Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

CARRERA DE ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

TRABAJO FINAL DE ESPECIALIZACIÓN

Desafíos de la tecnología Blockchain: su relación con el crimen organizado durante la pandemia de COVID-19 en Argentina

AUTOR: LIC. SANDOVAL FERNANDO DANIEL

DOCENTE DEL TALLER:
CTE. GRAL. GN(R) LIC. LUIS PIBERNUS
DIRECTOR DE CARRERA:
CTE. GRAL. GN(R) DR. JOSE RICARDO SPADARO

JULIO 2022

Resumen

En el presente trabajo se analiza descriptivamente la problemática de la implementación de la tecnología Blockchain y sus derivados relacionados con el crimen organizado en el país de Argentina durante el periodo del aislamiento obligatorio por la pandemia del COVID-19.

Para ello, en principio se puso el foco en explorar y recolectar información de distintas fuentes abiertas digitales, luego se realizó una evaluación de pertinencia a la temática abordada.

A partir del trabajo de investigación, se redactó el marco teórico con las concepciones principales para el abordaje integral del tema propuesto, proponiendo un enfoque desde la perspectiva de la Inteligencia Estratégica y Criminal en el campo de la seguridad pública.

Se incorporaron una selección de casos de investigación judicial de la actualidad como antecedentes de la relación entre la tecnología Blockchain y el crimen organizado en el país.

Por último se abordó una conclusión preliminar del trabajo investigativo y se consideraron algunos instrumentos para la comprensión integral de la temática, con el objetivo de asesorar a los agentes y funcionarios que trabajan en el tema, considerando que una información actualizada es fundamental para una correcta toma de decisión.

Palabras claves: BLOCKCHAIN – INTELIGENCIA ESTRATEGICA – CRIMEN ORGANIZADO

Índice

1. Introducción

Fundamentación

En la actualidad, el mundo está atravesando quizás unas de las mayores crisis en la historia de la humanidad a causa de la pandemia Covid- 19 que surgió a finales del año 2019. Esta situación de emergencia sanitaria acarrea drásticas consecuencias que ponen en jaque la continuidad de la humanidad por la globalización y transnacionalización del virus, que funcionó como catalizador de las distintas crisis sociales políticas y culturales preexistentes en el mundo.

Una de estas consecuencias es la agudización de las crisis económicas y sociales en varios países. En Argentina, particularmente, mientras esta situación se desplegaba se fue resintiendo la desigualdad social y económica, con el aumento de la pobreza y el desempleo, materializándose en cierres de centenares de empresas y comercios locales.

Paradójicamente la digitalización del dinero y el comercio electrónico favoreció el ecosistema de los cripto activos, que fue ganando mayor uso y dominancia en las personas en busca de una salida rentable a sus situaciones financieras particulares debido al fomento del uso de billeteras digitales y transacciones virtuales para evitar el contacto con el billete papel con el fin de disipar la transmisión del virus COVID-19.

En el caso de las organizaciones del crimen organizado, con la intención de seguir avanzado en sus objetivos, éstas se adaptaron a esta nueva modalidad financiera para seguir llevando a cabo sus actividades delictivas, incluso explorando nuevas técnicas de estafas en las nuevas circunstancias.

Planteamiento del problema

El proyecto se realizó en el marco de un trabajo integrador de investigación del posgrado Inteligencia Estratégica y Crimen Organizado de la Universidad de Buenos Aires. La pregunta que nos orientó en la investigación gira en torno a ¿cuáles son las problemáticas de la tecnología Blockchain en el contexto particular de Argentina durante la declaración de la pandemia del COVID-19?

Al mismo tiempo, se indagó ¿cuál sería su impacto en la Seguridad Interior del Estado-Nación? Es decir, cómo es su relación con el crimen organizado.

Ya que en la actualidad se carece de una regulación normativa clara y concreta por parte de los distintos organismos gubernamentales para el tratamiento de las problemáticas relacionadas con los *criptoactivos* abordamos dichas preguntas con el fin de indagar sobre la creciente popularidad que adquirió la tecnología Blockchain y sus *criptoactivos*.

Aspectos metodológicos

El presente proyecto de investigación se realizó desde un enfoque descriptivo-exploratorio de tipo cualitativo, con el fin de poder indagar sobre las dimensiones propuestas para el tema de la tecnología Blockchain y sus derivados.

Se consideró como unidad de análisis a los derivados de la Blockchain: las criptomonedas, en su dimensión económica financiera como variable de uso en la sociedad.

Para ello, se recolectaron y analizaron los datos obtenidos de diversas fuentes de información abiertas y digitales. A saber:

Fuentes primarias: se consideraron los documentos e informes emitidos por organismos gubernamentales y no gubernamentales.

Fuentes secundarias: los trabajos de investigaciones académicas compartidas por instituciones educativas públicas y privadas.

Y por último, los reportes periodísticos de comunicadores de distintos medios de comunicación que estén relacionados con la temática propuesta.

2. Marco teórico

Con el fin de otorgar sustento teórico al trabajo investigativo proponemos las principales concepciones como marco de referencia para abordar las problemáticas de la tecnología Blockchain en relación al crimen organizado en Argentina.

La Guerra Irrestricta

Como herramientas conceptuales retomamos el enfoque desarrollado por los coroneles Qiao Liang y Wang Xiangsui (1999) en su texto *La guerra más allá de los límites*. Estos autores proponen que en la actualidad de la época moderna, las sociedades vivenciamos nuevos descubrimientos tecnológicos y progresos técnicos de modo acelerado en un periodo corto de tiempo. Asimismo consideran que se abrió una "caja de pandora" en el desarrollo tecnológico donde no se avizora un claro horizonte en sus usos para la humanidad, ni tampoco quién será el responsable del uso y control de dichas tecnologías en los distintos ámbitos de aplicación, considerando las biotecnologías, las nanotecnologías y las tecnologías de la información entre otras.

Los autores Qiao Liang y Wang Xiangsui (1999) reportan que esta diversificación tecnológica constante y acelerada produce nuevos campos de aplicación donde se ensayan los distintos usos individuales e independientes que puede tener una invención tecnológica combinando las viejas tecnologías con las nuevas. Produciendo un "efecto de ramificación" que hace que se vinculen las distintas tecnologías entre sí, creando a su vez nuevas tecnológicas continuamente por medio de la unión; perdiendo de vista los objetivos del para qué y cuál es la necesidad que satisface dicha innovación creando un sinfín en sí mismo. Fusionando así todos los aspectos de la vida, incluso el de la guerra. Este fenómeno altera el modo en el que la humanidad se vincula con lo tecnológico y complejiza su relación, lo que convoca a adoptar un nuevo enfoque en relación a los asuntos estratégicos y militares.

La Cadena de Bloques (Blockchain)

En relación a la definición de la tecnología Blockchain, tomaremos la propuesta por Fernando Navarro Cardoso en su artículo Criptomonedas y blanqueo de dinero (2019). Allí define a la tecnología Blockchain como la columna vertebral que sostiene a todo el ecosistema de criptomonedas y sus derivados. Esta tecnología consiste en una cadena de bloques de información grabada y almacenada simultáneamente por los distintos usuarios que participan de la misma red en una determinada plataforma.

Dicha información que pueden ser datos o códigos criptográficos, es pública y se encuentra distribuida de manera descentralizada a través de los distintos nodos, que son constituidos por las máquinas o servidores de los participantes quienes resguardan a modo de notarios públicos o escribanos toda la información del tráfico y las transacciones realizadas en la red en un determinado periodo de tiempo. Lo que conforma un registro digital distribuido.

Así mismo este proceso de grabado y almacenamiento de datos exige que deben ser verificados por otros usuarios o servidores que ofrecen su poder de cómputos (Hash) para realizar la validación y resolución de cada bloque de información que incluye el historial de transacción de cada bloque anterior de la cadena, por lo que se va complejizando el algoritmo a medida que se suman bloques (paquetes de información) a dicha red. Por dicho proceso, llamado técnicamente como Prueba de Trabajo (POW) reciben una recompensa por prestar sus servicios o poder de cómputos, esta recompensa es una criptomoneda o token según la red o plataforma en la que se opera.

Aquí comienza otra dimensión de esta tecnología y sus derivados: los cripto activos. Estos pueden ser monedas digitales, criptomonedas, tokens, NFT entre otros. Poseen características particulares dentro de su propio ecosistema que son aceptadas por consenso entre las personas/ usuarios que forman parte del universo cripto.

Estas características son: pueden considerarse como reserva de valor, tiene un valor de intercambio, son intercambiables por otros productos o servicios dentro del ecosistema. Lo que permite el uso similar al del dinero fíat (papel moneda), incluso algunas están ancladas y representan 1 a 1, como por ejemplo el valor nominal del dólar norteamericano (USD) que son las denominadas Stablecoins, por considerar sus fluctuaciones y volatilidad más estables

que el resto.

El Crimen Organizado

También nos proponemos trabajar con la definición de Crimen Organizado como la actividad criminal que desarrolla un Grupo Criminal Organizado definido y caracterizado por la Convención de Palermo (2000) entendida en su Artículo 2º como:

"un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material".

La Inteligencia Estratégica

Para seguir trabajando, proponemos la conceptualización de la Inteligencia Estratégica como un proceso metódico y sistemático de recolección, evaluación y análisis de información con la finalidad de producir conocimiento útil y veraz para la toma de decisiones en el alto rango de conducción (Spadaro, 2016).

Este proceso es denominado "Ciclo de producción de inteligencia" y consta de varias fases:

1) Dirección: se planifican y organizan los elementos esenciales de información sobre el objeto de interés.

2) Obtención: se obtiene y recolecta toda la información requerida mediante distintas fuentes.

3) Análisis: Se procesan, integran y analizan los datos obtenidos.

4) Difusión: Se comunica y difunde los productos obtenidos cumpliendo con protocolos de confidencialidad y seguridad.

5) Retroalimentación: Se realiza un proceso de retroalimentación (feedback) para fortalecer el ciclo y la calidad de la inteligencia.

A partir de estas fases detalladas se obtiene el conocimiento necesario para la toma de decisión y su consecuente curso de acción en un determinado escenario o hecho concreto.

Dicho producto de inteligencia es el objeto de estudio que fundamenta la doctrina de la inteligencia para la obtención de la verdad que se intentó disimular mediantes técnicas de velo y engaño. (Spadaro 2016).

Asimismo, en Argentina en el año 2015 se restablece el marco jurídico y normativo para la producción de inteligencia y la creación de un organismo gubernamental centralizado denominado Agencia Federal de Inteligencia. Donde se especifica en su Artículo 2 que las actividades de la Inteligencia Nacional son:

"(...) la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación." (Ley 27.125)

La Inteligencia Criminal

La Ley de Inteligencia Nacional Nº 25.520 en su Art 2 inciso 3 propone la definición de inteligencia criminal como: *"la parte de la inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten a la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional".*

Esta misma Ley crea la Dirección Nacional de Inteligencia Criminal (DNIC) como organismo oficial encargado de producir conocimiento accionable a nivel operativo destinada a las fuerzas de seguridad (FFSS) con el fin de afrontar delitos complejos en el área de la seguridad publica en el marco de la seguridad interior.

Tal como menciona Evans (2018), los organismos de inteligencias deben tener el rol de encargados de producir un conocimiento que sea accionable, que sea capaz de informar sobre los riesgos concretos en los que se encuentran los ciudadanos. Dicho conocimiento debe contribuir al decisor a la reducción de la incertidumbre y a su consecuente toma de decisión para la prevención y lucha del Crimen Organizado en el ámbito de la seguridad pública.

Retomando al autor, la producción de inteligencia es un instrumento necesario para la gestión estatal de la lucha contra el Crimen Organizado en virtud de producir el conocimiento accionable necesario que permita entender los vínculos criminales, así cooperar en la toma

de decisión y su operatividad mediante el uso de las fuerzas de seguridad. Para la investigación de delitos complejos, es necesaria una intervención compleja, por la composición y sus actividades ilícitas de las organizaciones criminales en distintos territorios del país. Esto implicaría un perfil del analista de inteligencia más generalista, más diverso en conocimientos y en su formación actualizada.

3. Diagnóstico

A partir del trabajo análisis de datos relevados de las distintas fuentes primarias y secundarias obtenidas se produjo un diagnóstico situado sobre los diversos usos de la tecnología Blockchain y sus derivados en distinto campos de aplicación. Cabe recordar que los usuarios de esta tecnología siguen en fase de exploración para proyectar perspectivas de innovación y resolver problemáticas surgidas de su uso.

3.1 Perspectivas de uso y campos de aplicación

Dentro de las perspectivas se pueden visualizar varias aristas de la implementación de la cadena de bloques para múltiples usos que hasta la actualidad se siguen examinando. Desde la industria financiera descentralizada, los criptoactivos, el criptoarte, los No Fungible Token (NFT) en el gaming, la identidad auto soberana, la inteligencia artificial, los contratos inteligentes para realizar pólizas o certificar transacciones en las cadenas de producción, entre otros.

El potencial de la tecnología Blockchain aún está en exploración y experimentación de distintos usos y aplicación. Entre los más desarrollados se encuentran los usos ligados a la industria financiera, relacionadas a la actividad del intercambio de divisas. Esto supone establecer una red de transacción de personas a personas (P2P) mediante plataformas digitales que ofrecen servicios de compra y venta de activos a cambio de una comisión, para generar ingresos o rentabilidades a partir de la inversión (Nakamoto, 2008).

En relación al NFT implica un token criptográfico que contiene información sobre un archivo digital y su propietario registrado en una cadena de bloques, su función se relaciona con dar certificación digital de autenticidad del archivo y su transacción. Cuando

el contenido de ese archivo digital está ligado a una expresión artística, se habla de Criptoarte, entendida con una expresión moderna del arte a través del medio digital que puede ser desde contenidos visuales a no visuales la creación digital de un dibujo, un escrito, un meme, personajes de colección, poemas, composiciones musicales, etc.

También encontramos usos en la industria de los videojuegos y el gaming íntimamente relacionadas con el NFT. Ya que varias empresas dedicadas a esta industria venden los personajes y accesorios de sus juegos a través de plataformas en formato de token criptográfico. Donde los usuarios reciben recompensas por jugar los juegos de modo online y sostenido en el tiempo, generalmente en cois o tokens creados para esa comunidad gaming que tienen un valor económico en el mercado cripto y puede ser intercambiable por divisas. (Qin Wang, 2021)

Otro caso de uso frecuente es el contrato inteligente (Smart Contract). Es una herramienta digital que se programa sobre la Blockchain para ser auto-ejecutado, implica realizar las acciones pautadas cuando se cumplen determinados requisitos acordados por dos o más partes intervinientes. Su función es similar a la de un contrato o convenio tradicional, con la salvedad de que no es necesario un escribano o tercero físico que certifique la veracidad y cumplimiento de lo acordado.

Al formalizar un contrato inteligente toda la información queda almacenada y certificada de manera segura e inmutable sobre la cadena de bloques para que cualquier persona interviniente pueda tener acceso a dicha información acordada. Cuando se cumplen los requisitos formalizados, dicha herramienta puede generar las acciones programadas: como por ejemplo retener, recolectar, transferir o depositar activos o información a determinada dirección o cuenta. Actualmente el uso de los contratos inteligentes está enfocado a pólizas de seguros relacionados con distintas áreas pero principalmente agrícolas, ganaderas y en producción de alimentos industrializados a gran escala. (García Álvarez, 2020)

En lo respectivo a la Inteligencia Artificial (IA), que es una rama de las ciencias computacionales que se encarga de estudiar diversos modelos de cómputos capaces de realizar tareas propias del ser humano: relacionadas con el razonamiento y la conducta para automatizar actividades y procesos.

Su relación con la tecnología de cadena de bloques se encuentra en una fase exploratoria en la experimentación de programas informáticos de machine learning donde el Bot, es un artificio informático que monitorea, analiza, identifica patrones de datos y aprende de manera automática para optimizar la toma decisiones por sí mismo, reduciendo la intervención de una persona física.

Con relación al uso de la Identidad Auto Soberana hace referencia a un modelo de identidad digital en donde cada persona es la encargada y responsable como usuario de administrar las credenciales de sus datos personales pudiendo elegir que datos compartir para que sea verificados de manera descentralizadas sobre una red de Blockchain, sin tener la necesidad de depender de un tercero como ente centralizado verificador. Es un cambio de paradigma, en relación a la descentralización de la emisión y validación de credenciales de identidad de un individuo, que implica infraestructura tecnológica (hardware) e informática (software) como así también la educación y adopción de usos de billeteras electrónicas y firma digital entre otras herramientas (Alamillo 2019).

En el caso de Argentina, se encuentra el Proyecto Identidad Digital para la Inclusión (DIDI) que realizó experiencias territoriales en barrios populares como también eventos digitales (hackaton) para el desarrollo y exploración de usos de la identidad auto soberana. Con el objetivo de empoderar a las personas con vulnerabilidad, excluidas del sistema bancario tradicional sobre el uso y la administración de su identidad junto con sus datos digitales para el acceso a servicios financieros. Particularmente, en el marco del Proyecto DIDI en colaboración con ONG Bitcoin Argentina y el laboratorio del Banco Interamericano de Desarrollo (BID Labs), durante el 2021 se realizó un evento digital denominado “ID hackathon” que duró cuatro semanas. Este evento implica el encuentro de una comunidad de hackers o programadores para realizar el desarrollo de una solución a problemáticas determinadas por objetivos de manera colectiva, creativa y experimental, aportando así a la innovación.

Para dicho caso se aportó desde un enfoque interdisciplinario en la exploración de nuevos usos de la tecnología Blockchain. Desde un equipo de trabajo se propuso la creación de una wallet o billetera electrónica en donde se almacenan las credenciales digitales para personas no-binarias, para que puedan tener acceso a una identidad digital auto soberana, así

mismo al validar su identidad acceder a servicios financieros o laborales sin necesidad de ser asignados por una matriz sexo-genérica que impone roles y responsabilidades sociales determinando las subjetividades dentro de la sociedad, para prever exponerse a situaciones de tratos indignos o violentos por parte de un tercero.

Por otro lado el autor Javier Bastardo (2017) informa sobre el alcance del uso de la tecnología Blockchain, creada a partir del protocolo de Bitcoin, aplicada en otras industrias por fuera del uso financiero. Asociadas a un sistema de registro descentralizado para el seguimiento (tracking) de mercancías en la industria bélica o armamentística en este caso aplicadas al registro y control de armas letales y no letales inteligentes (smartguns) que mediante una plataforma digital estas armas podrían ser registradas con sus propietarios, ser rastreadas por geo localización e incluso bloqueadas para el disparo de manera remota. Proyectos tecnológicos que inciden en las políticas de seguridad ciudadana, por la regulación en el uso y control de armas de fuego y en la prevención de delitos.

También la cadena de bloques aplicada en el sector militar podría ser una interesante herramienta para los sistemas militares, se podrían codificar datos sensibles sobre satélites militares, aeronaves no tripuladas (Dron) y armas de destrucción masiva químicas o atómicas. Como el ejemplo de la empresa BlockSafe que construyo una plataforma digital para el registro de armar inteligentes bajo la administración del ex presidente Barack Obama en EEUU. En el caso Argentina no se encuentran registros de estas aplicaciones.

Recapitulando, vemos cómo a lo largo de las distintas experiencias relacionadas con la tecnología Blockchain forman parte de las perspectivas que se proyectan hacia un futuro no muy lejano, en donde se sigue explorando e investigando en esta industria emergente dentro de un contexto de la Cuarta Revolución Industrial 4.0 , donde el desarrollo tecnológico digital se fusiona con distintas disciplinas para crear nuevos campos de acción como la nanotecnología, el internet de las cosas, la computación cuántica, la inteligencia artificial, entre otras.

3.2 Abusos y problemáticas de aplicación

Retomamos como principal problemática de la implementación de la tecnología Blockchain, las relacionadas con las finanzas. Particularmente el financiamiento del crimen organizado por narcotráfico, el lavado de dinero y estafas financieras en Argentina.

Asimismo, la falta de interés y planificación estratégica para investigar la tecnología aquí abordada por parte de un organismo estatal.

En relación a estas problemáticas es vasta la información registrada en torno a las operaciones financieras con criptomonedas para lavar dinero proveniente de la actividad del narcotráfico, en países como España, Argentina, Colombia, México, Canadá, Honduras, Brasil Estados Unidos, entre varios de Europa del Este, informados en distintos medios periodísticos internacionales y principalmente en informe anual de la JIFE (2021).

En el caso de Argentina la justicia federal ha tomado cartas en el asunto en colaboración con las Unidades de Investigación Financieras (UIF) realizan investigaciones para desmantelar las operaciones de las organizaciones criminales con la cooperación de las fuerzas de seguridad locales e internacionales. Relacionados con los delitos de lavado de dinero y las estafas a civiles por esquemas Ponzi o piramidales como lo es actualmente la investigaciones iniciadas con el caso de Generación Zoe a cargo del CEO empresario imputado LeonardoOsitorto (TÉLAM 2022).

Durante el año 2021 en la localidad de Bahía Blanca de la provincia de Buenos Aires, el Tribunal Oral en lo Criminal Federal (TOF) condenó a un vendedor de criptomonedas (Bróker) junto con seis personas más sospechosas de lavado de dinero y narcotráfico. Quienes realizaban transacciones con Bitcoin para realizar operaciones de lavado de dinero por un monto de USD 468.400 dólares provenientes de un cártel narcotraficante mexicano. (Ámbito Financiero, 2021)

Otro caso más reciente en febrero del 2022 (Di Lodovico 2022), se volvió mediático por la intoxicación y la muerte de personas que consumieron cocaína adulterada es el caso de la “Puerta 8” donde se informó que en la localidad bonaerense de Tres de Febrero en uno de los accesos de un asentamiento denominado “puerta 8” se cocinaba y distribuía cocaína adulterada con fentanilo. Según las investigaciones esta elaboración y mezcla de cocaína, aún estaba en fase de prueba por la dosificación de fentanilo por lo que generó un producto muy nocivo para los consumidores que terminaron fallecidos u hospitalizados.

La autora Di Lodovico (2022) comenta que la organización criminal que elaboraba este producto está aprendiendo de los errores de sus antecesores. Son los hijos y herederos de los

capos del narcotráfico en Argentina y se están adaptando a las nuevas modalidades y tendencias del mercado.

Aprendieron a crear empresas fantasmas para el lavado del dinero, intercambiarlo e invertir en criptomonedas las ganancias procedentes de la producción, distribución y venta de estupefacientes para no tener intermediarios en las operatorias mediantes plataformas y billeteras *non custodials*.

A su vez eligen vías y códigos de comunicaciones con otros niveles de seguridad para no ser interceptados: como las redes sociales de comunicación como Whatsapp, Telegram, Twitch, Discord y los videojuegos por streaming (en línea).

Por otra parte la Organización de las Naciones Unidas, mediante la Junta Internacional de Fiscalización de Estupefacientes (JIFE) publicó en marzo del 2022 su reporte anual. Allí informan que durante el año 2021 se vio gravemente afectado la comunidad mundial por la pandemia del COVID19 que implico mucho sufrimiento en las personas, como así también un desafío a los sistemas de salud y al comercio internacional de insumos médicos y sustancias para fines médicos, científicos e industriales para los Estados.

Con el fin de trabajar y colaborar para lograr los Objetivos de Desarrollo Sostenible (ONU 2015): Salud y Bienestar, Reducción de las Desigualdades y Paz, Justicia e Instituciones Sólidas.

El reporte anual de la JIFE (2021) se centró en fiscalizar los flujos financieros ilícitos relacionados con el tráfico de drogas y sus repercusiones en el desarrollo y la seguridad de los países.

El flujo financiero ilícito es el sustento de las actividades de los grupos delictivos organizados y es por ello que para combatir el narcotráfico, se debe frenarlo restringiendo la oferta. Ya que es perjudicial para la salud de los consumidores, para la seguridad pública y para la estabilidad política, económica y social de un país.

Actualmente con la globalización, se ha potenciado exponencialmente la circulación de capitales con innovaciones financieras y nuevas tecnologías, como los pagos mediantes

dispositivos electrónicos y monedas digitales. Que han agravado la situación de amenaza del flujo financiero ilícito y el crimen organizado transnacional.

Según el informe de la JIFE (2021) El flujo financiero ilícito proviene principalmente de cuatro ámbitos: **formas tributarias y prácticas comerciales ilícitas** (evasión y elución tributaria-fiscal), **mercados ilegales** (tráfico de droga, tráfico de armas de fuego, tráfico de flora y fauna silvestre, minería ilegal, trata de personas, etc.), **corrupción** (malversación de fondos, sobornos, abuso de funciones, enriquecimiento ilícito, trata de influencias) y **actividades delictivas** (secuestros, robos, hurtos, financiamiento del terrorismo, explotación y trata de personas, esclavitud, etc.).

En todos estos ámbitos pueden operar las organizaciones criminales para generar ingresos monetarios y así adquirir posiciones de poder y ampliar sus redes. Para financiar los operativos, la logística, armas, el personal, corromper funcionarios, hasta debilitar gobiernos.

En relación al mal uso de las nuevas tecnologías, en el caso del ciberespacio y las criptomonedas se informa que las organizaciones criminales se están perfilando hacia una nueva frontera a controlar. Usando como instrumentos de financiación y blanqueo de dinero proveniente de los grandes mercados de tráficos de drogas, de armas y trata de personas, mediante el uso de Bitcoin. El uso de estos recursos va en aumento creciente por el anonimato y la rapidez de las operaciones a partir de la emergencia sanitaria.

Sumado a las problemáticas detalladas anteriormente, el financiamiento para operaciones terroristas es otra dimensión a considerar como antecedente para tener en cuenta en relación a la Defensa Nacional de nuestro país. Como por ejemplo en medios digitales no oficiales circula la información de que en el 2019 el grupo terrorista palestino Hamas realizo una campaña para recaudar fondos en criptoactivos, particularmente en Bitcoin, haciendo llegar a los usuarios de sus redes una dirección de billetera no-custodial para realizar las transferencias como donaciones (Mendoza,2019).

Así mismo en una entrevista realizada por el Instituto de Relaciones Internacionales (IRI) al Lic. López Ferucci en el año 2018, comenta que las criptomonedas representan un desafío para los Estados en relación al lavado de activos y la financiación del terrorismo,

porque también han sido utilizadas en países como Siria y Líbano para enviar y recibir dinero por parte de grupos terroristas. También les representa un problema mayor porque no tienen ningún tipo de control o regulación por no ser un instrumento emitido por algún organismo oficial. Cita como ejemplo la prohibición del uso de criptomonedas en China y que Argentina por su parte aún no tiene una postura clara con respecto al tema.

Durante la entrevista, se afirma que hasta ese momento no había registrado rastros específicos de que en América Latina se hayan usado las criptomonedas para el lavado de dinero por parte del crimen organizado (Ferucci, 2018).

Otro antecedente a tener en consideración, es la de redes y asociaciones sociales que se conforman a causa del fervor que generan los entusiastas que trabajan con las nuevas tecnologías digitales. Según el autor Javier Bastardo (2017) ampliar el uso de criptomonedas como un sistema financiero revolucionario permitiría la creación de nuevas organizaciones sociales y políticas con una economía digital y descentralizada. Tal como menciona en su articula se encuentra el caso de un joven empresario que en 2016 viajo a Siria en apoyo al pueblo kurdo radicalizado que luchaba en contra del Estado Islámico de Irak y Siria (ISIS).

Que contribuyó desde el comité económico de Rojava (Kurdistán) al desarrollo de proyectos agrícolas del pueblo kurdo con un sistema administrativo y económico descentralizado y digital, que opera con criptomonedas, como parte de sus políticas económicas para una nueva organización social, política y económica con más autonomía.

4. Propuesta de intervención

Durante el trabajo de investigación sobre la temática abordada se desprende que los delitos perpetuados a partir del uso malintencionado de parte de un grupo delictivo de los productos y servicios derivados de la implementación de la tecnológica Blockchain en Argentina, principalmente durante el aislamiento obligatorio de la pandemia Covid-19 se encuentran vinculados con la carencia de conocimiento y divulgación de las temáticas

abordadas, al igual que la falta de control en la regulación de las empresas y organización que lucran con la tecnología Blockchain.

La intervención se focalizará en analizar las raíces de las problemáticas en los usos y abusos sociales de la aplicación de las nuevas tecnologías, que durante la investigación surgió como principal problemática las victimas de fraude, de estafas y el lavado de dinero proveniente del narcotráfico.

Nuestra propuesta se proyecta como una intervención desde una perspectiva crítica que pretende la construcción de una herramienta de gestión de la información procedente de fuentes abiertas a partir de la creación de un **Observatorio Social de Información Nacional Tecnológica Argentino (OSINTAR) y la recomendación de un plan de capacitación en innovaciones tecnológicas.**

El observatorio tendría como misión de reducir el riesgo sobre el campo de acción tecnológico. Teniendo como estrategia un enfoque de investigación acción activa. Acompañada de la formación teórica-practica con el objetivo de recopilar la mayor parte de la información disponible en fuentes abiertas, la sistematización de los datos, elaboración de informes semestrales para su difusión en campañas de información claras y concretas.

El OSINTAR debe ser un organismo no gubernamental descentralizado, que incorpore a sus equipos de trabajos a profesionales y técnicos de distintos saberes que puedan formar parte de un abordaje interdisciplinario a la problemática para producir informes integrales de conocimiento de manera periódica.

Por otro lado, trabajar en capacitaciones a las personas intervinientes en los casos de delitos complejos del crimen organizado, para su formación y actualización en la materia que le permitan elaborar sus herramientas y mecanismos para la compresión integral de las problemáticas abordadas, en nuestro caso la tecnología Blockchain, mediante la conformación de un equipo técnico interdisciplinar que conforme un programa de capacitación introductorio y asesore a los funcionarios intervinientes en las causas a fin de orientar en la elaboración de un plan de acción de contingencia para futuros escenarios.

5. Conclusiones

Abordamos a las conclusiones de que existe una relación entre las personas malintencionadas u organizaciones criminales y la tecnología Blockchain para cometer sus actividades ilícitas.

Esta relación se encuentra aún en etapas tempranas o de exploración y de allí surgen las distintas problemáticas relacionadas con la implementación de la tecnología Blockchain en Argentina. Principalmente su mal uso y/o abuso de sus derivados para vender proyectos con rentas extraordinarias que luego fracasan dejando como secuelas a miles de personas víctimas de estafas y de extorsiones por parte de criminales.

Particularmente durante la emergencia COVID19, trajo por añadidura las crisis comerciales económicas y sociales que debilitaron a los gobiernos. Los controles fronterizos se reforzaron por partes de las fuerzas de seguridad para cumplir con el aislamiento preventivo y obligatorio, también la implementación masiva de dispositivos electrónicos y conectividad a internet para la realización de tareas laborales, la compra-vente online y el e-comerce vieron su auge.

La digitalización necesaria para sobrellevar las actividades de la vida diaria de las personas, fomento el uso de tecnologías de la comunicación e información, en dicha situación el crimen organizado se valió de esos mecanismos e instrumentos para sostener sus actividades no solo sociales sino también criminales.

En el 2020 se comienzan a rastrear los primeros casos de estafas por organizaciones empresariales de esquemas piramidales o “Ponzi” y por organizaciones criminales locales con el lavado de dinero mediante las criptomonedas, con dinero proveniente del narcotráfico principalmente.

El gran desafío que se encuentra en debate entre los gobiernos, las entidades supranacionales y los usuarios-consumidores de las tecnología Blockchain es por la lucha contra el narcotráficos y el abuso de las criptomonedas, se basa en la regulación o no regulación y de qué modo informar los usos de los usuarios, por parte de las empresas que ofrecen sus servicios criptográficos.

Entendiendo la complejidad y la dinámica con la que se desarrolla la industria de tecnología Blockchain al igual que sus servicios, es necesario seguir trabajando con las distintas líneas de acción en el devenir constante, que se aceleran gracias a los dispositivos tecnológicos y los avances en la conectividad. Surge como sugerencia tener en cuenta el factor de la implementación del internet de las cosas, el 5 G y la inteligencia artificial como futuras líneas de investigación.

Con estas conclusiones se desprende que nos encontramos en un escenario presente en la que la probabilidad de ocurrencia de futuros delitos relacionados con la tecnología Blockchain es posible y que su impacto es bajo pero con una tendencia a moderado, según la evaluación de riesgo. Lo que implicaría un análisis de los riesgos para determinar si las medidas y los controles que actualmente funcionan son suficientes o si es necesario implementar nuevas medidas de acción en materia de prevención.

Este trabajo de investigación muestra sus limitaciones en el análisis de la información, por estar acotado al segmento temporal, pero al mismo tiempo deja en evidencia los usos de las innovaciones tecnológicas y su relación con el crimen organizado como un rasgo de la época en la que vivimos como aldea global.

6. Referencias bibliográficas

Ámbito Financiero (septiembre 2021). Cayó un vendedor de Bitcoin en Argentina por lavar dinero para narcotraficantes mexicanos. Recuperado de: https://www.ambito.com/informacion-general/criptomonedas/cayo-un-vendedor-bitcoin-argentina-lavar-dinero-narcotraficantes-mexicanos-n5276565

Ammous, Saifedean (2018). El patrón Bitcoin. Ediciones Deusto. Editorial Planeta.

Bastardo Javier (2017). Fabricación y uso de armas pueden ser registrados y controlados con blockchain. Recuperado de: https://www.criptonoticias.com/opinion/fabricacion-armas-registrados-controlados-blockchain/

Bastardo Javier (2017). Amir Taaki: el anarquista de Bitcoin que viajó a Siria para luchar contra ISIS. Recuperado de: https://www.criptonoticias.com/comunidad/amir-taaki-anarquista-bitcoin-viajo-siria-luchar-contra-isis/

Cámara del Senado de Argentina (2019) Economía digital. Criptomonedas ventajas y desventajas. (desgrabación). Versión Taquigráfica, Dirección Nacional de Taquígrafos, Argentina.

Di Lodovico, Cecilia (febrero 2022). Pruebas con fentanilo, criptomonedas y Telegram: así opera la nueva generación narco en Argentina. Recuperado de: https://tn.com.ar/policiales/2022/02/11/pruebas-con-fentanillo-criptomonedas-y-telegram-asi-opera-la-nueva-generacion-narco-en-argentina/

Evans Glens, (agosto 2022). *Limitaciones actuales del sistema argentino de inteligencia criminal*. Revista Movimiento. Recuperado de: https://revistamovimiento.com/politicas/limitaciones-actuales-del-sistema-argentino-de-inteligencia-criminal/#_edn1

Faliero Johanna C. (2017). Criptomonedas: la nueva frontera regulatoria. Editorial Ad-Hoc.

García Álvarez, Roberto (2020). Análisis de Smart Contracts en Ethereum e identidad soberana. Tesis (Master), E.T.S. de Ingenieros Informáticos (UPM).

Grupo de Acción Financiera (GAFI) (2015). Directrices para un enfoque basado en el riesgo para monedas virtuales.

Instituto de Relaciones Internacionales, (Marzo 2018). Lic. Mariano Javier Lopez Ferrucci: En Argentina las criptomonedas son vistas más como una manera de obtener rentabilidad financiera que para el lavado de activos. Recuperado de: https://www.iri.edu.ar/wp-content/uploads/2018/03/entrevista_lopez.pdf

Junta Internacional de Fiscalización de Estupefacientes (JIFE), (2022). *Informe de la Junta Internacional de Fiscalización de Estupefacientes correspondiente a 2021*. Recuperado de: https://www.incb.org/incb/es/publications/annual-reports/annual-report.html

Ley de Inteligencia Nacional. Creación de la Agencia de Inteligencia. Nº 27.520. Boletín Oficial, 2001.

Ley de Inteligencia Nacional. Disolución de la Secretaría de Inteligencia. Creación de la Agencia Federal de Inteligencia. N°27.126. (Buenos Aires, 25 de febrero de 2015). Boletín Oficial, 5 de marzo de 2015.

Mendoza, Luis (Agosto 2019). Criptomonedas & Icos. Grupo terrorista palestino lanzará campaña de financiamiento a través del Bitcoin. Recuperado de: https://criptomonedaseico.com/noticias/hamas-palestina-bitcoin/

Nakamoto, Satoshi (2008). Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer. (https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf).

Navarro Cardoso, Fernando (2019). Criptomonedas (en especial Bitcoin) y blanqueo de dinero. Revista Electrónica de Ciencia Penal y Criminología. ISSN 1695-0194. Recuperado de: http://criminet.ugr.es/recpc/21/recpc21-14.pdf

Organización de las Naciones Unidas, (2015). Objetivos de Desarrollo Sostenible. Recuperado de: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Qiao Liang & Wang Xiangsui (1999). La guerra más allá de los límites. Recuperado de: http://www.terrorism.com/documents/unrestricted.pdf

Qin Wang (2021) Token no fungible (NFT): descripción general, evaluación, oportunidades y desafíos. Recuperado de: https://arxiv.org/abs/2105.07447

Spadaro, J.R. (2016). Inteligencia aplicada. Crimen transnacional y derecho de policía. Ciudad de Buenos Aires: Autores de Argentina.

TÉLAM, (abril 2022). Cositorto, de gira por las provincias para declarar por la Generación Zoe. Recuperado de: https://www.telam.com.ar/notas/202204/590507-indagatoria-leonardo-cositorto-generacion-zoe.html

Unidad de Información Financiera (2014) PREVENCION DEL LAVADO DE ACTIVOS Y DE LA FINANCIACION DEL TERRORISMO, Resolución 300/2014 monedas Virtuales. Resolución N° 70/2011. Modificación. Argentina.

Zocaro, Marcos. (2020). El marco regulatorio de las criptomonedas en Argentina. Comparativa con otros países. Centro de estudios de administración tributaria (CEAT). Universidad de Buenos Aires

7. Anexos

VALORACIÓN DE INFORMACION SOBRE BLOCKCHAIN Y CRIMEN ORGANIZADO 2022						
EJE	CATEGORÍA	DIMENSIÓN	CRITERIOS	VALORACIÓN		
				Baja	Media	Alta
I	Accesibilidad	Accesiilidad y seguridad de acceso	El acceso a la información es libre			1
			El acceso a la información es fácil			1
			El acceso a la información es permanente			1
		Oportunidad	La información esta disponible para cuando se la necesita			1
II	Contexto	Actualidad y oportunidad	Acceso a información actualizada(última versión)		0,5	
		Relevancia y valor agregado	La información contribuye a un riguroso entendimiento de la gestión del riesgo			1
			La información otorga validez al producto final			1
		Completa, cantidad de inform	La información es exahustiva para el fin previsto		0,5	
III	Presentación (Representación)	Interpretabilidad (lenguaje y u	La informacion se encuentra en un formato apropiado para su uso			1
			La informacion se completa con imágenes, gráficos o información pertinente			1
			La informacion escrita es clara, gramatial y ortograficamente correcta			1
		Consistente (metodologicam	El origen de la información es verificable			1
			La informacion no presenta contradicciones internas/externas			1
			El metodo de construccion de la informacion es explicito			1
IV	Intrínseca	Precisión	Los antecedentes de pueden verficar para determinar la exactitud de la información			1
			Es poisble medir, reproducir, comprobar los datos que la información aporta			1
			Hace referencia a objetos y/o situaciones pasadas/presentes y futuras			1
		Objetividad	Propósitos y objetivos que tiene la información			1
			Expresa posturas especificas		0,5	
			Esta abierta a diversas interpretaciones		0,5	
		Reputación y credibilidad	La información es oficial (pública, privada, libre, restringida, gobierno, esducación)			1
			Usos anteriores de información de la misma fuente			1
			SUBTOTAL	-	2	18
			TOTAL			20
			CONFIABILIDAD		90%	

Fuente: Elaboracion propia para Trabajo Integrador Final de Inteligencia Estrategica y Crimen Organizado. Año 2022

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Solicitud de evaluación de TRABAJO FINAL DE ESPECIALIZACIÓN (TFE)	Código de la Especialización **097**
Nombre y apellido del alumno FERNANDO DANIEL SANDOVAL	Tipo y N° de documento de identidad DNI 36.118.857
Año de ingreso a la Especialización – Ciclo 2020	Fecha de aprobación del TFE en el Taller

Título del Trabajo Final

Problemáticas de la tecnología Blockchain, su relación con el crimen organizado durante la pandemia de COVID-19 en Argentina

Solicitud del docente a cargo del Taller

Comunico a la Dirección de la Especialización que el Trabajo Final bajo mi tutoría se encuentra satisfactoriamente concluido. Por lo tanto, solicito se proceda a su evaluación y calificación final.

Firma del docente ……

Aclaración……

Lugar y fecha……

Datos de contacto del Tutor	
Correo electrónico	Teléfonos

Se adjunta a este formulario:

- Trabajo Final de Especialización impreso (indicar cantidad de copias presentadas)
- CD con archivo del Trabajo Final en formato digital (versión Word y PDF)
- Certificado analítico

Fecha	Firma del alumno

Form. TFE v1

PRESENTAR EN LA RECEPCIÓN DE LA ESCUELA DE ESTUDIOS DE POSGRADO

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

EVALUACION TRABAJO FINAL INTEGRADOR

DOCENTE EVALUADOR: Mg José Luis Pibernus – Docente del Taller de Trabajo Final Integrador y de Contrainteligencia.

.

TEMA: "Problemáticas de la tecnología Blockchain, su relación con el crimen organizado durante la pandemia de COVID-19 en Argentina"

ALUMNO: Fernando Daniel SANDOVAL

CRITERIOS DESARROLLADOS:

1. Conocimiento del tema:
   El presente TFI de la EIEyCO, analiza descriptivamente la problemática de la implementación de la tecnología Blockchain y sus derivados relacionados con el crimen organizado en Argentina durante el periodo del aislamiento obligatorio por la pandemia del COVID-19. Para ello, en principio se puso el foco en explorar y recolectar información de distintas fuentes abiertas digitales, luego se realizó una evaluación de pertinencia a la temática abordada, siendo adecuada para definir el tema y dar lugar a la contextualización de la investigación. Con estos elementos, se redactó el marco teórico con las concepciones principales para el abordaje integral del tema propuesto, proponiendo un enfoque desde la perspectiva de la Inteligencia Estratégica y Criminal en el campo de la seguridad pública y específicamente hacia las acciones del crimen organizado.

2. Actualización del Diagnóstico
   La descripción es adecuada, basando su análisis de buceos de casos a nivel global y otros de nuestro país, que le permitieron tener un estado de situación para confrontar con las teorías vigentes sobre el blockchian y del delito complejo.

3. Pertinencia y coherencia de la propuesta de intervención

   El TFI es pertinente y coherente con los aspectos centrales de la Especialización, ya que trata un accionar importante del Crimen Organizado en oportunidad de la pandemia del Covid 19; y para ello, propone una intervención desde una perspectiva crítica que pretende la construcción de una herramienta de gestión de la información procedente de fuentes abiertas, a partir de la creación de un Observatorio Social de Información Nacional Tecnológica Argentino (OSINTAR) y la recomendación de un plan de capacitación en innovaciones tecnológicas. Es decir, una etapa de formación entorno a la problemática, con vistas a instalar conductas preventivas.

4. Aspectos formales y metodológicos:
   El TFI evaluado, reúne los procedimientos de metodología de investigación exigidos para el nivel académico de la carrera; y cumple con la Guía de la FCE establecida para TFE y con el Reglamento de Posgrado de la UBA.

5. Breve juicio del TFI.
   Además de realizar un muy buen diagnóstico de la incidencia de los delitos informáticos durante una etapa particular del mundo – Covid 19, donde la criminalidad organizada buscó mantener sus negocios ilícitos, efectúa una original propuesta formativa entorno a las conductas a tener con los manejos de las tecnologías del Blockchain en ascenso y por lo tanto de relevancia para la especialización. Muy buen trabajo.

5. Propuesta de calificación numérica: OCHO (8). -

INFORME FINAL DE EVALUACIÓN DEL DIRECTOR DE LA ESPECIALIZACIÓN EN INTELIGENCIA ESTRATEGICA Y CRIMEN ORGANIZADO:

Consideraciones: De un modo reflexivo y conciso, el autor de este Trabajo de Integración Final ha conciliado las incumbencias de al menos tres disciplinas de la carrera, para concluir con acierto en la importancia de promover un Centro de observación de la complejidad de la tecnología Blockchain , en conexión con actividades criminales de lavado de activos y otras figuras inquietantes, como el terrorismo o incluso en otros delitos que impliquen cancelaciones de secuestros extorsivos por las víctimas. Su estimativa general es apropiada, clara y oportuna, cumpliendo satisfactoriamente las exigencias académicas y presentando un aporte significativo para su consideración en próximas políticas de seguridad.

Calificación: Ratifico la intervención del docente que precede en un todo y en mérito a la iniciativa de abordaje de un tema tan complejo, discierno como calificación final

Excelente. (Nueve). – (9). -

Dr. José Ricardo Spadaro
Dir Esp en Icia Est y Crim Org
(097) – ENAP-FCE-UBA