ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA

ESTUDIO DE LAS TECNOLOGÍAS BLOCKCHAIN Y SUS APLICACIONES EN REDES CELULARES 5G, 6G Y EN SEGURIDADES

ESTUDIO DE LA TECNOLOGÍA BLOCKCHAIN Y SU APLICACIÓN EN CIBERSEGURIDAD

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

JEAN PIERRE SANGO VÁSQUEZ

jean.sango@epn.edu.ec

DIRECTOR: MSc. WILLIAMS FERNANDO FLORES CIFUENTES

fernando.flores@epn.edu.ec

DMQ, abril 2024

CERTIFICACIONES

Yo, JEAN PIERRE SANGO VÁSQUEZ declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

JEAN PIERRE SANGO VÁSQUEZ

Certifico que el presente trabajo de integración curricular fue desarrollado por JEAN PIERRE SANGO VÁSQUEZ, bajo mi supervisión.

MSc. WILLIAMS FERNANDO FLORES CIFUENTES
DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JEAN PIERRE SANGO VÁSQUEZ

MSc. WILLIAMS FERNANDO FLORES CIFUENTES

DEDICATORIA

Dedico sinceramente trabajo a mis amados padres, cuyo amor y apoyo incondicional constante han sido mi fuerza durante cada fase de mi vida académica. A mis hermanos, agradezco su compañía y aliento. También a mis valiosos amigos, cuyos sabios consejos y guía siempre serán recordados con mucho cariño y gratitud.

AGRADECIMIENTO

A Dios por brindarnos de salud y muchas bendiciones a mí y a mi familia.

A mis padres por la invaluable educación que me han proporcionado y el inmenso sacrificio que han hecho a lo largo de mi vida para asegurarse de que no me falte nada. Por siempre confiar en mí y por brindarme su apoyo incondicional para alcanzar cada una de mis metas. No hay palabras suficientes para expresar mi gratitud por todo lo que han hecho por mis hermanos y por mí. Los amo profundamente.

A mi hermano Bryan, porque siempre se ha mantenido a mi lado, siendo mi ejemplo y apoyándome de cualquier forma a sobrepasar todos los obstáculos y los malos momentos.

A Kiara y Theo, mis fieles compañeros, les agradezco por regalarme su inigualable cariño y amor incondicional desde el mismo instante en que llegaron a casa.

A mi siempre recordado Panchito, agradezco por todo su amor y compañía durante los momentos de estudio, por estar a mi lado en los buenos momentos y especialmente cuando la tristeza se hacía presente. Aunque no llegó hasta el final de esta etapa académica, estoy seguro de que desde el cielo continúa cuidándome y brindándome su apoyo.

A Pao, por estar para mí en todo momento, por su incondicional apoyo, sabios consejos y amor incondicional.

A David y Andrés, por darle el toque divertido a esta etapa universitaria, por brindarme su tiempo para poder conversar, reír, estudiar y distraernos. Gracias por convertirse en mis hermanos.

A todos mis amigos, ya que han sido un pilar fundamental a lo largo de esta etapa, regalándome inolvidables recuerdos que atesoraré siempre.

Al Msc. William Flores, expreso mi profundo agradecimiento por su orientación constante y el tiempo dedicado en cada reunión. Gracias por su valioso apoyo que ha sido fundamental para culminar con éxito esta etapa académica.

A la Escuela Politécnica Nacional, por brindarme la oportunidad invaluable de moldear mi desarrollo profesional, personal y académico.

ÍNDICE DE CONTENIDO

RESUMEN

La tecnología Blockchain, originada para respaldar criptomonedas, ha transformado su función, siendo ahora un componente esencial en el ámbito de la ciberseguridad. Su descentralización y habilidad para asegurar la integridad de los datos la posicionan como una herramienta valiosa en la lucha contra amenazas cibernéticas.

El presente documento representa una investigación exhaustiva que analiza detenidamente la influencia de la tecnología Blockchain en la ciberseguridad. El enfoque cualitativo se distingue por el análisis minucioso de diversas fuentes. El primer capítulo introduce el componente desarrollado, delineando objetivos, alcance y un marco teórico integral sobre términos clave, diseño y clasificación de Blockchain, así como niveles, algoritmos de consenso y las respectivas aplicaciones.

El segundo capítulo detalla la metodología, explorando la importancia de la ciberseguridad, las amenazas, la integración de Blockchain y su contribución a este ámbito. Se examinan aspectos clave como la triada de la ciberseguridad, el programa de riesgo cibernético, y se abordan vulnerabilidades específicas junto con contramedidas.

En el capítulo final se presentan los resultados, destacando las vulnerabilidades identificadas y las contramedidas propuestas. Las conclusiones abordan la convergencia entre ciberseguridad y Blockchain, brindando una visión global. Las recomendaciones sugieren enfoques para futuras investigaciones, proporcionando una guía valiosa para investigadores venideros. En resumen, esta tesis ofrece un análisis detallado de las aplicaciones, beneficios y riesgos de Blockchain en ciberseguridad, fomentando su adopción futura en el ámbito de la seguridad informática.

PALABRAS CLAVE: blockchain, ciberseguridad, tecnología, investigación, integración, riesgos cibernéticos, autenticación, privacidad, seguridad en línea.

ABSTRACT

The Blockchain technology, originally designed to support cryptocurrencies, has evolved into an essential component in the field of cybersecurity. Its decentralization and ability to ensure data integrity position it as a valuable tool in the fight against cyber threats.

This document represents a comprehensive investigation meticulously analyzing the impact of Blockchain technology on cybersecurity. The qualitative approach distinguishes itself through a thorough analysis of diverse sources. The first chapter introduces the developed component, outlining objectives, scope, and a comprehensive theoretical framework covering key terms, Blockchain design, classification, levels, consensus algorithms, and respective applications.

The second chapter details the methodology, exploring the importance of cybersecurity, threats, the integration of Blockchain, and its contribution to this field. Key aspects such as the cybersecurity triad, the cyber risk program, and specific vulnerabilities along with countermeasures are examined.

In the final chapter, results are presented, highlighting identified vulnerabilities and proposed countermeasures. Conclusions address the convergence between cybersecurity and Blockchain, providing a comprehensive view. Recommendations suggest approaches for future research, offering valuable guidance for upcoming researchers. In summary, this thesis provides a detailed analysis of the applications, benefits, and risks of Blockchain in cybersecurity, fostering its future adoption in the field of information security.

KEYWORDS: blockchain, cybersecurity, technology, research, integration, cyber risks, authentication, privacy, online security.

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

La tecnología Blockchain, definida como una estructura descentralizada que facilita el registro y verificación de transacciones de manera segura e inmutable, se destaca como una herramienta revolucionaria para abordar los desafíos de seguridad en los entornos digitales contemporáneos [1]. Desde la salvaguarda de información crítica hasta la verificación segura de identidades digitales y la mitigación de posibles amenazas, la tecnología Blockchain emerge como un pilar innovador en la lucha contra las vulnerabilidades cibernéticas. Su integración estratégica no solo promete abordar los desafíos actuales de seguridad, sino que también sienta las bases para un ecosistema digital más seguro y confiable en el futuro.

En el dinámico y complejo paisaje de la ciberseguridad actual, los ataques cibernéticos han evolucionado hacia formas más específicas y sofisticadas. Los ciberdelincuentes no solo buscan acceder a información sensible, sino que también intentan alterar sistemas cruciales, lo que ha suscitado un debate sobre el potencial de la tecnología Blockchain para fortalecer o entorpecer la ciberseguridad. Según expertos en la materia, la tecnología Blockchain puede convertirse en un pilar esencial para mejorar la seguridad cibernética en múltiples aspectos, como la gestión de identidades y accesos, trazabilidad de datos, almacenamiento seguro y ejecución de contratos inteligentes [2].

El enfoque principal de este componente de investigación es realizar un análisis meticuloso y exhaustivo de las aplicaciones de la tecnología Blockchain, en primera instancia desde una perspectiva general y, posteriormente, focalizándose específicamente en su implementación y efectividad en el ámbito de la ciberseguridad. Se persigue identificar y examinar en detalle las ventajas y beneficios tangibles que esta tecnología aporta en términos de protección de datos, autenticación de usuarios y prevención de ataques cibernéticos. La tecnología Blockchain se caracteriza por su inmutabilidad, transparencia, capacidad de auditoría, sólido cifrado de datos y su resiliencia operativa, elementos que la posicionan como una solución potencialmente eficaz para reforzar la seguridad en el entorno digital.

La integración de la tecnología Blockchain en el ámbito de la ciberseguridad representa una oportunidad significativa para fortalecer la defensa en el mundo digital. A medida que esta investigación profundiza en sus aplicaciones específicas, se espera no solo revelar su potencial, sino también sentar las bases para su implementación efectiva como un componente vital en la preservación de la seguridad en la era digital.

La relevancia y el impacto potencial de la tecnología Blockchain en la ciberseguridad se encuentran en constante evolución. Conforme avanzamos hacia un entorno digital más complejo y conectado, comprender y aprovechar plenamente las capacidades de la tecnología Blockchain se convierte en un factor crucial para garantizar la seguridad y confiabilidad de nuestras redes digitales.

1.1 Objetivo general

Realizar una investigación y análisis exhaustivos sobre la influencia de la tecnología Blockchain en el campo de la ciberseguridad, con el propósito de identificar y destacar las ventajas y beneficios que esta tecnología ha generado a lo largo de los últimos años.

1.2 Objetivos específicos

1. Conocer cómo la tecnología Blockchain fortalece la protección de datos sensibles en entornos cibernéticos, garantizando su integridad, confidencialidad y disponibilidad.
2. Investigar las aplicaciones de la tecnología Blockchain en la autenticación de usuarios, explorando su enfoque seguro para disminuir riesgos de suplantación de identidad y fraude.
3. Descubrir el impacto de la tecnología Blockchain en la prevención de ataques cibernéticos, incluyendo la detección de actividades maliciosas y la reducción de riesgos asociados con amenazas como los ataques DDoS.

1.3 Alcance

El objetivo del presente componente es realizar un estudio sobre la tecnología Blockchain y sus aplicaciones en ciberseguridad. El estudio presentará las ventajas y los riesgos de utilizar esta tecnología, con la finalidad de ampliar el conocimiento sobre ella y promover su adopción en los años futuros.

Para llevar a cabo este trabajo, se comenzará realizando una revisión de la literatura existente que relacione la tecnología Blockchain con la ciberseguridad. Esto se hará con el propósito de conocer la arquitectura que se maneja en esta tecnología. La revisión de la literatura se realizará a través de una búsqueda bibliográfica en bases de datos académicas y de internet. Los documentos que se encuentren serán seleccionados según su relevancia con el tema de estudio.

Una vez que se haya realizado la revisión de la literatura, se identificarán los campos en los que la tecnología Blockchain ha tenido más apego a lo largo de los años desde su aparición. Estos campos se analizarán en detalle, identificando los beneficios y riesgos de utilizar esta tecnología en cada uno de ellos. Finalmente, los resultados de la investigación serán presentados en un informe final, que incluirá una discusión de los beneficios y riesgos de utilizar la tecnología Blockchain en ciberseguridad, así como una serie de recomendaciones para trabajos futuros de investigación.

1.4 Marco teórico

1.4.1 Términos clave en Blockchain

Con el objetivo de brindar una comprensión más detallada de los términos específicos utilizados en el ámbito de la tecnología Blockchain, se ofrece la **tabla 1.1**. La misma que proporciona una visión concisa y contextualizada de los conceptos clave relacionados con la Blockchain, lo que permite a los interesados una mayor familiarización con términos fundamentales importantes.

Tabla 1.1. Términos clave en Blockchain *[3]*

Término	Definición
Nodo	Computadoras en la red blockchain con réplicas del libro mayor y verificación de transacciones.
Transacción	Mantenimiento de registros, datos e información de remitente, receptor y valor en blockchain.
Dirección	Identificador único para representar información del remitente y receptor en la red blockchain.
Bloque	Conjunto de datos válidos almacenados en orden consecutivo en la base de datos digital.
Cadena	Serie de bloques organizados secuencialmente formando la red de blockchain.

Nonce	Número arbitrario generado por mineros para crear un hash válido en el bloque.
Minería	Proceso de formación del valor de hash del bloque para garantizar la integridad en blockchain.
Consenso	Conjunto de reglas supervisadas para agregar nuevos bloques a la estructura de blockchain.
Hard Fork	Cambio de reglas para autenticar bloques en la red blockchain.
Árbol de Merkle	Estructura que genera un único valor de hash para un bloque, permitiendo la autenticación de grandes estructuras de datos.

1.4.2 Concepto de Blockchain

Blockchain es una estructura de registro innovadora que permite la realización de transacciones de valor directamente entre los usuarios, sin depender de intermediarios de confianza, como entidades bancarias o servicios de corretaje. Esta tecnología revolucionaria de cadenas de bloques se destaca por su capacidad para mantener la integridad, seguridad y privacidad en cada fase de las transacciones realizadas en su red descentralizada.

El término "Blockchain" constituye un elemento tecnológico clave asociado al funcionamiento de bitcoins. Además, se refiere a una serie de bloques de datos que se encuentran interconectados mediante criptografía. Por otro lado, también se define como una base de datos distribuida que alberga una cadena de bloques de información, donde cada bloque está identificado mediante una firma criptográfica y todos están enlazados en secuencia hacia atrás, lo que implica que cada bloque contiene la firma del bloque previo en la cadena, pudiendo rastrearse hasta el bloque inicial. [4] [5]

Blockchain es una tecnología digital en ascenso que amalgama conceptos de criptografía, gestión de datos, redes y sistemas de incentivos. Su finalidad radica en respaldar la verificación, ejecución y registro de transacciones entre distintas partes involucradas. [6]

Redes P2P enlazadas hacia Blockchain

La tecnología Blockchain ganó relevancia con la aparición de la criptomoneda Bitcoin, desempeñando un papel crucial en la resolución del problema del doble gasto en transacciones. En una red P2P, cualquier individuo puede realizar una transacción sin necesidad de un intermediario central. Para abordar posibles conflictos, Blockchain utiliza un enfoque de consenso durante este proceso [3].

Por otro lado, la red Peer-to-Peer (P2P) es una estructura distribuida ampliamente empleada en aplicaciones que facilitan la transferencia de datos en línea, como la distribución de contenido o el intercambio de archivos. Cada computadora o participante en esta red, conocidos como pares, tiene igual importancia. Esta arquitectura descentralizada permite que cada nodo se comunique directamente con otros en la red y difiere significativamente del modelo Cliente/Servidor [7].

La **figura 1.1** proporciona una representación visual que contrasta las redes Cliente/Servidor y Peer-to-Peer (P2P).

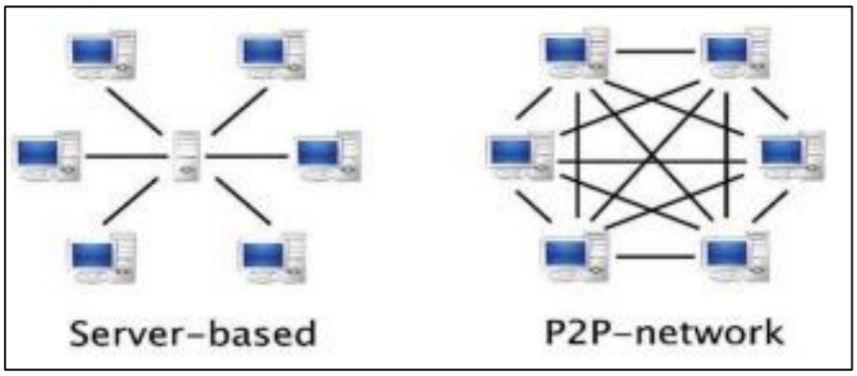

Figura 1.1. Cliente/Servidor y red P2P *[3]*

La diferencia clave entre estas arquitecturas radica en la distribución de recursos y la gestión de transacciones. Mientras que el modelo Cliente/Servidor se basa en una estructura jerárquica con un servidor central controlando la red, la red P2P fomenta la descentralización y la interconexión directa entre los participantes. Esto ofrece mayor flexibilidad y resistencia a fallos al evitar puntos únicos de fallo y control centralizado.

La característica esencial de Blockchain, al operar de manera peer-to-peer (P2P), es permitir transacciones directas entre participantes individuales sin necesidad de validación de terceros. Esta descentralización elimina la dependencia de intermediarios, otorgando a los usuarios mayor control sobre sus transacciones y asegurando una mayor transparencia en el proceso. [3]

1.4.3 Diseño de la tecnología Blockchain

Es esencial definir claramente el diseño y proporcionar una visión general de los elementos dentro de la tecnología de blockchain. Los enfoques para desarrollar la estructura de esta tecnología varían entre investigadores, debido a las diversas aplicaciones que se adaptan a las necesidades de los usuarios, lo que impide la estandarización de su arquitectura. En este documento, se describe la estructura general de blockchain, ampliamente acordada por la mayoría de los expertos, compuesta por las siguientes capas [8]:

- Incentivos
- Aplicación
- Red
- Contrato
- Datos
- Consenso.

Arquitectura de Blockchain

La arquitectura de Blockchain es un conjunto de niveles interconectados que se deben incorporar en todo sistema de este tipo. La cantidad de estas capas puede adaptarse según las aplicaciones específicas que se estén utilizando y los criterios individuales exigidos por los usuarios. Dentro de la investigación académica y en el ámbito profesional, se ha consensuado mayoritariamente en torno a la existencia de una estructura compuesta por seis capas fundamentales. Estas capas, delineadas en la **Figura 1.2**, conforman un esquema esencial que comprende desde los elementos básicos de incentivos hasta las complejidades de la capa de consenso, permitiendo así la operatividad y eficacia de la tecnología de la cadena de bloques [8].

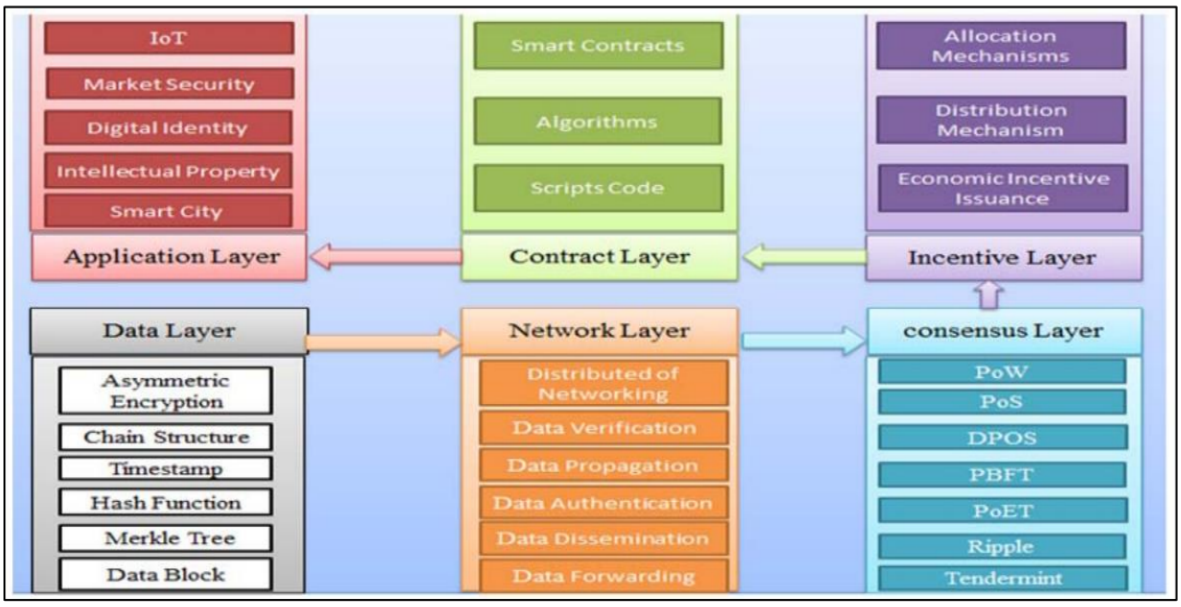

Figura 1.2. Arquitectura de la tecnología Blockchain. *[8]*

- **Capa de Datos**

Este estrato representa la base de la arquitectura de blockchain y engloba diversas técnicas, tales como funciones hash, cifrado asimétrico, marcas de tiempo, estructura de la cadena, árbol de Merkle y bloque de datos, según se muestra en la figura 1.3. La operatividad en esta capa se ejemplifica a través del nodo triunfante en la competencia de consenso. Este nodo desempeña múltiples funciones en el sistema de blockchain, como (1) instaurar un nuevo bloque, (2) almacenar los datos relacionados con el proceso de transporte y la marca de tiempo que indica el momento de creación del bloque en una estructura de datos conocida como árbol de Merkle. [8] [9] [10].

- **Capa de Red**

Esta capa contiene varios mecanismos, tales como la propagación de datos, verificación de datos, redes distribuidas, autenticación de datos, difusión de datos y reenvío de datos. El objetivo principal de esta capa es verificar si las transacciones generadas en la red son válidas o no. Si una transacción es válida, se envía a otro nodo; de lo contrario, se ignora [8] [9] [10].

- **Capa de Consenso**

En esta capa se emplean varios algoritmos de consenso para tomar decisiones en la red de blockchain. Entre estos algoritmos se encuentran, "practical Byzantine fault tolerance (PBFT)", "proof of work (PoW)", "proof of elapsed time (PoET)" y "proof of stake (PoS)". Estos algoritmos se explicarán detalladamente en la sección de algoritmos de consenso [8] [9] [10].

- **Capa de Incentivo**

Esta capa representa la fuerza clave dentro de la red de blockchain, ya que motiva la contribución efectiva de los nodos a la red, otorgándoles factores económicos. Estos factores incluyen la emisión de incentivos económicos, mecanismos de distribución y asignación [8] [9] [10].

- **Capa de Contrato**

Este estrato es fundamental en las características programables de blockchain. Incluye diversas técnicas, como contratos inteligentes, algoritmos y códigos de scripts. Estas técnicas funcionan como un estímulo importante para los datos y el dinero pertenecientes a las personas en la red [8] [9] [10].

- **Capa de Aplicación**

Este estrato es la capa superior en la arquitectura de blockchain y alberga una diversidad de aplicaciones que incorporan los principios y conceptos de esta tecnología. Se emplea en diversos contextos de aplicaciones, como ciudades inteligentes, propiedad intelectual, identidad digital, seguridad en el mercado, aplicaciones empresariales e IoT (Internet de las cosas). Se ofrecerán más ejemplos sobre estas aplicaciones en la sección correspondiente más adelante. [8] [9] [10].

Estructura de Blockchain

La configuración de la tecnología blockchain se representa en la **figura 1.3**. Los componentes de esta estructura son la marca de tiempo, otra información, la función hash y los datos [8].

- **Datos**

  Los datos en el bloque se derivan de la aplicación empleada o los servicios brindados por la red, como información de cuentas bancarias o registros de dispositivos IoT. Estos datos tienen aplicaciones variadas en campos como la banca y la IoT [8].

- **Hash**

Cada bloque utilizará una función hash. La entrada puede ser de cualquier longitud y generará una salida fija y única. La salida cambiará y será significativamente diferente si se edita cualquier valor de la entrada. Esta función se ejecuta después de que las transacciones en el bloque se realizan y se transmiten a cada nodo en la red [8].

- **Marca de tiempo**

La marca de tiempo es una herramienta y método para seguir el tiempo de cada bloque cuando se establece o edita en la red [8].

- **Otra información**

La otra información podría ser cualquier dato relacionado con la definición del usuario, valores de nonce, nBits y la firma de bloques [8].

Las transacciones en Blockchain ocurren en una secuencia organizada de bloques, siendo visibles para todos los miembros de la red. Se utiliza una red de pares para sincronizar estas operaciones. En cada bloque se almacena información crítica, como registros de transacciones, encriptados y coordinados entre nodos. Los bloques se enlazan mediante punteros que indican la posición del siguiente bloque, y cada bloque se refiere al anterior mediante un valor hash, estableciendo una relación de 'padre' y 'hijo'. El 'bloque génesis' representa el primer bloque en una red blockchain y se enlaza al bloque anterior mediante un algoritmo hash seguro, generalmente de 256 bits. La marca de tiempo identifica el momento de creación de cada bloque y el nonce genera una cadena de caracteres específica, que incluye elementos matemáticos y alfanuméricos [11]. La cadena de bloques utiliza el árbol de Merkle para generar un valor hash final que verifica la autenticidad de un bloque. Cualquier modificación en este árbol altera el valor de la raíz de Merkle, reduciendo el tiempo de difusión de datos [3]. La representación visual de la raíz del árbol de Merkle se muestra en la **figura 1.4**.

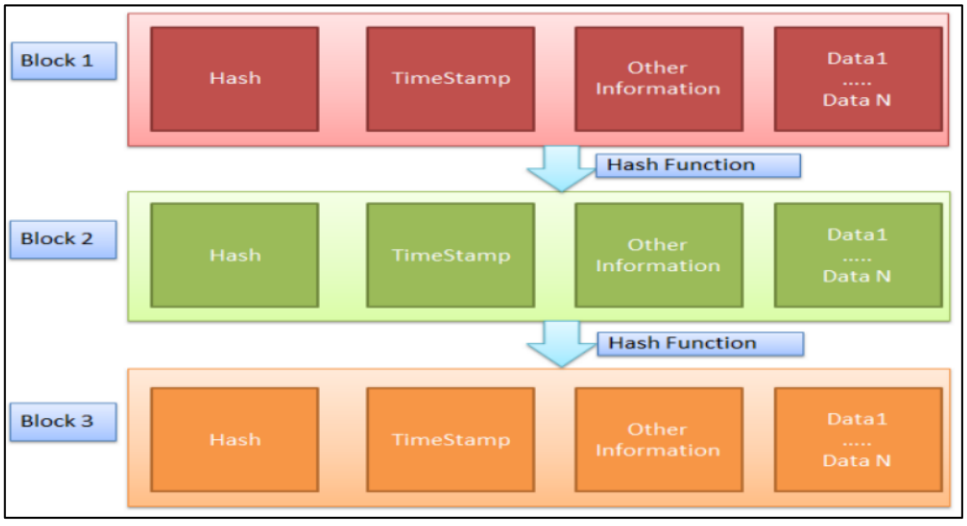

Figura 1.3. Estructura de una blockchain. *[8]*

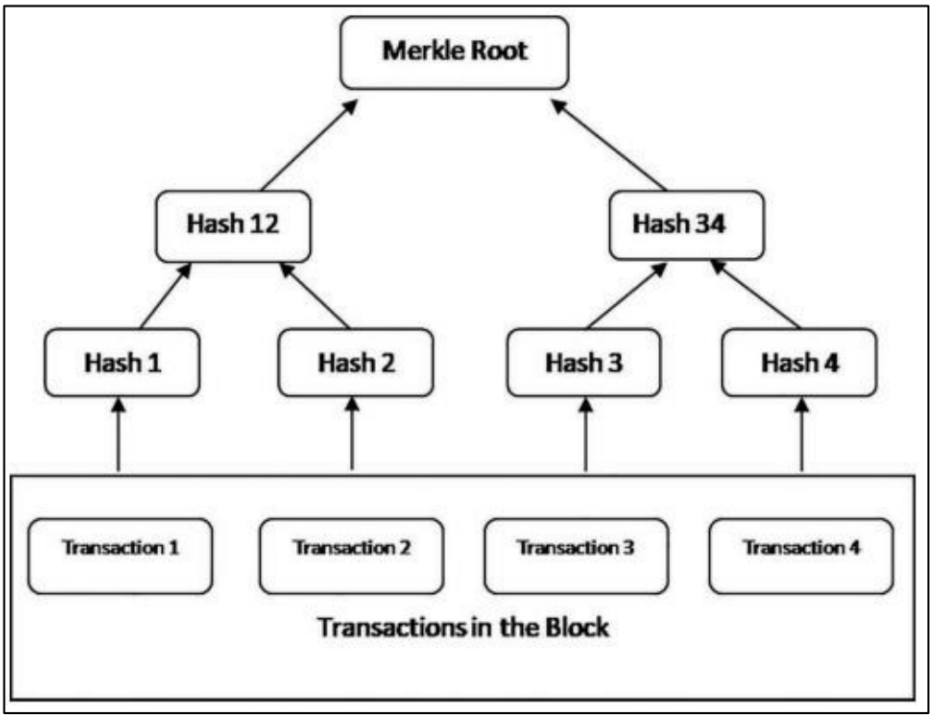

Figura 1.4. Raíz del árbol de Merkle. *[3]*

Funcionamiento de Blockchain

El proceso operativo de la cadena de bloques se puede visualizar en la **figura 1.5**, desglosado en una serie de pasos que ilustran la secuencia de eventos [3]:

Paso 1: Un participante de la red, denominado nodo, inicia una solicitud para llevar a cabo una transacción específica, por ejemplo, la transferencia de fondos de A a B.

Paso 2: Esta transacción se registra como una operación genuina en un bloque, un componente fundamental en la estructura de la cadena de bloques que contiene información detallada sobre la transacción.

Paso 3: La solicitud de transacción se difunde a lo largo de todos los demás nodos conectados en la red de la cadena de bloques, garantizando que cada parte de la red esté informada sobre la transacción propuesta.

Paso 4: La validación de la transacción se somete a un proceso riguroso de verificación por parte de los nodos en la red. Esta verificación busca garantizar que la transacción cumpla con los criterios específicos y sea auténtica.

Paso 5: Una vez que se confirma y valida la transacción por la red de nodos, se crea un nuevo bloque que contiene esta transacción verificada y validada.

Paso 6: La transacción se completa oficialmente, lo que significa que los fondos se transfieren de manera exitosa de la cuenta A a la cuenta B, y esta acción queda registrada de forma permanente en la cadena de bloques.

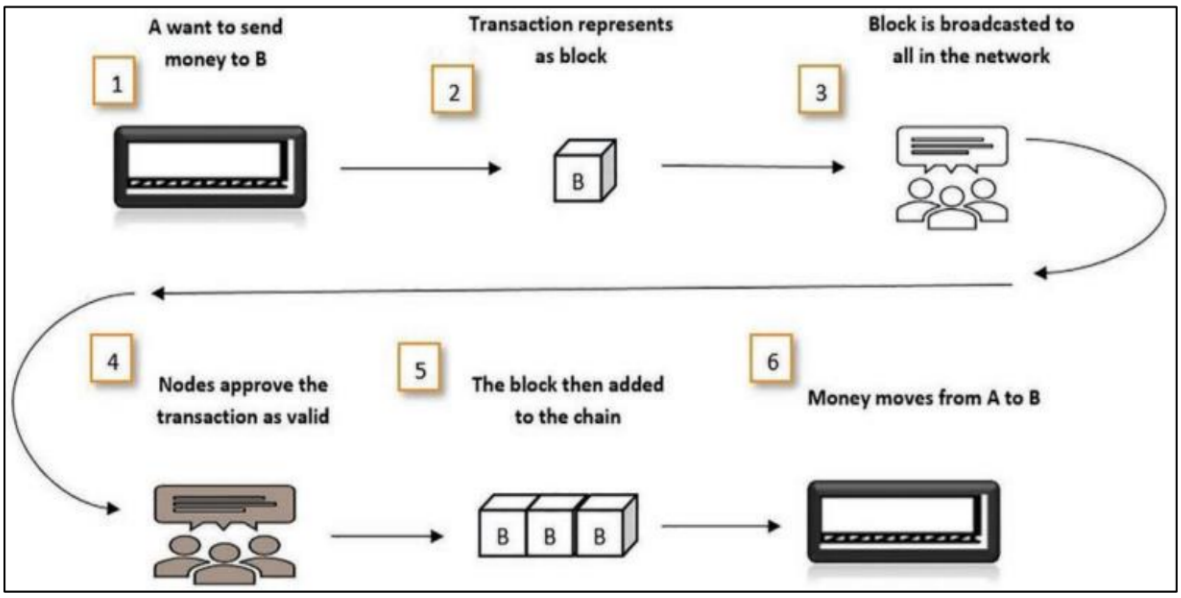

Figura 1.5. Funcionamiento de blockchain.

1.4.4 Clasificación de una Blockchain

Es crucial comprender que no todas las blockchains disponibles se adecúan a los requisitos de cualquier proyecto. Por lo tanto, resulta fundamental comprender los diversos tipos de blockchains y sus diferencias para seleccionar la más idónea según el caso de uso específico. Antes de profundizar en las discrepancias, es esencial resaltar las características compartidas que deben cumplir para ser consideradas blockchains [12]:

- Operan como bases de datos o registros que solo permiten la adición de datos, donde la estructura de la cadena de bloques asegura la vinculación de cada bloque de transacciones al bloque anterior [12].
- Funcionan como una red de nodos o pares, donde cada uno mantiene una copia de la red y se consideran equivalentes, interactuando en un entorno punto a punto (p2p) [12].
- Requieren un mecanismo de consenso para que los nodos acuerden qué transacciones serán añadidas a la blockchain y propagadas en la red [12].

Los sistemas de blockchain en la actualidad pueden ser clasificados en tres categorías distintas, las cuales se encuentran representadas en la **figura 1.6**.

Blockchain Pública

Las blockchains públicas, conocidas como blockchains sin permisos, se caracterizan por su total apertura a la participación. Estos sistemas descentralizados permiten a cualquier persona actualizar el libro mayor distribuido, sin requerir la firma de una autoridad central. Esta ausencia de liderazgo garantiza que nadie tenga control absoluto sobre la red.

Esta naturaleza abierta y descentralizada fomenta la transparencia al permitir que cualquiera se una y participe en el mantenimiento de la red. La falta de un ente central asegura la igualdad de poder entre los nodos, fortaleciendo la seguridad de los datos y promoviendo la inalterabilidad de los registros. Cualquier cambio en la información almacenada necesita el consenso de la mayoría de los nodos, lo que agrega una capa adicional de protección y confianza en la integridad de los datos. [3] [12].

Blockchain Privada

Las blockchains privadas, también llamadas blockchains con permisos, limitan la visibilidad de las transacciones solo a los miembros de su red, a diferencia de las blockchains públicas. Estas plataformas, centralizadas, son controladas por una entidad específica, como un banco, una institución gubernamental o una empresa. En ellas, se establecen reglas estrictas para el acceso y la participación, restringiendo la entrada a usuarios autorizados y validados. Las transacciones se mantienen cifradas con una clave privada, lo que asegura la confidencialidad de la información almacenada.

Su uso principal se encuentra en entornos que manejan datos confidenciales, como instituciones financieras, organizaciones de salud y empresas, donde se requiere un mayor control de acceso para preservar la privacidad y la seguridad de la información. [3] [12].

Blockchain de Consorcio

La categoría de blockchain consorcio se presenta como un interesante punto intermedio entre los sistemas de blockchain públicos y privados. En este tipo particular, se configura una red que amalgama nodos con distintos niveles de acceso y visibilidad. En otras palabras, algunos nodos tienen restricciones de acceso, mientras que otros se mantienen como partes abiertas al público [3] [12].

Esta peculiaridad permite que ciertos nodos específicos se involucren activamente en las transacciones, a la vez que otros se encargan de asegurar y validar la integridad de las

operaciones a través del proceso de consenso. Lo fascinante de esta estructura es su versatilidad: estos blockchains pueden adaptarse y transformarse según las necesidades del momento. Dependiendo del contexto o las circunstancias particulares, pueden operar ya sea como blockchains completamente privados, restringidos a ciertos usuarios, o pueden adoptar un enfoque más abierto y público, permitiendo una mayor participación y transparencia. [3] [12].

La Tabla 8.1 ofrece una comparación detallada entre las blockchains públicas, privadas y consorcio, analizándolas desde distintos ángulos o puntos de vista.

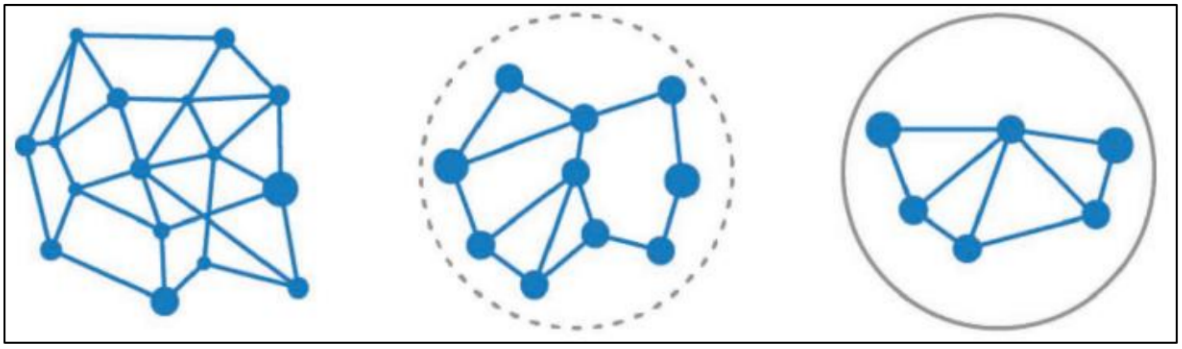

Figura 1.6. Blockchains públicas, de consorcio y privadas *[3]*.

Tabla 1.2. Comparación de las Blockchains Públicas, Privadas y Consorcio *[3] [8] [12]*.

Perspectivas	Públicas	Privadas	Consorcio
Acceso	Lectura y escritura para un solo formato	Lectura y escritura para un solo formato	Lectura y escritura para múltiples formatos seleccionados.
Velocidad	Más lenta	Más rápida	Más rápida
Eficiencia	Baja	Alta	Alta
Seguridad	Mecanismos de consenso	Consenso de varios nodos	Consenso de varios nodos
Inmutabilidad	Los datos no pueden ser alterados	Pueden ser alterados	Pueden ser alterados.
Proceso de consenso	Sin necesidad de permisos	Requiere permisos	Requiere permisos
Riesgo para los participantes	Riesgo de comportamientos maliciosos	Confiables	Confiables

1.4.5 Niveles de Blockchain

La rápida evolución en la innovación de blockchain ha dado lugar a la creación de diversas aplicaciones a lo largo del tiempo. Algunas ya están en uso, mientras que otras podrían desarrollarse más adelante, según el ritmo actual de avance en esta tecnología. Los niveles de blockchain se definen en base a las aplicaciones en cada categoría.

Blockchain 1.0: Moneda

La versión 1.0 de Blockchain surgió con la creación del Bitcoin y se emplea para las criptomonedas. Esta versión permite transacciones monetarias basadas en la tecnología de blockchain o DLT (Distributed Ledger Technology) [3].

Blockchain 2.0: Contratos Inteligentes

Blockchain 2.0 se conoce como Contratos Inteligentes. Estos consisten en códigos de computadora independientes que se ejecutan automáticamente y cuyas condiciones se definen con anticipación. Son difíciles de modificar y su finalidad es reducir costos de verificación, ejecución, establecimiento y prevención de fraudes. La blockchain de Ethereum es una de las más destacadas que permite la implementación de Contratos Inteligentes [3].

Blockchain 3.0: Aplicaciones Descentralizadas (DApps)

Una aplicación descentralizada (DApp) emplea almacenamiento y comunicación descentralizados y ejecuta su código de backend en una red descentralizada de pares. A diferencia de las aplicaciones tradicionales, que tienen su código de backend en servidores centralizados con infraestructura centralizada. La principal característica de una DApp es que su código de frontend y sus interfaces de usuario pueden estar escritos en cualquier lenguaje y, como una aplicación tradicional, realizar llamadas a su backend [3].

Blockchain 4.0: Industria 4.0

Blockchain 4.0 se emplea en la industria según sus demandas. La automatización, la planificación de recursos y la combinación de diferentes sistemas de ejecución son algunas de las necesidades empresariales. Blockchain 4.0 define métodos y soluciones para satisfacer las demandas de las empresas, proporcionando un alto nivel de confianza y protección de la privacidad [3].

1.4.6 Algoritmos de consenso

Los mecanismos de consenso son los que facilitan la adición de bloques a la estructura. En la red blockchain, todos los nodos deben alcanzar un acuerdo común para añadir un

nuevo bloque. Estos mecanismos de consenso ayudarán a los nodos a llegar a un acuerdo común, lo que confirma la confianza entre pares desconocidos de la red. Existen varios mecanismos de consenso y abordaremos brevemente algunos de ellos.

PoW (Proof of Work)

El algoritmo de Prueba de Trabajo (PoW) es un mecanismo fundamental en las blockchains públicas como Bitcoin, donde los nodos compiten por resolver operaciones matemáticas complejas para proponer y agregar bloques de transacciones a la cadena. Este método utiliza el poder de cómputo para alcanzar un consenso, donde los nodos compiten por encontrar un valor de nonce que cumpla con un requisito específico establecido por la red. Los nodos que logran encontrar este valor tienen derecho a agregar un bloque a la cadena y reciben una recompensa, pero este proceso es intensivo en recursos y energía [3] [12].

Sin embargo, el PoW ha sido objeto de críticas debido a su alto consumo de energía, que en redes como la de Bitcoin, se estima equivalente al consumo de energía de un país pequeño. Esta demanda energética ha llevado a buscar alternativas más eficientes en el uso de recursos, como otros algoritmos de consenso, entre ellos el Proof of Stake (PoS) y otros mecanismos de consenso más ecológicos y eficientes. A pesar de su eficacia en garantizar la seguridad de la red, el PoW ha suscitado preocupaciones debido a su ineficiencia energética y la lentitud en el proceso de transacciones, aspectos que han impulsado la búsqueda de nuevos enfoques para mejorar la escalabilidad y sostenibilidad en las blockchains públicas [3] [12].

PoS (Proof of Stake)

La mecánica de prueba de trabajo requiere más energía eléctrica y resulta en un alto consumo energético. Una alternativa a PoW es la Prueba de Participación (PoS). El algoritmo PoS autentica el bloque según la participación de los miembros y utiliza un proceso de selección pseudoaleatorio para elegir a un participante como el autenticador del próximo bloque, basado en la combinación de la antigüedad de la participación, la aleatorización y la riqueza del participante. Los bloques se forjan en lugar de minarse. Las personas que desean participar en el proceso de forja deben invertir una cierta cantidad de monedas en la red como su participación. A mayor participación, mayores son las posibilidades [3] [12].

PBFT (Practical Byzantine Fault Tolerance)

La falla bizantina ocurre cuando diferentes observadores reciben diferentes indicaciones. La falla es cualquier tipo de daño en el servicio del sistema debido a una falla bizantina. Por lo tanto, la Tolerancia Práctica a Fallas Bizantinas (PBFT por sus siglas en inglés)

requiere que cada nodo sea conocido por todos en la red. El PBFT puede tolerar hasta un tercio de las copias bizantinas maliciosas. Cuando se determina un nuevo bloque, el proceso puede dividirse en tres etapas distintas: pre-preparada, preparada y comprometida. Cada ronda necesita seleccionar una clave, basada en las pautas de consenso, que sería responsable de llevar a cabo la operación. Para que un nodo avance a la siguiente etapa, necesita obtener votos de 2/3 de todos los nodos [3] [12].

PoB (Proof of Burn)

Proof of Burn (Prueba de Quema) se introdujo como un algoritmo de consenso alternativo diseñado para aliviar algunas de las problemáticas asociadas con el Proof of Work (Prueba de Trabajo). Con PoB, se incentiva a los mineros a enviar sus criptomonedas a una dirección donde estas monedas no pueden ser accedidas ni utilizadas posteriormente. Básicamente, al quemar o destruir sus propias criptomonedas, los mineros obtienen la oportunidad de participar en el proceso de minería. Este método contribuye a reducir la oferta circulante total de las monedas en cuestión. El concepto detrás de la Prueba de Quema motiva a los mineros a realizar un compromiso a largo plazo, fomentando un sentido de dedicación y confianza. Además, PoB sirve como un mecanismo para mitigar problemas relacionados con el doble gasto dentro de la red blockchain [3].

1.4.7 Aplicaciones de Blockchain

La tecnología blockchain está siendo adoptada comercialmente por diferentes industrias, con casos de uso variados. Plataformas como Bitcoin y Ethereum lideran este desarrollo al permitir la creación de aplicaciones descentralizadas con contratos inteligentes. Las aplicaciones emergentes de blockchain abarcan votaciones, identidad digital, banca, cadena de suministro y salud, mostrando su potencial para resolver desafíos empresariales diversos [3].

Finanzas

Las aplicaciones de blockchain se han implementado en servicios financieros de diversas maneras, obteniendo una amplia gama de beneficios. Los contratos inteligentes permiten dirigir transacciones financieras sin necesidad de intermediarios, posibilitando la ejecución automatizada de valores, acciones, pagos y privilegios. Actualmente, bancos y otras instituciones financieras han comenzado a utilizar la tecnología blockchain [3].

Sector de seguros

La tecnología blockchain está transformando el ámbito de los seguros al mejorar la eficiencia y la transparencia al compartir información. Esta revolución conlleva un cambio de estrategia en el sistema de seguros, pasando de lo físico a lo digital mediante contratos inteligentes en redes peer-to-peer (P2P). Las aseguradoras y los solicitantes de seguros pueden obtener numerosos beneficios al utilizar esta tecnología, lo que permite al sector ser más eficiente y seguro al descentralizar las transacciones de datos y evitar gastos innecesarios [3].

Industria Musical

La tecnología blockchain ha transformado la industria musical y ha permitido que los músicos obtengan mayores beneficios. Esta tecnología ayuda en la gestión de los derechos de propiedad de la música y en el pago justo a los músicos por su trabajo, de manera transparente [3].

Gestión de Identidad

La tecnología blockchain está demostrando su participación en transformar la gestión de identidades a nivel mundial. El trabajo realizado por la gestión de identidades consiste en rastrear y manejar las identidades digitales de manera protegida y eficiente, lo que reduce la filtración de datos y el fraude. La verificación y autenticación de identidad son aspectos esenciales en todas las industrias [3].

Cadena de suministro

Cuando los procesos de fabricación/negocios tienen lugar a nivel global, la transparencia entre proveedores y cadenas de suministro es esencial. Una de las aplicaciones de la tecnología blockchain es la gestión de la cadena de suministro. Requiere un seguimiento en tiempo real de bienes y es especialmente atractivo para empresas que tienen diversas cadenas de suministro. Con la ayuda de la tecnología blockchain, se eliminan todas las cadenas de suministro ineficientes y poco calificadas. Los intercambios están cambiando gracias a soluciones de cadena de suministro basadas en blockchain. Ofrece procesos descentralizados a través de la tecnología de libro mayor distribuido y un registro público digital. La cadena de suministro se integra con la industria logística, carga, transporte por camión, envío y todos los modos de transporte disponibles que usamos para transportar bienes. La necesidad esperada es optimizar el proceso de la cadena de suministro y hacerlo transparente [3].

2 METODOLOGÍA

El desarrollo de este componente se centró en una investigación exhaustiva orientada hacia una revisión bibliográfica detallada con el fin de obtener conocimientos sobre la aplicación y adopción de la tecnología blockchain en el ámbito de la ciberseguridad, presentada como una solución viable para resguardar la integridad de los datos sensibles. Se llevó a cabo una exploración minuciosa en diversas fuentes bibliográficas de alta credibilidad con el propósito de identificar información pertinente relacionada con soluciones prácticas, vulnerabilidades potenciales, así como ventajas y desventajas inherentes que la tecnología blockchain presenta en el panorama actual de la seguridad cibernética.

La investigación inicia con una revisión pormenorizada de los principios fundamentales de la seguridad cibernética, con el objetivo de establecer conexiones sólidas entre estos principios y los respaldados por la tecnología blockchain. A medida que se avanza en el desarrollo, se profundiza en la integración de la blockchain en el ámbito de la ciberseguridad, explorando de qué manera esta innovación ha influido y enriquecido este campo específico. Posteriormente, se abordan conceptos más avanzados, como la triada de la ciberseguridad y el programa de riesgo cibernético, con la finalidad de obtener una comprensión más profunda de la interrelación entre los elementos clave. El enfoque culmina destacando las vulnerabilidades identificadas y las contramedidas propuestas que han surgido con el tiempo, especialmente a medida que se han evidenciado casos de ataques contra la ciberseguridad. Esta estructurada aproximación permite explorar de manera exhaustiva la convergencia entre la ciberseguridad y la tecnología blockchain

El enfoque adoptado en el presente escrito se caracteriza por su naturaleza cualitativa, ya que se fundamenta en la exhaustiva revisión y análisis de información proveniente de una variedad de fuentes, entre las que se incluyen artículos académicos, libros especializados y diversas fuentes documentales. Mediante la aplicación de esta metodología, se persigue el objetivo de comprender a fondo y deducir las múltiples ventajas y desventajas que la tecnología blockchain presenta en la actualidad, especialmente a través del examen de sus vulnerabilidades y las posibles contramedidas que pueden implementarse.

Esta aproximación cualitativa se erige como un medio riguroso para explorar y contextualizar los diferentes aspectos relacionados con blockchain, permitiendo una comprensión holística de su impacto en la ciberseguridad. Al sumergirse en la revisión de literatura especializada, se busca discernir no solo las características intrínsecas de

blockchain, sino también identificar patrones emergentes, tendencias y consideraciones clave que definen su posición en el ámbito de la seguridad informática.

2.1 Ciberseguridad

2.1.1 Importancia de la ciberseguridad

La trascendencia de la ciberseguridad es innegable en un entorno donde las tecnologías experimentan mejoras constantes y las tendencias de seguridad se transforman con tal rapidez que incluso los equipos de inteligencia de amenazas encuentran desafíos para mantenerse al tanto de los cambios. La urgencia en la implementación de medidas de ciberseguridad surge debido a las vastas cantidades de datos almacenados por diversas organizaciones, ya sean de índole militar, corporativa, financiera o médica. Estos datos se encuentran alojados en sistemas que, de una u otra manera, pueden ser susceptibles a ataques [13].

La magnitud de la información almacenada en estos sistemas es significativa, pudiendo incluir datos confidenciales y sensibles. La vulnerabilidad de estos datos frente a accesos no autorizados o a la obtención ilegítima plantea un riesgo sustancial, con el potencial de generar repercusiones negativas de alcance considerable, tanto a nivel individual como a escala global. La ciberseguridad se convierte, así, en un imperativo esencial para salvaguardar la integridad, confidencialidad y disponibilidad de estos datos críticos, evitando posibles consecuencias perjudiciales que podrían repercutir no solo en el ámbito individual, sino también en la estabilidad y seguridad de la sociedad en su conjunto [14].

2.1.2 Amenazas

La prevalencia de delitos cibernéticos encuentra sus raíces en descuidos y en la ausencia de medidas de seguridad adecuadas, concentrándose en el uso exclusivo de software o aplicaciones que carecen de las debidas protecciones. La materialización de un delito cibernético se consuma al apuntar hacia redes informáticas y dispositivos que, lamentablemente, no cuentan con las defensas necesarias para resguardarse [14].

Para alcanzar un nivel efectivo de ciberseguridad, es imperativo abordar este desafío con una visión integral que abarque todos los elementos presentes en el extenso y complejo entorno cibernético. Este enfoque holístico implica no solo reconocer las vulnerabilidades inherentes a las tecnologías utilizadas, sino también evaluar la capacitación y concienciación de los usuarios, implementar políticas de seguridad sólidas y mantenerse

actualizado con las últimas innovaciones en el ámbito de la protección digital. En última instancia, la ciberseguridad eficaz requiere una comprensión profunda y una acción proactiva en todos los frentes para contrarrestar las amenazas cada vez más sofisticadas que acechan en el mundo digital [14].

- **Seguridad de Red (Network Security):** Se refiere a la protección de la infraestructura de red contra intrusiones, ataques y accesos no autorizados.
- **Seguridad de Aplicaciones (Application Security):** Implica la implementación de medidas para proteger las aplicaciones de software contra posibles amenazas y vulnerabilidades.
- **Seguridad de Puntos Finales (Endpoint Security):** Se centra en asegurar dispositivos finales como computadoras, tabletas y teléfonos móviles contra amenazas y accesos no autorizados.
- **Seguridad de Datos (Data Security):** Involucra la implementación de medidas para proteger la integridad y confidencialidad de los datos almacenados.
- **Gestión de Identidad (Identity Management):** Se refiere al control y manejo de las identidades de usuarios, asegurando que solo personas autorizadas tengan acceso a recursos.
- **Seguridad de Bases de Datos e Infraestructura (Database and Infrastructure Security):** Implica proteger las bases de datos y la infraestructura de sistemas contra posibles amenazas y ataques.
- **Seguridad en la Nube (Cloud Security):** Se centra en garantizar la seguridad de los datos y servicios almacenados en entornos de nube.
- **Seguridad Móvil (Mobile Security):** Aborda la protección de dispositivos móviles y las aplicaciones utilizadas en ellos contra posibles amenazas.
- **Recuperación ante Desastres/Planificación de Continuidad del Negocio (Disaster Recovery/Business Continuity Planning):** Implica la preparación y planificación para mantener la continuidad de las operaciones después de eventos adversos.

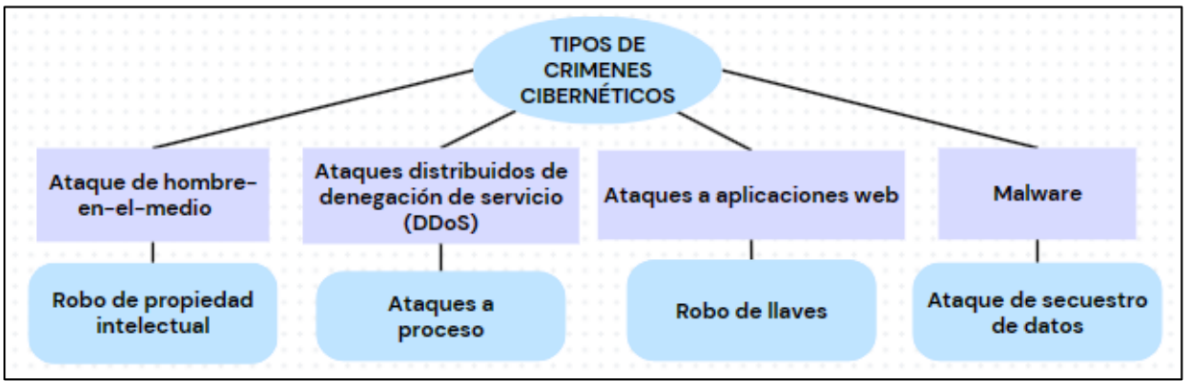

Figura 2.1. Tipos de delitos cibernéticos *[14]*.

2.2 Integración de Blockchain a la Ciberseguridad

La tecnología Blockchain, caracterizada por su estructura intrincada y bien definida, se erige como una de las salvaguardias tecnológicas más sólidas a nivel global. Su reputación de seguridad la coloca en el centro de la atención, impulsando así la adopción de Blockchain en diversas esferas con el propósito fundamental de prevenir fraudes y robustecer la seguridad de los datos [14]. En el contexto de la ciberseguridad, la tecnología Blockchain, al sustentarse en un método de mantenimiento liderado por una entidad pública, despliega un potencial extraordinario en campos críticos, tales como:

- **Procesamiento de Big Data:** La capacidad de Blockchain para gestionar grandes volúmenes de datos de manera segura y transparente resulta crucial en entornos donde la integridad y la confidencialidad son imperativos.
- **Software de Protección de Puntos Finales:** La aplicación de Blockchain en la protección de puntos finales se traduce en una capa adicional de seguridad para dispositivos, salvaguardando contra posibles amenazas y accesos no autorizados.
- **Herramientas Financieras:** En el sector financiero, Blockchain proporciona una base segura para transacciones y operaciones, mitigando riesgos asociados con fraudes y manipulaciones.
- **Software de Gestión de Cadena de Suministro:** La transparencia inherente a la tecnología Blockchain encuentra una aplicación valiosa en la gestión de la cadena de suministro, asegurando la autenticidad y trazabilidad de productos a lo largo de toda la cadena.

Un ejemplo paradigmático de esta convergencia entre Blockchain y ciberseguridad es HYPR Corp, con sede en Nueva York. La empresa se especializa en soluciones de autenticación descentralizadas, permitiendo a consumidores y empleados acceder de forma segura y sin complicaciones a aplicaciones móviles, web e Internet de las cosas (IoT). La aplicación de Blockchain en las soluciones de HYPR Corp descentraliza credenciales y datos biométricos, facilitando una autenticación basada en riesgos más efectiva. En un gesto significativo de confianza en esta plataforma, la empresa destinó una inversión de 10 millones de dólares en 2018 [14]. Este caso ejemplifica cómo la tecnología Blockchain, al integrarse en soluciones de autenticación, no solo fortalece la seguridad, sino que también abre nuevas vías hacia la autenticación digital avanzada.

2.3 Aporte de Blockchain a la Ciberseguridad

2.3.1 Eliminación del factor humano

La adopción de la tecnología blockchain elimina la necesidad de que las empresas autentiquen a usuarios y dispositivos mediante contraseñas, proporcionando un acceso seguro. Esta supresión de errores humanos contribuye a prevenir métodos de ataque. A menudo, a pesar de las inversiones significativas en seguridad, la efectividad se ve comprometida si empleados y clientes utilizan contraseñas vulnerables. La implementación de blockchain no solo garantiza un proceso de autenticación sólido, sino que también aborda simultáneamente el punto de ataque [15].

Un sistema de seguridad basado en blockchain puede emplear una infraestructura de clave pública distribuida que autentica los dispositivos, asignándoles certificados SSL en lugar de contraseñas. La gestión de los datos de estos certificados recae en blockchain, impidiendo el uso de certificados falsos por parte de atacantes [14].

En el ámbito de la ciberseguridad, esta perspectiva innovadora no solo perfecciona la autenticación, sino que también enfrenta de manera eficaz las vulnerabilidades asociadas con contraseñas convencionales. La eliminación de la necesidad de contraseñas disminuye significativamente el riesgo de ataques basados en contraseñas débiles o comprometidas. Además, la implementación de certificados SSL a través de la infraestructura de clave pública distribuida de blockchain refuerza la autenticación de dispositivos, creando un entorno más resistente ante intentos de ataques fraudulentos que involucren certificados falsificados [14]. Este enfoque integral no solo fortalece la seguridad, sino que también simplifica y optimiza los procedimientos de autenticación en entornos

empresariales, ofreciendo una solución más robusta y avanzada en la protección de datos y sistemas [14].

Mensajería Privada Segura

La comunicación relativa a documentos y otros datos relacionados con el trabajo dentro de una organización es esencial para que se realicen las tareas laborales. Sin embargo, en muchas ocasiones, este tipo de datos o información se transfiere a través de diversas aplicaciones de mensajería y redes sociales, lo que aumenta el riesgo de robo de datos. Por esta razón, las empresas utilizan la tecnología Blockchain para ofrecer una plataforma segura para la transferencia de información a los empleados, la cual solo puede ser accedida en dispositivos seguros, haciéndola impenetrable en caso de un ataque [14].

Almacenamiento Descentralizado

Blockchain permite a los usuarios mantener y almacenar datos en sus propias computadoras y redes, asegurando que la cadena no colapse [15]. Si un atacante intenta modificar o realizar alguna acción con respecto a los datos en un bloque, el sistema garantiza la seguridad al verificar cada bloque de datos, identificando bloques manipulados dentro de la cadena y reconociéndolos como falsos, para luego eliminarlos de la cadena. Blockchain asegura que no existe una ubicación de almacenamiento única; cada usuario o sistema en la red almacena parte o incluso toda la cadena de bloques. Este método garantiza que cada sistema en la red tenga la tarea de verificar los datos compartidos y mantener la integridad de estos para evitar la manipulación de datos existentes y la adición de datos falsos [14].

Rastreabilidad

Cada transacción o acción que ocurre en una cadena de bloques ya sea pública o privada, se firma digitalmente. Esto asegura que una organización o entidad pueda rastrear cada transacción y también localizar la entidad correspondiente en la cadena de bloques utilizando su dirección pública [15]. Cualquier nueva transacción modifica el libro de contabilidad, con el estado anterior almacenado en el registro histórico, lo que lo hace completamente rastreable. Para la ciberseguridad, esta característica única añade un nivel adicional de tranquilidad de que los datos no han sido manipulados de ninguna manera, haciendo que sean completamente rastreables [14].

Ataques de Denegación de Servicio Distribuido (DDoS)

Un ataque distribuido de denegación de servicio (DDoS) representa una amenaza importante para la integridad de la cadena de bloques, ya que puede detener fácilmente

una transacción si una de las unidades se detiene de enviar transacciones. La dificultad para detener los ataques DDoS se debe al Sistema de Nombres de Dominio (DNS) [14].

Sistema de Nombres de Dominio (DNS)

El Sistema de Nombres de Dominio es en gran medida centralizado, lo que facilita el ataque a la conexión entre un sitio web y una dirección IP, permitiendo la posibilidad de cachear un sitio web o incluso dirigir a los usuarios a sitios web fraudulentos. Este enfoque centralizado brinda a los atacantes la capacidad de manipular la conexión entre un sitio web y su dirección IP de manera relativamente sencilla [14].

2.4 Triada de la Ciberseguridad: Integración con Blockchain

La Tríada CID, o Confidentiality, Integrity y Availability (Confidencialidad, Integridad y Disponibilidad), es un grupo de principios con un elevado nivel de importancia de la ciberseguridad que se centran en proteger los datos **[16]**.

La confidencialidad se refiere a la protección de los datos para que solo puedan ser accedidos por las personas autorizadas. La integridad se refiere a la protección de los datos para que no sean modificados sin autorización. La disponibilidad se refiere a la protección de los datos para que estén disponibles cuando sea necesario. La tecnología blockchain puede ser una herramienta eficaz para proteger los datos. Al cumplir con los principios de la Tríada CID, la blockchain puede ayudar a garantizar que los datos estén protegidos de accesos no autorizados, alteraciones y pérdidas **[16]**.

En el análisis que sigue, se realizará una exploración detallada de cómo los principios fundamentales de la Tríada CID se traducen y aplican de manera específica en la intersección entre la ciberseguridad y la tecnología blockchain. Este enfoque destaca no solo la importancia de estos principios en la protección de datos en línea, sino también cómo la tecnología blockchain emerge como un habilitador clave para alcanzar de manera efectiva y eficiente los objetivos de seguridad.

2.4.1 Confidencialidad

La confidencialidad de los datos es un principio fundamental de la ciberseguridad que se refiere a la protección de la información sensible de los accesos no autorizados. En el contexto de la tecnología blockchain, es importante garantizar que solo las partes interesadas y autorizadas tengan acceso a los datos [16].

Para proteger la confidencialidad de los datos en blockchain, es necesario implementar controles de acceso, como la autenticación y la autorización. La autenticación se refiere al proceso de verificación de la identidad de un usuario o sistema, mientras que la autorización se refiere al proceso de otorgar a un usuario o sistema acceso a recursos específicos [16].

Las implementaciones de blockchain originales no incluían controles de acceso específicos, lo que las hacía vulnerables a los ataques. Sin embargo, algunas implementaciones más recientes están comenzando a abordar este desafío mediante la implementación de encriptación completa de datos de bloque y capacidades AAA. La encriptación completa de datos de bloque garantiza que los datos no sean accesibles por partes no autorizadas mientras están en tránsito. Esto es especialmente importante si los datos se transmiten a través de redes no confiables [16].

Acceso a la Red

En las blockchains públicas, cualquier individuo tiene la capacidad de acceder a la red sin requerir autenticación o autorización. Contrariamente, en las blockchains privadas, se deben establecer medidas de seguridad para salvaguardar el acceso a la red [16].

En un escenario ideal, se asumiría que las redes privadas ya cuentan con una protección sólida respaldada por diversas capas de seguridad, como firewalls, redes privadas virtuales (VPN) y sistemas de detección y prevención de intrusiones (IDS/IPS). Sin embargo, en la realidad, estos controles no siempre resultan suficientes. Por ello, las prácticas óptimas de seguridad sugieren la implementación de controles de acceso directamente a nivel de la aplicación [16].

Adicionalmente, las organizaciones deben contemplar la gestión de nodos que no mantienen comunicación constante o que presentan actividad intermitente. Es imperativo que las blockchains continúen operando incluso si algunos nodos se desconectan, pero también deben contar con la capacidad de sincronizar la información cuando estos nodos se reconectan [16].

Acceso y Divulgación de Datos

La tecnología blockchain puede ayudar a proteger la confidencialidad de los datos mediante el cifrado completo de los bloques de datos. El cifrado de extremo a extremo, que solo permite que los usuarios autorizados con acceso a la clave privada puedan descifrar los datos, es una forma eficaz de proteger la privacidad [16].

Sin embargo, el robo de claves privadas sigue siendo un riesgo elevado. Las organizaciones deben seguir procedimientos adecuados de gestión de claves para proteger sus claves privadas [16].

Los algoritmos criptográficos utilizados hoy en día para la generación de claves públicas/privadas se basan en problemas de factorización de enteros, que son difíciles de resolver con la potencia informática actual. Sin embargo, los avances en la computación cuántica podrían hacer que estos algoritmos sean vulnerables. Por lo tanto, las organizaciones deben planificar el cambio a la criptografía resistente a la computación cuántica [16].

2.4.2 Integridad

La integridad de los datos se refiere a su protección contra la modificación o destrucción no autorizada. Es un principio fundamental de la ciberseguridad que es esencial para garantizar la confiabilidad de los datos [16].

En los sistemas de información, es importante mantener la consistencia de los datos y salvaguardar su integridad a lo largo de su ciclo de vida. Hay varias técnicas que se pueden utilizar para garantizar la integridad de los datos, como el cifrado, la comparación de hash y el uso de firmas digitales. Por otro lado, las características inherentes de blockchain, como la inmutabilidad y trazabilidad, también pueden ayudar a garantizar la integridad de los datos. La inmutabilidad significa que los datos almacenados en blockchain no se pueden modificar sin el consentimiento de la mayoría de los nodos de la red. La trazabilidad significa que se puede seguir el historial de cambios de los datos [16].

En conjunto, estas técnicas hacen de blockchain una plataforma sólida para proteger la integridad de los datos.

Inmutabilidad

La tecnología blockchain se considera segura porque dificulta la manipulación de los datos. Esto se debe a tres características clave:

- **Hash secuencial**: Los datos se almacenan en bloques que están vinculados entre sí mediante un hash secuencial. Esto significa que cualquier cambio en un bloque se reflejaría en todos los bloques posteriores, lo que haría que la manipulación de los datos fuera muy difícil o imposible [16].
- **Criptografía**: Los datos se cifran utilizando algoritmos criptográficos avanzados. Esto hace que sea muy difícil para los atacantes acceder o modificar los datos sin autorización [16].

- **Descentralización**: La red blockchain está descentralizada, lo que significa que no hay una sola entidad que controle los datos. Esto hace que sea más difícil para un atacante tomar el control de la red y manipular los datos [16].

Además de estas características clave, los protocolos del modelo de consenso también ofrecen un nivel adicional de seguridad sobre los datos. En las blockchains públicas y privadas, generalmente el 51 % de los usuarios deben estar de acuerdo en que una transacción es válida antes de que se agregue a la plataforma. Esto hace que sea muy difícil para un atacante tomar el control de la red y manipular los datos [16].

Las organizaciones pueden implementar mecanismos adicionales para prevenir y controlar la división del libro mayor en caso de un ataque cibernético del 51 %. Por ejemplo, pueden monitorear si uno de los nodos aumenta su potencia de procesamiento y está ejecutando un número significativamente mayor de transacciones [16].

Trazabilidad

Cada transacción introducida en una blockchain, ya sea de carácter público o privado, se certifica digitalmente y se registra con un sello temporal. Este proceso implica que las entidades tienen la capacidad de retroceder en el tiempo para cada transacción y identificar a la parte correspondiente (mediante su dirección pública) en la cadena de bloques. Este aspecto guarda relación con una propiedad crucial en términos de seguridad de la información: la no repudiación, que garantiza que alguien no pueda replicar la autenticidad de su firma en un archivo o la autoría de una transacción que hayan originado [16].

La funcionalidad integrada en la cadena de bloques refuerza la confiabilidad del sistema al detectar intentos de manipulación o transacciones fraudulentas, dado que cada transacción está vinculada criptográficamente a un usuario. Cada nueva transacción incorporada a una cadena de bloques induce un cambio en el estado global del libro mayor. La consecuencia de esto es que, con cada iteración subsiguiente del sistema, se conservará el estado previo, generando así un historial completamente rastreable. La capacidad de auditoría de la tecnología confiere a las organizaciones un nivel de transparencia y seguridad con respecto a cada interacción [16]. Desde la perspectiva de la ciberseguridad, esto proporciona a las entidades un grado adicional de seguridad al asegurar que los datos son auténticos y no han sido objeto de manipulación.

Contratos Inteligentes

Los contratos inteligentes, programas informáticos que se ejecutan en el libro mayor, se han convertido en una característica central de las blockchains hoy en día. Este tipo de

programa puede utilizarse para facilitar, verificar o hacer cumplir reglas entre partes, permitiendo un procesamiento directo e interacciones con otros contratos inteligentes. Este software proporciona una amplia superficie de ataque, por lo que un ataque a un contrato inteligente podría tener un efecto dominó en otras partes de la plataforma, como el propio lenguaje o la implementación de contratos [16].

La tecnología blockchain introduce un nuevo paradigma en el desarrollo de software y, como tal, se deben implementar (y actualizar) estándares y prácticas seguras de desarrollo (como la implementación de codificación segura y pruebas de seguridad) para tener en cuenta el ciclo de vida de los contratos inteligentes (creación, prueba, implementación y gestión). El ataque a The DAO, una organización descentralizada construida sobre Ethereum, es un ejemplo de un ataque a contratos inteligentes. Un atacante logró explotar un error en un contrato inteligente que resultó en el robo de 60 millones de Ether [16].

Calidad de los Datos

La tecnología blockchain no garantiza ni mejora la calidad de los datos. Las blockchains privadas y públicas solo pueden responsabilizarse de la precisión y calidad de la información una vez que ha sido ingresada en la cadena de bloques. Esto implica que es necesario confiar en que los datos extraídos de los sistemas fuente existentes de las organizaciones sean de buena calidad, al igual que en cualquier otro sistema tecnológico [16].

La mayor vulnerabilidad en el marco de la cadena de bloques estará fuera del marco en oráculos 'confiables'. Un oráculo corrupto podría potencialmente causar un efecto dominó en toda la red. Un ataque a un oráculo podría ser directo o indirecto a través de terceros conectados al oráculo [16]. Los oráculos permiten que datos no confiables ingresen a un entorno confiable, por lo que las organizaciones podrían considerar el uso de varios oráculos para aumentar la confianza en la integridad de los datos que ingresan a la cadena de bloques desde el oráculo.

2.4.3 Disponibilidad

Disponibilidad se define como la acción de asegurar acceso oportuno y confiable a la información y su uso. Los ciberataques que buscan afectar la disponibilidad de los servicios tecnológicos continúan aumentando. Los ataques de denegación de servicio distribuido (DDoS), siendo uno de los tipos más comunes de ataques, también pueden causar la mayor interrupción a los servicios de internet y, por ende, a las soluciones habilitadas por blockchain [16].

Las implicaciones resultantes son que los sitios web se interrumpen, las aplicaciones móviles dejan de responder y esto puede generar pérdidas y costos cada vez mayores para las empresas. Dado que las blockchains son plataformas distribuidas, los ataques DDoS en blockchains no son como los ataques regulares. Son costosos ya que intentan sobrecargar la red con grandes volúmenes de pequeñas transacciones (o, en el caso de los recientes ataques DDoS a Ethereum, acciones con costos de gas desproporcionadamente bajos que costaban 3,000 euros) [16].

Las características de descentralización y peer-to-peer de la tecnología hacen que sea más difícil de interrumpir que las arquitecturas de aplicación distribuida convencionales (como cliente-servidor), pero aún están sujetas a ataques DDoS, por lo que son necesarias medidas de protección adecuadas, tanto a nivel de red como de aplicación. La red Bitcoin resistió un ataque DDoS en 2014 [17], donde los atacantes intentaron desbordar la red con solicitudes. Según estudios, es probable que esto vuelva a ocurrir, y estima que los ataques DDoS aumentarán en tamaño y escala, con ataques regulares de terabit por segundo que tensionarán la capacidad de la infraestructura de Internet regional e incluso global [16].

Aunque las soluciones de blockchain descentralizadas son resistentes, dependen de una alta disponibilidad, y los ataques DDoS seguirán siendo una amenaza persistente.

Sin Punto Único de Fallo

Las blockchains, al carecer de un punto único de fallo, reducen significativamente las posibilidades de interrupciones por ataques DDoS basados en IP. Si un nodo se cae, los datos siguen siendo accesibles a través de otros nodos en la red, ya que todos mantienen copias completas del libro mayor. Bitcoin, siendo la plataforma más probada, ha resistido ciberataques durante más de 7 años, proporcionando un nivel adicional de accesibilidad a los datos, incluso ante ataques DDoS que afecten algunos nodos [16].

Aunque se considera que una red blockchain no tiene un solo punto de fallo, las organizaciones podrían enfrentar riesgos de eventos externos fuera de su control. Una interrupción global de Internet podría afectar incluso a redes blockchain públicas como Bitcoin o Ethereum, creando interrupciones que impactarían las operaciones de las organizaciones. Las redes privadas de blockchain, con menos nodos, deben garantizar una distribución global y resistencia sin puntos únicos de fallo a nivel de organización o plataforma, para mantener la operación continua incluso en situaciones de desastre o ataques coordinados [16].

Resiliencia operativa

La resiliencia operativa de las blockchains proviene de su naturaleza distribuida y la cantidad de nodos en la red, permitiéndoles funcionar sin problemas incluso durante ataques. Tanto en blockchains públicas como privadas, la redundancia de nodos permite que la red continúe operando normalmente incluso si algunos nodos enfrentan ataques. Sin embargo, esta resistencia no implica invulnerabilidad total [16].

A lo largo de los años, las blockchains han enfrentado diversos desafíos, como ataques de maleabilidad de transacciones en Bitcoin y exploits de contratos inteligentes en Ethereum. Aunque estas situaciones han llevado a soluciones como hard forks, es esencial reconocer que la resiliencia operativa no garantiza la ausencia total de vulnerabilidades. Los reguladores juegan un papel crucial en la promoción de estándares y pruebas rigurosas para respaldar la resiliencia operativa de las blockchains, y la colaboración con ellos se considera esencial para su desarrollo y adopción comercial [16].

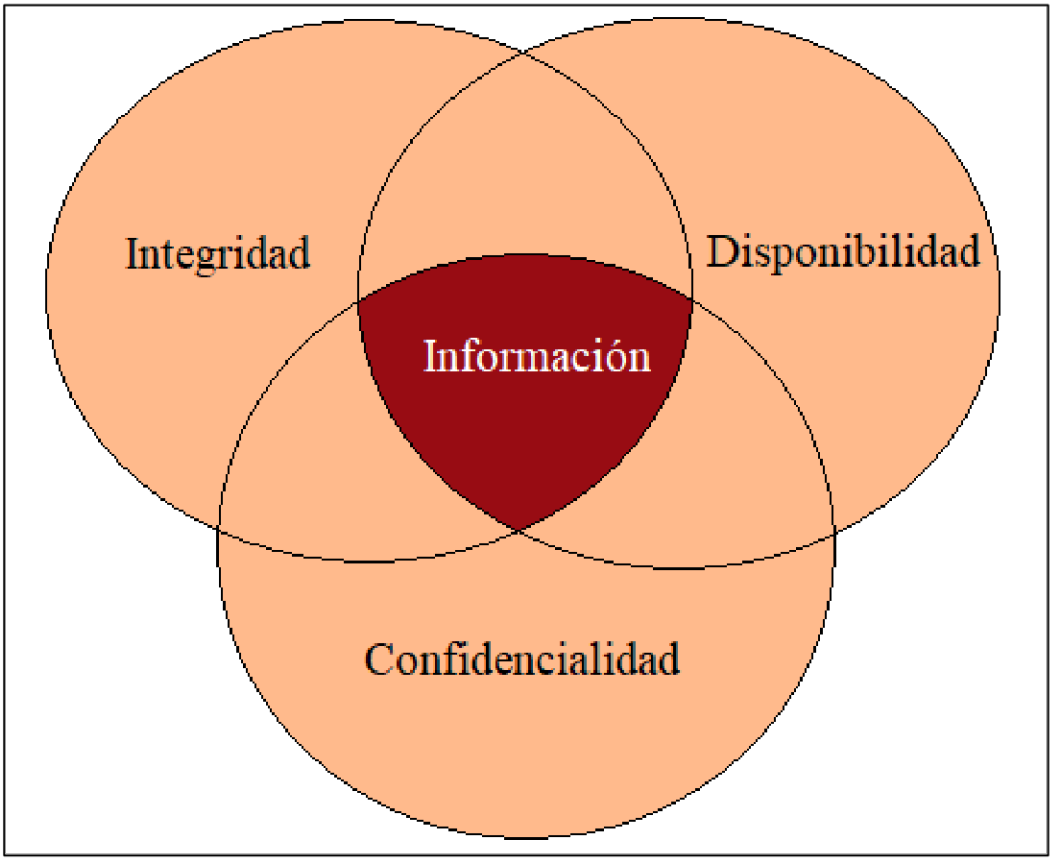

Figura 2.2. Diagrama representativo de la triada CID.

2.5 Programa de Riesgo Cibernético SVR

La total seguridad de ningún sistema de ciberdefensa o gestión de información puede garantizarse al 100%. La constante evolución y la naturaleza rentable del ciberdelito, junto con la creatividad de los delincuentes en la búsqueda de nuevos métodos de ataque,

impiden afirmar con certeza que lo considerado seguro hoy seguirá siéndolo mañana. Aunque las cadenas de bloques ofrecen características intrínsecas de confidencialidad, integridad y disponibilidad de datos, similares a otros sistemas, resulta esencial que las organizaciones que las incorporan a su infraestructura tecnológica implementen controles y estándares de seguridad cibernética para protegerse de amenazas externas [16].

Los expertos en ciberseguridad de Deloitte en todo el mundo promueven la adopción del enfoque cibernético Seguro, Vigilante y Resiliente (SVR). Este enfoque no solo refuerza la seguridad de las entidades, sino que también las hace más alerta y resistentes ante las amenazas cibernéticas en constante evolución. Eric Piscini, líder global de Blockchain de Deloitte en EE. UU., destaca que, aunque la ciberseguridad es crucial para la amplia adopción de blockchain, también es fundamental considerar aspectos como operaciones, arquitectura tecnológica, formación de consorcios, talento y regulaciones globales. Se recomienda contactar con los equipos especializados de ciberseguridad y blockchain en su región para obtener orientación sobre cómo proteger su blockchain o negocio contra ataques cibernéticos [16] [18].

Para poder tener un poquito más de profundidad sobre los términos mencionados, se proporciona la **figura 2.3.**

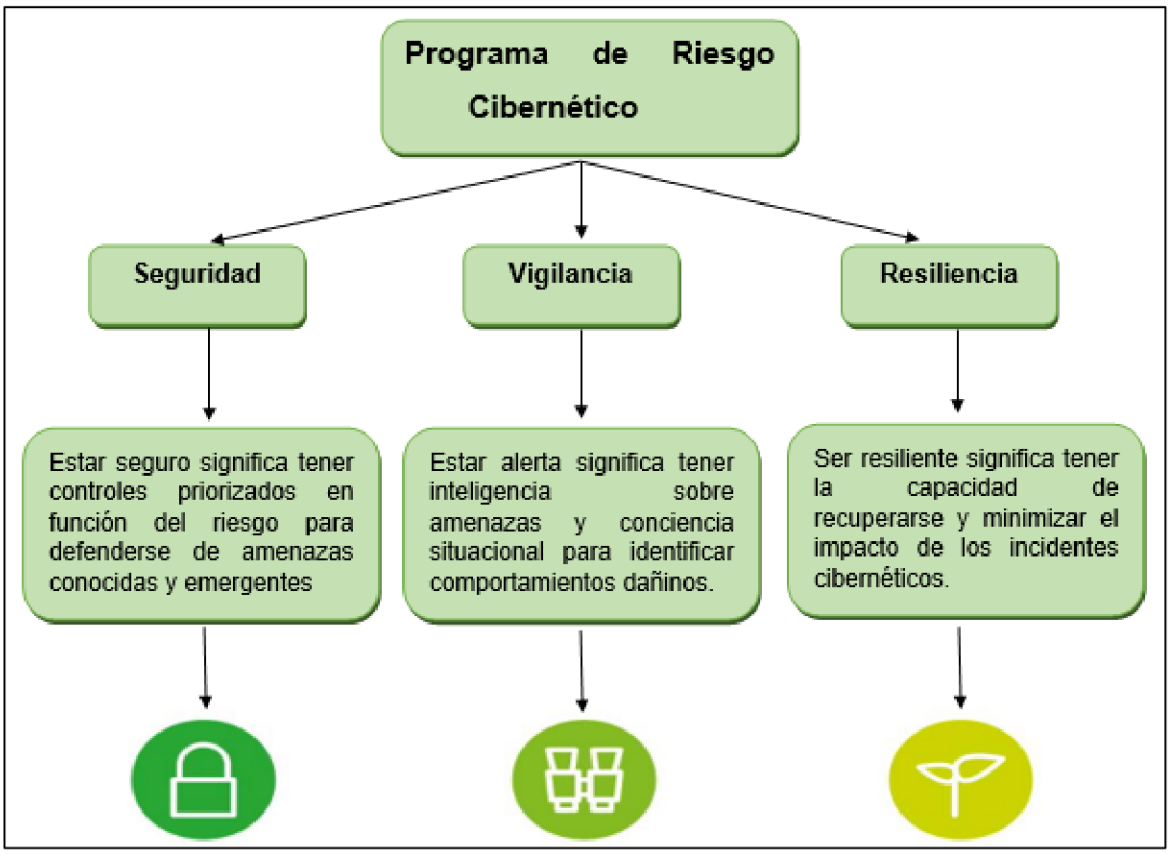

Figura 2.3. Programa de Riesgo Cibernético *[16] [18]*.

2.6 Vulnerabilidades de Blockchain para la Ciberseguridad

A raíz de la investigación, se han identificado diversas vulnerabilidades clave en el entorno de blockchain que pueden tener implicaciones significativas para la seguridad cibernética. En este módulo, nos sumergiremos en un análisis exhaustivo de algunas de estas vulnerabilidades críticas, explorando los riesgos asociados y examinando estrategias de mitigación. La **figura 2.5** proporciona un resumen visual de estas vulnerabilidades, estableciendo la base para nuestra exploración detallada. Este enfoque permitirá una comprensión más completa de los desafíos específicos que enfrenta la tecnología blockchain en términos de seguridad.

2.6.1 Riesgos Generales de Blockchain 1.0

Doble Gasto

El gasto doble se produce cuando un usuario realiza varios pagos utilizando una única forma de financiamiento en una red P2P. Este problema surge debido a que las transacciones se validan mediante la resolución de un problema matemático, lo que implica un lapso de tiempo antes de su confirmación. Al anunciar pagos no procesados en la red o al actualizar los nodos con transacciones aún no confirmadas, pueden ocurrir interrupciones en las transmisiones en momentos diferentes. En Bitcoin, resolver exitosamente un problema toma alrededor de 10 minutos, dictado por la dificultad del cálculo y los ajustes en la potencia de procesamiento de los mineros [19].

El proceso se basa de la siguiente manera: un atacante (A) busca engañar a un minorista (R) para que acepte una transacción (TrR) que no pueda revertir. Para lograr esto, A crea otra transacción (TrA) con los mismos insumos que TrR, pero con una dirección de destinatario controlada por A. Si ambas transacciones se inician simultáneamente hacia nodos en la cadena, la cadena solo aceptará la versión de la transacción que llegue primero para su inclusión en los bloques generados, ignorando otras versiones. Así, un ataque de gasto doble tiene éxito si R recibe TrR, pero la mayoría de los nodos en la red reciben TrA, que tiene una posibilidad significativa de ser incluida en un bloque generado [19].

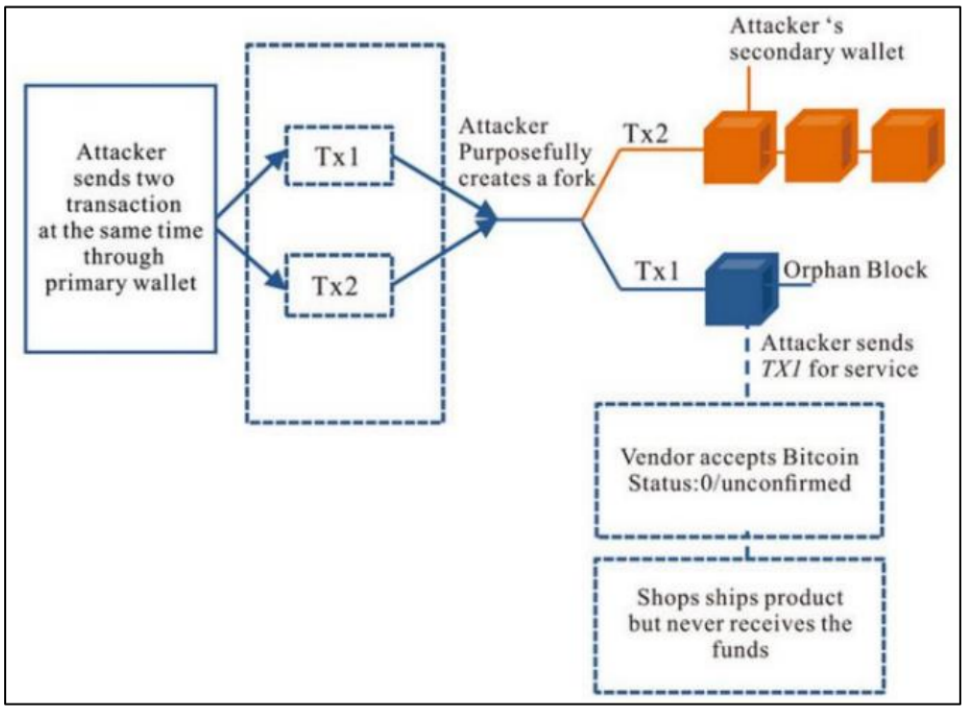

Figura 2.4. Principios de funcionamiento del ataque de doble gasto *[19]*.

El ataque del 51% o Goldfinger

Las estructuras de consenso presentes en las blockchains exhiben una notoria susceptibilidad a los ataques de doble gasto y del 51%, los cuales no pueden ser evitados en estos sistemas y, teóricamente, tienen la posibilidad de manifestarse en cualquier momento. El ataque del 51%, también conocido como "Goldfinger", fue inicialmente dirigido contra Bitcoin y tiene la capacidad de ser implementado en otros sistemas basados en la tecnología blockchain (BT). Se considera que un sistema BT está protegido cuando los nodos de confianza controlan al menos el 51% de la potencia de procesamiento minero en la red. En este escenario, el costo asociado con la adquisición de un control significativo podría superar el costo de obtener una capacidad minera considerable, lo que aumenta la complejidad de llevar a cabo estos ataques [19].

Durante un ataque del 51%, el tiempo de la moneda del atacante puede ser compensado, lo que complica su habilidad para evitar que las transacciones se incorporen a la cadena principal. Adicionalmente, existe la posibilidad de que un atacante interfiera con la confirmación de nuevas transacciones, obstaculizando así la recepción de fondos por parte de algunos o todos los nodos. En situaciones de un ataque del 51%, sería sumamente desafiante para el atacante tomar el control de la cadena de bloques, ya que las transacciones se bloquean antes del inicio del ataque si se intenta modificar los bloques históricos [19].

Seguridad de billetera (seguridad de clave privada)

En términos generales, las criptomonedas resguardan su valor utilizando un dispositivo de almacenamiento denominado billetera, en la cual cada usuario posee un conjunto de claves públicas y privadas para acceder a la misma. La vulnerabilidad principal de esta billetera radica en su susceptibilidad a influencias externas, manipulaciones y traslados, aspecto compartido con otras formas de almacenes. Con frecuencia, los usuarios olvidan sus códigos PIN o contraseñas de protección, o pueden extraviar el dispositivo de almacenamiento que contiene la clave privada, impidiendo así el acceso a la billetera. Esta situación puede equipararse al problema que genera el ransomware. Los métodos para el robo de billeteras incluyen tácticas convencionales como el phishing, que abarca desde el pirateo del sistema hasta la instalación de software defectuoso y el uso indebido de las billeteras [19].

La explotación de un sistema blockchain puede ocurrir fácilmente mediante cualquier vulnerabilidad que pueda afectar a la solución criptográfica. Es evidente que cualquier error de programación o la ausencia de una clave privada segura pueden constituir la base de una brecha de seguridad significativa. En un escenario hipotético, un atacante criptográfico no debería poder comprender el texto original sin formato, que está cifrado. Sin embargo, la estructura de los bloques, aunque cifrada, no es difícil de entender, y un criptoatacante habilidoso podría intentar descifrar parcialmente el texto original en cada bloque cifrado, ya que cada bloque es una función del bloque anterior [19].

2.6.2 Fallo específico en PoS

Cuando una participación se desplaza en una blockchain basada en Prueba de Participación (PoS), la vulnerabilidad del "nada en juego" se manifiesta, ya que los participantes honestos pueden validar claves de cuentas pasadas sin participación actual, facilitando la creación de una cadena de bloques alternativa por parte de un conjunto malicioso de participantes. Este tipo de ataque se simplifica porque los participantes mantienen varias blockchains simultáneamente, aprovechando la baja potencia computacional necesaria en las blockchains basadas en PoS. Aunque los participantes tienen un incentivo para actuar correctamente en la cadena más larga, surgen desafíos, como la baja probabilidad de ser una parte crucial de un ataque y la necesidad de sobornos para inducir la participación en un ataque [19].

Además, la arquitectura de PoS enfrenta vulnerabilidades, como el riesgo de un ataque de largo alcance, donde un atacante con el 1% de todas las monedas podría iniciar una bifurcación sin los bloques más recientes en la cadena principal. Se plantea la posibilidad

de un ataque de corto alcance mediante la manipulación de bloques con marcas de tiempo, presentando desafíos para nuevos usuarios al identificar la cadena más larga. Aunque existen contramedidas como la inclusión de marcas de tiempo en cada bloque, la probabilidad de un ataque se reduce con el tiempo y se detecta fácilmente en el caso de un atacante con una participación significativa. Estas vulnerabilidades destacan la necesidad de abordar aspectos clave en la seguridad de las blockchains basadas en PoS [19].

2.6.3 Bifurcaciones privadas y ataques en grupo

La cadena de bloques basada en Prueba de Trabajo (PoW) es extensamente utilizada en el sistema de moneda digital, ocupando una parte significativa de la capitalización total del mercado. La seguridad de esta arquitectura PoW se vincula directamente con la condición de seguridad del sistema blockchain, donde un atacante, en caso de existir, debe tener control computacional igual o inferior al 50%. Eyal y Sirer presentaron la minería egoísta, un ataque que desafía la sabiduría convencional y permite a un minero egoísta con entre el 25% y el 33% del poder de extracción ganar el 50% del poder minero. Si supervisado a un alto nivel, el atacante puede publicar bloques de manera selectiva, generando una alianza con nodos imparciales y aumentando así su control sobre la red. La estrategia implica crear una cadena privada distinta de la pública [19].

Inicialmente, ambas cadenas, pública y privada, se inician simultáneamente, permitiendo al atacante buscar oportunidades para minar en la cadena privada y asegurar derechos de retención en los bloques disponibles. Este enfoque estratégico implica un equilibrio entre la publicación de bloques y la gestión de ingresos para el atacante y otros participantes. La temporalidad de las reducciones de ingresos para el atacante se compensa con la creación de incentivos para que nodos imparciales se unan a la alianza del atacante, aumentando su control sobre la red y creando una cadena privada distintiva [19].

2.6.4 Ataque a nivel de red

Los problemas de seguridad en las redes blockchain son actualmente un área destacada de investigación en seguridad en internet. Aunque se han abordado aspectos como la escalabilidad, seguridad y sostenibilidad, persisten inquietudes en torno a estos temas. Con el auge del mercado de monedas digitales, los ataques cibernéticos, especialmente los de denegación de servicio distribuido (DDoS), representan una amenaza creciente para los servicios. Las plataformas basadas en blockchain, como Ethereum y Bitcoin, a pesar

de su naturaleza descentralizada, aún son susceptibles a ataques DDoS, requiriendo medidas de protección a nivel de red y aplicación para mitigar estos riesgos [19].

En el ecosistema de criptomonedas, los intercambios de monedas desempeñan un papel crucial, pero con frecuencia enfrentan ataques DDoS. Mt. Gox, uno de los principales intercambios de Bitcoin, experimentó cierres debido a estos ataques. Investigaciones revelan que los ataques DDoS afectan de manera desproporcionada a intercambios, grupos de minería, operadores de juegos de azar y servicios financieros en comparación con otros. Este escenario plantea un desafío continuo para la seguridad en un entorno donde la resiliencia y la protección contra ataques DDoS son esenciales [19].

Ataque de maleabilidad

Un usuario deshonesto con bitcoins en un intercambio puede aprovechar la vulnerabilidad de la maleabilidad de transacciones para duplicar transacciones y recibir las monedas nuevamente. Al cambiar la firma digital y retransmitir la transacción con un nuevo ID, existe la posibilidad de que la red la acepte como válida antes de que la transacción original se confirme. Este enfoque puede explotarse en intercambios que no gestionan adecuadamente estas situaciones [19].

Además, un atacante podría causar daño significativo a la red de Bitcoin mediante ataques intencionados de maleabilidad de transacciones en varios intercambios simultáneamente. El uso de software diseñado para crear transacciones mutantes podría abrumar a los sistemas internos de los intercambios, generando problemas logísticos. Además de estos ataques, existen riesgos, como el ataque Sybil, en redes que carecen de controles de admisión, permitiendo que un usuario cree múltiples identidades y manipule el consenso, facilitando el doble gasto. La dominancia en la red también puede lograrse controlando el 51% de la potencia de minería en una red PoW [19].

Ataque DDoS contra la red Ethereum

Un ataque DDoS (computacional) afectó la red de Ethereum en septiembre de 2016, provocando que mineros y nodos pasaran mucho tiempo esperando para procesar bloques. La causa principal fue el opcode EXTCODESIZE, un opcode de bajo costo de gas que obligaba a los nodos a leer información de estado almacenada en un disco. Los atacantes ejecutaron este opcode aproximadamente 50,000 veces por bloque, lo que resultó en una drástica desaceleración de la velocidad de la red [19].

En octubre de 2016, se produjo otro ataque DoS debido a fallas inherentes en el protocolo. Los atacantes simplemente crearon grandes cantidades de cuentas vacías y económicas en el estado de Ethereum mediante el uso de opcodes SUICIDE que transferían [19].

2.6.5 Vulnerabilidades en Blockchain 2.0 (Ataque contra contratos inteligentes)

Los contratos inteligentes en Ethereum, como la segunda generación de cadenas de bloques públicas, ofrecen una plataforma global para el intercambio de criptomonedas (Ether). A pesar de su popularidad, Ethereum y sus contratos inteligentes son susceptibles a vulnerabilidades derivadas de errores de codificación simple. Ethereum es la plataforma de cadena de bloques más destacada en la actualidad en cuanto a capitalización de mercado de criptomonedas. Investigaciones han proporcionado taxonomías de vulnerabilidades en contratos inteligentes, destacando problemas de seguridad explotables con fines de lucro y herramientas como oyente para identificar posibles errores de seguridad [19].

Vulnerabilidad de reentrada (ataque DAO)

Basándose en el ataque más importante al mundo de criptomoneda, la vulnerabilidad de reentrada se presenta como la falla más crítica en los contratos inteligentes. Esta vulnerabilidad surge de la posibilidad de reinserción de una función no recursiva durante su ejecución debido al mecanismo de recuperación, lo que conlleva a un comportamiento inesperado y bucles potenciales que agotan todo el gas disponible. El ataque DAO en junio de 2016 causó una interrupción sustancial en Ethereum, obligando a los desarrolladores a implementar un hard fork, lo que resultó en la creación de dos plataformas separadas: Ethereum y Ethereum Classic [19].

En el ataque DAO, el agresor despliega un contrato inteligente malicioso, utilizando específicamente la función "splitDAO" para manipular los saldos y totales de los usuarios. A través de este método, el atacante ejecuta numerosas transacciones, recolectando Ether múltiples veces en una sola transacción. Como respuesta a estos ataques, la comunidad DAO propuso un hard fork de software con una función "NO ROLLBACK", a partir del bloque número 1760000, para rechazar o invalidar transacciones que implementan llamadas/códigos de llamada/ejecuciones delegadas que ejecutan código con un código hash del atacante [19].

Cartera multifirma de paridad

En julio de 2017, se llevó a cabo el segundo ataque más significativo en la red Ethereum, donde se robaron más de 150,000 ETH (alrededor de $30 millones). La vulnerabilidad, reportada por el equipo de Parity, afectó a los contratos de cartera multisig en la versión 1.5+ de Parity. El atacante explotó la combinación de modificadores de visibilidad inseguros y el uso indebido de la llamada a delegados con datos arbitrarios. Al enviar dos transacciones para cada contrato afectado, el atacante obtuvo la propiedad exclusiva de la multisig y transfirió todos los fondos, aprovechando la ejecución automática debido a su condición como único propietario [19].

Este incidente reveló una brecha en la seguridad de Parity y sus contratos multisig, resultando en una pérdida significativa de activos. La estrategia del atacante se basó en modificar el estado de propiedad del contrato, permitiendo la transferencia automática de fondos a una cuenta controlada por él. La complejidad del ataque residió en la explotación efectiva de las funciones y la estructura del contrato multisig, lo que llevó a la comunidad a implementar medidas más sólidas para prevenir futuras vulnerabilidades en este tipo de contratos en Ethereum [19].

King of the ether throne

King (del Ether Throne) no tuvo éxito debido al alto costo de gas necesario para enviar Ether a una dirección de contrato en comparación con una billetera simple. El contrato defectuoso, un esquema de apuestas para adquirir la "corona," tenía la peculiaridad de que al coronar a un nuevo "rey," el precio aumentaba, y la mayoría de los pagos iban al rey actual. Sin embargo, surgieron problemas ya que, al utilizar direcciones de contrato en lugar de billeteras, el proceso resultaba costoso y llevaba a errores. El contrato no verificaba correctamente el éxito de las transacciones ni asignaba suficiente gas en algunas instancias, lo que ocasionalmente revertía los pagos y dejaba las ganancias del rey anterior atrapadas en el contrato [19].

El intento de King de Ether Throne fracasó principalmente debido a los altos costos de gas asociados con las transacciones hacia direcciones de contrato en lugar de billeteras simples. El contrato, diseñado como un esquema de apuestas para obtener la "corona," presentó inconvenientes cuando coronaba a un nuevo "rey," incrementando el precio y dirigiendo la mayoría de los pagos al rey actual. Sin embargo, al usar direcciones de contrato en lugar de billeteras, surgieron problemas, ya que el contrato no verificaba adecuadamente el éxito de las transacciones y asignaba gas insuficiente en algunas ocasiones, resultando en pagos revertidos y ganancias bloqueadas para el rey anterior [19].

Gubernamental

GovernMental se enfrenta a un dilema similar, aunque de manera más sutil en su enfoque. El contrato en cuestión operaba como un esquema Ponzi, donde los usuarios invertían Ether con la promesa de obtener retornos incrementados y la posibilidad de ganar un "jackpot". Este último se constituía a partir de un porcentaje de la entrada de cada participante y se entregaba al último usuario que se uniera al contrato si durante un periodo de 12 horas nadie más enviaba Ether [19].

En cuanto a su funcionalidad interna, el contrato almacenaba las direcciones de los usuarios en un array de tamaño dinámico y requería realizar iteraciones sobre estos arrays para realizar la limpieza cuando se alcanzaba un jackpot. No obstante, carecía de una limitación en el tamaño del array. A medida que GovernMental atraía a un número significativo de usuarios, la asignación de gas ya no podía cubrir completamente el tamaño del array. Esto resultaba en fallos recurrentes para reiniciar el juego y otorgar el jackpot al ganador, dejando efectivamente el estado del contrato congelado y sin cambios [19].

2.6.6 Vulnerabilidades en Blockchain 3.0

En esta sección, abordaremos las amenazas de seguridad existentes y sus contramedidas para las blockchains privadas y sus tecnologías subyacentes. Realizaremos un análisis detallado de posibles vulnerabilidades en la red de blockchain privada, examinando de cerca el amplio vector de ataques y su impacto en los componentes específicos. Entre las implementaciones de blockchain privadas prometedoras se encuentran Hyperledger, Corda, Quorum, Exonum, Ethereum, así como el uso privado de Quorum y Ethereum en blockchains públicas de Ethereum, que pueden bifurcarse y reconfigurarse para su uso en blockchains privadas. Corda fue diseñada para ser una plataforma de tecnología de libro de contabilidad distribuido (DLT) de grado financiero. Sin embargo, Corda, diseñada para redes semiprivadas, requiere obtener una identidad firmada por una autoridad principal para la admisión. Por lo tanto, abordaremos la blockchain privada de Hyperledger desde una perspectiva de seguridad. Además, esta sección proporcionará un resumen general de los posibles riesgos en las blockchains privadas [19].

Ataque contra Hyperledger Fabric

Hyperledger, una iniciativa de la Linux Foundation, surge como una respuesta evolutiva a las amenazas cibernéticas que afectaron la red de blockchain de Bitcoin (BT). Diseñado como un proyecto de código abierto, Hyperledger tiene como objetivo facilitar el desarrollo colaborativo de libros de contabilidad distribuidos basados en blockchain, con un enfoque específico en mejorar el rendimiento y la confiabilidad. Sus cinco marcos modulares, que

incluyen Fabric, Burrow, Iroha, Sawtooth e Indy, ofrecen funciones avanzadas para abordar las necesidades empresariales e industriales. IBM opera un contrato inteligente en Fabric, destacando la modularidad y el rendimiento de este marco para redes de permisos, donde todos los participantes tienen identidades conocidas. Aunque Hyperledger Fabric presenta una variedad de Software Development Kits (SDK) para lenguajes como Node.js y Java, se señala la necesidad de abordar vulnerabilidades en Node.js, que incluyen la susceptibilidad a ataques de denegación de servicio y ataques de reenvío de DNS [19].

Por otro lado, se destaca que las pruebas de penetración realizadas en Hyperledger Fabric revelan que, según el perfil de riesgo, las preocupaciones de seguridad principales y las vulnerabilidades identificadas, se requiere una atención moderada. Se subraya la importancia de abordar las vulnerabilidades de seguridad en Node.js y Go, utilizados en el desarrollo de chaincodes, ya que pueden ser explotados para ejecutar código de forma remota. A pesar de estas preocupaciones, Hyperledger ofrece un enfoque prometedor para mejorar la confianza, transparencia y rendimiento en la implementación de libros de contabilidad distribuidos, proporcionando una base sólida para la evolución de soluciones blockchain privadas [19].

Riego general en la implementación privada de Blockchain

En el ámbito de la seguridad, las blockchains privadas ofrecen ventajas significativas, especialmente cuando los mineros o validadores no pueden mantener el anonimato. La preselección de participantes por parte de la organización implica un alto nivel de confianza, reduciendo las posibilidades de comportamiento malicioso en la red. Las blockchains privadas también garantizan una solución de privacidad más sólida en comparación con las públicas. Sin embargo, la elección entre plataformas blockchain públicas o privadas depende de las necesidades específicas de cada caso de negocio. Para casos que requieran alta confidencialidad, alto rendimiento transaccional y finalidad inmediata, las blockchains privadas y permisionadas se presentan como una tecnología prometedora [19].

Al abordar la implementación de blockchains privadas, es esencial considerar posibles problemas de seguridad. Entre ellos se encuentran el diseño deficiente de la arquitectura, que puede resultar en la división y replicación de la red de contabilidad privada en cadenas de bifurcación paralelas, generando ambigüedades entre bloques hijos y cadenas paralelas. La seguridad de la red también puede verse comprometida por un diseño deficiente, lo que podría exponer a la red a ataques de denegación de servicio (DoS) o

spam de transacciones. Además, la criptografía deficiente puede dar lugar a la vulnerabilidad de las claves privadas y, por ende, a transacciones fraudulentas o pérdida de activos. La gestión de acceso inadecuada en contratos inteligentes también es un punto crítico, ya que las vulnerabilidades en la lógica de negocio codificada pueden desviar la ejecución prevista de los contratos hacia transacciones maliciosas o incluso toma de control no deseada. En el ámbito de los consensos, las blockchains empresariales presentan desafíos adicionales debido a la complejidad de las transacciones. El mecanismo de consenso, a menudo basado en algoritmos BFT (tolerancia a fallas bizantinas), debe adaptarse a roles diversos y garantizar la conexión total de los nodos en la red [19].

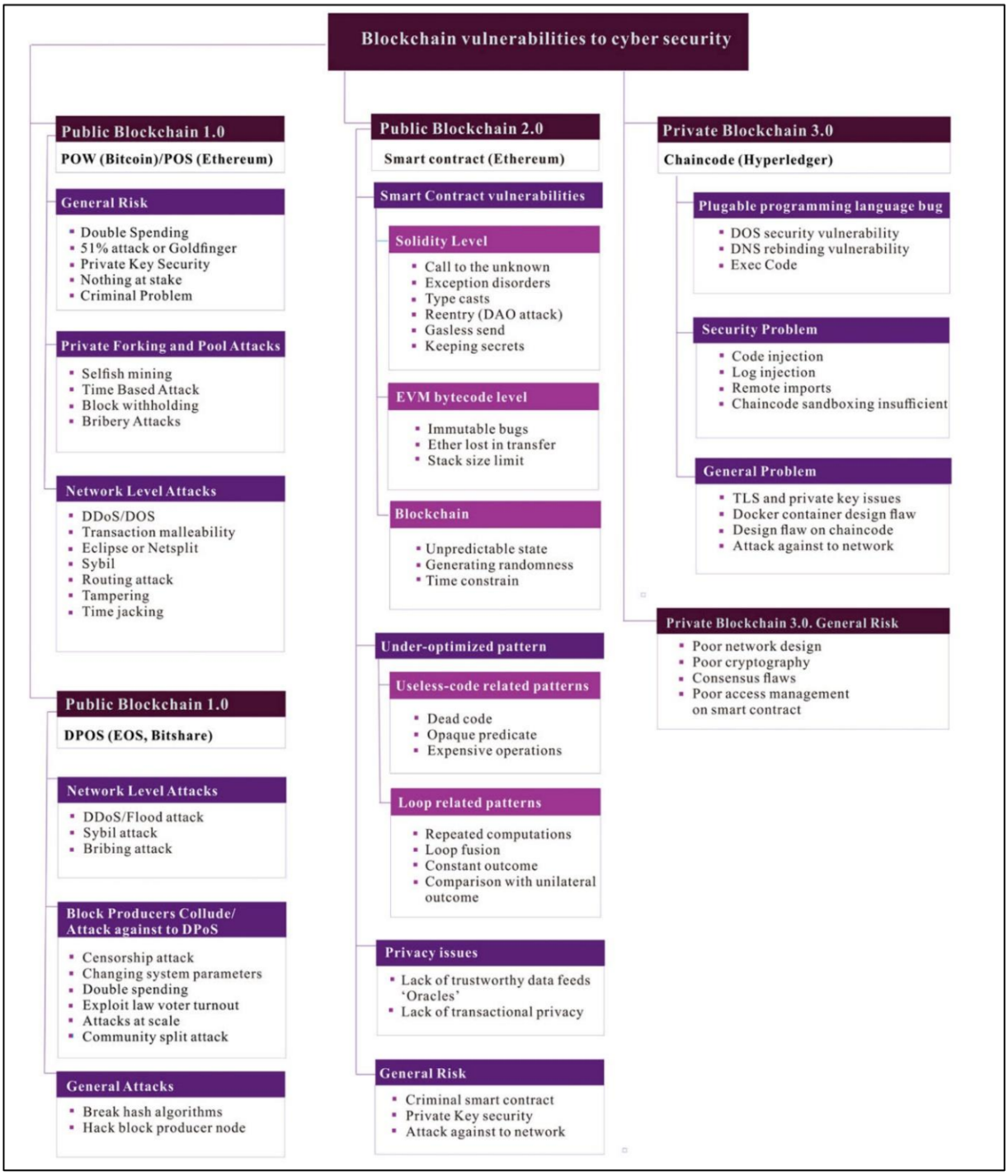

Figura 2.5. Vulnerabilidades en Blockchain para la Ciberseguridad [19].

2.7 Posibles contramedidas a las vulnerabilidades

En esta sección, se detallan las contramedidas y algoritmos de detección disponibles para BT con el propósito de asegurar la privacidad y la seguridad en el contexto de una tesis. Para obtener una visión exhaustiva sobre este tema, se ha realizado una exhaustiva revisión de literatura, extrayendo información de diversos documentos y recursos en línea provenientes de bases de datos científicas. Los resultados de esta revisión se presentan de manera consolidada en la **figura 2.7**, destacando las soluciones de vanguardia aplicadas a entornos blockchain que abordan las amenazas de seguridad y fortalecen la protección de la privacidad en el ámbito de estudio.

2.7.1 Slasher: Un algoritmo PoS punitivo

La técnica Slasher, concebida por Vitalik Buterin para Ethereum, representa una fusión de los algoritmos PoW/PoS, incorporando elementos de ambos. En Slasher, se utiliza PoW para la generación y minería de bloques, pero cada unidad debe ser validada por ambos algoritmos. Durante la creación de un bloque, el minero incluye un valor H(n) generado aleatoriamente, actuando como prueba de minería. La recompensa por la minería se reclama mediante una transacción especial después de 100 bloques, y la validación criptográfica se realiza por usuarios signatarios seleccionados al azar. Slasher utiliza un mecanismo similar a Tendermint para prevenir bifurcaciones del bloqueo, penalizando a los votantes que respaldan la bifurcación incorrecta. La técnica presenta una ventaja significativa sobre las arquitecturas PoS al requerir una potencia informática sustancial para ataques a largo plazo, dada su utilización de PoW [19].

En resumen, Slasher integra eficientemente PoW y PoS en Ethereum, garantizando la seguridad y la resistencia a bifurcaciones a corto plazo. La asignación de recompensas y privilegios de firma proporcionales al valor monetario respaldado refuerza la integridad del sistema, mientras que la combinación de elementos PoW impide carreras competitivas entre mineros, consolidando la estabilidad del protocolo [19].

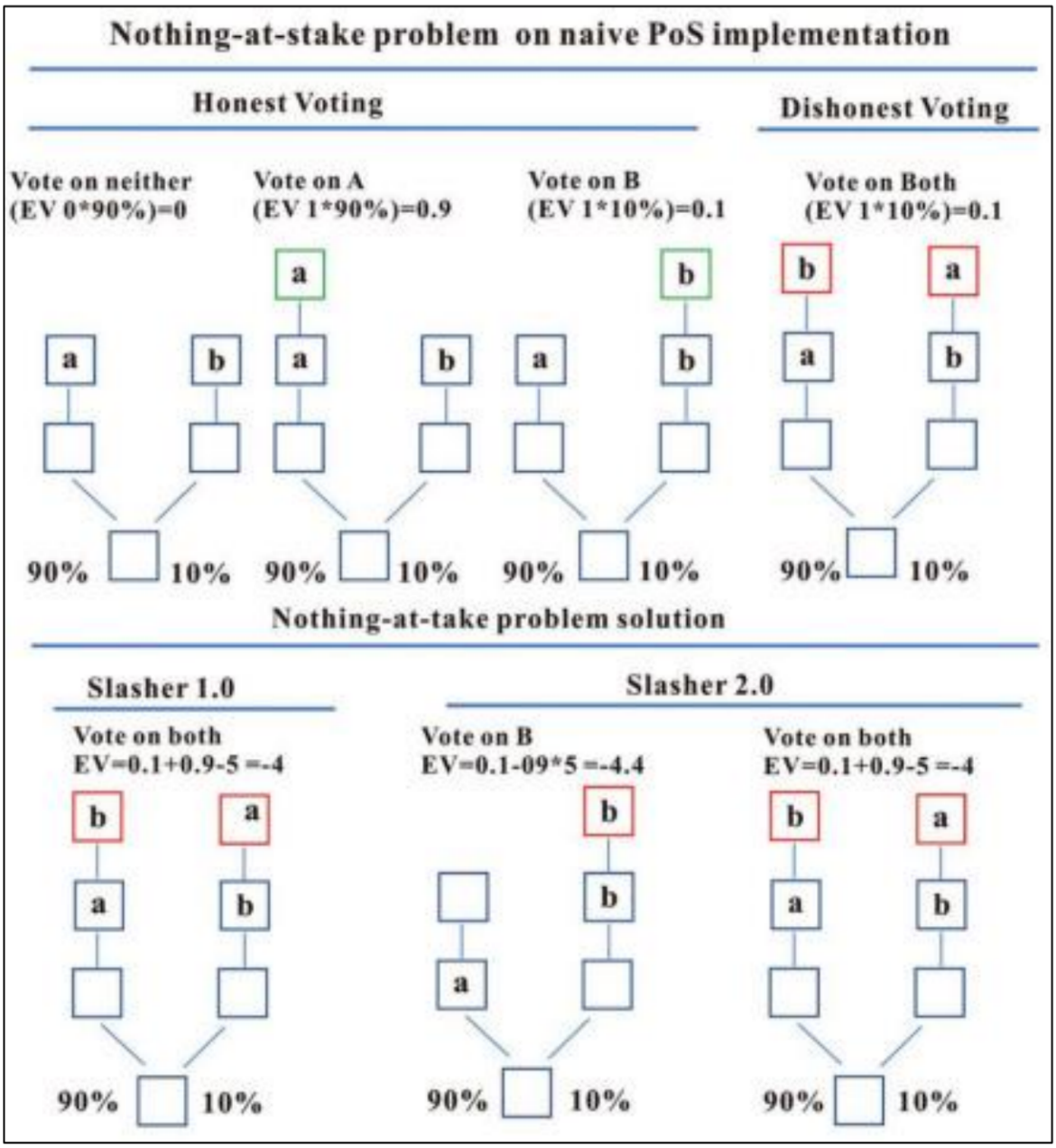

Figura 2.6. Problema de “nada en juego” con la solución Slasher [19].

2.7.2 Protocolo Casper

Diversos algoritmos de consenso en criptomonedas recompensan a los certificadores que participan en el algoritmo PoS. Desde una perspectiva algorítmica, hay dos tipos principales de PoS: el basado en cadena y la tolerancia a fallas bizantinas (BFT). El enfoque BFT del PoS permite a los certificadores "votar" mediante condiciones de finalidad y condiciones de reducción, enviando mensajes firmados. En este contexto, Vitalik et al. introdujeron CASPER, un sistema de finalidad basado en PoS que sigue la tradición BFT, incorporando algunas modificaciones. CASPER es un mecanismo de consenso parcial, un sistema híbrido PoW/PoS diseñado para sancionar elementos maliciosos y que fusiona la

investigación del algoritmo PoS con la teoría del consenso BFT. Entre las características novedosas de CASPER, se describen algunas a continuación [19].

Responsabilidad

CASPER, un algoritmo innovador en el ámbito del consenso en criptomonedas, utiliza contratos inteligentes para supervisar las apuestas y la generación de fondos. Al aprovechar esta tecnología, CASPER ha abordado de manera efectiva el dilema de "nada en juego" inherente a los algoritmos de Prueba de Participación (PoS) basados en cadenas. Logra esto imponiendo penalidades a los certificadores que violan las reglas establecidas, garantizando la responsabilidad en la red. Esta solución no solo proporciona una resolución parcial al problema de "nada en juego" mediante penalizaciones a los apostadores, sino que también introduce un mecanismo integral que permite a los usuarios elegir servidores centralizados fuera de la cadena para determinar la legitimidad de una cadena de bloques en medio de múltiples opciones. El sistema de penalizaciones implica un "depósito" bloqueado por un período predefinido, destacando el compromiso de CASPER con la seguridad de la integridad de las actividades de apuestas [19].

Además, las medidas de responsabilidad de CASPER establecen que si se finalizan puntos de control en conflicto (HASH1 y HASH2), como mínimo, un tercio de todos los certificadores deben haber infringido condiciones de penalización, lo que resulta en la pérdida de al menos un tercio del depósito total. Este enfoque único contribuye a la efectividad de CASPER al prevenir actividades maliciosas y garantizar la solidez del consenso PoS dentro del panorama de las criptomonedas [19].

Certificados Dinámicos

En el contexto del algoritmo CASPER, es imperativo que el conjunto de certificadores sea dinámico y pueda experimentar cambios. Esta flexibilidad posibilita la incorporación de nuevos certificadores y la salida de aquellos ya existentes. La capacidad de modificación en el conjunto de certificadores desempeña un papel crucial al fortalecer la resistencia de CASPER frente a ataques conocidos en el ámbito de Prueba de Participación (PoS), como las revisiones a largo plazo y los fallos catastróficos [19].

2.7.3 Tendermint

Tendermint introdujo el concepto de bloqueo, donde la seguridad se garantiza mediante un protocolo de reconciliación modificado basado en la confirmación compartida. En el protocolo de consenso de Tendermint, cada bloque debe estar firmado criptográficamente por certificadores, quienes son usuarios que confirman su interés en la seguridad del

sistema al bloquear sus fondos mediante una transacción de vinculación. El peso de la opinión de cada certificador es proporcional al monto total de fondos bloqueados. Después de desempeñar el papel de certificador, el usuario recupera el acceso a los fondos bloqueados mediante una transacción de desvinculación, sujeta a un período designado conocido como el período de desvinculación. La validez de un bloque depende de que esté firmado por certificadores cuyo peso acumulado constituye al menos dos tercios del total de votos [19].

En consecuencia, la posibilidad de un tenedor en la cadena de bloques surge solo si un subconjunto de certificadores, con al menos un tercio de los votos, firma bloques en ambas cadenas de bloques competidoras. En el caso de certificadores de tenedores, la firma de múltiples bloques puede ser castigada mediante la publicación de una transacción arbitraria con un certificado que contenga evidencia de su intención maliciosa. Esta transacción anula todos los fondos comprometidos de los certificadores que actúan fuera del protocolo, evitando efectivamente los ataques a corto plazo. No obstante, es importante señalar que el sistema sigue siendo susceptible a ataques a largo plazo, ya que los certificadores con una mayoría de dos tercios pueden conspirar y comenzar un tenedor en la cadena de bloques después de desbloquear sus fondos. Para mitigar tales amenazas a largo plazo, se puede implementar un mecanismo para restringir tenedores prolongados en la cadena de bloques, similar al enfoque adoptado por Nxt [19].

2.7.4 Smart Pool

Las agrupaciones de minería, que se basan en un sistema centralizado, permiten que los mineros individuales se unan, combinando recursos para aumentar su potencia informática y dividir las recompensas de manera proporcional. Sin embargo, esta centralización, como se ve en el control ejercido por un pequeño número de agrupaciones sobre la mayoría del poder de hash en Bitcoin y Ethereum, plantea problemas de descentralización y aumenta la vulnerabilidad a ataques DDoS [19].

SMARTPOOL ofrece una solución al proponer un diseño de protocolo descentralizado ejecutado como un contrato inteligente en la red Ethereum. Gestiona reclamaciones de participaciones, las verifica y realiza pagos de manera atómica en una transacción de Ethereum. Este enfoque descentralizado elimina la necesidad de un operador central, protegiendo a los participantes contra ataques y asegurando una recompensa justa basada en la proporción de sus contribuciones [19].

2.7.5 Prevención de ataques DoS/DDoS y SPAM

Las amenazas más significativas para los sistemas centralizados continúan siendo los ataques de denegación de servicio (DoS/DDoS) y el spam. Sin embargo, los sistemas descentralizados también están expuestos a tales ataques, por lo que ambos requieren soluciones. En términos de políticas de seguridad, si se detecta un ataque de DoS o DDoS, es esencial registrar la incidencia para futuras auditorías. Diversos servicios no vinculados a la seguridad, como la redirección de tráfico a través de canales alternativos y servidores de respaldo, pueden ser empleados para detectar y contrarrestar ataques DDoS. Existen diversas estrategias preventivas y reactivas contra estos ataques, incluyendo el uso de computadoras seguras y sistemas de alerta temprana basados en análisis de tráfico cualitativo o cuantitativo. Las detecciones basadas en anomalías se han vuelto populares, comparando parámetros del tráfico observado con el tráfico normal [19].

Aunque las redes blockchain demuestran una sólida resistencia a los ataques DDoS, no son inmunes. La descentralización inherente a cada nodo distribuido dificulta que los hackers ataquen eficientemente toda la red. Sin embargo, para combatir eficazmente estos ataques, los usuarios deben informar rápidamente a los servicios de seguridad sobre el tipo y características del ataque. Ajustar el sistema puede ayudar, pero determinar si un ataque proviene de un programador malintencionado o de interferencia no autorizada es complicado. Bitcoin cuenta con ciertas protecciones contra ataques DDoS, pero sigue siendo vulnerable a ataques más sofisticados. Algunas versiones del protocolo de Bitcoin incluyen reglas para defenderse de ataques de DoS. Además, se han propuesto nuevas técnicas para detectar transacciones DDoS/DoS o SPAM en entornos anónimos. Estas medidas incluyen estrategias reactivas como diseños basados en tarifas y edad, destinados a optimizar el tamaño del mempool y contrarrestar los efectos de los ataques DDoS [19].

2.7.6 Tecnología de gas

Ethereum implementa el mecanismo de gas para asegurar que cada operación en los contratos inteligentes ejecutados en la Máquina Virtual Ethereum (EVM) eventualmente se detenga, así como para difundir y confirmar transacciones en la red. El protocolo de Ethereum cobra una tarifa por cada paso computacional en una transacción. Cada transacción debe incluir un límite de gas y una tarifa de gas que el minero está dispuesto a aceptar; los mineros tienen la opción de incluir la transacción. El precio del gas por transacción o contrato se establece para manejar la naturaleza Turing completa de Ethereum y su código EVM, evitando bucles infinitos. Si no hay suficiente Ether en la cuenta para realizar la transacción o mensaje, se considera inválida. El propósito es prevenir

ataques de denegación de servicio (DoS) por bucles infinitos, fomentar la eficiencia en el código y hacer que un atacante pague por los recursos que utiliza, incluyendo la computación, el ancho de banda y el almacenamiento. Sin embargo, establecer incorrectamente los costos de gas de las operaciones de EVM permite a los atacantes lanzar ataques DoS en Ethereum [19].

Por otro lado, configurar correctamente el costo de gas de cada operación es difícil, ya que requiere una comprensión profunda de los detalles internos de la EVM, así como una medición precisa del consumo de recursos por parte de las operaciones de la EVM en diferentes tipos de recursos informáticos. Como se mencionó anteriormente, en 2016 se identificaron dos ataques DoS que explotaron operaciones subvaluadas, ejecutando repetidamente dos operaciones, EXTCODESIZE y SUICIDE, lo que resultó en un procesamiento lento de transacciones, espacio en disco duro desperdiciado y largos tiempos de sincronización. Por lo tanto, los atacantes pueden lanzar ataques DoS en Ethereum a bajo costo mediante la explotación de operaciones subvaluadas [19].

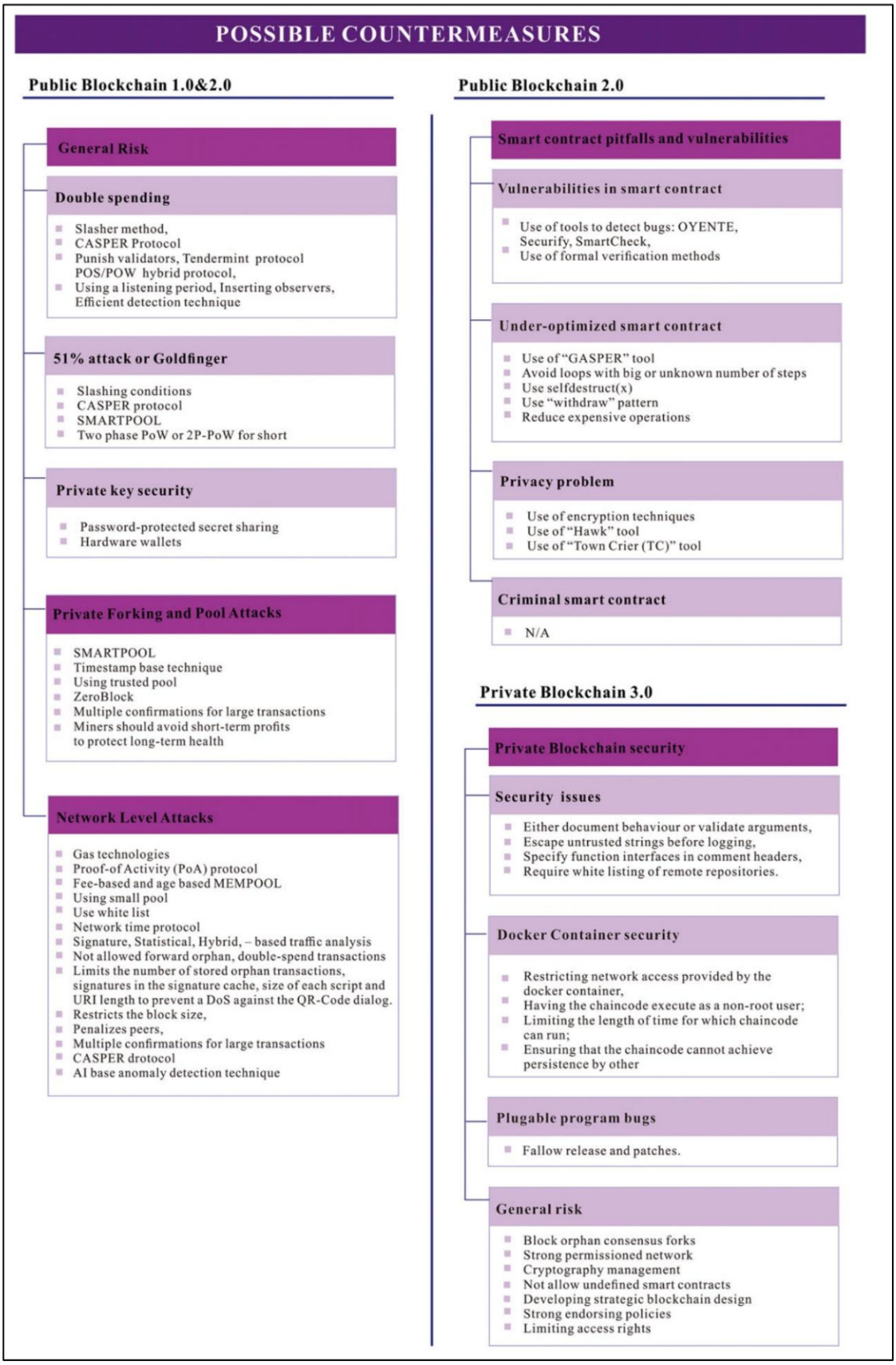

Figura 2.7. Posibles contramedidas para las vulnerabilidades [19]

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

En el presente apartado, se expondrán los resultados discernidos de la investigación enfocada en la aplicación de la tecnología blockchain en el contexto de la ciberseguridad. Bajo un riguroso análisis, se abordarán detalladamente los descubrimientos, delineando tanto los aspectos positivos como negativos identificados. A través de la interpretación de los resultados, se derivarán conclusiones fundamentales que arrojarán luz sobre la eficacia y la influencia de la implementación de blockchain en la seguridad cibernética. Asimismo, se presentarán recomendaciones concretas, fundamentadas en las lecciones extraídas, con el propósito de ofrecer orientación práctica para aquellos profesionales interesados en optimizar esta vanguardista integración tecnológica para proteger activos digitales y mitigar riesgos cibernéticos. Este apartado se erige como la culminación reflexiva y orientadora de la investigación documental, consolidando el acervo de conocimientos en la convergencia entre blockchain y ciberseguridad.

3.1 Resultados

La revisión exhaustiva de la literatura reveló soluciones avanzadas para abordar amenazas de seguridad y fortalecer la protección de la privacidad en entornos blockchain. A continuación, se presentan detalladamente los resultados obtenidos, destacando algoritmos clave y sus características, así como las ventajas y desventajas asociadas al uso de blockchain en ciberseguridad.

La **tabla 3.1** compara distintos algoritmos de consenso que fusionan elementos de Prueba de Trabajo (PoW) y Prueba de Participación (PoS). Estos algoritmos, como Slasher, Protocolo Casper, Tendermint y Smart Pool, han demostrado eficacia en la garantía de seguridad y resistencia frente a amenazas específicas.

Tabla 3.1. Comparación de Algoritmos de Consenso.

Algoritmo	Tipo	Características clave	Ventajas	Desventajas
Slasher	PoW/PoS	Integración de PoW y PoS, previene bifurcaciones.	Seguridad y resistencia a bifurcaciones a corto plazo.	Requiere potencia informática sustancial para PoW.

Protocolo Casper	PoS	Finalidad basada en PoS, responsabilidad.	Resolución parcial al problema de "nada en juego".	Necesidad de supervisar apuestas y generación de fondos.
Tendermint	PoS	Protocolo de bloqueo, certificadores.	Seguridad mediante confirmación compartida.	Vulnerable a ataques a largo plazo.
Smart Pool	Descentralizado	Protocolo descentralizado, ejecutado en Ethereum.	Elimina necesidad de operador central.	Necesita gestión de reclamaciones y verificación.

La **tabla 3.2** constituye una herramienta fundamental para analizar y comprender de manera integral las distintas estrategias diseñadas para contrarrestar los ataques de denegación de servicio distribuido (DDoS) en el entorno específico de blockchain. Este instrumento ofrece una visión detallada y estructurada que permite evaluar las fortalezas y debilidades de cada estrategia, así como su capacidad para adaptarse a las peculiaridades de la tecnología blockchain.

Dicha tabla no solo sirve como un recurso informativo valioso para los profesionales de la ciberseguridad y los desarrolladores de blockchain, sino que también destaca la necesidad de enfoques multifacéticos y estratégicos para abordar una amenaza tan persistente como los ataques DDoS en el contexto de la revolucionaria tecnología blockchain.

Tabla 3.2. Comparación de Estrategias DDoS.

Estrategia	Características Principales	Aplicabilidad en Blockchain y Ciberseguridad
Detección de Anomalías	Emplea análisis de tráfico cualitativo o cuantitativo para identificar patrones anómalos.	Efectiva en entornos descentralizados; complica la coordinación de ataques.
Redirección de Tráfico	Desvía el tráfico a través de canales alternativos y servidores de respaldo.	Puede mitigar ataques, pero la descentralización dificulta la implementación.

Servicios de Respuesta	Implementa servicios no vinculados a la seguridad para contrarrestar ataques DDoS.	Requiere coordinación eficiente y rápida notificación de los usuarios ante ataques.
Alerta Temprana	Utiliza sistemas de alerta basados en análisis de tráfico para detectar indicios de ataques.	Necesita una infraestructura robusta y respuestas rápidas para ser eficaz.
Resiliencia Descentralizada	Aprovecha la descentralización para dificultar ataques eficientes a toda la red.	Brinda protección, pero la coordinación precisa es esencial para una defensa sólida.

Por otro lado, se pudo abstraer la **tabla 3.3**, la misma que se presenta como un recurso esencial para resaltar los aspectos clave relacionados con la triada de la ciberseguridad, específicamente en términos de Confidencialidad, Integridad y Disponibilidad, en el marco de la implementación de tecnologías blockchain. Cada uno de estos elementos es evaluado detenidamente para obtener una comprensión exhaustiva de cómo la tecnología blockchain aborda y contribuye a la robustez de estos pilares fundamentales de la ciberseguridad.

Tabla 3.3. Evaluación de la Triada de Ciberseguridad en Relación con Blockchain.

Aspecto	Descripción	Confidencialidad	Integridad	Disponibilidad
Consenso Distribuido	Proceso de validación descentralizado que asegura acuerdos en la red.	Alta	Alta	Alta
Criptografía de Clave Pública	Uso de claves para firmar transacciones y garantizar la identidad.	Alta	Alta	Media
Inmutabilidad de la Cadena	Imposibilidad de modificar	Alta	Alta	Alta

	bloques antiguos.			
Privacidad Selectiva	Capacidad de controlar el acceso a la información.	Media	Alta	Media
Resistencia a Ataques	Seguridad ante amenazas comunes y ataques maliciosos.	Alta	Alta	Alta
Disponibilidad Continua	Mantenimiento de la operatividad incluso en escenarios adversos.	Alta	Alta	Alta

La salvaguarda contra ataques cibernéticos se posiciona como una prioridad crucial en la actualidad digital, y la tecnología blockchain emerge como una herramienta valiosa en este campo. Es por eso que, del análisis realizado, se extrae la **tabla 3.4**, la misma que sintetiza la contribución de blockchain en la prevención de ataques, resaltando sus ventajas en detección temprana, resistencia a DDoS, fortaleza en el consenso y mejora en la transparencia y responsabilidad. Estos elementos combinados refuerzan la postura de seguridad cibernética, representando un progreso significativo en la defensa contra amenazas digitales.

Tabla 3.4. Impacto de la Tecnología Blockchain en la Prevención de Ataques Cibernéticos.

Aspecto	**Contribución de Blockchain**	**Beneficios**
Detección de Actividades Maliciosas	Empleo de registros inmutables para rastrear y auditar comportamientos sospechosos.	Posibilita la identificación precoz de actividades maliciosas, permitiendo

		respuestas ágiles y precisas.
Resistencia a Ataques DDoS	Descentralización que complica la focalización de un solo punto de ataque.	Mitiga eficientemente los ataques DDoS al distribuir la carga entre nodos, asegurando la disponibilidad del sistema.
Consenso Robusto	Sistemas de consenso que refuerzan la integridad de la red.	Previene alteraciones no autorizadas en la cadena de bloques, resguardando la integridad de la información.
Transparencia y Responsabilidad	Registros transparentes y responsabilidad mejorada mediante contratos inteligentes.	Mejora la confianza al proporcionar una visión completa de las transacciones y la responsabilidad de las partes involucradas.

En la culminación de los resultados obtenidos, se presenta una evaluación exhaustiva de las ventajas y desventajas asociadas con la aplicación de la tecnología blockchain en el ámbito de la ciberseguridad. Este análisis ofrece una visión equilibrada de los aspectos positivos y desafíos inherentes a la integración de blockchain en entornos cibernéticos.

3.1.1 Ventajas

- **Consensos Distribuidos**: La implementación de consensos distribuidos en blockchain refuerza la seguridad al descentralizar la toma de decisiones y validación de transacciones, aumentando la resistencia ante ataques y añadiendo redundancia a la red.
- **Inmutabilidad de la Cadena**: La característica de inmutabilidad en blockchain asegura la integridad de la información al prevenir la modificación de bloques antiguos, proporcionando un historial confiable y sin alteraciones.
- **Criptografía de Clave Pública**: La utilización de criptografía de clave pública establece un sólido mecanismo de seguridad en blockchain, garantizando la identidad y autenticación de las transacciones mediante claves criptográficas.

- **Privacidad Selectiva**: Implementar privacidad selectiva en blockchain permite un control preciso del acceso a la información, mejorando significativamente la privacidad de los datos.
- **Resistencia a Ataques**: La estructura robusta y la criptografía sólida de la red blockchain la hacen altamente segura contra amenazas comunes, mitigando eficazmente posibles ataques.
- **Disponibilidad Continua**: La descentralización y redundancia en la arquitectura de blockchain garantizan su disponibilidad constante, incluso en situaciones adversas, eliminando puntos únicos de fallo.

3.1.2 Desventajas

- **Eficiencia y Escalabilidad:** Abordar la velocidad de procesamiento y la capacidad de escala, especialmente en redes públicas y con grandes volúmenes de transacciones, plantea desafíos en la implementación de blockchain.
- **Costos de Energía:** Algunos algoritmos de consenso, como Proof of Work (PoW), pueden generar costos ambientales significativos debido al consumo de energía, destacando la necesidad de alternativas más sostenibles.
- **Privacidad Limitada:** Aunque la cadena de bloques ofrece privacidad selectiva, su transparencia intrínseca puede afectar la privacidad en ciertos contextos, subrayando la importancia de soluciones adaptadas a diferentes necesidades de privacidad.
- **Interoperabilidad:** La falta de estándares puede complicar la integración y la interoperabilidad de la cadena de bloques con sistemas existentes, subrayando la necesidad de enfoques estandarizados.
- **Complejidad Técnica:** La implementación y gestión de soluciones basadas en blockchain pueden exigir habilidades técnicas especializadas, lo que destaca la importancia de una preparación técnica adecuada.
- **Regulación y Cumplimiento:** El entorno regulatorio en constante evolución presenta desafíos para la adopción y el cumplimiento normativo de tecnologías blockchain, resaltando la importancia de abordar las preocupaciones normativas.
- **Adopción Inicial:** Superar la resistencia al cambio y lograr una adopción generalizada de la tecnología blockchain puede requerir tiempo, enfatizando la necesidad de estrategias de implementación efectivas y campañas de concientización.

Estas ventajas y desventajas brindan una visión general de los aspectos clave a considerar al evaluar la implementación de tecnologías blockchain en el ámbito de la ciberseguridad.

Cada organización debe sopesar cuidadosamente estos factores según sus necesidades y requisitos específicos.

3.2 Conclusiones

- La adopción de blockchain se consolida como un refugio inquebrantable para datos sensibles en el ciberespacio. Su capacidad para garantizar la integridad, confidencialidad y disponibilidad establece un nuevo estándar de seguridad, desafiando las debilidades de los métodos tradicionales.
- La incursión de blockchain en la autenticación de usuarios no solo erradica los riesgos de suplantación de identidad y fraude, sino que redefine la seguridad en la identificación. La tecnología emerge como un aliado indispensable, estableciendo prácticas seguras y eficaces.
- Blockchain se revela como un contraataque efectivo frente a las amenazas cibernéticas. Su arquitectura resistente y tácticas criptográficas robustas se combinan para contrarrestar actividades maliciosas, incluidos los temidos ataques DDoS, señalando un cambio significativo en la lucha contra la ciberdelincuencia.
- La adopción de blockchain marca una evolución significativa en el panorama de la ciberseguridad. Su capacidad para proporcionar un entorno resistente y transparente redefine la forma en que las organizaciones abordan las amenazas cibernéticas.
- La implementación de blockchain en ciberseguridad revela una dinámica fascinante entre desafíos y oportunidades. Si bien enfrenta obstáculos, como la eficiencia y la escalabilidad, abre nuevas oportunidades para abordar problemas persistentes en seguridad digital.
- Más allá de su impacto técnico, la integración de blockchain en ciberseguridad impulsa una transformación cultural. La confianza descentralizada y la transparencia promovidas por la tecnología están influyendo en las percepciones y prácticas relacionadas con la seguridad.
- La investigación ha proporcionado una comprensión profunda de la intersección entre la ciberseguridad y la tecnología blockchain. Este estudio no solo contribuye a la literatura existente, sino que también destaca la importancia de explorar continuamente nuevas formas de fortalecer la seguridad cibernética mediante enfoques innovadores como la tecnología blockchain. La experiencia adquirida en este proceso de investigación ofrece una base sólida para futuras exploraciones y avances en esta área dinámica y en constante evolución.

3.3 Recomendaciones

- En la implementación de soluciones basadas en blockchain, es aconsejable centrarse en una evaluación constante de la eficiencia y privacidad. La escalabilidad y la salvaguarda de la privacidad son metas continuas, exigiendo una travesía constante de mejora.
- Dada la evolución constante del entorno regulatorio, se recomienda que las organizaciones mantengan flexibilidad y adapten sus estrategias a las regulaciones cambiantes. La conformidad normativa se vuelve esencial en un campo tan dinámico.
- Se recomienda realizar pruebas piloto controladas antes de una implementación completa de soluciones basadas en blockchain. Estas pruebas permitirán evaluar el rendimiento, identificar posibles obstáculos y ajustar la estrategia de seguridad según sea necesario.
- Es recomendable fomentar la colaboración entre expertos en ciberseguridad y profesionales de blockchain. Un enfoque interdisciplinario facilitará una comprensión más completa de las implicaciones de seguridad y promoverá soluciones más robustas.
- Se aconseja a los futuros investigadores que profundicen en estrategias avanzadas de privacidad dentro de las implementaciones blockchain. La creciente preocupación por la protección de datos resalta la necesidad de soluciones que ofrezcan un equilibrio adecuado entre transparencia y privacidad.
- Considerando el rápido avance de la tecnología, se recomienda a los futuros investigadores explorar integraciones de blockchain con tecnologías emergentes como inteligencia artificial e Internet de las cosas. Estas sinergias pueden fortalecer aún más la ciberseguridad.
- Es crucial tener en cuenta los factores humanos y culturales al implementar soluciones blockchain en entornos cibernéticos. La aceptación y comprensión por parte de los usuarios finales son fundamentales para el éxito, y la adaptación a las dinámicas culturales puede influir en la efectividad de las medidas de seguridad.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] Deloitte, «Deloitte,» 17 Marzo 2023. [En línea]. Available: https://www2.deloitte.com/es/es/pages/technology/articles/blockchain-vision-tecnologica.html.

[2] E. Piscini, D. Dalton, L. Kehoe, N. O'Connell y G. Campos, «Deloitte,» 2022. [En línea]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-blockchain-and-cyber-security-lets-discuss.pdf.

[3] R. Sharma, D. Sharma, D. Bhatt y B. Pham, «Fundamental Concepts and Applications of Blockchain Technology,» de *Big Data Analysis for Green Computing: Concepts and Applications*, New York, CRC Press, 2022, pp. 113-131.

[4] J. Mela y E. Cedeño, *Tecnologías Blockchain y sus aplicaciones,* Panamá: Visión Antataura, 2019.

[5] Y. Yuan y F.-Y. Wang, *Blockchain and Cryptocurrencies: Model,,* Tiajin,China: IEEE: transactions on systems,man, and cibernetic, 2018.

[6] X. Xu, I. Weber y M. Staples, *Architecture for Blockchain Applications,* Suiza: Springer, 2019.

[7] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008. [En línea]. Available: https://bitcoin.org/bitcoin.pdf.

[8] Y. Muneer, F. Shatnawi, S. Rawashdeh y W. Mardin, *Blockchain Technology: Characteristics, Security and Privacy; Issues and Solutions,* IEEE/ACS, 2019.

[9] J. Xie, H. Tang, T. Huang, F. R. Yu, Fellow, IEEE, R. Xie, J. Liu y Y. Liu, *A Survey of Blockchain Technology Applied to,* Communications surveys & Tutorials, 2019.

[10] R. Xu, L. Zhang, H. Zhao y Y. Peng, *Design of Network Media's Digital Rights Management Scheme Based on,* Bangkok: IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), 2017.

[11] V. Martínez, L. Hernandez-Álvarez y L. Encinas, *Analysis of the Cryptographic Tools for Blockchain and Bitcoin.,* Madrid: Mathematics, 2020.

[12] M. Gómez, *Seguridad en el enrutamiento utilizando tecnología,* Buenos Aires: Universidad Nacional de la Plata, 2023.

[13] J. Li, T. Liu†, D. Niyato, P. Wang, J. Li y Z. Han, *Contract-based Approach for Security Deposit in Blockchain Networks with Shards,* Atlanta, GA, USA: IEEE International Conference on Blockchain, 2019.

[14] P. Bansal, S. Bassi, R. Panchal y A. Kumar, *Blockchain for Cybersecurity: A Comprehensive Survey,* Gwalior, India: IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)., 2020.

[15] M. Gillespie, L. Ampofo, B. Cheesman, E. Iliadou, A. Issa, S. Osseiran y D. Skleparis, *Mapping Refugee Media Journeys Smartphones and Social Media Networks,* 2016.

[16] E. Piscini, D. David y K. Lory, *Blockchain & Cyber Security. Let's Discuss,* Deloitte, 2017.

[17] L. King, *Bitcoin Hit By 'Massive' DDoS Attack As Tensions Rise,* 2014.

[18] M. Carmuega, A. Gil, J. Ardita, F. Jamardo, S. Peroni y L. Martins, *Servicios de Cyber Risk,* 2018.

[19] H. Hasanova, U. Baek, M.-g. Shin, K. Cho y M. Kim, *A survey on blockchain cybersecurity vulnerabilities and possible countermeasures,* 2019.

[20] J. Golosova y A. Romanovs, *The Advantages and Disadvantages,* Vilnius, 2018.