https://repository.uaeh.edu.mx/revistas/index.php/tepexi/issue/archive

TEPEXI Boletín Científico de la Escuela Superior Tepeji del Río

Publicación semestral, Vol. 9, No. 18 (2022) 15-20

Tepexi

ISSN: 2007-7629

Blockchain y la ciberseguridad

Blockchain and cybersecurity

Mónica García-Munguía [a], Silvia S. Moreno-Gutiérrez [b], Héctor D. Molina-Ruiz [c], José L. Alvarado-Reséndiz [d]

Abstract:

The world is interconnected, the pandemic advanced at least 7 years of interconnectivity in Mexico and the world is becoming one, this pandemic allowed people to be connected with people from other countries, cities, states, without the need to leave their place of residence, this excess connectivity creates something known as a cyber society. The purpose of this document is to analyse, based on technological criteria, the impact of Blockchain technology in the area of cybersecurity and how said dynamics could have direct effects on data protection. Blockchain technology will be discussed to protect the cyber society where new criminals arise, but with different profiles, finally, the proposals on its application in the field of computer security will be analysed where Blockchain becomes an option to ensure any type of digital information and that its use by cybercriminals becomes inoperable and unaffordable.

Keywords:

Blockchain, cybersecurity, digital information.

Resumen:

El mundo está interconectado, la pandemia adelantó al menos 7 años de interconectividad en México y el mundo se está volviendo uno, esta pandemia permitió que las personas estén conectadas con personas de otros países, ciudades, estados, sin necesidad de salir de su lugar de residencia, este exceso de conectividad crea algo conocido como una sociedad cibernética. El objeto de este documento es analizar, en base a criterios tecnológicos, el impacto de la tecnología Blockchain en el ámbito de la ciberseguridad y cómo dicha dinámica podría tener efectos directos en la protección de datos. Se hablará de la tecnología Blockchain para proteger a la ciber sociedad donde surgen nuevos delincuentes, pero con diferentes perfiles, finalmente se analizarán las propuestas sobre su aplicación en el campo de la seguridad informática donde Blockchain se convierte en una opción para asegurar cualquier tipo de información digital y que su uso por parte de los ciberdelincuentes se vuelve inoperable e inaccesible.

Palabras Clave:

Blockchain, ciberseguridad, información digital.

Introducción

El presente trabajo expone el uso de la aplicación de la tecnología Blockchain (cadena de bloques) en la seguridad informática y surgió como un mecanismo por medio del cual se busca el intercambio de información y la estructuración de procesos a través de mecanismos descentralizados con nodos de información interconectados y justificados en esquemas criptográficos [1].

Así también contextualizando, hoy en día se manejan muchos y grandes capitales, el dinero es una cuenta que está en una página web donde el usuario observa las transacciones y movimientos, el dinero físico tiende a desaparecer a nivel mundial en los próximos años, lo que se estima es que todo se dé a través de dinero virtual y se da por muchas condicionantes, por ejemplo es más fácil controlar los flujos de dinero para cuestiones fiscales o cobrar los impuestos ya que se reflejan las transacciones de la banca de manera inmediata en

[a] Autor de Correspondencia, Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-0507-3933, Email: monicagm@uaeh.edu.mx

[b] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-8957-3707, Email: silviam@uaeh.edu.mx.

[c] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0003-4657-3237, Email: hmolina@uaeh.edu.mx

[d] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0003-1473-7727 Email: jose_alvarado4225@uaeh.edu.mx

Fecha de recepción: 10/02/2022, Fecha de aceptación:15/03/2022, Fecha de publicación: 05/07/2022

tiempo real. En una búsqueda con Google resalta que se obtienen más de 11 000 000 referencias sobre criptomonedas y más de 238 000 000 sobre Blockchain, siendo está la principal tecnología que las soporta [2].

Tecnología Blockchain y su alcance

Una de las ventajas de la tecnología Blockchain es que permite que los procesos sean más ágiles, seguros, transparentes y que se realicen con una significativa reducción de costos en relación con procesos centralizados de información. La tecnología Blockchain representa hoy en día una revolución en el mundo entero por el posible impacto que puede traer en sectores tales como administración de justicia, salud, educación, servicios notariales, procesos de supervisión por parte de órganos de control, auditorías, ejecución de contratos, monedas virtuales, mercados financieros, funcionamiento de empresas y de entidades estatales, entre otros. [3]

El uso del dinero digital en el ciber mundo atrae también a que surjan personas para delinquir en la red, los delitos no terminan, solo se adaptan a las nuevas circunstancias; el ciberdelincuente cambia su perfil, en el mundo convencional, el delincuente es una persona con cierto nivel de valor para usar un arma, para someter a sus víctimas; ese valor se traduce en exhibir mucho el dinero, por ejemplo los narcotraficantes se vuelven visibles y por lo tanto se necesitan policías con esos mismos perfiles.

Por tanto, en ciberseguridad o ciberdelitos el perfil de un delincuente es diferente en el mundo real ya que suele ser mucho más joven, se ha evidenciado que la edad ha bajado mucho [4], a diferencia del tradicional que casi nunca son personas preparadas para realizar actos de delincuencia, el ciberdelincuente si lo es, y no necesariamente tiene estudios universitarios, si no que al menos es autodidacta fortaleciéndose en ciertos temas, son personas cuidadosas que saben esconder su rastro convirtiéndose en anónimos gracias a la estructura de la tecnología, por ejemplo en una denuncia penal con todos los elementos en la mano, se podría llegar a la computadora donde se realizó el delito pero no así saber quién la uso, nunca se va a poder conocer quien estuvo detrás de un equipo y quien realizo el delito, en una causa penal se señalan a las personas que se presume son los culpables y se va contra esa persona, pero si no se tiene a alguien identificado no se tiene nada, todo se cae y los ciberdelincuentes lo saben aprovechándose de eso, de que esta el mundo interconectado y que en algunos países la tecnología no es la más actual ni tampoco cuentan con la cultura de ciberseguridad.

Por tanto, el perfil de experto en ciberseguridad se vuelve importante, ya que se tiene que perseguir a ciertos personajes que tiene además otras características como la accesibilidad y ubicuidad -particularidad relativa a la localización del ilícito-, haciendo su persecución más compleja siendo la característica fundamental del modus operandi el anonimato, que se presume en el sujeto activo, pues es más fácil que dicho agente pase inadvertido, por lo que es importante tener un equipo robusto de seguridad que ayude a blindar y a proteger datos de los sistemas [5].

Considerando que hoy por hoy existen tecnologías para la seguridad como antivirus, hardware, firewall, pero no van a garantizar al 100% la seguridad de la empresa, por ejemplo muchos apuestan tener una red privada virtual (VPN) combinada con estas herramientas, pero no se puede afirmar que se está protegido, de manera particular, los Ransomware sí pueden entrar a los sistemas debido a cómo opera, logra pasar los firewalls, red privada virtual (VPN) y antivirus, por ser archivos de texto que se introducen en los equipos anclándose en diferentes rutas y en algún momento enviarán un email con archivos adjuntos o enlaces trampa de supuestas instituciones de confianza, el delincuente va a un paso delante de los avances tecnológicos y es aquí donde aparece el Blockchain [6].

Originalmente esta tecnología es usada en el uso de las criptomonedas y no está pensada como herramienta de ciberseguridad, sin embargo, sí tiene aplicaciones de ciberseguridad y se empiezan a explotar al ser una tecnología nueva. El primer caso que estuvo en la red fue en el 2008, inició con 2 proyectos, uno para descarga de música y otro que fue la base del Blockchain, el proyecto del astrónomo Carl Sagan denominado Communication with extraterrestrial intelligence (CETI) y su investigación en astronomía.

Elementos del Blockchain

Al hablar de Blockchain se necesita tener presente dos aspectos vinculados; criptomonedas y criptografía.
Bitcoin, la más famosa de las criptomonedas, solo existe en el ciberespacio y se asocia a redes de computadoras punto a punto (peer to peer o P2P) [2], y su uso más común es para adquirir productos y servicios como cualquier otra moneda y no tiene nada que ver con ciberseguridad solo con cuestiones bursátiles, a diferencia de la criptografía que sí está altamente relacionada.
Para que Blockchain ayude a proteger información digital se tiene que trabajar en cumplir con tres características importantes:
Por una parte, está la confidencial que significa que la información no va a salir más allá del grupo que estrictamente está obligado a conocer la información, no debe haber filtros de información por lo que se debe

utilizar la encriptación, aunque existen técnicas de desencriptación que logran desencriptar sin la contraseña, y como ejemplo está el *Ransomware* y aquí los expertos de ciberseguridad deberán desencriptar generando a través de algoritmos matemáticos.

La siguiente es la integridad, cuando la información debe estar completa y sin modificación, por ejemplo, un contrato, su contenido no debe de ser manipulado o alterado.

Por último, el reconocimiento, es la trazabilidad y origen de la información, en el ciber mundo no hay mucha legislación aún, pero se busca erradicar el fraude y robo de información en todos los países.

En conjunto, estos tres elementos son muy evidentes cuando se habla de criptomonedas por eso la relación con Blockchain ya que la cripto tiene que ser confidencial y solo debe conocerse entre las carteras denominadas también *wallets.*

Su contenido debe de ser integro y tener un reconocimiento de quién es el dueño de la cripto, de lo contrario se van a asumir que se cuenta con dos bitcoins iguales y no se sabrá quien en realidad es el dueño y todo el sistema de dinero en línea se corrompe ya que cada bitcoin tiene el reconocimiento de ser único e integro siendo uno de los grandes logros de la criptomoneda mencionada.

Por lo anterior, al momento en que se realiza la transferencia de un bitcoin, el usuario que la envía pierda esa cantidad, y no la conserva en su billetera, por eso no se puede duplicar o falsificar, porque tiene esta parte de contar con una clave única que va a mantener el nivel de cifrado [7].

Por consiguiente, el bitcoin pone a prueba la estructura del Blockchain, así como su potencia, siendo entonces el reto a proteger los datos que valen más que el dinero y por lo tanto se debe asegurar que estén disponibles, protegidos y visibles, para poder tomar decisiones de manera rápida.

Entre las herramientas que existen, Blockchain empieza a mostrar robustez, que vale la pena empezar a migrar en la parte de protección de datos y por consiguiente se debe tener presente conceptos como firma digital que permite al usuario validar y autenticar su contenido digital, formada por una cadena alfanumérica que se genera de varios métodos, los bancos usan decodificador del usuario, decodificador de inicio de sesión y de los números dinámicos del token construyendo así la firma electrónica, el Servicio de Administración Tributaria (SAT) lo hace con dos archivos, el key y cer creando la cadena que permite incorporar las garantías básicas de seguridad de: autenticidad, confidencialidad, integridad y no repudio, además, identifica (con una llave criptográfica) a una persona autora y emisora (certificada) de un documento informático [8].

Entonces, para que algo funcione a través de Blockchain se debe firmar digitalmente ya que la firma encripta los datos, la ley ya establece como hacer una firma digital, normalmente para encriptar y desencriptar se relaciona el termino de llave publica, y llave privada.

Otro concepto son las funciones hash criptográficas que permiten crear identificadores únicos para contenido digital.

Las funciones hash son parte fundamental en aplicaciones relacionadas con seguridad informática, como los sistemas de autenticación y las firmas digitales [9].

La función hash es la huella digital de un archivo digital, que va a tomar todos los bits de cualquier archivo (texto, película, imagen) y los convierte a una cadena de tamaño fijo, depende de la función que se trabaje será el tamaño del hash, toda la información la convierte en una cadena alfanumérica que puede ser de 32 bits generando un valor único.

Por lo que sí al archivo que se le aplicó la función hash se llegará a modificar tan solo con un carácter, como por ejemplo una coma (,) de más o menos la función hash cambiará, por lo que entonces los hashes tienen 5 características que son:

1) Determinista, siempre va a tener el mismo valor, sí se tiene el mismo archivo sin modificación el hash será siempre el mismo y suele ser importante para hacer cotejos de documentos, sí se sospecha de la modificación de alguno de los dos, deberán obtener su hash para cotejarlos, si fuera diferente los hashes, un documento fue alterado, por lo que resulta ser muy útil en contratos digitales o evidencia para entregar a los peritos.

2) Fácil y rápido, ya que no se necesita tanta potencia de cómputo; hasta con un celular se puede calcular.

3) Si se cuenta con un documento al cual se obtiene su hash, no hay un método para poder decodificarla en el documento original, ya que es un algoritmo de una sola vía, garantiza que no se pueden reconstruir a partir del hash y con ello se garantiza la confidencialidad.

4) Si se modifica el archivo se obtendrá otro valor hash por mínima que sea la modificación y eso da integridad siendo casi imposible tener 2 valores iguales de la función.

5) Es casi imposible encontrar dos mensajes diferentes con el mismo valor de hash.

Una vez que se posee la firma electrónica y el hash se está en la posibilidad de crear Blockchain, por consiguiente, si se cuenta con cualquier tipo de información, por ejemplo, proteger la identidad de los usuarios como su categoría, contraseña, georreferencia de su protocolo de internet (IP), entre otros datos

sensibles, sí se aplica Blockchain estarán referenciados por su hash recordando que Blockchain es una cadena de bloques, por lo que cada bloque tendrá un hash, a diferencia de una seguridad tradicional, estos datos están altamente vulnerables porque podrían ser víctimas de robo o hackeo, como sucedió en el 2021 donde los ciberataques incrementaron 151% [10].

Blockchain y Ciberseguridad

Teniendo esta estructura de Blockchain desde una lógica de ciberseguridad, un atacante debe de considerar algunos aspectos que están en detalle en la figura 1:
Primero, sí un atacante modifica el bloque N2 ya no van a corresponder los hashes con el bloque N1 porque están vinculados, por lo que N1 ya no reconoce a N2; para que el hacker pase desapercibido tendrá que modificar al bloque N1 pero tampoco ya no va a reconocer el bloque N, como se observa en la figura 1.

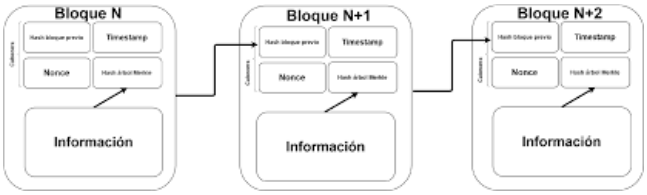

Figura 1. *Estructura de los bloques de Blockchain de bitcoin*

Fuente: Retamal, C. D., Roig, J. B. and Tapia, J. L. M. (2017) [11].

Al final el hacker tendrá que alterar todos los apuntadores de la cadena hasta llegar al final, por lo tanto, si se cuenta con toda la información en bloques vinculados a través de un hash, no significa que no se pueda hackear; como se mencionó anteriormente, Blockchain puede ser hackeable pero solo sí logran entrar a la red y obtienen un bloque, esté solo será un pequeño fragmento de la información que por sí misma no tiene ningún valor o significado y que no les servirá de nada.
En pocas palabras, para tener información útil se tendrá que hackear todo el Blockchain, pero para hackaer un bloque se necesitará hacer la intrusión a toda la cadena, por lo que se tendrá que realizar N intentos de hackeo, si se tienen 10 mil bloques, 10 mil intentos se tendrán que hacer y con uno que no salga bien todo lo demás es basura para el delincuente.
En realidad, la estructura no es inhackeable pero sí lo vuelve muy costosa y se invierte mucho poder de cómputo, entonces, trabajar con hash es sencillo, y es excelente cuando se trabaja con Blockchain porque el delincuente tendrá que recalcular muchos valores hash.
Además, Blockchain todavía utiliza otra idea que lo vuelve más complicado, se trata de Proof of Work, para que funcione el Blockchain debe tener medidas de verificación externa no centralizada, a diferencia de instituciones bancarias que centralizan el dinero; Blockchain está pensado en un sistema no centralizado, es decir cualquier persona puede convertirse en un ente verificador, no necesariamente debe ser un banco, cualquier persona lo puede hacer y esto refuerza la seguridad de los hash ya que son en sí mismos pocos seguros, y ahora tienen mecanismos de verificación de externos.
En la siguiente figura 2, se observa un ejemplo gráfico de cómo funciona el Blockchain para las transacciones bancarias [12].

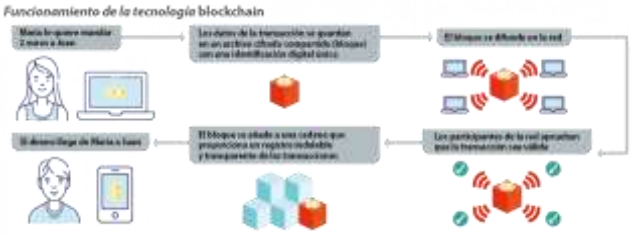

Figura 2. *Funcionamiento de la tecnología Blockchain*

Fuente: CaixaBank Research (2019) [12].

María quiere enviar dos euros a Juan, los datos de transacción se guardan en un archivo cifrado compartido que es el bloque (firma digital), con una identificación digital única (hash), es decir están los dos elementos que se necesitan.
En Blockchain el paquete de datos se manda a la red de manera abierta para que muchos entes (nodos) empiecen a validarlo, si un atacante captura bloque de datos, existen tres nodos que harán la validación, podrá realizar modificaciones, incluso indicar que el envío se redirija a su equipo y no al de Juan y lo coloca nuevamente en la computadora para que continúe la validación , esa computadora tendrá que validar el paquete de datos con un hash pero ya será diferente al de las otras tres, por lo que el hash modificado no se aceptará y lo va a mandar como algo incierto y la transacción del hacker nunca va a operar porque las otras tres hicieron la validación.
Las tres computadoras tienen un hash igual pero distinto al hash de la computadora que se intervino, entonces los participantes de la red aprueban que la transacción sea válida, si uno de esos cuatro dice que no es válida de todas maneras el proceso va a correr con los otros.

El bloque se añade a una cadena que proporciona un registro indeleble y transparente de las transacciones, es decir se ancla al Blockchain o la cadena de bloque y el paquete llegue a Juan que puede ser dinero, contrato digital, paquete de datos, etc., es decir, una transacción en la cadena de bloques es un proceso relativamente sencillo, pero implica a más personas y es donde a diferencia de una transacción bancaria, porque solo están dos personas que están realizando el envío de dinero, dependen de los bancos y de su forma de hacer las cosas para completar esa transacción, además de que están sujetos a sus condiciones (y a sus comisiones, por supuesto).

Es ahí donde entra la cadena de bloques, que básicamente elimina a los intermediarios, descentralizando toda la gestión. El control del proceso es de los usuarios, no de los bancos, y son ellos los que se convierten básicamente parte de un enorme banco con miles, millones de nodos, cada uno de los cuales se convierte en partícipe y gestor de los libros de cuenta del banco.

Por lo tanto, la cadena de bloques, es un gigantesco libro de cuentas en los que los registros (los bloques) están enlazados y cifrados para proteger la seguridad y privacidad de las transacciones. Es decir, en otras palabras, una base de datos distribuida y segura (gracias al cifrado) que se puede aplicar a todo tipo de transacciones que no tienen por qué ser necesariamente económicas.

Esa cadena de bloques tiene un requisito importante: debe haber varios usuarios (nodos) que se encarguen de verificar esas transacciones para validarlas y que así el bloque correspondiente a esa transacción (en cada bloque hay un gran número de transacciones que eso sí, es variable) se registre en ese gigantesco libro de cuentas.

Si se traslada a un ejemplo que no sea financiero y se aplica al área de ciberseguridad o en otros ámbitos, por ejemplo, en una empresa que envía un contrato a un cliente, ya les va a llegar validado, asegurando que no tenga modificaciones.

Hasta ahora se ha dicho que se necesita la firma digital y un identificador único que es el hash, pero la figura 2 aparece otro concepto, como son las computadoras o esos entes, nodos o personas que validan esos paquetes de datos y deciden si se pueden anclar o no a la cadena conociéndolos como mineros, siendo una nueva actividad laboral.

Los nodos son esas computadoras que hacen la validación, existen nodos completos, simples o super nodos, entre otros, siendo su característica principal que cuentan con una copia de todo el Blockchain, entonces, sí el usuario firmo y el software determinó el hash del paquete de datos que se va a enviar, se envía por una red y se distribuye a muchas computadoras que contienen todo el Blockchain completo, es decir si se tiene 40 bloques en el Blockchain, es porque se han hecho ese número de transacciones, esos equipos tendrá esa misma cantidad de bloques cada una, esto es, esa cadena de Blockchain esta clonada en n equipos, 100, 200 o mil equipos, etc., que quiere decir, ante un ataque a una de esas computadoras, existen N computadoras más con la información completa, siendo que solo se necesitará una computadora con la información completa para restablecer el Blockchain, con ello se asegura restablecer y nunca se va a perder la información.

Entonces, el minero está vinculado al Blockchain, si no existen el minero el concepto pierde sentido, ya que es el que va a validar los hashes y si hay varios mineros que lo validan y que coinciden ese bloque se añade a la cadena y esta cadena va creciendo entonces los mineros darán estabilidad y mecanismos de seguridad.

Conclusiones

Un hacker puede atacar una computadora, pero no a mil que están en diferentes partes del mundo y con diferente seguridad, por lo que no es rentable hacer hackeo a Blockchain.

En ciberseguridad el Blockchain se usa en protección de identidad, de datos y trazabilidad del flujo de la información, no todos los implementan, las grandes empresas sí, los bancos en México aún no, y poco a poco se va a ir avanzando.

En definitiva, las nuevas tendencias en ciberseguridad son tres: inteligencia artificial, Blockchain y computación cuántica, entonces el experto en ciberseguridad deberá de conocer estas tecnologías para dar los servicios adecuados a las empresas para proteger a sus usuarios.

Blockchain y cómputo cuántico dan un sistema muchísimo más seguro donde los expertos lo catalogan como imposible que sea hackeable, el sistema perfecto en aplicaciones como WhatsApp o Telegram se dan transacciones no reconocidas debido a los problemas que tiene la llave pública y la llave privada, entonces se requiere líneas de Blockchain para que se validen las claves y evitar cuentas piratas para validar usuarios, por lo que se convierte en un nicho que aprovechar ya que se puede reemplazar la llave pública y usar tecnología en Blockchain.

Blockchain es nuevo, su fortaleza está en las criptomonedas, pero ya empiezan las aplicaciones en ciberseguridad debido a que como se explicó, la tecnología Blockchain tiene mucho potencial, gracias a que utiliza la criptografía, cada bloque de información se identifica de forma única y los participantes de la red

deben aprobar y validar toda la información que entra en la ella, volviendo el registro inalterable e inmutable y, por ello, extremadamente complicado de hackear o modificar. En resumen, las brechas de datos en las empresas son una problemática real, sin las medidas de ciberseguridad no se puede evitar el robo, secuestro o alteración de datos e información, entonces Blockchain puede garantizar el almacenaje seguro de datos mediante su descentralización y la información cifrada además, permite es pública e inmutable basada en una secuencia creciente de bloques y proporcionando de forma privativa tolerancia a fallos en nodos, robustez frente a manipulación y al ser pública, transparencia convirtiéndose en una de las tecnologías con más potencial disruptivo de los últimos años.

Referencias

[1] Corredor Higuera, J. A., & Díaz Guzmán, D. (2018). Blockchain y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología Blockchain en los mercados de crédito de América Latina. Derecho PUCP, 81, 405–439

[2] Blanco Encinosa, Lázaro J.. (2021). Criptomonedas. Breve análisis desde la perspectiva económica y financiera. Cofin Habana, 15(2), e16. Epub 29 de julio de 2021. Recuperado en 19 de enero de 2022, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612021000200016&lng=es&tlng=es

[3] Corredor Higuera, J. A., & Díaz Guzmán, D. (2018). Blockchain y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología Blockchain en los mercados de crédito de América Latina. Derecho PUCP, (81), 405-439. https://doi.org/10.18800/derechopucp.201802.013

[4] Pérez, M. H. (2020) Cibercrimen adolescente: la punta de un iceberg que crece año a año, El Pais. Available at: https://elpais.com/tecnologia/2020-07-14/cibercrimen-adolescente-la-punta-de-un-iceberg-que-crece-ano-a-ano.html (Accessed: October 1, 2021).

[5] Aguilar Cárceles, Marta María. (2015). Ciber crimen y ciber victimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. Revista Criminalidad , 57 (1), 121-135. Recuperado el 19 de enero de 2022, de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082015000100009&lng=en&tlng=es

[6] Nieto Ramírez, Nathaly, & Nieto Londoño, Rubén Darío. (2019). Implementación hardware de la función Hash SHA3-256 usando una arquitectura Pipeline. Ingeniare. Revista chilena de ingeniería, 27(1), 43-51. https://dx.doi.org/10.4067/S0718-33052019000100043.

[7] Redacción (2021) ¿Puede haber bitcoin falso? No, y esta es la razón, El Financiero. Available at: https://www.elfinanciero.com.mx/tech/2021/11/04/puede-haber-bitcoin-falso-no-y-esta-es-la-razon/ (Accessed: January 19, 2022).

[8] Rojas López, M. D., Suarez Botero, D. M, Meneses Durango C. N. (2011) "Firma digital: instrumento de transmisión de información a entidades financieras," Revista Avances en Sistemas e Informática, pp. 7–14.

[9] García-Córdoba, J, & Herrero-Pérez, L. (2020). La ciberdefensa en los sistemas de información sanitarios militares. Sanidad Militar, 76(3), 140-142. Epub 08 de marzo de 2021.https://dx.doi.org/10.4321/s1887-85712020000300001.

[10] Pool, C. E. O. (2022) Ciberataques incrementaron 151% en el 2021, EL CEO. Available at: https://elceo.com/tecnologia/ciberataques-incrementaron-151-en-el-2021/ (Accessed: January 20, 2022).

[11] Retamal, C. D., Roig, J. B. and Tapia, J. L. M. (2017) "La blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas," Economía industrial, (405), pp. 33–40. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=6207510 (Accessed: January 20, 2022)

[12] CaixaBank Research (2019) "Funcionamiento de la tecnología Blockchain." CaixaBank Research. Available at: https://www.caixabankresearch.com/es/economia-y-mercados/politica-monetaria/blockchain-y-criptomonedas-bienvenidos-al-nuevo-paradigma