Revista
MINERVA

Plataforma digital de la revista: https://minerva.sic.ues.du.sv

Articulo Científico | Scientific Article

Grado de riesgo en el uso de criptoactivos para usuarios sin un nivel de educación especializado en el ramo: aspectos a priorizar en la mitigación

Level of risk in the use of cryptoassets for users without a specialized level of education in the field: aspects to be prioritized in mitigation

Nelson Ernesto Rivera-Díaz[1]

Correspondencia:
ernesto.rivera@ues.edu.sv

Presentado: 14 de marzo de 2022
Aceptado: 23 de agosto de 2022

1 Universidad de El Salvador, Facultad de Jurisprudencia y Ciencias Sociales, Director de laEscuela de Relaciones Internacionales.

RESUMEN

El uso de criptoactivos, como instrumento de inversión, se encuentra en creciente auge, colocando el tema en perspectiva hacia un avance por posicionarse en el espectro financiero global. Desde luego, la incursión en una tecnología novedosa y combinada con las reglas del mercado crea una situación que, de no saberse manejar, puede representar severos riesgos para usuarios animosos y poco educados. Por un lado, el riesgo de ciberseguridad y criptoseguridad queda en primer plano, dejando en exposición al usuario ante ataques diversos de los que solo se podrá defender mediante buenas prácticas en el manejo de sus activos; por el otro, está, el riesgo financiero que aumenta en la medida que existan factores agravantes producto de una gestión deficiente. En tal sentido, es necesario prevenir al usuario novato de los principales riesgos a los que se expone, brindándole mediciones aproximadas para que considere su involucramiento y las condiciones del mismo.

Palabras clave: Criptoactivo, ciberseguridad, criptoseguridad, riesgo financiero

ABSTRACT

The use of cryptoactives as an investment instrument is growing, putting the issue in perspective towards an advance to be placed in the global financial spectrum. Of course, the incursion into a new technology merged with the rules of the market creates a combination that, if not known how to handle it, can represent severe risks for users who are as courageous as they are uneducated. First, the risk of cybersecurity and cryptosecurity remains in the foreground, leaving the user exposed to various attacks from which they can only be defended through good practices in the management of their assets. Second, financial risk increases as long as

there are aggravating factors resulting from poor risk management. In this sense, it is necessary to warn the novice users about the main risks to which they are exposed, providing approximate measurements so that he considers their involvement and its conditions.

Key words: criptoactive, cybersecurity, cryptosecurity, financial risk

INTRODUCCIÓN

Los criptoactivos son, en muchos sentidos, una incógnita técnica y económica para la mayor parte de la población mundial, la cual se enfrenta a una realidad apremiante, compleja y retadora: el ciudadano común sigue sin comprender la teoría monetaria, por lo que los criptoactivos representan un riesgo en sí mismos en comparación con la simpleza monetaria de la divisa tradicional, en tanto que suman al escenario todo el carácter tecnológico que se asocia a la fluctuación cambiaria. El uso de tales activos criptográficos ha pasado de la excepcionalidad a la regularidad en muchos países como España, Estados Unidos, India, Alemania y Corea del Sur, y muestra un avance contundente, aunque con un ritmo dispar (Cabrera Soto & Lage Codorniu, 2022). En el desarrollo de dicho progreso, los riesgos de seguridad han ido creciendo de forma proporcional, al grado de registrarse estafas, desde las más burdas hasta las más cruciales vulneraciones de seguridad digital, afectando a usuarios individuales, empresas e instancias gubernamentales.

Si bien, el tema puede ser abordado desde el enfoque normativo, esto solo haría que las autoridades persiguiesen infructuosamente el delito, siendo que conlleva a una complejidad técnica, legal, económica e informática que trasciende de la capacidad meramente legislativa. A eso debe sumarse el riesgo financiero producto de la alta volatilidad, siendo que el inversionista, incluso si hubiere superado las barreras de la criptoseguridad y la ciberseguridad, se enfrentará a la probabilidad inminente de resultados negativos producto de la fluctuación del mercado, lo cual deberá mitigar vehementemente para resguardar su capacidad operativa (Ordinas, 2017). Sin duda alguna, los gobiernos deberán extender su ámbito de acción para prevenir la vulnerabilidad ante las inevitables transacciones con criptoactivos, tomando en cuenta que estas se volverán en la generalidad en el mediano plazo, sin que esto signifique que deba abandonarse del todo la vía de la legislación (Perafán, 2019).

METODOLOGÍA

Se basó en la revisión de cifras que incluyen el ciberdelito en todas sus formas, contrastándolas con las cifras relacionadas con modalidades más complejas que incluyen criptoactivos. Cabe la aclaración acerca de la selección de data que corresponde a estafas provenientes del desconocimiento técnico de la víctima, así como la incapacidad estatal para atajar dichas acciones delictivas. Tras la revisión de los casos de pérdida de activos, producto del delito en cualquiera de sus presentaciones, se ha incluido en el análisis de riesgo, las cifras registradas en concepto de volatilidad de mercado de criptoactivos, extrapolando data contra la estadística de pérdida financiera producto de las operaciones con activos no crípticos que fluctúan en el mercado.

El riesgo financiero, asociado al uso de criptoactivos, acaba por ser determinado a través de la comparación de resultados, evidenciando la necesidad de adoptar medidas técnicas, para mitigar la posibilidad de pérdida, especialmente en el término de la liquidez de inversión. En tal sentido, una vez establecido el grado de riesgo (según perfil de usuario y condiciones agravantes, parametrizado según la propuesta de Cox, Babayev y Huber), se procede a realizar una estimación de riesgo ponderado en el uso de criptoactivos.

RESULTADOS Y DISCUSIÓN

Los riesgos identificables para el inversionista en criptoactivos versan, fundamentalmente, sobre la seguridad y el resguardo financiero, sin cometer el error de separarlos como riesgos independientes. Por tanto, el estudio de ambos factores confluye en precauciones mínimas que se deben guardar para la mitigación de la probabilidad de pérdida.

Riesgos de seguridad en el uso de criptoactivos

La tecnología criptológica basa su seguridad en el principio de encadenamiento de bloques custodiado por muchos ordenadores que, en teoría, es imposible que exista una vulneración ya que no se podría generar una coordinación global en pro de un delito puntual, encargando la gestión del riesgo de fraudes al franco fracaso de la coordinación social (Sartor, 2019; Tapscott & Tapscott, 2018), dejando de lado las múltiples formas de sofisticación tecnológica que puedan desarrollarse para violentar las capas de encriptación.

No obstante, la seguridad de los criptoactivos, con el tiempo, se ha vuelto más compleja, haciéndose cada vez, más robusta e informáticamente más confiable (Díaz Gutiérrez & Cueva Lovelle, 2018). Sin embargo, la seguridad del *Blockchain* poco puede hacerles frente a otras formas de vulneración que exceden la criptología, tal como la inexperiencia del usuario, la ingeniería social o las filtraciones intencionales de un funcionario (Rocohano Ramos & Silva Ordóñez, 2021).

Este artículo no abordará los pormenores tecnológicos de la seguridad críptica, sino aquellos aspectos conexos que representan un riesgo en el uso de criptoactivos, tomando en cuenta que, como toda tecnología incipiente, conlleva una curva de aprendizaje que traerá más o menos costos, dependiendo de la capacidad social para adoptarla en el ideario y comprenderla intrínsecamente.

Un buen inicio para el abordaje de la seguridad en el uso de criptoactivos será la separación conceptual entre criptoseguridad y ciberseguridad. Mientras que la seguridad cirptológica versa sobre el encadenamiento de bloques en un sistema autónomo de protección, que desliga la toma de decisiones informáticas de la capacidad humana para reaccionar ante las amenazas (Tapscott & Tapscott, 2018), la ciberseguridad amplía su definición en múltiples aristas, confluyendo en la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos (Linares-Morales, 2021). Como puede observarse, todos los aspectos mencionados están fuera del alcance de la seguridad del encadenamiento de bloques, pero se relacionan con él, volviéndolo vulnerable en múltiples aspectos, sin que la criptología pueda abastecerse de mecanismos de defensa en tanto que le es imposible dar lectura a las múltiples reacciones técnicamente incorrectas que pueden tener las personas. En resumen, se puede afirmar que la criptotecnología tiene un enemigo constante: el desconocimiento técnico de sus usuarios ya que no existe sistema informático que pueda superar la capacidad humana para cometer errores (Eterovic et al., 2020).

Si bien los sistemas de defensa informática se han sofisticado, aún distan mucho de convertirse en infalibles, y aunque técnicamente llegasen a serlo, el usuario les vuelve igualmente endebles ante las malas prácticas observables en demasía. A modo de marco referencial, el ciberdelito financiero ha causado grandes estragos en múltiples sistemas bancarios a nivel mundial, proyectándose que, a final de 2022, las pérdidas ascenderían a ocho billones de dólares estadounidenses, únicamente incluyendo el dinero tradicional, entendido como las monedas sujetas al control del Estado (Ochoa, 2021).

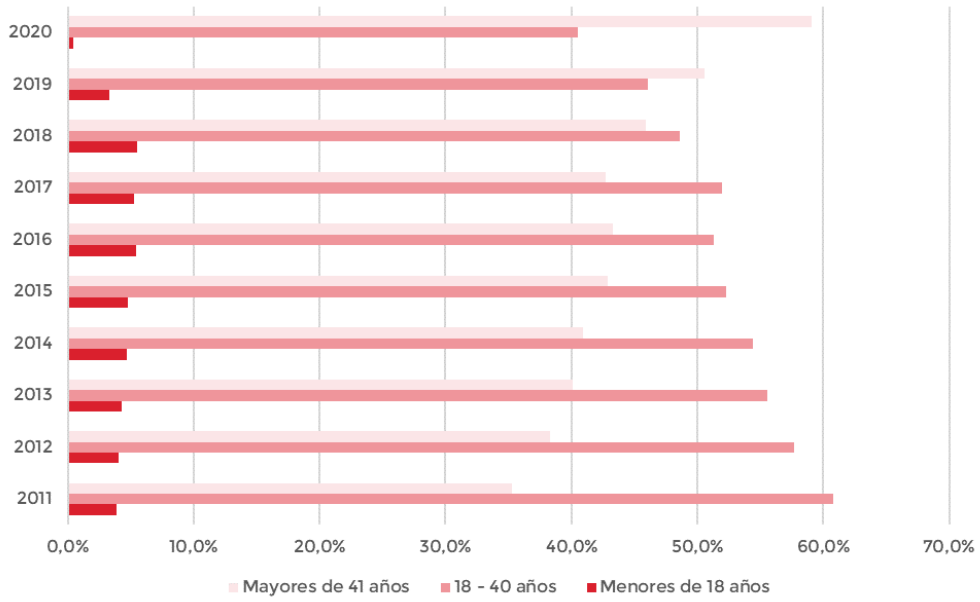
Al respecto, España es, por mucha diferencia, uno de los países europeos con mayor apertura a las transacciones electrónicas y pionero en la legislación del uso de criptoactivos, liderando el esfuerzo jurídico que conllevaría a la normativa en toda la Unión Europea (García-Ramos Lucero & Rejas Muslera, 2022). En tanto la difusión del comercio electrónico y criptológico es amplia, vale la pena hacer una revisión de las estadísticas de ciberdelito en una economía tan permisiva, resultando hallazgos reveladores durante la década de 2010. A inicios de la década de 2011, se registraron ciberestafas equivalentes al 20 % de las estafas en todas sus modalidades; sin embargo, pese a todos los esfuerzos legislativos y judiciales, la proporción crecería en un 31 % de casos comprobados hacia 2018 (López Gutiérrez et al., 2020), aunque la proporción en cuanto a procedimientos de investigación abarca incluso hasta el 55 % de la totalidad (López Fonseca, 2019).

Además, hacia el final de la década de 2010, la mayor parte de ciberestafados son hombres, lo que representa un 53.3 % de los casos (López Gutiérrez et al., 2020). Sin embargo, la cifra más reveladora se sitúa sobre la edad de los ciberestafados, la cual exhibe que el desconocimiento de la tecnología vuelve vulnerable al usuario. Según los datos presentados en la Figura 1, el estudio español revela que en 2011 hubo una mayoría significativa de jóvenes estafados, lo cual resulta lógico en tanto que el incipiente comercio internacional se popularizaba entre la generación nativo-digital (Sánchez Torres & Arroyo Cañada, 2016). Sin embargo, a medida que los grupos sociales de mayor edad se animaban a ingresar a la tendencia del *e-commerce* en detrimento del comercio tradicional (Pulido López, 2021), la incidencia de las ciberestafas iba teniendo un creciente impacto en los usuarios de mayor edad, llegando a 2020 con una clara tendencia al "envejecimiento" de las víctimas (López Gutiérrez et al., 2020).

Tal como puede apreciarse en la Figura 2, la tendencia al envejecimiento de la víctima de una ciberestafa crece en la medida que el flujo de comercio electrónico llega a los grupos

Figura 1

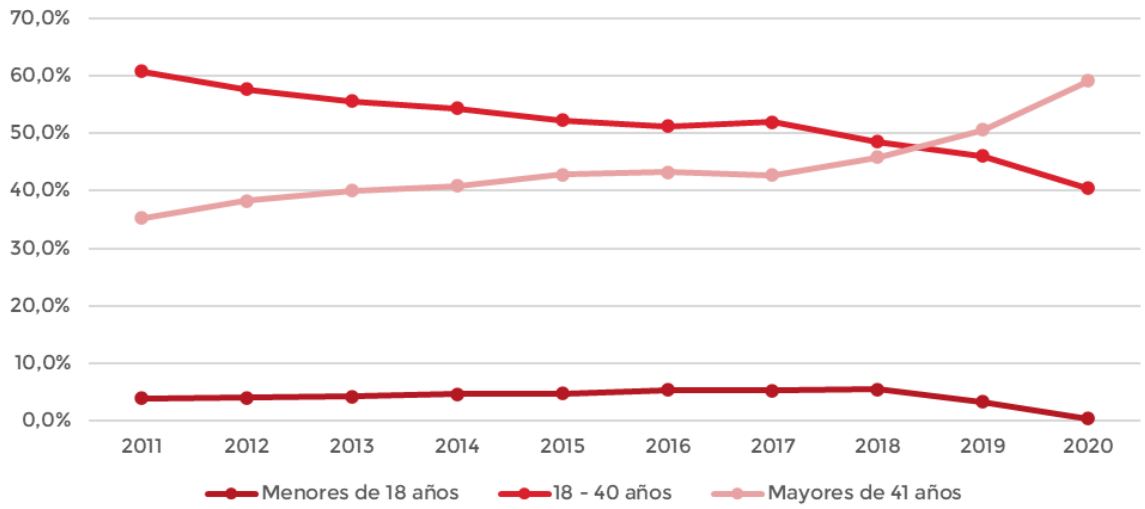
Víctimas de ciberdelito por grupos de edad en España



Nota. Elaboración propia con datos de López Gutiérrez et al., 2020.

Figura 2

Evolución del ciberdelito por grupos de edad de las víctimas en España



Nota. Elaboración propia con datos de López Gutiérrez et al., 2020.

con menor tradición de seguridad informática producto de los limitados conocimientos en la materia, sin que se descarte el notable número de ciberestafados entre las edades nativo-digitales y conexos. Entre los datos destaca un número de casos registrados entre menores de 18 años, lo cuales, si bien representan un porcentaje menor, no deben ser desatendidos en tanto que existe comisión de delito.

Al respecto, el caso europeo es paradigmático ya que sigue la tendencia española, llegando a abarcar el 42 % de cibercrimen a nivel global, escasamente seguido por Asia con un 19 % (Secretaría General de INTERPOL, 2020). No obstante, la asimetría en el flujo comercial electrónico y, por consecuencia, en el volumen de cibercrimen, América Latina se posiciona como una región muy vulnerable, sosteniendo una cifra de proporción de ciberestafas muy similar a la española, situándose en el 46 % de los casos totales (Aguilar-Antonio, 2020).

Las múltiples modalidades de estafa *Fintech* tienen su base en el pírrico conocimiento del usuario sobre los pormenores técnicos de las plataformas que utiliza para manejar su dinero, por lo que no será de extrañar que la mayor cantidad de ciberdelitos financieros se registren en países con menos acceso a educación tecnológica (CEPAL, 2021), convirtiéndose en una incipiente forma de castigo en el esquema de brecha de conocimiento.

En efecto, la ingeniería social usa la ignorancia para vulnerar información, que luego es utilizada para el cibercrimen, lo que implica costes elevados a nivel privado por las flagrantes pérdidas producto de negocios fallidos. Esto deja en graves problemas a los gobiernos ante la dificultad de persecución efectiva del delito por la incapacidad técnica de identificación del delincuente, y esto, tomando en cuenta que se trata de dinero tradicional, trazable en cada transacción (Rosero Gomezcoello, 2020).

Para efectos de ilustración y estudio, veamos un caso puntual: la COVID-19 representa un hito en muchos campos, pero particularmente aprovechable para los estafadores. De las técnicas de engaño reconocidas, la cantidad de vulneraciones producto de la pandemia ocurrió en modalidad de cibercrimen, tal como se evidencia en la Figura 3.

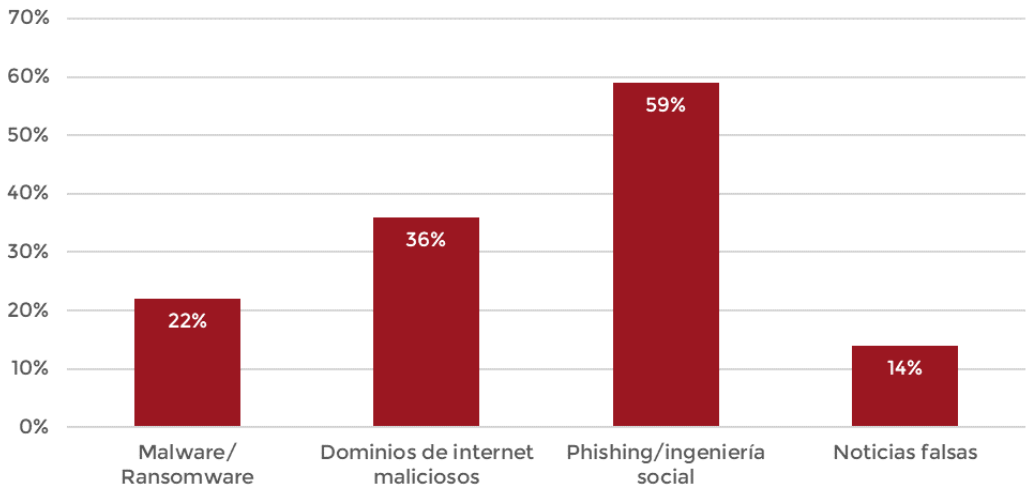
Si para complejizar el asunto, se incluye en el escenario a los criptoactivos, la oportunidad para el cibercrimen crece exponencialmente siendo que el conocimiento sobre el manejo técnico de dichos activos es casi nulo. Por ejemplo, para el inicio lectivo de 2021, se registró cero países que incluyeron en sus programas educativos el tema de criptofinanzas (Ordóñez Sánchez, 2021), por lo que la información en el ramo es escueta y altamente especulativa, sumándose a la tendencia de la animosidad hacia usar un activo de avanzada en un contexto de insipiencia jurídica y mercantil. La pandemia, además, aceleró el uso de dichos activos (Soto Galindo, 2020), poniéndolos en manos de jóvenes nativo-digitales, entusiastas e idealistas, pero con un recorrido corto por los vericuetos financieros modernos, volviéndoles presa fácil para la ciberestafa.

Desde luego, si la persecución del ciberdelito a nivel de dinero tradicional ya era un problema, cuando se involucra la irrastreabilidad de los *hashes* en las transacciones criptológicas, la situación se complica aún más para los gobiernos, y los deja casi desarmados para ejercer una verdadera soberanía en el espectro criptomonetario incipiente (Gabela Salvador, 2019).

Justamente es la irrastreabilidad transaccional la que vuelve imposible contabilizar los casos de estafa; sin embargo, se tienen bien identificadas las formas utilizadas: smodelos de Ponzi, *Pump and dump*, falsos respaldos de celebridades, falsos *exchanges*, *apps* fraudulentas, *fakenews*, *phishing* y *Crypto clipping* (Narosky, 2022), la mayoría de estas no se encuentran tipificadas en los códigos penales, es decir, se carece de leyes especializadas en la mayoría de los casos, lo cual vuelve imposible la persecución y judicialización del delito (Oxman, 2013; Ruani, 2020). Dicha carencia jurídica ya ha motivado a que varios países realicen intentos de combate por la vía legislativa, siendo Colombia uno de los pioneros en el ramo; sin embargo, pese a los esfuerzos, el lavado de dinero a través de criptoactivos ya se sitúa entre las tres modalidades más populares de comisión de delitos (Manrique Morales & Pedraza Castañeda, 2019; Parra Tabares, 2019). De igual manera ha ocurrido en El Salvador, primer país en adoptar

Figura 3

Técnicas de engaño en el marco de la pandemia por COVID-19



Nota. Elaboración propia con datos de Secretaría General de INTERPOL, 2020

un criptoactivo como moneda de curso legal, ya que la *app* que funge como *wallet* estatal presenta unas condiciones de seguridad tan pobres que el número de casos de suplantación de identidad se cuenta por miles (Engler, 2021), dejando al descubierto que, sin una verdadera pericia en el uso de las herramientas tecnológicas, el manejo de criptoactivos se puede volver un riesgo relevante.

La incapacidad técnica para prevenir este tipo de hechos, ha propiciado a nivel mundial el cometimiento de cientos de ciberataques por la vía física, esparciendo maliciosamente *pendrives* que contienen *malware* instalable en el ordenador de los incautos, que, por curiosidad o avaricia, deciden utilizarlo (Raya, 2021). Desde luego, ninguno de esos ataques ha alcanzado la envergadura del caso Mt Gox, habiéndose «perdido» un total de 54 billones de dólares estadounidenses, según la cotización más alta de Bitcoin (Cheung et al., 2015). Al respecto, el uso de *malware* conlleva un riesgo de pérdida significativo y preocupantemente creciente (Mena Roa, 2021), tal como puede observarse en la Figura 4.

Sin embargo, la popularidad de los criptoactivos lleva a que las estafas sean cada vez más fáciles y veloces en su ejecución, atándose a los eventos de cultura popular que abrazan a los sectores de la población que, si bien tienen algún conocimiento más avanzado sobre ciberseguridad, son vulnerables por su relación emocional hacia las olas especulativas. Tal es el caso de Squidcoin, que se constituye en una criptoestafa producto de la ingeniería social que utiliza el imaginario popular como canal de instalación de una *wallet* fraudulenta.

En 2021 se popularizó una serie de Netflix llamada *Squid Game*, cuyo contenido estaba clasificado para mayores de 18 años por su alto nivel de violencia. Pese a sus características, la serie alcanzó un altísimo grado de audiencia, lo que se vio como una ventana para que estafadores instalasen una inusitada modalidad de captación de víctimas: la creación de una *wallet* donde se depositaría dinero que sería convertido en una criptomoneda llamada *Squidcoin*, la cual serviría para pagar la participación en una simulación de realidad virtual del juego inspirado en la serie (Cheng, 2021). En las condiciones de venta se especificaba que la cantidad de boletos sería limitada, así que la subasta habría iniciado en 1 dólar estadounidense, subiendo rápidamente producto de la alta demanda. Cada vez las transacciones se volvían más robustas, habiendo depósitos cuantiosos hasta alcanzar la cifra de 2,856 dólares estadounidenses por *token* en apenas 6 días. Tras una advertencia publicada en blogs de criptología, la sospecha de que no existía tal simulación de realidad virtual disparó las alarmas; sin embargo, cuando los usuarios quisieron poner sus criptoactivos a resguardo, la *wallet* dejó de operar, desapareciendo del espectro *web*, registrándose una cotización bajista hasta los 0.00322 dólares estadounidenses por *token*, provocando pérdidas por ciberestafa calculadas en los 3.38 millones de dólares estadounidenses, producto de la ingenuidad de los usuarios (Muni, 2021).

Riesgos financieros en el uso de criptoactivos

El riesgo de pérdida producto del ciberdelito es latente, creciente y, aparentemente, incontrolable a nivel de Estado; sin embargo, los usuarios de criptoactivos deben estar preocupados por otros riesgos que no se ocultan en el espectro criminal, sino que se exhiben en pleno día ya que están relacionados a las normas tácitas o explícitas del mercado, así como a las legislaciones nacionales.

Inicialmente, el inversionista en criptoactivos debe cuidarse del riesgo de liquidez, producto de la volatilidad de un mercado inusitadamente veloz en su fluctuación. Una inversión en criptoactivos jamás debe ser pensada para el inmediato plazo, ya que los cambios de cotización pueden poner a

prueba el músculo financiero por prolongados periodos, restringiendo el capital operativo de aquel que se decidió por este mercado (Asto Paredes & Villavicencio Flores, 2019). En tal sentido, la gestión del riesgo de liquidez debe ser una prioridad en estos casos, debido a que una noticia convulsa en una latitud lejana puede causar un desplome inmediato del activo, dejando al inversionista a expensas del mercado que, si bien afecta al dinero tradicional, las fluctuaciones no resultan tan violentas como en los *criptoactivos*. De hecho, no es necesario que exista un suceso severo que afecte la cotización; es más, resulta hasta innecesario un hecho real, ya que basta con el *tweet* de una personalidad para que se registre un desplome, por ejemplo: el caso de la dependencia de Bitcoin con respecto a las declaraciones del empresario Elon Musk (Hamurcu, 2022).

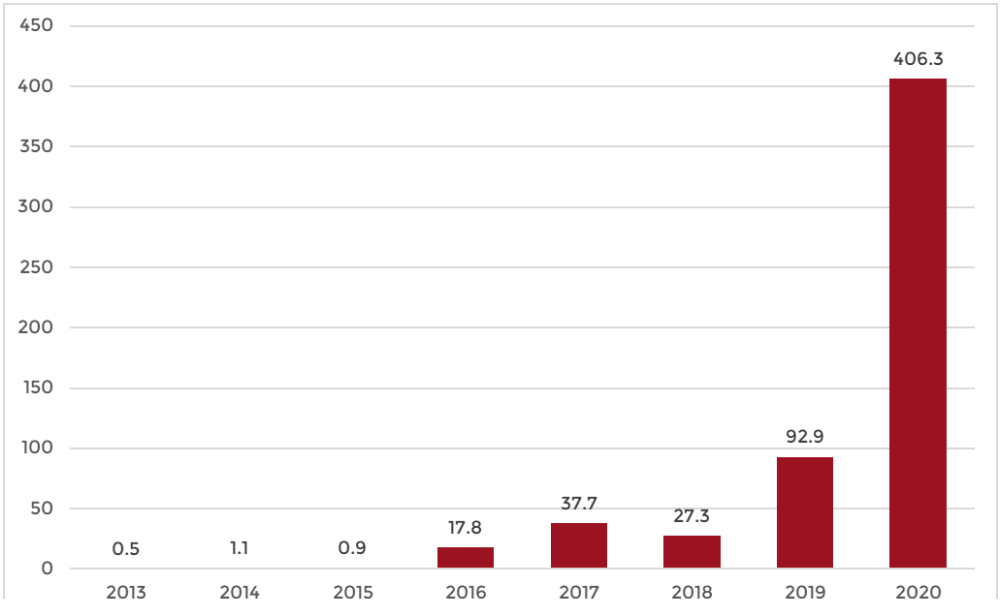
Por otro lado, es bien sabido que los activos financieros criptológicos no son sujetos de depósito de valor dada su volatilidad desaforada; por tanto, aquel inversionista que resguarde su capital operativo en esta modalidad se enfrenta a un riesgo multiplicado, pues fácticamente lo utilizaría como moneda de curso legal, lo cual es incompatible con el concepto mismo de este tipo de activos de inversión (Asto Paredes & Villavicencio Flores, 2019). Desde ese punto de vista, si no se tiene la solidez financiera y la gestión de riesgo oportuna, el uso de criptoactivos fácilmente puede implicar la quiebra técnica de cualquier inversionista mediante la merma en su flujo de caja por la volatilidad del mercado (Bermúdez Pacheco et al., 2021).

Tal como puede observarse en la Figura 5, aquel inversionista que, entusiasmado por el repunte de cotización en 2017, se hubiere aventurado a realizar una fuerte inversión en criptomonedas diversas, habría tenido que esperar hasta 2020 para tener una recuperación factible, poniendo a prueba su capacidad para sostener una inversión en el largo plazo.

Igualmente, si un inversionista es tan incauto como para usar como moneda de curso legal un activo que fue diseñado como instrumento

Figura 4

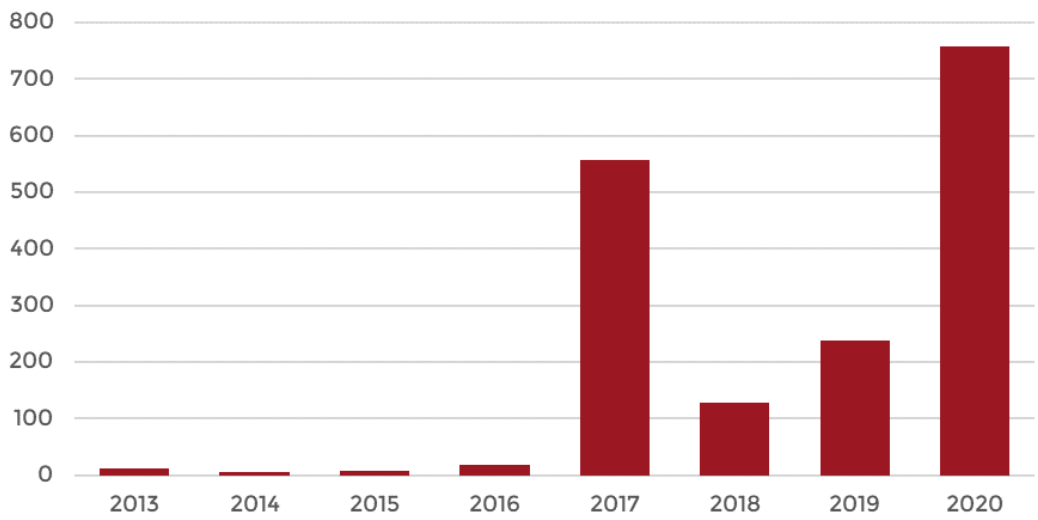
Pérdida por ataques de malware sobre criptomonedas en millones de dólares



Nota. Elaboración propia con datos de Mena Roa, 2021

Figura 5

Valor de capitalización bursátil a nivel mundial de criptomonedas, en miles dólares estadounidenses



Nota. Elaboración propia con datos de Bermúdez Pacheco et al., 2021.

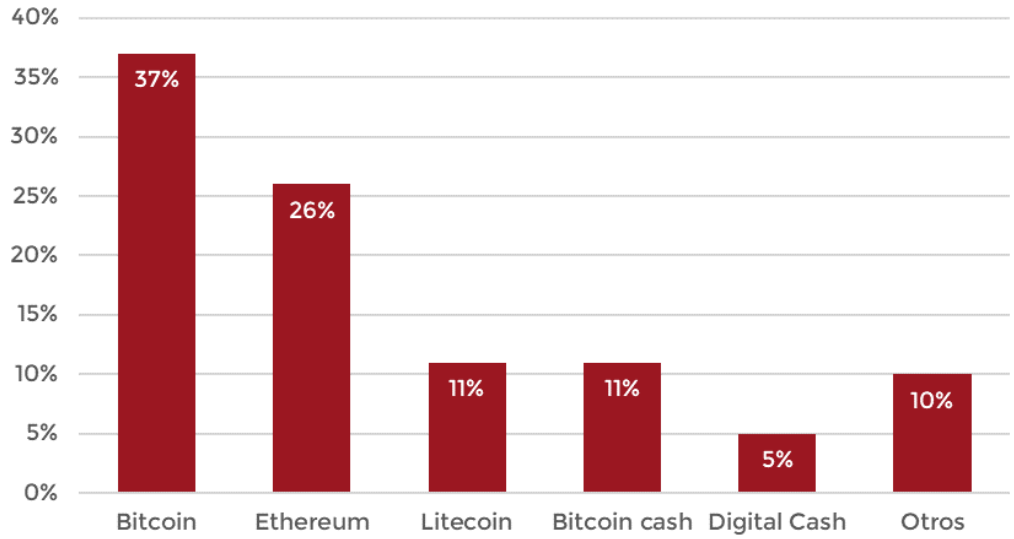
de inversión, este agravaría su condición, si por desconocimiento, decide casarse con un solo activo en el mercado, ignorando una de las reglas más prominentes en la gestión del riesgo financiero: la diversificación (Bravo de Mansilla et al., 2000). Para tomar como base la región latinoamericana, esta sigue bastante bien la norma de diversificación, y logra una repartición de inversión como la expresada en la Figura 6.

Aquel que se lance al mercado de criptoactivos erraría de lleno si escogiese una sola criptomoneda como foco de su inversión, haciéndose depender en su totalidad de la cotización que puede ir al alza o a la baja, según las circunstancias. Por ejemplo, un inversionista con mayor pericia jamás depositaría la totalidad de su inversión en Bitcoin, a sabiendas de que es, por excelencia, el criptoactivo más volátil en el mercado. En cambio, con una adecuada gestión de riesgos, diversificaría la cartera para combinar el uso de Bitcoin con *stablecoins* y otros criptoactivos de mayor seguridad que le servirán como refugio y reserva de liquidez sobre su inversión (Domínguez et al., 2019). En el caso latinoamericano, casi la totalidad de países cumplen con el criterio de diversificación (unos de forma legislada y otros por ausencia de legislación), excepto El Salvador, donde la normativa restringe al uso de Bitcoin como única criptomoneda de curso legal.

En este punto, los riesgos financieros ya son considerables, incluso sin haber tocado el tema de la complejidad del *trading* y su asocio fáctico con el acontecer internacional. La lectura prospectiva de la criptoinversión es más compleja que el *trading* sobre activos tradicionales, considerando que el fanatismo de los criptoentusiastas hace que el mercado reaccione hasta con eventos irrelevantes tales como las opiniones de grandes empresarios o políticos prominentes, lo que convierte al criptomercado en una burbuja especulativa, inestable y exigente de un dominio magistral de las técnicas de *charting* (Ordinas, 2017; Ruíz Rosas & Décaro Santiago, 2019). Un *noob* en la inversión en criptoactivos debería ser sumamente cauto, y gestionar el riesgo desde una posición defensiva y conservadora. Incluso guardando tales precauciones, la cotización igualmente representará un riesgo de liquidez por volatilidad impredecible en los esquemas

Figura 6

Distribución de principales criptomonedas minadas en América Latina en 2020



Nota. Elaboración propia con datos de Bermúdez Pacheco et al., 2021.

de análisis *charting*, ya que las decisiones políticas repentinas pueden modificar la cotización hasta la pérdida del capital operativo (Sachdeva Keswani et al., 2021). Por ejemplo, solo en enero de 2022 se registraron pérdidas de hasta 200 millones de dólares estadounidenses producto de las fluctuaciones en el mercado de criptodivisas, sin que 60 días después se vislumbre una recuperación (Fernández, 2022).

Además, la liquidez del inversionista no es la única que hay que observar, ya que el ritmo de creación de criptodivisas también compromete el índice de liquidez global; muchas veces el *Blockchain* no ha podido abastecer la demanda, comprometiendo así la operatividad del comercio. Los inversionistas, ante la inminente caída de la cotización por causa de la falta de liquidez, inyectan capital para sostener de forma artificial el precio, lo que causa un círculo vicioso que alimenta la burbuja financiera (Ventura, 2021).

Otro riesgo que debe tomarse en cuenta es que, a diferencia de los mercados tradicionales, no existe un regulador o superintendente en el mercado, por lo que la fijación del precio no está sujeta a la observación continuada, y se entrega en su totalidad a la oferta y demanda, que es influenciada por las olas especulativas. Para mayor claridad, la situación del mercado de criptoactivos es equiparable a los lapsos *Over The County* (OTC) en el mercado bursátil, condición en la que se advierte al inversionista que está bajo su entera responsabilidad y riesgo (Steenkamp & Ter Hofstede, 2002). Sin embargo, la condición OTC es eventual, temporal y excepcional en la cotización bursátil tradicional, mas no en el mercado de criptoactivos, en el cual se convierte en la norma cotidiana (Nieves, 2021).

Por otro lado, el inversionista debe tener en cuenta que los Estados se encuentran aún en etapa de asimilación normativa acerca del tema, por lo que los cambios legislativos son rápidos, constantes y extrapolares (Barroilhet, 2019). En tal sentido, el riesgo de que un país decida proscribir o sobrerregular el criptomercado es cada vez más común, especialmente cuando los Estados se dan cuenta de que esta modalidad comercial representa un dreno relevante en la captación tributaria (Alvarez-Pincay et al., 2018).

Al respecto, hay países cuyas legislaciones ya han incluido la tributación en criptoactivos como parte de su modelo fiscal, aunque también debe considerarse que, por muy sofisticada que la ley se elabore, siempre deja huecos importantes en el marco de la irrastreabilidad transaccional dada la incapacidad técnica para identificar al tributante potencial. Sin embargo, como puede haber un país que regule el uso de criptoactivos, igualmente habrá otro que los legalice en su totalidad, así como otro los proscriba sin previo aviso. El abanico de posibilidades es tan amplio que el inversionista debe plantearse múltiples escenarios que generen una diversidad de planes de contingencia ante la posibilidad de un cambio en la normativa, debiendo considerar opciones tales como el resguardo de los activos en *wallets* que permitan transacciones consecutivas entre diferentes criptoactivos con el fin de eludir las consecuencias en los cambios de normativa.

Ya en el campo político, el inversionista debe considerar el riesgo de mezclar el mercado con los intereses de los gobiernos (o, peor aún, de sus gobernantes), ya que la combinación puede resultar en un rendimiento indeseable, en tanto que se rompen los principios más básicos de las criptofinanzas, las cuales fueron diseñadas para eludir el control estatal sobre las relaciones monetarias. La inversión en una *govcoin* (moneda digital no críptica emitida por el Estado) o la utilización de una *wallet* oficial disparan todas las alarmas financieras y de ciberseguridad, y dejan al inversionista en un campo del que difícilmente logre salir sin convertirse en un dependiente de los flujos estatales (Pilacuán Cadena et al., 2021).

Riesgo ponderado en el uso de criptoactivos

La gestión del riesgo va más allá del hecho de identificar las potenciales amenazas; es necesario un plan de mitigación, que solo puede ser elaborado si existe una ponderación de dichas amenazas, identificando las probabilidades de ocurrencia. En tal sentido, conviene invocar los estándares que las Normas ISO 31000 establecen acerca del lavado de dinero y activos, así como exigir una gestión del riesgo basada en el uso de una matriz bidimensional que parametrice la probabilidad de ocurrencia de un suceso en combinación con sus consecuencias (Ortiz Alulema, 2020). Para tal efecto, se plantea el cálculo del riesgo, a través de los parámetros propuestos por Cox, Babayev y Huber, en el que se asignan valores porcentuales ponderando, en el eje de las abscisas, la probabilidad de que un suceso ocurra, basado en el histórico estadístico y, en el eje de las ordenadas, las consecuencias del suceso, con un crecimiento exponencial dada la siniestralidad esperada (Cox et al., 2005), tal como se ejemplifica en la Figura 7.

Vale la pena distinguir dos grandes dimensiones de riesgo en el uso de criptoactivos: a) el riesgo de ciberseguridad/criptoseguridad; y b) el riesgo financiero. Ambos deben analizarse por separado, aunque luego se vuelven mutuamente operativos, planteando diversos escenarios.

En primer lugar, pueden establecerse dos categorías de usuarios de criptoactivos: los que están adecuadamente informados sobre el correcto uso técnico y de las prevenciones de seguridad, y aquellos que son tan entusiastas como incautos en el campo. Del primer tipo, según lo que se ha demostrado en apartados previos, la probabilidad de verse envueltos en una vulneración es muy baja, pudiéndose ubicar en la categoría de «remoto»; al respecto, dado que es un grupo de usuarios informados, estos toman precauciones de diversificación adicional a los aspectos de seguridad, por lo que las consecuencias (de llegarse a dar) podrían clasificarse como «marginales», arrojando un cruce de un riesgo de seguridad del 1 %, lo cual es completamente aceptable según la propuesta de Cox, Babayev y Huber. Ya en el campo financiero, el riesgo de ocurrencia podría clasificarse en «esporádico»

Figura 7

Matriz de Riesgo Financiero parametrizada según la Norma ISO 31000

Valor	Nivel	Magnitud de vulnerabilidad					
1	Constante	2,00%	4,00%	10,00%	20,00%	40,00%	100,00%
2	Habitual	1,75%	3,50%	8,75%	17,50%	35,00%	87,50%
3	Frecuente	1,50%	3,00%	7,50%	15,00%	30,00%	75,00%
4	Moderado	1,25%	2,50%	6,25%	12,50%	25,00%	62,50%
5	Ocasional	1,00%	2,00%	5,00%	10,00%	20,00%	50,00%
6	Esporádico	0,75%	1,50%	3,75%	7,50%	15,00%	37,50%
7	Remoto	0,50%	1,00%	2,50%	5,00%	10,00%	25,00%
8	Improbable	0,25%	0,50%	1,25%	2,50%	5,00%	12,50%
Consecuencias		Insignificante	Marginal	Grave	Crítico	Desastroso	Catastrófico
Valor		1	2	4	8	16	32

Aceptable Tolerable Inaceptable Inadmisible

Nota. Elaboración propia con datos de Cox et al., 2005.

y las consecuencias en «marginales», dadas las múltiples medidas de mitigación aplicadas, las cuales dejan un promedio global de riesgo del 1.25 %, completamente en el margen de lo aceptable.

En cambio, el segundo tipo, debido a la desinformación y falta de precauciones, está notablemente más expuesto al riesgo. Las cifras de INTERPOL arrojan una oscilación entre el 46 % y el 55 % de incidencia de ciberestafas con respecto al total (Aguilar-Antonio, 2020; López Fonseca, 2019), agravado por la ausencia de planes educativos sobre el tema (Ordóñez Sánchez, 2021), es factible afirmar que la probabilidad de ocurrencia se situaría en «moderado», con unas consecuencias «catastróficas» en tanto que la falta de información impide que se tomen medidas de mitigación extra. En tal sentido, para el ciudadano común, el uso de criptoactivos representa un riesgo de seguridad del 62.5 %, pasando al rango de lo inaceptable según el planteamiento de Cox, Babayev y Huber.

Ya en el campo del riesgo financiero, la posibilidad de ocurrencia y profundidad de consecuencia para un usuario sin educación especializada en el manejo de criptoactivos irá modificándose según diversos escenarios planteados, para luego promediarse con el riesgo de seguridad del 62.5 % anteriormente planteado, en una operación de media aritmética (Figura 8).

1 Usuario sin educación especializada en el manejo de criptoactivos que realizare inversión con cartera diversificada; su posibilidad de un imprevisto financiero podría clasificarse como «moderada» con consecuencias «marginales» en tanto que la diversificación le generaría una protección de liquidez. En tal sentido, su riesgo financiero sería del 2.5 %, esto al promediarlo con su riesgo de seguridad, resultaría en 32.5 % de riesgo global en el uso de criptoactivos, lo cual es clasificado por Cox, Babayev y Huber como «inadmisible».

2 Usuario sin educación especializada en el manejo de criptoactivos que realizare inversión sin cartera diversificada: la posibilidad de un imprevisto financiero podría clasificarse como «moderada» con

Figura 8

Porcentaje de riesgo ponderado en el uso de criptoactivos según nivel de educación especializada en el ramo y condiciones agravantes

1.25 % de riesgo ponderado en el uso de criptoactivos para un usuario debidamente educado especializadamente en el ramo.

32.5 % de riesgo ponderado en el uso de criptoactivos con inversión en cartera diversificada para un usuario sin educación especializada en el ramo.

37.5 % de riesgo ponderado en el uso de criptoactivos con inversión en cartera no diversificada para un usuario sin educación especializada en el ramo.

75.0 % de riesgo ponderado en el uso de criptoactivos como moneda de curso legal con cartera no diversificada para un usuario sin educación especializada en el ramo.

Nota. Elaboración propia con promedios basados en Cox et al., 2005.

consecuencias «críticas» ya que no gozaría de la protección que brinda la diversificación. En tal sentido, su riesgo financiero sería del 12.5 %, lo cual, promediado con su riesgo de seguridad, marcaría un 37.5 % de riesgo global en el uso de criptoactivos, esto es clasificado por Cox, Babayev y Huber como «inadmisible».

3 Usuario sin educación especializada en el manejo de criptoactivos como moneda de curso legal sin cartera diversificada: la posibilidad de un imprevisto financiero podría clasificarse como «habitual»" ya que estaría usando un instrumento financiero con un fin para el cual no fue diseñado (Asto Paredes & Villavicencio Flores, 2019); además, las consecuencias serían «catastróficas»" en tanto que no gozaría de la protección brindada por la diversificación y tendría que sostener la fluctuación con músculo financiero propio, tomado de su capital operativo. En tal sentido, su riesgo financiero sería del 87.5 %, esto, promediado con su riesgo de seguridad, marcaría un 75.0 % de riesgo global en el uso de criptoactivos, lo cual es clasificado por Cox, Babayev y Huber como «inadmisible».

Por tanto, como resulta evidente en la Figura 8, el manejo de criptoactivos solamente se mantiene dentro de los márgenes de seguridad aceptables cuando el usuario tiene educación especializada en el manejo de tales activos financieros, tanto en las dimensiones de ciberseguridad, criptoseguridad y gestión del riesgo financiero. En cambio, al haber ausencia de esa educación especializada, la condición se vuelve indefectiblemente riesgosa hasta el grado de la inadmisibilidad, agravándose con condiciones extra que suponen prácticas inadecuadas en el manejo de los criptoactivos.

CONCLUSIONES

El uso de criptoactivos es creciente y acelerado, por lo que es ilusorio pensar que no van a posicionarse en la cúspide de las relaciones monetarias en algún tiempo; de hecho, en pleno 2022 ya ocupan una porción importante del mercado, retando a los gobiernos en su soberanía monetaria. En tal sentido, huir de ellos sería un error estratégico para cualquier inversionista; sin embargo, la gestión del riesgo debe ser meticulosa y con cambios estructurales profundos en la sociedad.

Un inicio sano sería la educación en criptofinanzas desde la enseñanza básica, de tal manera que sea la generación nativo-digital la que lidere el proceso de inclusión conceptual en el ideario colectivo. La falta de comprensión técnica de los criptoactivos facilita todo tipo de estafas y ciberdelitos, debe iniciarse por combatir la ignorancia para que el futuro del dinero se acerque sin dejar estragos colaterales, muy especialmente en aquellas sociedades tradicionalmente más vulnerables producto de su bajo nivel educativo (Ordóñez Sánchez, 2021).

Desde luego, no se está hablando de un curso libre en las universidades ni de una charla en las secundarias; más bien se trata de un agresivo plan de educación técnica integral que prepara las generaciones para encarar cambios desde lo informático hasta lo financiero, incorporando las buenas prácticas en el quehacer comercial cotidiano. Este tipo de educación hallará, con plena seguridad, severa resistencia entre los sectores más conservadores de los sistemas tradicionales, considerándole como un desmán estrafalario en detrimento de otras ramas de las ciencias que habitualmente ocupan la currícula. En tal sentido, sin demeritar la importancia de conocer sobre la célula eucariota, por mencionar un ejemplo, el joven educando requerirá más inmediatamente la educación criptofinanciera que tales conocimientos especializados de biología, los cuales probablemente podrá adquirir más adelante, sin que esto le represente un riesgo tan latente como ignorar el funcionamiento del mercado que le apremia.

Si bien la educación desde la base es la alternativa más viable, los resultados pueden demorar, condenando a muchos adultos a la debacle financiero producto de su entusiasmo por los criptoactivos. Para efectos de inmediatez, y sin descuidar el largo plazo, los gobiernos deben establecer normas y programas de gestión de riesgo en las criptofinanzas, amortiguando el uso de activos volátiles en extremo y presionando hacia la concientización colectiva de que, si bien el tema resulta atractivo y prometedor, se requiere de un conocimiento profundo para obtener resultados positivos.

REFERENCIAS

Aguilar-Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de Estudios en Seguridad Internacional*, *6*(2), 17-43. https://doi.org/10.18847/1.12.2

Alvarez-Pincay, D. E., Toala-Bozada, S. P., Delgado-Gutierrez, Z. M., Peñafiel-Loor, J. F., Lucio-Pillasagua, A. del J., & Saltos-Buri, V. del R. (2018). Sistemas de Contabilidad con Criptomonedas: Retos para la Auditoría Pública Tradicional. *Polo del Conocimiento*, *3*(8), 196. https://doi.org/10.23857/pc.v3i8.607

Asto Paredes, N., & Villavicencio Flores, M. (2019). *¿Las criptomonedas deben ser consideradas dinero?* [Universidad Peruana de Ciencias Aplicadas]. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/626341/Asto_PN.pdf?sequence=1

Barroilhet, A. (2019). Criptomonedas, economía y derecho. *Revista Chilena de Derecho y Tecnología*, *8*(1), 29. https://doi.org/10.5354/0719-2584.2019.51584

Bermúdez Pacheco, D., Guarín Avella, N., & Rojas Camargo, S. (2021). *Avances e impacto generado tras la circulación de las criptomonedas en la negociación de los mercados financieros* [Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/bitstream/20.500.12494/36440/3/2021_avances_impacto_generado.pdf

Bravo de Mansilla, G., Torres Gutiérrez, J. J., & Jiménez, J. I. (2000). *La gestión del riesgo financiero*. Pirámide.

Cabrera Soto, M., & Lage Codorniu, C. (2022). Criptomonedas: ¿qué son y qué pretenden ser? *Economía y Desarrollo*, *166*(1). http://scielo.sld.cu/scielo.php?script=sci_rttext&pid=S0252-85842022000100008

CEPAL. (2021). *Marco de referencia para los sistemas estadísticos de seguridad y justicia penal en América Latina y el Caribe*. Undécima Reunión de la Conferencia Estadística de las Américas de la Comisión Económica para América Latina y el Caribe, Reunión Virtual. https://repositorio.cepal.org/bitstream/handle/11362/47463/1/S2100701_es.pdf

Cheng, A. (2021). 'Squid Game'-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam. *The Washington Post*. https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/

Cheung, W.-K., Roca, E., & Su, J.-J. (2015). Crypto-currency bubbles: An application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics*, *47*(23), 2348-2358. https://doi.org/10.1080/00036846.2015.1005827

Cox, L. A. (Tony), Babayev, D., & Huber, W. (2005). Some Limitations of Qualitative Risk Rating Systems. *Risk Analysis*, *25*(3), 651-662. https://doi.org/10.1111/j.1539-6924.2005.00615.x

Díaz Gutiérrez, Y., & Cueva Lovelle, J. M. (2018). Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos. *Redes de Ingeniería*, *9*(2), 82-87. https://doi.org/10.14483/2248762X.14383

Domínguez, P. E., López, M. I., Rivera, N. E., & Sandoval, K. M. (2019). *Uso de criptomonedas como alternativa de alivio financiero al endeudamiento externo salvadoreño*. Aequus. http://ri.ues.edu.sv/id/eprint/21056/1/Libro%20digital%20Criptomonedas1.pdf

Engler, A. (2021). Hackers roban identidades con el sistema de verificación de la Chivo Wallet en El Salvador. *CoinDesk Insights*. https://www.coindesk.com/business/2021/11/01/hackers-roban-identidades-con-el-sistema-de-verificacion-de-la-chivo-wallet-en-el-salvador/

Eterovic, J., Cipriano, M., García, E., & Torres, L. (2020). *Seguridad en Internet de las Cosas usando soluciones Blockchain*. 823-828. http://sedici.unlp.edu.ar/bitstream/handle/10915/104030/Documento_completo.pdf?sequence=1

Fernández, R. (2022). Criptomonedas—Datos estadísticos. *Statista*. https://es.statista.com/temas/8092/criptomonedas/#dossierKeyfigures

Gabela Salvador, R. (2019). *Criptomonedas como medios comisorios de delitos de estafa y lavado de activos: Mecanismos para impedir el uso delictivo de las criptomonedas* [Universidad San Francisco de Quito]. http://repositorio.usfq.edu.ec/jspui/bitstream/23000/8401/1/143605.pdf

García-Ramos Lucero, M. Á., & Rejas Muslera, R. (2022). Análisis del desarrollo normativo de las criptomonedas en las principales jurisdicciones: Europa, Estados Unidos y Japón. *Universitat Oberta de Catalunya*, *35*, 2-13.

Hamurcu, Ç. (2022). Can Elon Mask's Twitter Posts About Cryptocurrencies Influence Cryptocurrency Markets by Creating a Herding Behavior Bias? *Fiscaoeconomia*, *6*(1), 2015-2228.

Linares-Morales, J. (2021). Una mirada desde el sur al tema de la ciberseguridad.

IPSA Scientia, revista científica multidisciplinaria, *6*(1), 123-124. https://doi.org/10.25214/27114406.1073

López Fonseca, Ó. (2019). *Cuatro veces más ciberestafas*. https://elpais.com/politica/2019/02/09/actualidad/1549712764_503144.html

López Gutiérrez, J., Sánchez Jiménez, F., Herrera Sáncez, D., Martínez Moreno, F., Rubio García, M., Gil Pérez, V., Santiago Orozco, A. M., & Gómez Martín, M. Á. (2020). *Estudio sobre la cibercriminalidad en España* (pp. 1-62). Ministerio del Interior del Gobierno de España. http://www.interior.gob.es/documents/10180/11389243/rcriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3

Manrique Morales, C. A., & Pedraza Castañeda, D. S. (2019). Impacto en el déficit fiscal de Colombia durante el 2017 a partir de una regulación tributaria sobre las operaciones realizadas con el criptoactivo Bitcoin. *Fundación Universitaria Empresarial de la Cámara de Comercio de Bogotá*, 2-23.

Mena Roa, M. (2021). Los pagos de rescate con criptomonedas por ataques ransomware se dispararon en 2020. *Statista*. https://es.statista.com/grafico/25240/valor-total-de-las-criptomonedas-recibidas-por-direcciones-de-ransomware--en-mill-de-dolares-%252A/

Muni, P. (2021). Squid Coin: A Crypto Scam That Robbed Investors Off $3.38 Million. *The Logical Indian Crew*. https://thelogicalindian.com/technology/squid-coin-32078

Narosky, S. (2022). Ciberestafas y esquemas Ponzi a la orden del día: Las más comunes y los errores más frecuentes que cometen usuarios y ahorristas. *Infobae*. https://www.infobae.com/economia/2022/01/22/ciberestafas-y-esquemas-ponzi-a-la-orden-del-dia-las-mas-comunes-y-los-errores-mas-frecuentes-que-cometen-usuarios-y-ahorristas/

Nieves, V. (2021). Los cinco grandes riesgos de invertir en criptomonedas como el bitcoin, según la CNMV y el Banco de España. *El Economista*. https://www.eleconomista.es/mercados-cotizaciones/noticias/11039982/02/21/El-Banco-de-Espana-y-la-CNMV-revelan-los-cinco-grandes-riesgos-de-invertir-en-criptomonedas-como-Bitcoin.html

Ochoa, D. (2021). El costo del cibercrimen alcanzará los 8 billones de dólares en 2022. *Expansión*. https://expansion.mx/tecnologia/2021/12/07/el-costo-del-cibercrimen-alcanzara-los-8-billones-de-dolares-en-2022

Ordinas, M. (2017). Las criptomonedas: ¿Oportunidad o burbuja? *BancaMarch*. https://www.bancamarch.es/recursos/doc/bancamarch/20170109/2017/informe-mensual-de-estrategia-octubre-2017.pdf

Ordóñez Sánchez, S. G. (2021). Educación financiera basada en el bitcoin y la inclusión en planes de estudio. *RIDE Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *11*(22). https://doi.org/10.23913/ride.v11i22.973

Ortiz Alulema, I. D. (2020). *Implementación de la Norma ISO 31000 en la administración del riesgo de lavado de activos y el financiamiento del terrorismo, en bancos privados* [Universidad Andina Simón Bolívar]. https://felaban.s3-us-west-2.amazonaws.com/coplaft/monografias/ganadores/2018/Monografia%20COPLAFT%20Dr%20

Ivan%20Danilo%20Ortiz.pdf

Oxman, N. (2013). Estafas informáticas a través de Internet: Acerca de la imputación penal del «phishing» y el «pharming». *Revista de Derecho (Valparaíso)*, *41*, 211-262. https://doi.org/10.4067/S0718-68512013000200007

Parra Tabares, B. (2019). *Las criptomonedas: Una nueva modalidad de lavado de activos en Colombia* [Universidad Militar de Nueva Granada]. https://repository.unimilitar.edu.co/bitstream/handle/10654/32161/ParraTabaresErikaBrigette2019.pdf?sequence=1&isAllowed=y

Perafán, L. (2019). *Evaluación actual del mercado de las criptomonedas*. Universidad Autónoma de Occidente de Cali. https://red.uao.edu.co/bitstream/10614/10947/5/T08508.pdf

Pilacuán Cadena, J., Espinoza Herrera, X., Carreño Llaguno, S., & Palacios Alcivar, B. (2021). Criptomonedas: Funcionamiento, oportunidades y amenazas: Cryptocurrency: Operation, opportunities and threats. *Res Non Verba Revista Científica*, *11*(2), 174-193. https://doi.org/10.21855/resnonverba.v11i2.604

Pulido López, P. (2021). *El crecimiento del comercio electrónico. Repercusión en el comercio tradicional* [Universidad de Sevilla]. https://idus.us.es/bitstream/handle/11441/129451/2020-21-161-47392568-2-PULIDO_LOPEZ_P.pdf?sequence=1&isAllowed=y

Raya, A. (2021). Cuidado con el nuevo robo de criptomonedas: Sospecha si te dan esto. *El Economista*. https://www.eleconomista.es/tecnologia/noticias/11283270/06/21/Cuidado-con-el-nuevo-robo-de-criptomonedas-sospecha-si-te-dan-esto.html

Rocohano Ramos, R. G., & Silva Ordóñez, L. D. (2021). *Comportamiento de las personas para evitar ser víctimas de ataques de ingeniería social* [Universidad de las Fuerzas Armadas]. http://repositorio.espe.edu.ec/bitstream/21000/25916/1/T-ESPESD-003164.pdf

Rosero Gomezcoello, J. M. (2020). *Detección y mitigación de ataques de ingeniería social tipo Phishing utilizando minería de datos* [Universidad de las Fuerzas Armadas]. http://repositorio.espe.edu.ec/bitstream/21000/23409/1/T-ESPE-044176.pdf

Ruani, H. M. (2020). Los Estados, las criptomonedas y la ciberseguridad. *Revista Mexicana de Ciencias Penales*, *3*(10), 111-125.

Ruíz Rosas, M., & Décaro Santiago, L. (2019). Las burbujas financieras y el nacimiento del mercado de las criptomonedas. *Revista Ciencia Administrativa*, *1*. https://www.uv.mx/iiesca/files/2019/10/14CA201901.pdf

Sachdeva Keswani, A., López Rodríguez, S., & Pérez Acosta, C. (2021). *Las criptomonedas en el sistema económico y financiero* [Universidad de La laguna]. https://193.145.118.245/xmlui/bitstream/handle/915/24759/Las%20criptomonedas%20en%20el%20sistema%20economico%20y%20financiero.%20.pdf?sequence=1&isAllowed=y

Sánchez Torres, J. A., & Arroyo Cañada, F. J. (2016). Diferencias de la adopción del comercio electrónico entre países. *Suma de Negocios*, *7*(16), 141-150. https://doi.org/10.1016/j.sumneg.2016.02.008

Sartor, L. (2019). *Criptomonedas y la tecnología Blockchain* [Universidad Siglo 21]. https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/18407/Sartor_

Lucas_TFG%20-%20Lucas%20Sartor.pdf?sequence=1

Secretaría General de INTERPOL. (2020). *Ciberdelincuencia: Efectos de la COVID-19*. INTERPOL. https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

Soto Galindo, J. (2020). La pandemia cambió el comercio electrónico para siempre. *El Economista*. https://www.eleconomista.com.mx/opinion/La-pandemia-cambio-el-comercio-electronico-para-siempre-20201109-0057.html

Steenkamp, J.-B. E. M., & Ter Hofstede, F. (2002). International market segmentation: Issues and perspectives. *International Journal of Research in Marketing*, *19*(3), 185-213. https://doi.org/10.1016/S0167-8116(02)00076-9

Tapscott, D., & Tapscott, A. (2018). *Blockchain revolution*. Penguin Supports.

Ventura, V. (2021). ¿Por qué se hunde el bitcoin? La «madre de todas las burbujas» que alentó el "tether" deja caídas del 20%. *El Economista*. https://www.eleconomista.es/divisas/noticias/10985674/01/21/Por-que-se-hunde-el-bitcoin-La-madre-de-todas-las-burbujas-que-alento-el-tether-deja-caidas-de-mas-del-20.html