Capítulo 2

Blockchain y ciberseguridad: fortaleciendo la confianza digital*

DOI: https://doi.org/10.25062/9786287602700.02

Jaider Ospina Navas
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo explora el estado del arte de la tecnología *blockchain,* con miras a identificar su papel en la construcción de un ecosistema digital seguro. Para ello precisa los aspectos que caracterizan la cadena de bloques como la descentralización, la inmutabilidad y el consenso; discute sus ventajas en términos de seguridad, transparencia y resistencia a la manipulación; analiza los diferentes tipos de ataques en materia de inmutabilidad que se reconocen a la fecha; describe los diferentes tipos de aplicaciones en que se emplea *blockchain,* y presenta los desafíos y limitaciones actuales, proporcionando una visión holística de las posibilidades y obstáculos en este campo en evolución.

Palabras clave: *blockchain;* confianza digital; descentralización; ecosistema digital; inmutabilidad; transparencia.

* Capítulo de libro resultado del proyecto de investigación *"Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio"*, del grupo de investigación *"Ciberespacio Tecnología e Innovación"*, de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no necesariamente reflejan los de las instituciones participantes

Jaider Ospina Navas
Doctorando en Sistemas de Información. Magíster en Ciencias de la Información y las Comunicaciones e ingeniero electrónico, Universidad Distrital Francisco José de Caldas, Colombia. Consultor en ciberseguridad y arquitecto en soluciones en la nube.
https://orcid.org/0000-3251-3017 - Contacto: **jaider.ospina@esdeg.edu.co**

Citación APA: Ospina Navas, J. (2024). Blockchain y ciberseguridad: fortaleciendo la confianza digital. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 47-76). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.02

TECNOLOGÍAS DISRUPTIVAS, LOGÍSTICA Y SEGURIDAD Y DEFENSA NACIONAL EN EL CIBERESPACIO
ISBN impreso: 978-628-7602-69-4
ISBN digital: 978-628-7602-70-0
DOI: https://doi.org/10.25062/9786287602700

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra “General Rafael Reyes Prieto”
Bogotá D.C., Colombia
2024

Introducción

Este capítulo explora el estado del arte de la tecnología cadena de bloques (*blockchain*), con miras a identificar su papel en la construcción de un ecosistema digital seguro. Como objetivo general se busca precisar las características que permiten construir un ecosistema digital confiable, mediante agentes habilitadores que garanticen la privacidad, confidencialidad y disponibilidad de los datos, así como una visión de las principales limitaciones para su adopción. Para esto se revisan: artículos orientados a la evaluación de aspectos propios de la ciberseguridad, documentación de aplicaciones o iniciativas tendientes a la mejora de la confianza digital y estudios en que se realiza una revisión sistemática de literatura.

Nacimiento de las cadenas de bloque

Si bien el origen de la *blockchain* (BC) se asocia a la publicación del *whitepaper* "*Bitcoin: A Peer-to-Peer Electronic Cash System*", en realidad debe atribuirse al trabajo de Stuart Haber y W. Scott Stornetta, quienes en su artículo "*How to Time-Stamp a Digital Document*", publicado en el *Journal of Criptology*, en 1991, presentaron un sistema de sellado de tiempo digital para certificar la fecha de creación o modificación de un documento electrónico, sin depender del medio físico, mediante el uso de *hash* criptográficos para generar resúmenes únicos de los documentos y su almacenamiento en una cadena de bloques (Haber & Scott, 1991).

Posteriormente, el 1.o de noviembre de 2008, Satoshi Nakamoto, seudónimo empleado por la persona o grupo que creó el concepto y la tecnología subyacente de bitcoin, envía un mensaje a la lista de correos especializado en criptografía metzdowd, en el que anunciaba un nuevo sistema de dinero electrónico basado en

redes *Peer-to-Peer* (P2P). Este documento sentó las bases teóricas y técnicas de la tecnología *blockchain* y expuso de manera concisa los aspectos técnicos que proponía una nueva moneda digital, así como el objeto principal de su creación: prescindir de terceros de confianza.

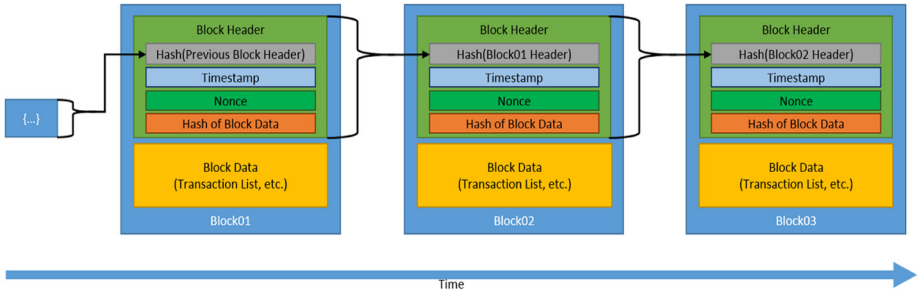
"Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, permitiendo así que dos partes interesadas realicen transacciones directamente sin necesidad de una tercera parte de confianza" (Nakamoto, 2008, s.p.).

De esta manera, nace la más reconocida moneda digital, el bitcoin; y se propone una solución a uno de los mayores problemas de este tipo de divisa: el doble gasto. Mediante el uso de una cadena de bloques descentralizada y un consenso distribuido para validar y registrar las transacciones de forma segura y transparente, características estas heredadas por diferentes sistemas y aplicaciones para generar protección de los datos y generar un ecosistema digital confiable.

Fundamentos de la tecnología *blockchain*

La cadena de bloques se define como una base de datos distribuida y segura que ha revolucionado la forma en que se almacenan y verifican los datos (Xu et al., 2019). Cada bloque de la cadena contiene un *hash* criptográfico del bloque anterior entrelazado mediante un *hash* garantizando una "firma digital" 1 que garantiza su integridad y eventual manipulación, una marca de tiempo y datos de la transacción efectuadas (Figura 1).

Figura 1. *Cadena de bloques genérica*



Fuente: NISTIR 8202 (2018).

En términos generales, BC puede ser concebida como una tecnología de registro de datos descentralizada y segura, que ha emergido como un componente fundamental en la era digital. Según Nakamoto (2008), *blockchain* se define como un "registro público de transacciones" que almacena información de manera inmutable y transparente. La fortaleza de BC radica en su naturaleza descentralizada, donde múltiples nodos de la red verifican y validan las transacciones, eliminando la necesidad de un intermediario central de confianza (Swan, 2015). Esto garantiza la seguridad y la integridad de los datos almacenados, ya que cualquier intento de alteración requeriría el consenso de la mayoría de los participantes, lo que lo hace altamente resistente a la manipulación y a los ataques cibernéticos (Mougayar, 2016; Krichen et al., 2022; Yli-Huumo et al., 2016). Como ya se mencionó, la estructura única de BC la hace resistente a la manipulación, ya que cualquier cambio en un bloque requeriría cambios en todos los bloques siguientes para mantener la coherencia de la cadena (Popchev et al., 2021).

Hablando específicamente del protocolo bitcoin descrito originalmente por Nakamoto, este se apoya sobre la pila de protocolos TCP/IP a partir del cual se construye una red de nodos superpuesta a internet. En ella, los nodos conforman una red P2P donde todos los nodos proveen y consumen servicios simultáneamente mientras colaboran vía un servicio de consenso Vamsi_Cz5cgo y Vamsi_Cz5cgo (2020).

Blockchain y Distributed Ledger Technology

Tecnología de libro distribuido (DLT)

Estrictamente hablando, BC es un tipo específico de DLT y, a su vez, DLT es un caso particular de base de datos distribuida, caracterizada por su proceso de validación consensuado (Romero, 2018). DLT se caracteriza por hacer uso de tres elementos tecnológicos articulados para conformar su arquitectura, ellos son las redes P2P, criptografía asimétrica y algoritmos de consenso. Una diferencia significativa entre DLT y BC radica en su estructura y funcionamiento. Mientras que la DLT puede tener diferentes grados de descentralización y puede ser pública o privada, la BC es completamente descentralizada y generalmente pública (Hurtado, 2021). Algunos ejemplos de plataformas que hacen uso de DLT son Hyperledger Fabric, Corda y Quorum por citar algunas de las más representativas. Estas tecnologías pueden

ser públicas o privadas y customizadas para adaptarse a las necesidades específicas de una aplicación o industria.

Tipos de blockchain

Existen varios tipos de BC, cada uno con sus propias características y capacidades que se adaptan a diferentes necesidades.

Blockchain públicas

Redes a las que cualquier persona puede unirse, verificar transacciones y participar en la validación de bloques. En general, los usuarios son anónimos y ningún participante tiene más derechos que los demás, por lo cual no hay administradores de la red. Son consideradas impulsoras de las tecnologías de contabilidad distribuida DLT y el uso de redes P2P para la distribución de datos (Haleem et al., 2021). Las redes públicas más conocidas son Bitcoin, Bitcoin Cash, Ethereum y Litecoin.

Blockchain privadas

Redes donde el acceso está restringido a un grupo específico de entidades. Suelen ser utilizadas por empresas que desean aprovechar las ventajas de la tecnología BC, pero manteniendo el control sobre quién puede participar en la red y todas las labores de gestión como la creación y aceptación de bloques.

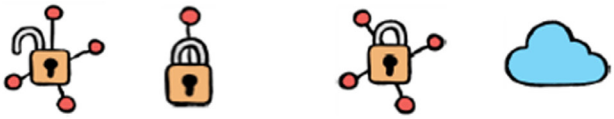
Blockchain federadas o de consorcio

Implementación híbrida de las anteriores. El control no recae en una sola entidad, sino en un grupo, lo que permite que se mantenga cierto nivel de privacidad al tiempo que se aprovecha la seguridad y transparencia de la tecnología BC.

Blockchain como un servicio (BaaS)

Productos que permiten a los usuarios crear sus propias redes sin tener que preocuparse por la infraestructura subyacente, permitiendo a los usuarios centrarse en desarrollar sus aplicaciones sin tener que preocuparse por aspectos técnicos. Finalmente se recogen algunas particularidades de los diferentes tipos de BC en la Figura 2.

Figura 2. *Tipos de redes blockchain*



	Públicos Bitcoin, Ethereum, Litecoin	**Privados** Hyperledger, Corda, Quorum	**Federados** Hyperledger, Corda, Quorum	***Blockchain as a Service*** IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	~	~	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA
No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart *Contracts*	✓	✓	✓	NA
Existe recompensa por minado de bloques	~	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	~	NA
Seguridad basada en protocolos de consenso	✓	✗	~	NA
Seguridad basada en funciones *hash*	✓	~	~	NA
Provee servicios en la nube	NA	NA	NA	✓

✓ Sí ✗ No ~ A veces **NA** No Aplica

Fuente: López (2018).

Generaciones de *blockchain*

En el artículo *"Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption Using BIoT for Smart Government and Industry 4.0"*, Hasan et al. (2022) identifican cinco generaciones de BC desde su aparición: 1.a generación: se centra en la creación de bitcoin por Satoshi Nakamoto en 2008, moneda digital descentralizada que permite transacciones P2P sin necesidad de un intermediario; 2.a generación: introduce la idea de los contratos inteligentes (*Smart Contracts*), programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Ethereum es el ejemplo más conocido; 3.a generación: se centra en resolver los problemas de escalabilidad e interoperabilidad que enfrentan las generaciones anteriores. Proyectos como Cardano y Polkadot están trabajando en soluciones para permitir que diferentes BC interactúen entre sí y para manejar un mayor número de transacciones, pasando de 6 transacciones por segundo (TPS) a 100.000 TPS. Esta generación introdujo las aplicaciones descentralizadas (dApps); 4.a generación: se enfoca en la integración de sistemas empresariales y gubernamentales existentes, proporcionando soluciones para problemas de interoperabilidad, privacidad y seguridad (Banafa, 2022). Ya se alcanza un nivel de 300.000 TPS y aumenta el abanico de aplicaciones a campos como la cadena de suministro, el voto electrónico y Smart Grid, y 5.a generación: la actual y en pleno proceso de gestación, que surge según los expertos con la aparición de proyectos como Relictum Pro (Bitcoin.es, 2020). Se distingue por el uso de máquinas inteligentes y analítica de datos para la automatización de procesos de aplicaciones inteligentes (Choi & Siqin, 2022).

Rasgos distintivos de la tecnología *blockchain*

Algunas características de la BC, y que se convierten en elementos potencializadores de estrategias de ciberseguridad, son la descentralización, la inmutabilidad, la transparencia y el consenso. Estos pilares han transformado la confiabilidad y la seguridad en las operaciones en línea, y su comprensión es esencial para apreciar el potencial de esta tecnología.

Descentralización

En palabras de Tapscott y Tapscott, (2016), la descentralización significa que no existe una autoridad central que controle la red. En lugar de depender de una

entidad centralizada como un banco o un Gobierno, las transacciones se verifican y registran en una red distribuida de nodos que trabajan juntos de manera colaborativa. La eliminación de intermediarios genera confianza y reduce los puntos únicos de fallo, lo que hace que la red sea altamente resistente a la censura y a eventuales ataques que comprometan los datos. La descentralización tiene varias ventajas:

- Proporciona un entorno sin confianza: en una red BC descentralizada, nadie tiene que conocer o confiar en alguien más. Cada miembro posee una copia exacta de los mismos datos en forma de un libro de contabilidad distribuido.
- Mejora la reconciliación de datos: todos los nodos tienen acceso a una vista compartida y en tiempo real de los datos.
- Reduce puntos de debilidad: la descentralización puede reducir los puntos de debilidad en sistemas donde exista dependencia de actores específicos. Un punto de debilidad puede deberse a dependencia de recursos específicos como capacidad de almacenamiento o cómputo.
- Optimiza la distribución de recursos: se optimiza la distribución de recursos, mejorando rendimiento y consistencia de red mediante estrategias como mejora en los tiempos de entrega de contenido.

Inmutabilidad

La inmutabilidad, según Mougayar (2016), es un principio que se refiere a la incapacidad de cambiar o borrar una vez que se ha registrado una transacción en la cadena de bloques. Cada bloque de datos en la cadena se vincula criptográficamente al anterior, lo que hace que sea extremadamente difícil, si no imposible, modificar el contenido de un bloque sin modificar todos los siguientes. Ello asegura que las transacciones registradas sean permanentes y confiables, lo que es esencial en aplicaciones donde la integridad de los datos es crucial, como la atención médica y la gestión de identidades.

Transparencia

En una red BC, todas las transacciones son visibles para todos los participantes de la red, lo que proporciona un alto nivel de transparencia. Es de aclarar que esta transparencia puede presentar desafíos, especialmente cuando se trata de datos sensibles.

Según Sedlmeir et al. (2022), la transparencia establece desafíos en empresas y el sector público relacionados con un grado excesivo de esta. Se señala cómo los tipos de datos sensibles involucrados en diferentes patrones de casos de uso de *blockchain* y se argumenta que las implicaciones de la exposición de información de las BC causada por el almacenamiento y ejecución de transacciones replicadas van más allá de los conflictos a menudo mencionados con el "derecho al olvido" del GDPR y pueden ser más problemáticos de lo previsto. Los autores presentan el equilibrio entre proteger información sensible y aumentar la eficiencia del proceso mediante contratos inteligentes. También exploran hasta qué punto las *blockchain* con permisos y las nuevas aplicaciones de tecnologías criptográficas como las identidades autónomas y las pruebas de conocimiento cero pueden ayudar a superar el desafío de la transparencia y, por lo tanto, actuar como catalizadores para la adopción y difusión de BC en las organizaciones.

Como se acaba de mencionar, una de las maneras propuestas de atacar esta problemática es mediante el empleo de prueba de conocimiento cero o *zero-knowledge proof* (ZKP), técnica criptográfica que puede utilizarse en el entorno de *blockchain* para verificar si el probador tiene suficiente cantidad de transacciones sin filtrar ningún dato privado de transacciones (Konkin & Zapechnikov, 2023).

De manera similar, Sun et al. (2021) realiza un estudio sobre ZKP en el entorno de *blockchain* con el objetivo de resaltar los problemas de seguridad y sus desafíos y discuten un marco, los modelos y las aplicaciones de ZKP. A manera de conclusión, ZKP resulta una herramienta valiosa para mejorar la privacidad y la seguridad en las transacciones de *blockchain*, permitiendo la verificación de las transacciones sin revelar detalles sensibles.

Consenso

El consenso se logra mediante algoritmos gracias a los cuales la "red va tomando decisiones consensuadas, valida la información y asigna las tareas a cada uno de los nodos que la componen" (Criptodemy, n.d.). Este concepto fue expuesto originalmente por Adam Back en mayo de 1997 y buscaba regular el abuso desmedido de recursos de internet, como correos electrónicos y *remailers* anónimos (Back, 2002).

En palabras de Narayanan et al. (2016), el consenso puede ser definido como un proceso mediante el cual los nodos llegan a un acuerdo sobre la validez de una transacción antes de agregarla a la cadena de bloques. El ejemplo más significativo de este tipo de protocolos de consenso se puede hallar en la prueba de trabajo

(PoW), empleada por la criptomoneda bitcoin. Dicho protocolo implica que los mineros compitan para resolver complejos problemas matemáticos y el primero en hacerlo tiene el derecho de agregar un nuevo bloque. Este mecanismo garantiza que todas las partes de la red estén de acuerdo en el estado de la cadena de bloques y que las transacciones sean válidas y seguras.

Algoritmos de consenso

Existen diversos protocolos y algoritmos de consenso para garantizar la seguridad y la confiabilidad de la red; cada uno define sus propias características y ventajas. Algunos son:

Prueba de trabajo (*Proof of Work, PoW*)

PoW es el protocolo de consenso más conocido, asociado principalmente con bitcoin y Ethereum, aunque se utiliza en otras criptomonedas y redes *blockchain.* En esencia, la prueba de trabajo requiere que los nodos de la red realicen un cálculo computacional intensivo para demostrar que han invertido tiempo y recursos en la verificación de transacciones. Este proceso se conoce como *minería* y los participantes se denominan *mineros,* y se repite continuamente para mantener la cadena de bloques segura y distribuida.

Según Narayanan et al. (2016), la prueba de trabajo es esencialmente un rompecabezas matemático complejo que requiere una gran cantidad de poder de cómputo para su resolución. Los mineros compiten para resolver este rompecabezas, y el primero en hacerlo tiene el derecho de agregar un nuevo bloque a la cadena y es recompensado con nuevas monedas (por ejemplo, bitcoins) y tarifas de transacción.

Nakamoto (2008) introdujo por primera vez el concepto de *prueba de trabajo* en el contexto de bitcoin y proporcionó los fundamentos teóricos de su funcionamiento. Su adopción se asemeja, según las propias palabras de Nakamoto, a la presentada por Back (2006) Hashcash, algoritmo que inicialmente se utilizó para abordar el *spam* por correo electrónico y los ataques DDoS, y en la actualidad se utiliza para fines de verificación de transacciones.

PoW, como protocolo de consenso, ha demostrado ser efectivo en la prevención de ataques maliciosos y en la creación de un registro seguro y confiable de transacciones en la red *blockchain.* Aunque su mayor debilidad es su poca capacidad

de escalamiento y rendimiento limitado en términos de transacciones por segundo (TPS). Este protocolo es quizás uno de los mayores aportes de Nakamoto a la creación de la BC, y al mismo tiempo, ha proporcionado una solución a uno de los problemas más desafiantes en el campo de la informática, conocido como el problema de los generales bizantinos. Ventajas: seguridad comprobada, alta resistencia a ataques del 51 %. Desventajas: consumo energético elevado, centralización en minería.

Prueba de participación (*Proof of Stake, PoS*)

En PoS, los validadores bloquean una cierta cantidad de criptomonedas como garantía, y la probabilidad de ser seleccionados para validar un bloque se basa en la cantidad de monedas en juego. Ethereum ha migrado PoS con Ethereum 2.0. Este tipo de consenso se introdujo como una alternativa más eficiente y menos costosa a (PoW). En lugar de requerir que los mineros realicen cálculos computacionales intensos, PoS permite a los participantes de la red crear bloques y validar transacciones en función de la cantidad de monedas que poseen y están dispuestos a "apostar" para el consenso (Ge et al., 2022).

Existe una gran variedad de algoritmos de consenso derivados de PoS, entre ellos DPoS, Snow White, Sleepy Consensus, Ouroboros, Ouroboros Praos, Ouroboros Genesis, Ouroboros Crypsinous, EOS, Improvement of DPoS, entre otros (Ge et al., 2022).

Ventajas: eficiencia energética, menos centralización, incentiva a los poseedores de monedas. Menor barrera de entrada (la red acepta participantes sin necesidad de comprar y configurar hardware costoso). Transacciones más rápidas en comparación con las redes PoW. Desventajas: posible centralización en función de la riqueza, ya que aquellos con más monedas tienen más oportunidades de crear bloques. Problema del "nada en juego", en PoS, no hay un costo real asociado con la validación de bloques incorrectos, lo que puede llevar a problemas de seguridad.

Prueba de participación delegada (*Delegated Proof of Stake, DPoS*)

Se trata de una variante de PoS donde un grupo seleccionado de validadores, elegidos por la comunidad, es responsable de validar las transacciones. EOS es un ejemplo de una cadena de bloques que utiliza DPoS. Ventajas: alta escalabilidad, rapidez en la confirmación de transacciones. Desventajas: menos descentralización, poder concentrado en los nodos elegidos.

Proof of Authority (PoA)

Algoritmo basado en la reputación, donde los validadores no arriesgan criptodivisas sino su reputación, en consecuencia, estos son elegidos de manera arbitraria al considerárseles confiables. Su uso se da principalmente en redes privadas; entre ellas, se distingue su uso en logística, donde se le considera una solución eficiente y razonable, ya que su naturaleza permite aprovechar las características de BC manteniendo la privacidad de los participantes. Ventajas: eficiencia energética, alta velocidad en comparación con PoW y PoS, incentivos monetarios. Desventajas: menor descentralización, ya que se basa en un número limitado de validadores de bloque. Vulnerable a la colusión, pues se confía en un número limitado de validadores, existiendo el riesgo de que estos puedan coludir para actuar malintencionadamente.

Proof of Space and Time (PoST)

Se trata de un nuevo primitivo criptográfico que permite a un probador convencer a un verificador de que ha gastado un recurso de "espacio-tiempo". En palabras de Ortega (2023), "…en el algoritmo de Proof of Space and Time, los nodos de la red deben demostrar que están almacenando una cantidad específica de datos mediante un proceso denominado agricultura" (s.p.). Ventajas: eficiencia energética, llegando incluso a ser posible minar con este algoritmo en dispositivos comunes. Accesible para más participantes. Descentralización del proceso. Desventajas: crecimiento permanente debido que a medida que se añaden más mineros a la red, se requiere más espacio de almacenamiento (Moran & Orlov, 2019).

Round Robin

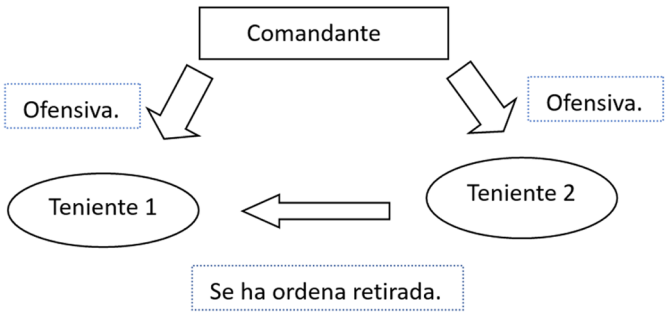
Round Robin en BC ha sido estudiado en varios artículos científicos. Una propuesta de su uso se presenta en Raikwar y Gligoroski (2021), quienes proponen el protocolo de consenso R3V. Este selecciona un conjunto de candidatos a líder de manera rotativa según su antigüedad. Luego, estos compiten para ser el líder del bloque resolviendo un rompecabezas basado en una Función de Retardo Verificable (VDF) (Raikwar & Gligoroski, 2021). Ventajas: mayor resistencia contra la mayoría de los ataques comunes en los protocolos PoS, además de menor consumo de energía, menos complejidad de comunicación y una mayor equidad. Para finalizar, otros algoritmos existentes de menor difusión son prueba de peso (PoW), la prueba de importancia (PoI), la prueba de cobertura (PoC) y gráficos acíclicos dirigidos (DAG).

El problema de los generales bizantinos: una mirada militar

El problema de los generales bizantinos fue anunciado por Robert Shostak y desarrollado con Leslie Lamport y Marshall Pease en 1982 en el centro de investigación científica y tecnológica SRI International (BBC News Mundo, 2020). Y, sin duda, recoge la esencia de la problemática de un consenso en una red en la que existen agentes no confiables. En ella, desde la perspectiva de la teoría de juegos, se proporciona una descripción de la medida en que las partes descentralizadas experimentan dificultades para llegar a un consenso sin que exista un agente central de confianza.

En esencia, se plantea un escenario de guerra donde existe un grupo de generales bizantinos asediando una ciudad desde varios puntos y debe ser acordado si atacar o retirarse de manera coordinada. Entre los generales, solo uno puede impartir la orden a toda la fuerza, pues es el comandante. Al resto de generales se les considera tenientes. Los tenientes se comunican entre sí cuando reciben las órdenes del comandante, y las dos órdenes posibles del comandante son "atacar" y "retirarse". Se conoce que uno o más generales pueden ser traidores. El objetivo es que todos los generales leales NO estén de acuerdo. Para ello, pueden proporcionar información incorrecta. Por ejemplo, si el comandante es un traidor, puede enviar órdenes contradictorias a diferentes tenientes. Si su lugarteniente es un traidor, puede mostrárselo a los demás lugartenientes, para confundirlos y hacerles creer que el traidor es el comandante, que el comandante les envió órdenes contrarias a las órdenes que realmente les envió (Soto, 2020). Una solución acertada en el campo de batalla debe llevar a uno de dos objetivos: 1) todos los tenientes leales toman la misma decisión, y 2) si el comandante es leal, todos los tenientes cumplirán fielmente sus órdenes. La Figura 3 ilustra el caso en que el "teniente 2" es un traidor.

Figura 3. *Teniente 2 es un traidor*



Fuente: Lamport et al. (1982).

Este tipo de problemas son asociados a la necesidad de consenso y la posibilidad de que existan actores poco confiables en el sistema. Un sistema informático confiable debe lidiar con componentes que funcionan mal y que brindan información contradictoria a varias partes del sistema. El problema es encontrar un algoritmo que garantice que los generales leales lleguen a un acuerdo. Se demostró que, utilizando únicamente mensajes verbales, este problema podría resolverse si y solo si más de dos tercios (2/3) de los generales fueran leales. Un traidor puede confundir a dos generales leales. Esta problemática se traslada al mundo de *blockchain* cuando se requiere agregar un nuevo bloque a la cadena, donde cada nodo debe estar de acuerdo en el estado del sistema antes de que este pase a ser parte de esta. Claramente en el contexto que nos atañe, la "lealtad" es un aspecto constitutivo de la confianza.

Amenazas en una red *blockchain*

El aspecto más sobresaliente en la construcción de un sistema seguro que ofrece BC es su inmutabilidad. No obstante, esta no tiene garantía del 100 % de ser invulnerable. BC puede ser comprometida bajo ciertas circunstancias. Algunos de estos posibles escenarios son:

- Ataque del 51% (51% Attack): este tipo de ataque se debe a la posibilidad de que un grupo de mineros controle más del 50 % del poder de cómputo de la red, pudiendo con ello cambiar y reorganizar la cadena de bloques (afectando su integridad), invalidando transacciones anteriores y creando una cadena alternativa. Sin embargo, realizar un ataque del 51 % en una red con una gran cantidad de mineros es extremadamente costoso, aunque se han identificado ataques de este tipo (Sayeed & Marco-Gisbert, 2019).
- Ataque Sybil: recibe su nombre del libro *Sybil* (Schreiber, 1973) y del relato de una mujer diagnosticada con trastorno disociativo. El ataque se caracteriza por corromper redes P2P mediante la creación de identidades falsas. La vulnerabilidad de una red BC a este ataque dependerá del costo de generar identidades, el grado en que el sistema de reputación acepta nuevas identidades, y si el sistema de reputación trata a todas las entidades de manera idéntica. Mohaisen y Kim (2013) identifican tres principales estrategias de defensa: 1) entidades certificadoras de confianza; 2) pruebas

de recursos (pruebas de IP, coordenadas de red y resolución de algoritmos entre otros), y 3) redes sociales (Mohaisen y Kim, 2013).

- Ataques de doble gasto: aunque la mayoría de las cadenas de bloques están diseñadas para prevenir el doble gasto, en ciertas circunstancias, un atacante podría intentar gastar la misma criptomoneda dos veces antes de que la red actualice su estado. Este riesgo se da en cadenas con confirmaciones de transacciones lentas. Existen diferentes tipos de ataques de doble gasto, entre ellos un estudio reciente presenta un tipo de ataque bautizado Adaptive Double-Spending Attack (Adaptive DSA) como un ataque avanzado de doble gasto en BC basadas en PoW. En este, el atacante duplica una transacción válida en la red y se convierte en un proceso de decisión de Márkov (PDM) y mediante la explotación focalizada en programación dinámica estocástica (SDP), se explotan estrategias optimizadas de ataque Adaptive DSA (Zheng et al., 2023).
- Presencia de vulnerabilidades del protocolo: los errores o vulnerabilidades en el *software* o el protocolo de una cadena de bloques pueden ser explotados para comprometer la inmutabilidad. Por ejemplo, errores en la implementación del código pueden permitir que un atacante realice transacciones inválidas o altere el estado de la cadena.
- *Forks* y actualizaciones del protocolo: a veces, una cadena de bloques puede experimentar una bifurcación (*fork*) o una actualización del protocolo que podría afectar la inmutabilidad. Si una comunidad no está de acuerdo sobre los cambios en el protocolo, podría dar lugar a dos cadenas separadas (*hard fork*), lo que podría tener implicaciones para la inmutabilidad y la continuidad de la cadena.

Blockchain, tecnología disruptiva

La tecnología BC es una de las mayores innovaciones del siglo XXI, con un impacto significativo en sectores que van desde el financiero, manufactura, votaciones electrónicas y educación, por citar algunos. Esta sección recoge algunas revisiones sistemáticas realizadas por terceros en los que se ha evaluado el impacto de BC en diferentes áreas, buscando con ello validar la hipótesis de cómo la implementación de la tecnología *blockchain* puede incrementar significativamente la confianza digital al proporcionar un sistema descentralizado y transparente que garantiza la integridad y la inmutabilidad de los datos, lo que podría redundar en

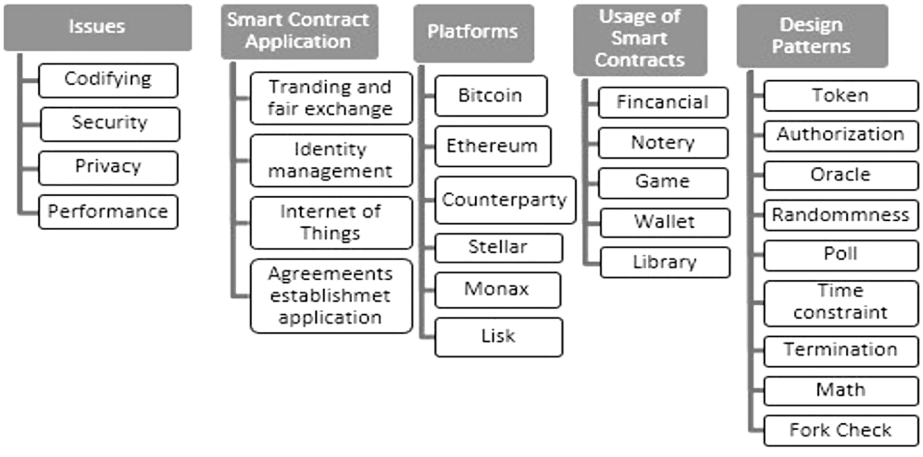
una mayor adopción de servicios digitales, una reducción en el fraude y una mejora en la eficiencia de las transacciones digitales.

Trabajos como el de Baena y García (2022) permiten, tras una rigurosa revisión bibliográfica, establecer un consenso respecto de los beneficios de seguridad, transparencia, trazabilidad, confianza, autenticidad y privacidad y la reducción de costes en las cadenas de suministro, mediante el uso de la cadena de bloques.

Por su parte, Xu et al. (2019) realizan un estudio de 756 artículos, los cuales fueron decantados a 119 bajo los criterios de economía y negocios y destacan el potencial impacto en áreas como el *crowdfunding* y la gestión contable, el almacenamiento y compartición de datos, la administración de las cadenas de suministro y el comercio inteligente para beneficiarse de las características de BC (Xu et al., 2019).

El estudio de Leka evalúa 292 *papers* extraídos de bases de datos como IEEE, ACM, Science Direct y Springer; centrando su diagnóstico final en 28 y se centra en el uso de BC en *smart contratcs,* identificando como sus principales vulnerabilidades los errores de código, los ataques maliciosos y las explotaciones de los mineros y los usuarios. También revisa algunas herramientas y métodos para verificar y auditar los contratos inteligentes. En la figura 4 se aprecia un esquema de clasificación que resulta interesante, toda vez que se aprecia qué aspectos como la codificación, la seguridad, la privacidad y el desempeño son trasversales a cualquier tipo de aplicación y campo donde se haga uso de BC, por lo que conviene asumir su enfoque taxonómico para evaluar casos particulares de uso (Leka et al., 2019).

Figura 3. *Esquema de clasificación de smart contracts*



Fuente: Leka et al. (2019).

Romero (2018) resalta el uso de la tecnología de registro distribuido (DLT) en transacciones financieras, identificando ventajas como la aceleración del proceso de liquidación de transacciones financieras, la reducción del número de intermediarios y la mejora de la eficiencia del proceso de reconciliación. Además, se vislumbra cómo puede mejorar la transparencia y la trazabilidad de las transacciones, aspecto especialmente útil en el comercio internacional, donde hay muchos actores y facilita la negociación y posnegociación de valores, el cumplimiento regulatorio y la gestión de la identidad digital. Reforzando este aspecto, resulta clara la tendencia hacia una total digitalización de la economía. Aspectos como la transformación digital cimentada sobre la cuarta Revolución Industrial, lleva a una economía considerada como digital (Bogdanov et al., 2021), donde BC se esgrime como elemento habilitador tecnológico.

A esta altura, resulta evidente que el impacto de BC se ha expandido más allá de su uso en criptomonedas. BC se ha convertido en un pilar en diversos campos, como la cadena de suministro, la atención médica y la protección de la propiedad intelectual. Según Tapscott y Tapscott (2016), *blockchain* proporciona una mayor visibilidad y trazabilidad en la cadena de suministro, permitiendo el seguimiento en tiempo real de productos desde su origen hasta su destino. En el sector de la salud, Griggs et al. (2018) señalan que *blockchain* garantiza la seguridad y la privacidad de los registros médicos electrónicos, facilitando el intercambio seguro de información entre médicos y pacientes. Además, en el ámbito de los derechos de autor y la propiedad intelectual, *blockchain* ofrece un registro inmutable de la autoría y la propiedad de contenido digital, lo que puede ser fundamental para la protección de los derechos de los creadores (Lorenzo, 2020).

En general, BC puede ayudar a mejorar la confianza y la colaboración entre diferentes partes en sectores como la industria 4.0. Así lo presenta Haleem et al. (2012; 2022), quien destaca varios aspectos habilitadores de BC en campos como las *smart cities, smart factories,* productos inteligentes y cadena de suministro.

A nivel de responsabilidad social, resulta interesante la propuesta del uso de BC como instrumento de auditoría y modelo de operación (Martínez et al., 2020). Esto gracias al uso del modelo de registro de datos que se puede llevar a cabo en las billeteras (*wallets*).

Autores como Haleem et al. (2021) identifican una amplia gama de aplicaciones y funcionalidades de BC, como la contabilidad distribuida que permite la transmisión segura y auditada de registros médicos de pacientes y la gestión de la cadena de suministro de medicamentos; aunque se identifica como principal obstáculo la poca experiencia que se tiene en el medio de las aplicaciones que hacen

uso de la tecnología BC. Otra ejemplificación de uso de BC, se da en la cadena de suministro de medicamentos (Casino et al., 2019).

De otra parte, escenarios arquitecturales en los que se emplea BC como solución a problemáticas en la centralización de recursos en redes IoT permiten en lugar de almacenar datos de sensores centralizadamente, realizarlo sobre la base distribuida de BC donde los datos de los sensores pueden ser gestionados de manera similar a la filosofía *blockchain* (Conoscenti et al., 2017).

Blockchain y ciberseguridad

Si bien ya se han mencionado algunas características que convierten a BC en agente dinamizador de la ciberseguridad, algunos aspectos que vienen a reforzar son:

Ventajas y beneficios

- Mayor seguridad y protección de datos debido a su estructura inmutable.
- Mejora de la transparencia y la integridad de los datos mediante la auditoría y verificación distribuida.
- Arquitecturas con alta disponibilidad y resilientes.
- Reducción de los puntos de vulnerabilidad y riesgo mediante la descentralización y la resistencia a ataques cibernéticos.

Aplicaciones prácticas de *blockchain* en la ciberseguridad

- Protección de identidad y autenticación mediante sistemas IDMS (identity management systems). Estos permiten administrar, la autenticación, autorización y compartición de archivos.
- Registro y verificación de eventos de seguridad para la detección de intrusiones y análisis forense.
- Gestión de acceso y control de datos mediante contratos inteligentes.
- Contabilidad distribuida, transparencia operacional.
- Arquitecturas redundantes y resilientes.

Desafíos y consideraciones en el uso de *blockchain* en la ciberseguridad

- Escalabilidad y rendimiento.
- Privacidad y protección de datos personales en entornos BC transparentes.

- Actualización y mantenimiento de la infraestructura BC para garantizar la seguridad a largo plazo.
- Colaboración y desarrollo de estándares BC orientados en ciberseguridad.
- Colaboración entre los actores involucrados, como desarrolladores, investigadores y usuarios finales.
- Declaración de buenas prácticas de implementación BC en entornos ciberseguros.

Construcción de un ecosistema de confianza digital

Son numerosos y diversos los campos de uso de la tecnología *blockchain* y sus potencialidades de construcción de confianza digital. Pero esta, como toda tecnología, no representa una panacea y su adopción es un proceso que debe ser construido día a día y con la participación de todos los interesados (*stakeholders*) y sobre todo garantizar su uso como un medio y no como un fin. *A priori,* BC concibe una seguridad por diseño cimentada en sus características de inmutabilidad, integridad y transparencia. Una vez las transacciones se confirman, los datos se almacenan permanentemente en el libro mayor, a prueba de manipulaciones, y se salvaguardan estas transacciones. En términos de diseño, la tecnología BC incluye criptografía y consenso distribuido como mecanismos preventivos para reducir los riesgos de ciberataques y una arquitectura distribuida sin requerimientos de entidades centrales de "confianza". Sin intermediarios confiables, la confianza dentro de una red BC es posible gracias a cuatro características clave: 1) libro mayor (*ledger*): proporciona trazabilidad transaccional. A diferencia de las bases de datos tradicionales, las transacciones en BC no se eliminan; 2) seguridad: los datos se consideran criptográficamente seguros, garantizando la no manipulación; 3) compartido: el libro mayor es compartido entre varios participantes, lo que provee transparencia, y 4) carácter distribuido: permite escalar el número de nodos de una red BC para hacerla más resistente a eventuales ciberataques y optimizar la entrega y consumo de contenido.

De esta manera, aunado a pilares clave de la seguridad de la información (inmutabilidad-integridad, disponibilidad-redes distribuidas y redundantes, trasparencia-auditoria distribuida) aunado en la construcción y adopción de prácticas y estrategias en ciberseguridad, a la postre, permiten construir un ecosistema digital confiable.

En el plano nacional, es de resaltar que el Ministerio de Tecnologías de la Información y las Comunicaciones, de manera expresa, manifiesta la potencialidad en generación de confianza digital:

> La clave en DLT/*Blockchain* es generar "Confianza" en las transacciones que se realicen en la red, al punto que no se requieran ni documentos físicos (Papeles) o entidades centralizadas (Bancos o Notarios) para poseer un título que represente valor social o económico. (MinTIC, 2022, s.p.)

En el contexto nacional es importante resaltar la integración entre el gobierno y el Banco Interamericano de Deasarrollo (BID) para el impulso de BC mediante iniciativas como el espacio de experimentación de proyectos con BC en el sector público, que nace mediante la firma de un memorando de entendimiento con BID Lab, el laboratorio de innovación del BID.

Así mismo, el MinTIC publicó la "Guía de referencia para la adopción e implementación de proyectos con tecnología *blockchain* para el Estado colombiano". Esta facilita el acercamiento del Estado a esta tecnología y promueve un enfoque ético y de cumplimiento, proporciona además un enfoque de gobernanza, presenta lineamientos para el desarrollo de proyectos en entidades gubernamentales y brinda herramientas para que los proyectos sean diseñados y operados organizada, escalonada y estructuradamente.

Discusión

No obstante, lo prometedor de BC como tecnología de alto impacto en diferentes campos y sus potencialidades para garantizar prácticas de ciberseguridad deben abordarse responsablemente sus desafíos. Problemáticas como la limitación en escalabilidad derivada del tamaño que puede llegar a tener BC, se solucionaría mediante la implementación de algoritmos de poda de cadena, lo que implica que "transacciones antiguas podrían ser eliminadas, guardando de ellas solo su hash, para preservar la integridad de la cadena" (Pérez & Joancomartí, 2014).

Los desafíos a que se enfrenta la BC en entornos descentralizados pueden ser superados mediane el empleo de protocolos de red como Named Data Networking (NDN). Esto puede contribuir al impulso de BC en aspectos como la entrega efectiva de contenido, gracias al uso de enrutamiento basado en nombres y almacenamiento en caché en la red, permitiendo la entrega eficiente de contenido y mejorar

la entrega de datos, especialmente en redes descentralizadas donde la eficiencia es crucial (Guo et al., 2019; Kharjana et al., 2023). No obstante, es de aclarar que NDN no presenta compactibilidad directa con BC, ya que las aplicaciones de BC (sin permisos) generalmente requieren la transmisión de transacciones y bloques en tiempo real, lo cual no es compatible con el diseño *"pull"* de NDN.

Es bajo esta premisa que BoNDN (BC sobre NDN) se presenta como alternativa de integración. Este se basa en un diseño central de NDN y trata cada tipo de datos que necesita ser transmitido individualmente (Guo et al., 2019). BoNDN, además, propone un enfoque de suscripción-push para soportar la transmisión de bloques, en el cual cada minero realiza una suscripción, y una vez que se genera un bloque, el minero suscrito recibirá el bloque (Benmoussa et al., 2023).

En el campo del desarrollo de aplicaciones, el surgimiento de patrones arquitecturales propios para BC es ya una realidad que presagia la evolución de la tecnología en cuestión. Alzhrani et al. (2023) describen doce patrones aplicables a 400 aplicaciones existentes en la actualidad.

En esta misma línea, se halla el desarrollo de algoritmos y librerías tolerantes a fallas bizantinas BFT. Castro y Liskov (2001) describen un nuevo algoritmo BFT de replicación, concebido para el diseño de sistemas altamente disponibles que toleren fallos bizantinos. El algoritmo es empleado en entornos asíncronos como internet, incorpora mecanismos que previene nodos defectuosos y permite una rápida recuperación de réplicas de forma proactiva. Su tolerancia a fallos se garantiza siempre que menos de 1/3 de las réplicas presenten fallos en la ventana de falla. Castro y Liskov (2001) también presentan una implementación del algoritmo como una biblioteca genérica y su aplicación para construir el primer sistema de archivos NFS tolerante a fallos bizantinos.

Ahora bien, alternativas de autenticación diferentes a las tradicionales, como el uso de encriptación basada en atributos (ABE), garantizan que solo aquellos que poseen ciertos atributos pueden acceder a la información puede ser una solución efectiva para el control de acceso y la compartición de datos encriptados (Hong et al., 2022). ABE puede dividir generalmente en dos patrones: ABE de política de texto cifrado (CP-ABE) y ABE de política de clave (KP-ABE). La política de acceso se incorpora en los textos cifrados y la clave privada del usuario se asocia con una colección de atributos como la ubicación, rango de edad, direcciones de correo entra otros. No obstante, ABE puede ser vulnerable a ataques como el abuso y la custodia de claves (Arshad et al., 2023). En resumen, ABE es una herramienta poderosa

para el control de acceso y la compartición de datos, pero presenta desafíos que deben abordarse para su implementación efectiva.

En términos de confianza, las llamadas redes BC sin permiso, brindan capacidades de confianza entre partes sin conocimiento previo entre sí. Este principio puede permitir efectuar transacciones directamente, lo que resulta en que las transacciones se entreguen más rápido y con costos más bajos. Por otro lado, una red BC que controle más estrictamente el acceso, llamada redes con permiso y donde existe cierto nivel de confianza entre las partes, presenta capacidades que ayudan a reforzar esa confianza.

Otro aspecto fundamental es el desempeño que resulta de la alta relevancia para permitir la evolución de una tecnología; esto es prometedor dado el aumento de transacciones por segundo (TPS) al pasar de 4-6 TPS desde la primera generación BC a 100.000-300.000 TPS en la cuarta y las potenciales que se alcanzará en una quinta generación con la adopción de tecnologías como 6G (Hasan et al., 2022).

No podría faltar en este discernimiento la disponibilidad de las redes BC. El interactuar permanente con el ciberespacio ha creado una fuerte dependencia de las aplicaciones y espacios de interacción que constituyen un ecosistema "vital". En este contexto, es determinante la construcción de una alta disponibilidad de los recursos, garantizando un servicio sin fallos y sin interrupciones (Castro & Liskov, 2001).

Bien es sabido que la primera estrategia en disponibilidad la constituye la replicación. Gracias a esta se logra redundancia en aprovisionamiento de recursos que eventualmente puedan presentar falla, y la "toma de posta" por los recursos redundantes. En BC la replicación y el empleo de algoritmos tolerantes a fallos como BFT (Byzantine-fault-tolerant) permiten la construcción de estructuras jerárquicas que optimizan el uso de recursos y aumentan la escalabilidad (Rahulamathavan et al., 2017).

Este último aspecto puede resultar no deseable en dispositivos con baja capacidad de almacenamiento, con lo que se evidencia que BC debe tener la capacidad de adaptación a diferentes escenarios, sabiendo "explotar" características particulares a necesidades específicas. De esta manera, la ventaja que puede representar el resguardo total y acumulativo de data sobre la cadena de bloques puede no ser deseable en otros escenarios.

El almacenaje de la cadena de bloques se lleva a cabo con mucha redundancia: todos los nodos completos de la red contienen una copia entera de la BC (y

sus transacciones). Esto permite a estos nodos validar de manera correcta cada nueva transacción. Tener que mantener una copia completa de la cadena puede suponer un problema para los nodos que operan en dispositivos ligeros como los dispositivos móviles (Pérez & Joancomartí, 2014).

Para finalizar, vale la pena reflexionar sobre si BC se trata de "magia" capaz de resolver toda problemática moderna, como se ha pretendido o infiere de la gran cantidad de artículos que así lo sugieren y que como bien lo anunció en su tercera "ley" Clarke (1962), "Cualquier tecnología lo suficientemente avanzada es totalmente indistinguible de la magia". La respuesta es no. Esta debe ser asumida a la par con el desarrollo de una cultura de seguridad de la información y tras el estudio de su conveniencia ingenieril en el campo de exploración.

Conclusiones

Blockchain introduce aspectos disruptivos en la construcción de sistemas de información y aplicaciones que preserven inmutabilidad y registro de transacciones. Aspectos como la descentralización, la inmutabilidad y el consenso son conceptos fundamentales en BC que han revolucionado la forma en que manejamos y confiamos en los datos digitales. La descentralización elimina la necesidad de intermediarios; la inmutabilidad garantiza la integridad de los datos, y el consenso asegura que todas las partes lleguen a acuerdos confiables en una red distribuida. Estos principios son la base de la seguridad y la confianza en las aplicaciones basadas en BC y tienen el potencial de transformar numerosos sectores.

Aunque la transparencia es una de las principales ventajas de la tecnología *blockchain,* también puede presentar desafíos, especialmente cuando se trata de proteger datos sensibles y cumplir con las regulaciones de privacidad. Aspectos como este, al lado del alto consumo energético y el crecimiento de tamaño de los nodos pueden llegar a limitar la adaptación de BC como tecnología, aunque en este trabajo se han documentado varias estrategias para su superación.

De esta manera, combinaciones como el uso de NDN y BoNDN para enfrentar problemas de conectividad con la característica de libro mayor distribuido inmutable y confiable de BC pueden ser garantía de que los datos intercambiados sean confiables y menos susceptibles a pérdidas de paquetes y sufrir ataques cibernéticos.

Blockchain no es una solución en sí misma. BC es una herramienta tecnológica que ha de ser rodeada de un plan estratégico que entienda las necesidades

del proyecto, identifique el grado de transparencia y descentralización, determine los miembros que actuarán como nodos y establezca la estructura de *blockchain* adecuada, definiendo cómo van a ser las transacciones o los Smart Contracts por ejecutar (MinTIC, 2020).

Esta revisión crítica recoge aspectos sobre las diferentes consideraciones para el desarrollo de soluciones que, mediante el uso de BC, brinden garantías en ciberseguridad y con ello la construcción de un ecosistema digital confiable.

Referencias

Ali, R., Clarke, D., & McCorry, P. (2017). Towards developing a blockchain-based approach for the secure storage of patient records. En *IEEE International Conference on E-Health Networking, Applications and Services* (pp. 400-406). IEEE.

Alzhrani, F., Saeedi, K., & Zhao, L. (2023). Architectural patterns for blockchain systems and application design. *Applied Sciences, 13*(20), 11533. https://doi.org/10.3390/app132011533

Amazon Web Services. (s. f.). What is decentralization? https://aws.amazon.com/es/blockchain/decentralization-in-blockchain/

Arshad, H., Picazo-Sanchez, P., Johansen, C., & Schneider, G. (2023). Attribute-based encryption with enforceable obligations. *Journal of Cryptographic Engineering,* (13), 343-371. https://doi.org/10.1007/s13389-023-00317-1

Back. A. (2002). Hashcash - A denial of service counter-measure [Technical report]. http://www.hashcash.org/papers/hashcash.pdf

Baena-Luna, P., & García-Río, E. (2022). Tecnología Blockchain: Desafíos presentes y futuros en su aplicación. *Revista Conocimento Online,* (2), 258-273. https://doi.org/10.25112/rco.v2.2859

Banafa, A. (2022, 22 de diciembre). Blockchain 4.0. https://www.bbvaopenmind.com/tecnologia/mundo-digital/blockchain-4-0/

Benmoussa, A., Kerrache, C. A., Calafate, C. T., & Lagraa, N. (2023). NDN-BDA: A Blockchain-Based decentralized data authentication mechanism for vehicular named data networking. *Future Internet, 15*(5), 167. https://doi.org/10.3390/fi15050167

Bitcoin.es. (2020, 17 de noviembre). Vamos por la 5ta generación de la Blockchain ¿Cuáles son? https://bitcoin.es/actualidad/vamos-por-la-5ta-generacion-de-la-blockchain-cuales-son/

Brooks, D. (2020, 9 de febrero). Criptomonedas: Qué es el "problema de los generales bizantinos" y por qué explica el origen del bitcoin. https://www.bbc.com/mundo/noticias-51380491

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and informatics*, (36), 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Castro, M., & Liskov. B. (2001). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, (20)4, 398-461. https://doi.org/10.1145/571637.571640

Choi., T.-M., & Siqin., T. (2022). Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transportation Research Part E: Logistics and Transportation Review,* (160), 102653. https://doi.org/10.1016/j.tre.2022.102653

Conoscenti, M., Vetrò, A., & De Martin, J. C. (2017). Peer to peer for privacy and decentralization in the internet of things. En *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina* (pp. 288-290). https://doi.org/10.1109/ICSE-C.2017.60

Criptodemy. (2023, 20 de enero). Guía sobre algoritmos de consenso Blockchain. Criptodemy ®. https://criptodemy.com/guia-algoritmos-consenso-blockchain/

Guo, J., Wang, M., Chen, B., Yu, S., Zhang, H., & Zhang, Y. (2019). Enabling Blockchain applications over named data networking. En *2019 IEEE International Conference on Communications (ICC), Shanghai, China* (pp. 1-6). IEEE. https://doi.org/10.1109/ICC.2019.8761919

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. En A. J. Menezes & S. A. Vanstone (Eds.), Advances in Cryptology-CRYPTO' 90 (pp. 437-455). Springer. https://doi.org/10.1007/3-540-38424-3_32

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. I*nternational Journal of Intelligent Networks,* (2), 130-139. https://doi.org/10.1016/j.ijin.2021.09.005

Hasan, M. K., Akhtaruzzaman, Md., Kabir, S. R., Gadekallu, T. R., Islam, S., Magalingam, P., Hassan, R., Alazab, M., & Alazab, M. A. (2022). Evolution of industry and Blockchain era: Monitoring price hike and corruption using BIoT for smart government and industry 4.0. *IEEE Transactions on Industrial Informatics, 18*(12), 9153-9161. https://doi.org/10.1109/tii.2022.3164066

Hong, L., Zhang, K., Gong, J., & Qian, H. (2022). A practical and efficient blockchain-assisted attribute-based encryption scheme for access control and data sharing. *Security and Communication Networks*, (2022), 4978802. https://doi.org/10.1155/2022/4978802

Hurtado, J. S. (2021, 1 de julio). Qué son las DLT y en qué se diferencian de Blockchain. https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/

Kharjana, M., Pohrmen, F. H., Sahana, S. C., & Saha, G. K. (2023). Blockchain-based key management system in named data networking: A survey. *Journal of Network and Computer Applications,* (220), 103732. https://doi.org/10.1016/j.jnca.2023.103732

Konkin, A., & Zapechnikov, S. (2023). Zero knowledge proof and ZK-SNARK for private blockchains. *Journal of Computer Virology and Hacking Techniques,* (19), 443-449. https://doi.org/10.1007/s11416-023-00466-1

Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. *Sensors, 22*(14), 5274. https://doi.org/10.3390/s22145274

Leka, E., Selimi, B., & Lamani, L. (2019). Systematic literature review of blockchain applications: Smart contracts. En *2019 International Conference on Information Technologies (InfoTech)* (pp. 1-3). IEEE. https://doi.org/10.1109/InfoTech.2019.8860872

Lorenzo, C. (2020). Blockchain for copyright and intellectual property protection. En *Handbook of research on emerging business models and managerial strategies in the nonprofit sector* (pp. 180-198). IGI Global.

Martínez-Ríos, F. O., Marmolejo-Saucedo, J. A., & Abascal-Olascoaga, G. (2020). A new protocol based on blockchain technology for transparent operation of corporate social responsibility. En S. García-Álvarez & C. Atristain-Suárez (Eds.), *Strategy, power, and CSR: Practices and challenges in organizational management* (pp. 205–233). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83867-973-620201012

Ministerio de Tecnologías de la Información y Comunicaciones [Mintic]. (2022). *Guía de referencia de Blockchain para la adopción e implementación de proyectos en el Estado colombiano.* Mintic. https://gobiernodigital.mintic.gov.co/692/articles-161810_Ley_2052_2020.pdf

Mohaisen, A., & Kim, J. (2013, 22 de diciembre). The Sybil attacks and defenses: A survey. https://arxiv.org/abs/1312.6349

Moran, T., & Orlov, I. (2019). Simple proofs of space-time and rational proofs of storage. En A. Boldyreva & D. Micciancio (Eds.), *Advances in Cryptology–CRYPTO 2019* (pp. 381-409). Springer International Publishing. https://eprint.iacr.org/2016/035.pdf

Mougayar, W. (2016). *The business Blockchain: Promise, practice, and application of the next internet technology.* Wiley.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press.

Ortega Llorente, P. O. (2023). Estudio comparativo de algoritmos de consenso para una Blockchain orientado al consumo de energía [Tesis de pregrado, Universidad Politécnica de Madrid]. Repositorio UPM. https://oa.upm.es/75158/1/TFG_PABLO_ORTEGA_LLORENTE.pdf

Pérez Solà, C., & Joancomartí, J. (2014). Bitcoins y el problema de los generales bizantinos. En R. Álvarez Sánchez, J.-J. Climent Coloma, F. Ferrández Agulló, F. Martínez Pérez, L. Tortosa Grau, J. F. Vicent Francés, A. Zamora Gómez (Coords.), *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información RECSI XIII: Alicante, 2-5 de septiembre de 2014* (pp. 241-246). https://rua.ua.es/dspace/handle/10045/40461

Popchev, I., Radeva, I., & Velichkova, V. (2021). Blockchains in enterprise global risk management. En *2021 International Conference Automatics and Informatics (ICAI)* (pp. 282-287). IEEE. https://doi.org/10.1109/ICAI52893.2021.9639500

Raikwar, M., & Gligoroski, D. (2021). R3V: Robust round robin VDF-based consensus. En *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 81-88). IEEE. https://doi.org/10.1109/BRAINS52497.2021.9569781

Relictum Pro. (s. f.). Is blockchain 5.0 of the latest generation. https://relictum.pro/

Romero Ugarte, J. L. (2018). Distributed ledger technology (DLT): Introduction. *Economic Bulletin,* (4) 2-11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269731

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9*(9), 1788. https://doi.org/10.3390/app9091788

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electron Markets,* (32), 1779-179. https://doi.org/10.1007/s12525-022-00536-0

Soto, M. G. (2018, 6 de agosto). El problema de los generales bizantinos (PGB). https://marvin-soto.medium.com/el-problema-de-los-generales-bizantinos-pgb-e0cb8c4279c2

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network, 35*(4), 198-205. https://doi.org/10.1109/MNET.011.2000473

Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (1st. ed.). O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World.* Penguin.

Vamsi_Cz5cgo. (2016, enero 28). The Architecture of Blockchain (4/5). https://www.vamsitalkstech.com/blockchain/the-architecture-of-blockchain-45/

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation, 5*, 27. https://doi.org/10.1186/s40854-019-0147-z

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain Technology? A systematic review. *PLoS ONE, 11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zheng, J., Huang, H., Zheng, Z., & Guo, S. (2023). Adaptive double-spending attacks on PoW-based Blockchains. En *IEEE Transactions on Dependable and Secure Computing* (pp. 1-13). IEEE. https://doi.org/10.1109/TDSC.2023.3268668