# CIBERSEGURIDAD Y BLOCKCHAIN [1]

CYBERSECURITY AND BLOCKCHAIN

Por *Santiago GRIGERA DEL CAMPILLO*[2] (*)

**RESUMEN:** En un mundo hiperconectado donde las tecnologías emergentes aún continúan siendo estudiadas, no podemos estar desprevenidos. Así como las personas nos valemos de la tecnología para ser más productivos y eficientes, los ciberdelincuentes están a la orden del día innovando a con ataques cada vez más sofisticados. Blockchain se considera un ecosistema con mucho potencial en materia de ciberseguridad gracias a la tecnología subyacente, pero no es infalible.

**PALABRAS CLAVES:** Blockchain- ciberseguridad- seguridad- confidencialidad- criptografía- hacks- contratos inteligentes- billeteras virtuales- Exchange- criptojacking- ransomware- DAO- ataque del 51%- Ataque Sybil- Ataque eclipse- Internet de las cosas- Bitcoin- Ethereum.

**ABSTRACT:** In a hyper-connected world where emerging technologies are still being studied, we cannot be unprepared. Just as people use technology to be more productive and efficient, cybercriminals are innovating with increasingly sophisticated attacks. Blockchain is considered an ecosystem with a lot of potential in terms of cybersecurity thanks to the underlying technology, but it is not infallible.

**KEY WORDS**: Blockchain- cybersecurity- security- confidentiality- cryptography- hacks- smart contracts- wallets- exchanges- cryptojacking- ransomware- DAO, 51% attack- Sybil attack- Eclipse attack- Internet of things- Bitcoin- Ethereum.

[1] El presente es trabajo presentado se realizó en el marco de la DIPLOMATURA EN TECNOLOGÍA BLOCKCHAIN APLICADA A LOS NEGOCIOS Y LAS RELACIONES, en el año 2019.

[2] Abogado (UNC). Especialista en Derecho Informático (Universidad de Buenos Aires). Profesor en la Diplomatura en Tecnología Blockchain aplicada a los negocios y las relaciones (UCCOR), Profesor en Diplomatura de Derecho Digital: Herramientas teóricas prácticas (Acción Jurídica). Prosecretario de la Sala de Derecho y Tecnología del Colegio de Abogados de Córdoba. Maestrando en Derecho de la Ciberseguridad y entorno digital, Universidad de León, España.



DOI http://doi.org/10.22529/rbia.2021(3)05

## DISCLAIMER

Considerando que se trata de una tecnología en constante evolución, nos encontramos ante un panorama en el que hay mucho para hacer pero su implicancia en la ciberseguridad se aprecia promisoria. Esto no quiere decir que la tecnología sea infalible, como ha sido de público conocimiento, han habido ataques exitosos y siguen ocurriendo a diario diversas estafas que afectan a todo el ecosistema Blockchain.

## I. APROXIMACIONES A LA CIBERSEGURIDAD.

Para empezar es importante decir que cuando hablamos de ciberseguridad, básicamente estamos hablando de medidas necesarias para la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. (ISO 27032/2012).

Otro concepto que define a la ciberseguridad como las acciones tomadas tendientes a proteger los activos de información de las amenazas sobre el estado de la misma ya sea se encuentre procesada, almacenada y transmitida a través de sistemas de información interconectados.

Como venimos sosteniendo a lo largo del curso, el mundo actual transcurre en su mayoría en internet. Trabajamos, estudiamos, recibimos reportes de nuestros gastos, nos relacionamos y hasta pasamos horas viendo series o películas a través de medios tecnológicos conectados.

Estos avances y el hecho que cada vez más dispositivos se conecten a internet implican una proliferación desmedida los datos generados y con ellos, aparecen nuevos vectores de ataque, vulnerabilidades, atacantes con nuevas aptitudes. Al mismo tiempo que avanza el desarrollo tecnológico van sorteando los reparos propios de cada sistema con el fin de obtener grandes ganancias. El cibercrimen se ha convertido en uno de los negocios más rentables a nivel global.

A diario surgen noticias de hackeos millonarios a aerolíneas, bancos, cadenas hoteleras, Gobiernos y particulares. Nadie se encuentra a salvo en la red, ni siquiera los directivos de las multinacionales de empresas tecnológicas, recordemos el hackeo padecido por Jeff Bezos[3], esto demuestra que cualquiera puede ser víctima de un ciberataque.

[3] Recuperado de https://cnnespanol.cnn.com/2020/01/23/el-hackeo-de-telefono-de-jeff-bezos-explicado-esto-es-lo-que-debes-saber-para-tu-propia-seguridad/, Consultado el 25/04/2020.

## II. PRINCIPIOS DE LA CIBERSEGURIDAD

Conforme surge del concepto dado, el objetivo de la ciberseguridad es la protección de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

A grandes rasgos, la confidencialidad, garantiza la protección de la información para que sólo sea accesible por quien se encuentra autorizado. Según el Instituto Nacional de Estándares y Tecnología (NIST), confidencialidad se refiere a "la propiedad de que la información confidencial no se divulgue a personas, entidades o procesos no autorizados".[4] El mismo NIST define la integridad como las medidas para "protegerse en contra de la modificación o destrucción inadecuada de la información, e incluye asegurar el no repudio y autenticidad de la información". La integridad, garantiza que la información sea correcta y no sufra modificaciones. La disponibilidad, para el Instituto mencionado supone "asegurar el acceso y uso oportuno y confiable de la información", garantiza el funcionamiento y acceso por quienes estén autorizados evitando interrupciones.

En la cadena de bloques, se considera que la confidencialidad de los participantes de la red es alta debido a la criptografía de clave pública que autentica a los usuarios y cifra las transacciones. Respecto a la integridad, los bloques cifrados con un hash SHA 256 contienen datos inmutables, resistentes a la modificación no autorizada sobre lo que se indagará a continuación. Sobre la disponibilidad, se considera a la cadena de bloques un sistema resiliente, la información no se encuentra centralizada, además de que el servicio tiene alta disponibilidad desde que al estar distribuido se necesita un apagón global de internet para que dejara de funcionar. Una copia de los datos de las transacciones se encuentra almacenada en los distintos nodos de la red.

Blockchain es una compilación de registros que están protegidos criptográficamente. Los bloques se vinculan entre sí y contienen información de otros bloques, datos de transacciones y sellos de tiempo. Al ser un sistema distribuido aumenta la transparencia lo que permite la trazabilidad de las transacciones -dificultando cualquier tipo de fraude o manipulación arbitraria-. En virtud del algoritmo de consenso resulta de gran dificultad hackear sin contar que además requiere de un gran poder de cómputo que termina siendo más costoso que la eventual ganancia

[4] Recuperado de https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain&%20CiberseguridadESP%20(1).pdf, consultado el 28/03/2020.

pretendida. Los atacantes solo pueden impactar una red si logran obtener el control del 51 por ciento de los nodos de la red. Es por esto que la blockchain se considera prácticamente inmutable e inmanipulable.[5]

Debido a su naturaleza distribuida, las cadenas de bloques no presentan un punto único de falla lo que se traduce en que no hay una entrada fácil para el ciberdelincuente, por lo tanto, brindan más seguridad en comparación con varias estructuras transaccionales actuales basadas en bases de datos centralizadas.

Por todo lo mencionado, se considera que la tecnología blockchain puede potenciar la ciberseguridad.[6]

## III. ALGUNOS ATAQUES OCURRIDOS EN EL MUNDO BLOCKCHAIN.

Como se anticipó, no es un sistema infalible, toda actividad donde intervengan personas en algún punto se hace vulnerable. "Toda cadena es tan fuerte como su eslabón más débil."[7] Como se sabe, el eslabón más débil es el usuario. Las personas por su naturaleza son confiadas, y muchas veces por ignorancia, inexperiencia o inocencia terminan sufriendo todo tipo de estafas. Con esto quiero decir, la tecnología por sí es segura y tiene un gran potencial para serlo aún más. Esto no obsta a que sea infalible desde que al intervenir personas, aplicaciones, valores, es un nicho ideal que atrae delincuentes como todo otro rubro rentable.

Bitcoin a la fecha, es la plataforma más probada en el mercado, que ha resistido con éxito los ataques cibernéticos durante más de 7 años. Esto da una pauta de que mientras más grande es la blockchain más segura es, mientras que las más pequeñas son más vulnerables.[8] El tamaño está dado por la capacidad de cómputo o minería. Se sostiene a la fecha que el costo de consumo de electricidad de minería en bitcoin asciende a USD 300.000 por hora. Ante esto, por el momento los ciberdelincuentes son atraídos por blockchains más chicas o exchanges.

---

[5] Recuperado de https://empresas.blogthinkbig.com/blockchain-y-ciberseguridad-la-descentralizacion-como-solucion/. Consultado el 28/03/20.

[6] Recuperado de https://www.pandasecurity.com/spain/mediacenter/seguridad/blockchain-ciberserguridad/ .Consultado el 25/04/2020.

[7] Sosa Escudero Walter (2019). "big data". 3ra Edición.p. 137. Ciudad Autónoma de Buenos Aires, Argentina. Ed. Siglo XXI Editores.

[8] Recuperado de https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Blockchain&%20CiberseguridadESP%20(1).pdf. Consultado el 26/04/2020.

Las herramientas de terceros en el marco de los *Smart Contracts* son por lo general un objetivo más fácil porque cuentan con comunidades más pequeñas y menos recursos para proteger su código y responder a los problemas. En relación con el empleo generalizado de *smart contracts* para llevar a cabo transacciones, éstos se ven expuestos a los errores y vulnerabilidades derivados de su codificación y de los de la plataforma de cadena de datos en la que se ejecutan.[9] En el ecosistema crypto, afloran las startups y muchas de ellas dejan de lado la implementación de seguridad informática por los costos y deriva en errores que con frecuencia, les cuesta el emprendimiento.

Los ciberdelincuentes ya han dirigido sus ataques a muchas implementaciones de blockchain a través de la ingeniería social, el malware y los exploits. Esto quiere decir que es común que utilicen maniobras antiguas para insertarse y generar un impacto en blockchain. Otros mecanismos fraudulentos, para hacerse de credenciales a las wallets y cuentas de exchanges son phishing, inserción de Malware como el ransomware y criptojacking. Un ejemplo de ataque con la modalidad del phishing fue la sufrida por la criptomoneda IOTA, donde las víctimas perdieron 4 millones de USD. El atacante había registrado un sitio web para el monedero y se ganó la confianza de los usuarios durante 6 meses en los que iban generando y gestionando sus transacciones hasta que un día lo vació. Un caso conocido por inserción de malware es por ejemplo el caso sufrido por Coincheck, en enero de 2018. Un exchange Japonés, perdió 532 millones de dólares en monedas NEM, afectando a 260.000 inversores. El hacker había conseguido acceso al ordenador de un empleado y había instalado malware diseñado para robar claves privadas de monederos digitales.[10] El criptojacking es una actividad maliciosa, en la que un dispositivo infectado se utiliza para minar criptomonedas en secreto. Para hacerlo, el atacante hace uso del poder de procesamiento y el ancho de banda de las víctimas. [11] En mayo de 2019, la plataforma Binance sufrió el robo de 41 millones de dólares en bitcoins. Los hackers utilizaron varias técnicas, desde virus hasta phishing, para acceder en el sistema y a la cartera de bitcoins de la compañía desde la que sus clientes realizaban las transacciones.

[9] Recuperado de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari106-2019-alonsolecuit-seguridad-y-privacidad-del-blockchain-mas-alla-de-tecnologia-y-criptomoneda. Consultado el 26/04/2020.

[10] Recuperado de https://www.mcafee.com/enterprise/es-es/assets/reports/rp-blockchain-security-risks.pdf. Consultado el 26/04/2020

[11] Recuperado de https://www.binance.vision/es/security/what-is-cryptojackin. Consultado el 26/04/2020.

Uno de los ataques más resonantes en el mundo Ethereum fue el de "The DAO".[12] Se trataba de un programa informático que de manera autónoma realizaría inversiones financieras. El 17 de junio de 2016, el DAO fue objeto de un ataque que explotaba una combinación de vulnerabilidades. Este llevó a que se dividiera la blockchain en Ethereum y Ethereum Classic.

Otra modalidad de ataque a las cadenas de bloques es el llamado ataque del 51% ocurre cuando se logra tener control sobre más de la mitad del poder de cómputo y no sólo ralentiza las transacciones, sino que tiene la potencialidad de generar un doble gasto de recursos.[13] Se registró un ataque de este tipo en la blockchain de Ethereum Classic en Enero del 2019.[14]

En cuanto a los ataques que pueden darse exclusivamente en el ecosistema blockchain se pueden mencionar aparte de los ya nombrados ataques a los Smart contracts y el ataque del 51%, están los denominados ataques eclipse y Sybil.[15]

Respecto del primero el atacante "eclipsa" la red Peer-to-Peer de la criptomoneda con una red maliciosa y se queda con el control de un usuario de la red interfiriendo en sus comunicaciones entrantes y salientes de la red. Esto posibilita enviar dinero de las transacciones a una billetera virtual propia o ajena, permitiendo un doble gasto y que la víctima tenga una percepción distorsionada de la cadena de bloques.

El ataque Sybil, consiste en regar la red con nodos maliciosos para contaminar el sistema con usuarios que trabajan en grupo permitiendo una gran influencia para modificar información almacenada controlando las transacciones.

## IV. ALGUNAS RECOMENDACIONES DE CIBERSEGURIDAD EN EL ECOSISTEMA BLOCKCHAIN

Como se sostuvo a lo largo del presente trabajo, es complejo atentar contra la tecnología blockchain, pero ello no implica que no existan algunas vulnerabilidades. No obstante, los mayores riesgos no se encuentran en la tecnología subyacente sino en las aplicaciones que interactúan con ella.

[12] Recuperado de https://www.coindesk.com/understanding-dao-hack-journalists. Consultado el 26/04/2020
[13] Recuperado de https://www.binance.vision/es/security/what-is-a-51-percent-attack, consultado el 26/04/2020.
[14] Recuperado de https://www.bitcoin.com.mx/ethereum-classic-sufre-ataque-del-51-roban-1-1-millones-de-usd/. Consultado el 26/04/2020.
[15]Recuperado de https://medium.com/chainrift-research/bitcoins-attack-vectors-sybil-eclipse-attacks-d1b6679963e5 consultado el 26/04/2020.

Vincent Romney, especialista en Ciberseguridad y CEO de SK2Tech[16], afirma que "los ciberdelincuentes no van a atacar la cadena de bloques sino los procesos de *onboarding/offboarding* de información, aquí es donde se encuentran sus vulnerabilidades". Esto resalta que la gran mayoría de los ataques hayan sido dirigidos a las personas mediante ataques conocidos como de ingeniería social, para acceder a sus claves privadas como también a las wallets, exchanges y aplicaciones de contratos inteligentes.

Algunas recomendaciones que cualquier persona tiene que tener en cuenta en su interacción con entornos digitales pueden ser:

1) Utilizar contraseñas robustas, en lo posible frases mezcladas con símbolos y que no tengan que ver con aspectos de la vida personal.

2) Implementar la verificación de 2 pasos en las plataformas, perfiles y programas que se utilicen.

3) Utilizar Discos duros y pendrives encriptados.

4) Utilizar redes privadas virtuales.

5) Utilizar sistemas operativos actualizados con antivirus y firewalls.

6) Realizar copias de seguridad con frecuencia en distintos soportes. Mientras más, mejor.

7) Utilizar sentido común.

8) No almacenar crypto en wallets calientes o exchanges, en lo posible utilizar dispositivos de almacenamiento en frío.

Por supuesto que la lista de recomendaciones enunciada no debe ser considerada taxativa pero al menos es un buen comienzo respetar esas pautas.

## V. DESAFÍOS DE LA CIBERSEGURIDAD EN BLOCKCHAIN.

Considerando que la tecnología se encuentra en sus primeros estadíos, dentro de los desafíos que se presentan podemos identificar la falta de madurez y consenso técnico que facilite la convergencia de estándares en materia de ciberseguridad. Ante esto, es un buen inicio considerar el principio de privacidad y seguridad desde el diseño y por defecto para todos los proyectos que pretendan interactuar con blockchain.

En segundo lugar, el hecho que la tecnología se considera de código abierto muchos ciberdelincuentes hace tiempo pueden estudiar analizar vulnerabilidades inherentes al código

[16] Recuperado de https://www.sk2tech.com/

para atacar distintas estructuras, sobretodo, como se sostuvo, las más inmaduras y con menor presupuesto.

En tercer lugar, la posibilidad de computación cuántica se considera que puede ser un riesgo para el futuro en lo referente a la integridad y desarrollos de blockchain, que evidentemente podrían traer consigo no sólo manipulaciones en los distintos algoritmos de consensos sino también descifrar la criptografía del presente.

Otra preocupación que supone al ecosistema es la interoperabilidad de plataformas y aplicaciones. Si bien a medida que se van desarrollando nuevos proyectos van contemplando la posibilidad de adaptarse a las plataformas que se encuentran en el mercado, la complejidad de las matemáticas subyacentes resultan incompatibles.

Por último, sin perjuicio de la existencia de otros desafíos, la práctica de ingeniería social es cada vez más sofisticada convirtiéndose en la vulnerabilidad más importante e inevitable. Por lo tanto, todo interesado en el mundo blockchain debe estar atento a las novedades, capacitarse y ser cuidadoso.

## VI. REFLEXIÓN FINAL.

Podemos reconocer que la tecnología no es infalible sobre todo, por las aplicaciones que se acoplan a la cadena de bloques y las personas. Además, si uno no toma los recaudos mínimos puede ser víctima fácilmente de un ciberataque, sobretodo, en lo que hace al tema de la gestión de las claves, interacción con exchanges y wallets. Es importante informarse antes de realizar cualquier transacción y tratar de no dejar las criptomonedas en los exchanges. Sirve el consejo de utilizar los almacenamientos en frío para estos efectos y no los que proveen los sitios web.

Blockchain, como tecnología en general ayuda a prevenir los ciberataques, las filtraciones de datos, el robo de identidad, entre otras cosas pero como toda actividad en la que intervienen las personas no está exenta de estafas y peligros. Algunos optimistas ven que en blockchain sea factible en un futuro cercano monitorear y predecir ataques con inteligencia artificial y brindar una respuesta proactiva a los ciberataques.

Es un gran avance en la ciberseguridad, ya que puede garantizar el más alto nivel de confidencialidad, disponibilidad y seguridad de los datos. Técnicamente ha sido diseñada para prevenir el fraude y no es sencilla la manipulación de los datos, por que utiliza técnicas de encriptación que los hace transparentes y auditables.

Sin perjuicio de ello, no todo emprendimiento o negocio es viable con esta tecnología por lo tanto, se recomienda efectuar una evaluación de riesgos de implementación abordada de manera multidisciplinaria.

A futuro, expertos consideran que puede servir para mejorar la seguridad de los dispositivos conectados a internet a gran escala (IOT).

Aunque algunas de las capacidades subyacentes de blockchain proporcionan confidencialidad, integridad y disponibilidad de datos, al igual que otros sistemas, es necesario adoptar controles y estándares de seguridad cibernética para las organizaciones que usan blockchain dentro de su infraestructura técnica para proteger a sus organizaciones de ataques externos. Desde una visión realista, aunque hay numerosas investigaciones sobre la tecnología de la cadena de bloques, hay respuestas en relación a la confianza que proporciona la descentralización, aunque no se garantiza todavía la seguridad de los usuarios o las aplicaciones que se conectan a su red.[17]

[17] Recuperado de https://www.mcafee.com/enterprise/es-es/assets/reports/rp-blockchain-security-risks.pdf. Consultado el 26/04/2020