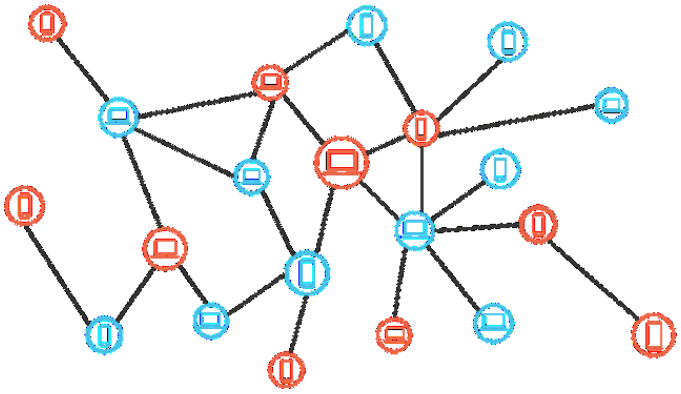

Figura 1

Aplicaciones distribuidas del blockchain.

2.3. Blockchain La Mayor Seguridad

Al ser una tecnología distribuida, cada nodo de la red guarda una copia exacta de la cadena y la disponibilidad de la información está siempre garantizada [8]. Si un atacante quisiera provocar un ataque de denegación de servicio, tendría que cerrar todos los nodos de la red, ya que al menos un nodo en funcionamiento es suficiente para que la información esté disponible. Por otro lado, es casi imposible de cambiar porque es un libro mayor de consenso donde todos los nodos tienen la misma información, lo que garantiza su integridad. Si un atacante quisiera cambiar información en la cadena de bloques, tendría que cambiar al menos el 51% de toda la cadena [9]. La tecnología Blockchain nos permite almacenar información que nunca se puede perder, cambiar o eliminar. Finalmente, dado que cada bloque está matemáticamente vinculado al siguiente, se vuelve inmutable cuando se agrega un nuevo bloque a la cadena. Si un bloque cambia su relación con la cadena, se rompe. Esto significa que toda la información registrada en el bloque es inmutable y permanente.

2.4. Proof-of-Stake (PoS)

La base es la prueba de membresía de algunos de los mecanismos de consenso que utilizan las cadenas de bloques para lograr un consenso compartido. En Prueba de trabajo, los mineros prueban que su capital está en riesgo al gastar energía. Ethereum usa Prueba de participación, donde un validador compromete explícitamente capital en forma de ETH para un contrato inteligente de Ethereum [10]. Este ETH comprometido puede quemarse como garantía si el verificador es deshonesto o perezoso. Los validadores son entonces responsables de verificar que los nuevos bloques distribuidos a la red sean válidos y, de vez en cuando, crean y distribuyen nuevos bloques ellos mismos.

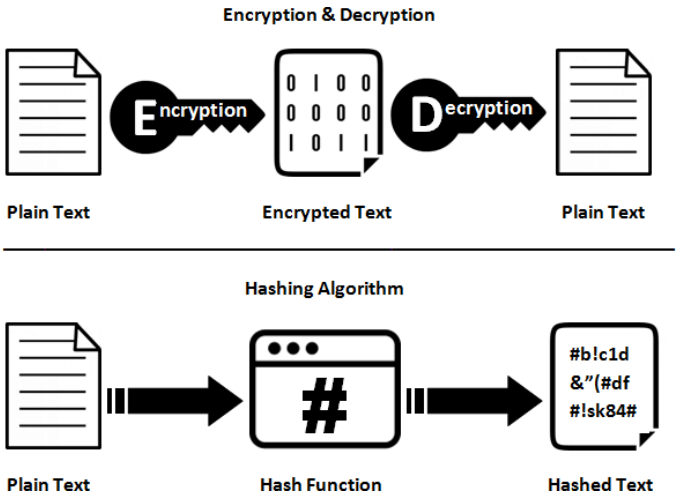

Figura 2

Blockchain encriptado público y privado.

2.5. Delegated Proof of Stake (DPOS)

Para ello, todos los miembros de la red votan por diferentes ”representantes”. Cuando se seleccionan, forman un grupo que permite la ejecución de protocolos tolerantes a fallas bizantinos. Esto se debe a que su número es fijo y finito y tienen una confiabilidad parcial. Los delegados determinan la rotación del liderazgo. Esto significa que cada iteración rota alternativamente el bloque. Como resultado de esta acción, dicho delegado puede crear un bloque y recibir una recompensa por ello [11]. Si el representante no está presente cuando es su turno, debe esperar a un nuevo representante. Los derechos de voto de cada miembro de la red son proporcionales a su nivel de membresía.

2.6. Byzantine Delegated Fault Tolerance (dBFT)

En su artículo de 1982, ”El problema de los generales bizantinos”, Leslie Lamport, Robert Shostak y Marshall Pease describen a un grupo de generales al mando de parte del ejército bizantino para sitiar una ciudad [12]. Los ”errores bizantinos” en el servidor pueden no corresponder al comportamiento del sistema de detección de errores y pueden tener diferentes síntomas para diferentes observadores.

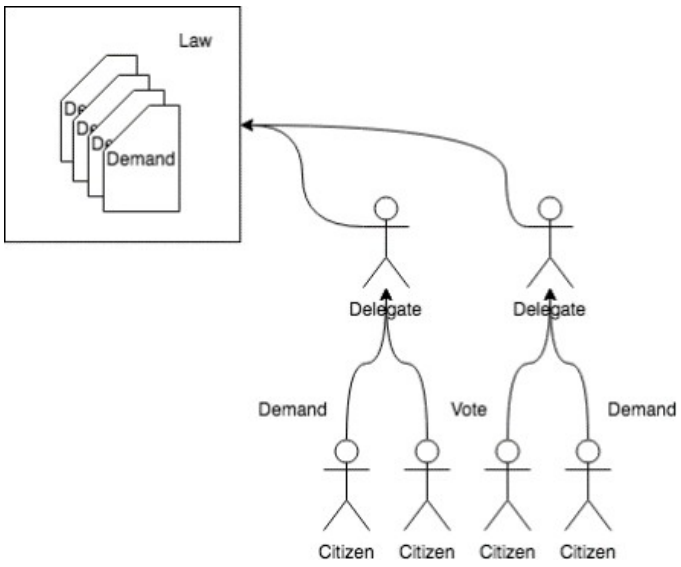

Figura 3

NEO Blockchain Concepts.

2.7. Proof of Capacity (POC)

La prueba de capacidad permite que los nodos de la red blockchain utilicen el espacio disponible en el disco duro para extraer las criptomonedas disponibles. En lugar de repetir constantemente los parámetros numéricos en el encabezado del bloque y volver a codificarlos [13], PoC crea una lista de posibles soluciones en el disco duro del minero antes de que comience la extracción. Cuanta más memoria haya en el disco duro, más soluciones se pueden almacenar, lo que aumenta las posibilidades de que un minero encuentre la función hash deseada en su lista y gane una recompensa en bloque.

Continuando con la analogía de la lotería, si debe acertar tantos números como sea posible para ganar, cuanto más larga sea la lista de posibles respuestas, mayores serán sus posibilidades de ganar. También puede guardar sus boletos de lotería y usarlos repetidamente. La prueba de capacidad incluye dos fases: monitoreo (preparación del disco duro) y extracción.

Uso del Consenso:

En blockchain, el algoritmo de consenso es el mecanismo que utiliza la red blockchain para elegir el estado correcto de un registro después de que se completa una transacción [14]. De esta manera, lo que muestra el algoritmo de consenso se convierte en la verdad para todos los nodos a seguir.

Para evitar que se agreguen bloques defectuosos a la cadena de bloques, cada bloque debe revisarse y verificarse [15], Este proceso ocurre en todas las blockchains, la primera en implementarlo fue Bitcoin. Usando el sistema de consenso de Bitcoin, se decide si un bloque contiene la información correcta y, por lo tanto, se puede agregar a la cadena de bloques.

Uno de los requisitos para que el proceso de verificación sea óptimo es que todos los nodos acepten los datos para confirmar su integridad. Esto también se aplica si algunos nodos están inactivos o no son confiables.

Los mineros son esenciales para incluir transacciones en un bloque. Sin embargo, los nodos de la red son los encargados de validar la información contenida en dichos bloques. Por esta razón, es importante contar con los nodos más completos de la red Bitcoin. Si desea ejecutar un nodo completo en la red Bitcoin, hay una buena guía en el sitio web oficial que puede seguir.

Si una persona quiere hacer una modificación de forma maliciosa o mal intencionada, tendrá que ser revisada por otros y si no concuerda, será desaprobada.

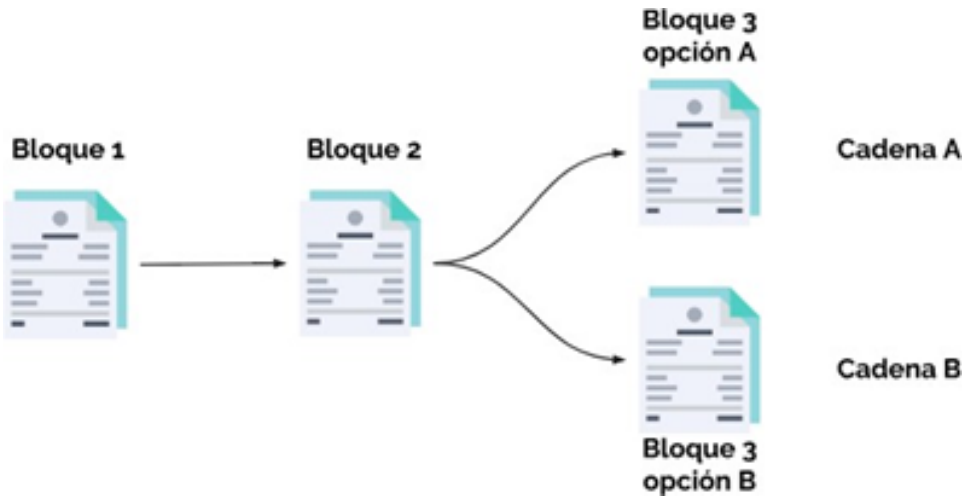

Figura 4

Consenso mediante bloques.

2.8. Males asociados al uso de Blockchain

Gartner descubrió que la mayoría de los proyectos de cadena de bloques solo están diseñados para registrar datos en la plataforma de cadena de bloques utilizando la tecnología de registro descentralizado (DLT), ignorando características clave como el consenso descentralizado, los tokens o los contratos inteligentes.

En su forma actual, la tecnología blockchain no logra un ”crear, leer” completo. ”Actualizar, eliminar” en la tecnología tradicional de administración de bases de datos solo admite ”crear” y ”leer”. ”Los CIO deben evaluar los requisitos de gestión de datos para sus proyectos de cadena de bloques. En algunos casos, las soluciones tradicionales de gestión de datos pueden ser la mejor opción”.

El Big data aplicado en blockchain

En las bases de datos crea un aumento en la seguridad y sirve como una relación fundamental a la hora de aumentar el procesamiento de información debido a que el Blockchain crea un panorama de red común con nodos similares que se conectan en una gran cantidad alcanzando los miles o millones, es por ello que aplicando el Big Data permite un mayor procesamiento de información que se complementa con el consenso para los respectivos cambios de información en los bloques de datos, teniendo críticas de algoritmo bien definidas como deontológico, teleológica y valores de diseño.

Los contratos inteligentes son quizás el aspecto más poderoso de la tecnología habilitada para blockchain. Añaden un comportamiento dinámico a las transacciones.

Conceptualmente, un contrato inteligente puede entenderse como un procedimiento almacenado asociado con un registro de transacción específico. Sin embargo, a diferencia de los procedimientos almacenados en los sistemas centralizados, todos los nodos de una red de igual a igual ejecutan los contratos inteligentes, lo que crea problemas de escalabilidad y capacidad de administración que no se han resuelto por completo. La tecnología de contratos inteligentes seguirá experimentando cambios importantes.

Si bien los problemas de gobernanza para las cadenas de bloques autorizadas o privadas generalmente los maneja el propietario de la cadena de bloques, la situación es diferente para las cadenas de bloques públicas [16]. La gobernanza de las cadenas de bloques públicas como Ethereum y Bitcoin se trata principalmente de cuestiones técnicas.

Se aborda el comportamiento humano o la motivación. Los CIO deben ser conscientes de los riesgos que los problemas de gobernanza de blockchain pueden representar para el éxito de sus proyectos [17]. Las grandes organizaciones deberían

considerar unirse o formar consorcios para ayudar a definir modelos de gobernanza para cadenas de bloques públicas.Conclusiones

Con el desarrollo actual de nuevas tecnologías basadas en blockchain, es posible que esto se aplique a áreas sin criptomonedas. Esta técnica proporciona una forma segura y encriptada para que las transacciones no puedan ser manipuladas, garantiza la inmutabilidad e inmutabilidad de los datos. Aunque la primera aplicación del blockchain es la criptomoneda y su uso se ha generalizado hacia los contratos inteligentes, los cuales recientemente han llamado la atención en diversos campos, por ejemplo: industrial, salud, IoT, inmobiliario, etc.

Para que un nuevo bloque sea incluido en la cadena de bloques es necesario que los nodos lleguen a un acuerdo único en la red, para tomar esta decisión se utiliza un método o protocolo de consenso. Por lo general, estos métodos de consenso se llaman en función de la naturaleza de cualquier aplicación. La tecnología Blockchain y su seguridad dependen de estos protocolos. Para estos métodos debe haber diferentes nodos o mineros participando en la red, la capacidad de enviar información entre sí con un alto grado de seguridad. garantiza una comunicación entre pares segura y eficiente.

Conflicto de Intereses

Todos los investigadores declaran no tener conflicto de intereses al momento de presentar o reproducir la información generada en el proceso de investigación.

References

[1] Chang L, Sheng P. Research on maximizing influence of blockchain social network based on BCLT model. Discrete Dynamics in Nature and Society. 2022;2022:1–8.

[2] Kably S, Arioua M, Alaoui N. Lightweight direct acyclic graph blockchain for enhancing resource-constrained IoT environment. Computers, Materials and Continua. 2022;71(3):5271–5291.

[3] Zhang W, Kaur M. A novel QACS automatic extraction algorithm for extracting information in blockchain-based systems. IETE Journal of Research. 2022;1–13.

[4] Yang W, Ziyang W, Xiaohao Z, Jianming Y. The optimisation research of Blockchain application in the financial institution-dominated supply chain finance system. International Journal of Production Research. 2022;66(1):1–21.

[5] Ramakurthi V, Manupati VK, Machado J, Varela L, Babu S. An innovative approach for resource sharing and scheduling in a sustainable distributed manufacturing system.

Advanced Engineering Informatics. 2022;52(9):101620.

[6] Mizuyama H, Yamaguchi S, Suginouchi S, Sato M. Simulation-based game theoretical analysis of Japanese milk supply chain for food waste reduction [Springer Nature Switzerland.]. IFIP Advances in Information and Communication Technology. 2022;2022:107–115.

[7] Shahbazi Z, Byun YC. Knowledge discovery on cryptocurrency exchange rate prediction using machine learning pipelines. Sensors (Basel). 2022 Feb;22(5):1740.

[8] Yadav AS, Singh N, Kushwaha DS. Sidechain: Storage land registry data using blockchain improve performance of search records. Cluster Computing. 2022;25(2):1475–1495.

[9] Chang R, Xames Y. Incorporating tamper-resistant, publicly verifiable random number seeds into permissionless blockchain systems. Articulo (ID); 2022. p. 165616.

[10] Priya J, Palanisamy C. Novel block chain technique for data privacy and access anonymity in smart healthcare. Intelligent Automation and Soft Computing. 2023;35(1):243–259.

[11] Taskou SK, Rasti M, Nardelli PH. Energy and cost-efficient resource allocation for blockchain-enabled NFV. IEEE Transactions on Services Computing. 2022;15(4):2328–2341.

[12] Zhao X, Wang S, Zhang Y, Wang Y. Attribute-based access control scheme for data sharing on hyperledger fabric. Journal of Information Security and Applications. 2022;67(103182):103182.

[13] Benedict S. Shared mobility intelligence using permissioned blockchains for smart cities. New Generation Computing. 2022;40(4):1009–1027.

[14] Xihua Z, Goyal SB, Tesfayohanis M, Verma C. Blockchain-based privacy-preserving approach using SVML for encrypted smart city data in the era of IR 4.0. Journal of Nanomaterials. 2022;2022:1–8.

[15] Yang Y, Liu Z, Liu Z, Xie Y, Chan KY, Guan X. Joint optimization of edge computing resource pricing and wireless caching for blockchain- driven networks. IEEE Transactions on Vehicular Technology. 2022;71(6):6661–6670.

[16] Yadav K, Alharbi A, Jain A, Ramadan AR. An IoT based secure patient health monitoring system. Computers, Materials and Continua. 2022;70(2):3637–3652.

[17] Yahaya AS, Javaid N, Ullah S, Khalid R, Javed MU, Khan RU, et al. A secure and efficient energy trading model using blockchain for a 5G-deployed Smart Community. Wireless Communications and Mobile Computing. 2022;2022:1–27. https://doi.org/10.1155/2022/6953125.