*El Criminalista Digital. Papeles de Criminología*

Núm. 6 (2017), ISSN: 2340-6046

Instituto Andaluz Interuniversitario de Criminología (Sección de la Universidad de Granada)

# ¿Por qué las organizaciones criminales utilizan criptomonedas? Los bitcoins en el crimen organizado.

**Patricia Saldaña Taboada**
Graduada en Criminología
Estudiante del doctorado en Criminología
*Universidad de Granada*

**RESUMEN:**
En las últimas décadas se han producido una serie de avances tecnológicos que han supuesto grandes beneficios para el crimen organizado. Esta situación lleva a reflexionar sobre cómo las nuevas tecnologías cuentan con una serie de propiedades que no solo facilitan el desarrollo de actividades legales, sino que también está facilitando la criminalidad organizada.
Este es el caso de las criptomonedas que, aunque fueron creadas para permitir legalmente las transacciones anónimas de forma descentralizada sin intermediarios, en la actualidad están siendo utilizadas por algunas organizaciones criminales atraídas por sus propiedades para escapar de las autoridades. Baste como muestra el famoso caso de la operación "Tulipán Blanca".
Por este motivo, el presente trabajo pretende señalar aquellas propiedades de las criptomonedas que las hacen atractivas para el crimen organizado, así como los delitos que cometen utilizándolas, de forma que pueda avanzarse en la investigación y prevención de este tipo de delincuencia.

**Palabras clave:** crimen organizado, criptomonedas, bitcoins, cibercrimen.

**ABSTRACT:**
In recent decades there have been technological advances that have been of great benefit to organized crime. This situation leads us to reflect on how the new technologies have a series of properties that not only facilitate the development of legal activities, but also facilitate organized crime.
This is the case of the cryptocurrencies that although they were created to allow legally anonymous transactions in a decentralized manner without intermediaries, are currently being used by criminal organizations attracted by their properties to get out of the law. For example, in some famous cases such as the "Tulipán Blanca" operation.
For this reason, this paper seeks to point out those properties of cryptocurrencies that make them attractive to organized crime, as well as the crimes they commit using them, so that progress can be made in the investigation and prevention of this type of crime.

**Key words:** organised crime, cryptocurrencies, bitcoins, cybercrime.

**SUMARIO:** I. INTRODUCCIÓN. II. CRIMEN ORGANIZADO Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TICS). 1. Definiendo el crimen organizado. 2. Introducción de las TICs en el crimen organizado. III. LAS CRIPTOMONEDAS: BITCOINS. 1. ¿Qué son las criptomonedas? 2. Tipos de criptomonedas: bitcoin. 2.1. Ecosistema bitcoin. 2.2. Transacciones de bitcoins. 2.3. Obtener bitcoins. IV. UTILIZACIÓN DE LAS CRIPTOMONEDAS EN EL CRIMEN ORGANIZADO. DELITOS COMETIDOS. 1. Características atractivas para el crimen organizado. 2. Delincuencia organizada en la que intervienen las criptomonedas. V.CONCLUSIONES

## I. INTRODUCCIÓN

Las nuevas Tecnologías de la Información y la Comunicación (TICs) y en especial el uso generalizado de Internet han tenido un papel relevante en el proceso de globalización y la eliminación de fronteras. Como resultado de esto, en la actualidad se pueden observar cambios relevantes e irreversibles en la sociedad, sobre todo en lo que respecta a la forma en la que nos comunicamos y compartimos información. Tal es este hecho que ya resulta imposible imaginar el desarrollo de cualquier trabajo sin la utilización de ordenadores, teléfonos móviles o conexión a Internet.

Un ejemplo de la escalofriante extensión del uso de las TICs e Internet lo recoge el Instituto Nacional de Estadística en uno de sus informes, exponiendo que, en el año 2017, un 94% de los menores de 15 años utilizaban el teléfono móvil[1], un dispositivo que les permite estar conectado a Internet de forma continuada y acceder al mismo contenido web que les permitiría un ordenador, contando con los mismos riesgos.

Como impulsor de la revolución tecnológica actual y del uso extendido de Internet ha sido relevante el papel de la globalización. Este fenómeno ha sido considerado como una de las características que definen el S.XXI permitiendo la disolución de fronteras y la unificación de los espacios en lo referente a lo económico, social, político y jurídico. Todo ello ha sido fundamental para contribuir en la obtención

[1] INSTITUTO NACIONAL DE ESTADÍSTICA, *Encuesta sobre Equipamiento y uso de las Tecnologías de Información y Comunicación en los hogares,* 2017. Obtenido de https://www.ine.es/prensa/tich_2017.pdf, p.3.

de comunicaciones más rápidas y fáciles, el movimiento de las finanzas, así como los viajes internacionales[2].

En definitiva, esta situación ha supuesto grandes beneficios para la sociedad, pero también ha traído consigo una serie de riesgos. De la misma forma que el resto de la sociedad, el crimen organizado también se ha beneficiado de estos avances y ha actualizado tecnológicamente sus formas de delinquir. En otras palabras, ha incluido en sus formas de actuación herramientas y metodologías propias de los nuevos avances tecnológicos y de la interconexión mundial que ofrece Internet.

Como resultado de esta situación, Europol ha señalado en un su informe SOCTA[3] (2017), que el cibercrimen se ha situado como uno de los mercados delictivos de la criminalidad organizada que más se ha ampliado en los últimos años, teniendo en cuenta que se considera cibercriminalidad tanto los delitos ciberdependientes[4] o cibernéticos, como los delitos de carácter más tradicional que se cometen empleando las TICs[5].

Por consiguiente, la tecnología se ha situado como uno de los facilitadores para el crimen organizado para llevar a cabo sus actividades delictivas junto con la corrupción, el lavado de dinero, el fraude documental, el comercio online, la violencia y la extorsión[6].

---

[2] UNODC, *Organized Crime,* 2018. Obtenido de https://www.unodc.org/unodc/en/organized-crime/intro.html

[3] EUROPOL, *Serious and Organised Crime Threat Assessment (SOCTA),* 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf

[4] *Ibídem*, p. 28: El término "delito ciberdependiente" empleado por Europol en su informe sobre amenazas del crimen organizado es utilizado para aquellos delitos que solo pueden cometerse usando un ordenador, redes de ordenadores u otras formas de las tecnologías de la información y la comunicación (…). Dentro de esta definición se podrían considerar delitos como el *malware* o los ataques de denegación de servicio (ataques DDoS).

[5] FERNÁNDEZ BERMEJO, D. y MARTÍNEZ ATIENZA, G., *Ciberseguridad, ciberespacio y ciberdelincuencia*, Navarra, Aranzadi, 2018, p.152: "Con la expresión delito informático, cibercrimen o ciberdelito se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las Tecnologías de la Información y la Comunicación o que tiene como fin estos bienes (…)". Pero además, la cibercriminalidad se considera como un concepto más amplio en el que se incluyen también la delincuencia considerada como tradicional que se facilita gracias a la utilización de las Tecnologías de la Información y la Comunicación.

[6] EUROPOL, *Serious and Organised Crime Threat Assessment* (SOCTA), 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.13.

De esta forma, muchos de los avances tecnológicos creados en las últimas décadas han sido utilizados por organizaciones criminales para desarrollar sus actividades delictivas beneficiándose de las mismas prestaciones que el resto de la sociedad. Este es el caso por ejemplo del correo electrónico que, aunque se trata de una herramienta para comunicarse de una forma rápida, efectiva y de forma internacional, ha sido empleada por algunas organizaciones criminales como medio para cometer delitos como el *phishing*[7].

De igual modo, las criptomonedas se presentan como una herramienta tecnológica que aunque no fue creada con ese propósito, finalmente ha sido utilizada por organizaciones criminales para facilitar sus actividades de la misma forma que sucede con otras herramientas tecnológicas como el correo electrónico.

Características propias de las criptomonedas como el anonimato y la descentralización han atraído a las organizaciones criminales a su utilización. Así se han visto varios casos de criminalidad organizada facilitada por esta moneda virtual.

Llegados a este punto, el propósito de esta investigación consiste en conocer por qué las organizaciones criminales utilizan la tecnología para desarrollar sus delitos, qué características de esta moneda virtual son atractivas para las organizaciones y qué tipo de delitos ha protagonizado. Es por esto por lo que se parte de la hipótesis de que las propias características de esta moneda virtual son las que atraen a los grupos y facilitan la criminalidad organizada y que solo a través de la investigación de estas peculiaridades y de los delitos cometidos se podrá avanzar en la persecución y prevención de estas conductas.

Por lo que se refiere a la organización del trabajo presente, en primer lugar, se va a exponer lo que se considera por crimen organizado y la relación que pudiera tener este con TICs. En el tercer apartado se va a recoger toda la información relacionada con las criptomonedas, en especial con los bitcoins (qué son, cómo se obtienen, cómo se

[7] El *Phishing* se trata de un tipo de delito ciberdependiente que consiste en el envío de correos electrónicos maliciosos que pretenden conseguir información personal, financiera o de seguridad del destinatario. Para conseguir que la persona que recibe el correo lo abra e interactúe con él hasta compartir su información, los ciberdelincuentes suplantan páginas webs de entidades oficiales que le piden información al usuario. Esta información se puede encontrar en la infografía elaborada por EUROPOL, *Cyber Scams Infographics*. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/es_1.pdf

utilizan, etc.). Por último, se expondrán las principales características de las criptomonedas que las hacen atractivas para el crimen organizado, finalizando con aquellos tipos de criminalidad organizada que han sido protagonizados por esta moneda virtual.

## II. CRIMEN ORGANIZADO Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TICs)

La frecuente aparición en prensa del término "crimen organizado" puede llevar a pensar que la criminalidad organizada es un fenómeno actual.

Sin embargo, aunque las consecuencias del crimen organizado se han perpetuado hasta la actualidad, este término se acuñó en el S.XX en Estados Unidos por lo que cuenta con menos de un siglo de uso.

En sus primeras apariciones, este término se utilizaba para hacer referencia a la mafia italiana que se caracterizaba por su organización jerárquica, las relaciones de patronazgo y el clientelismo, sus formas de extorsionar y controlar la sociedad, etc. Por lo que hablar de mafia italiana era lo mismo que hablar de una forma concreta de delinquir[8] que iba unida a una serie de tradiciones familiares y culturales propias de la zona en la que estaba asentada la mafia en cuestión.

De esta forma, en el siglo XX el crimen organizado era considerado como un fenómeno exclusivo de ciertos países, como una especie de singularidad cultural de los mismos[9], tal y como se puede ver en la representación que el cine de la época hace sobre estas organizaciones criminales.

Sin embargo, en la actualidad esta concepción del crimen organizado ha cambiado y ahora las organizaciones criminales no están adscritas a un único territorio, sino que desarrollan sus actuaciones en varios países o estados. Esto es lo que se conoce como criminalidad organizada transnacional.

---

[8] REDONDO, S. y GARRIDO GENOVÉS, V, *Principios de Criminología,* Valencia, Tiranch lo Blanch, 2013 (4.ª ed.),

[9] CORTE IBÁÑEZ, L. y GIMÉNEZ-SALINAS FRAMIS, A., *Crimen.org: evolución y claves de la delincuencia organizada,* Barcelona, Editorial Ariel, 2010.

Llegados a este punto, no cabe duda que la criminalidad organizada puede tener graves consecuencias para las personas tanto de forma individual como en sociedad, sobre todo ahora que las organizaciones han ampliado sus zonas de actuación.

Por ello es necesaria la lucha contra el crimen organizado y la actuación para su prevención. Pero para conseguir esto primero es necesario determinar qué es el crimen organizado de forma que todos los países puedan dirigir esta lucha hacia los mismos objetivos. En otras palabras, se debe comenzar definiendo el crimen organizado.

## 1. Definiendo el crimen organizado

La investigación, lucha y prevención del crimen organizado requieren de una definición del fenómeno que asegure que todas las actuaciones al respecto estarán orientadas hacia las mismas conductas y objetivos.

Sin embargo, escoger una única definición de crimen organizado es una tarea complicada ya que existen alrededor de 180 definiciones diferentes que han sido aportadas desde instituciones y desde la academia[10].

### *a) Definiciones institucionales*

En relación con las definiciones institucionales de crimen organizado, la más utilizada es la elaborada por Naciones Unidas en el año 2000 en la Convención contra el Crimen Organizado Transnacional en la ciudad de Palermo[11].

Según la Oficina contra la Droga y el Delito de las Naciones Unidas, más conocida por su nombre en inglés *United Nations Office on Drugs and Crime* (UNODC), se considera un grupo delictivo organizado:

---

[10] HOLMES, L., *Advanced introduction to organised crime,* Cheltenham, Edward Elgar, 2016: determinar una única definición de crimen organizado es una tarea complicada. Así, el criminólogo Klaus Von Lampe ha señalado que existen alrededor de 180 definiciones diferentes de crimen organizado.

[11] HOLMES, L., *Advanced introduction to organised crime,* Cheltenham, Edward Elgar, 2016, p.3: se ha puntualizado en este caso que no fue casualidad la elección de la ciudad de Palermo para la celebración de este evento. Esta ciudad fue escogida como localización simbólica, ya que Sicilia es considerada como la cuna de la mafia.

> 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[12] 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[13].

El hecho de que se consideren las organizaciones criminales como "grupos estructurados" diferencia estas agrupaciones de otras que se han constituido de manera fortuita para la ocasión, sin ningún tipo de continuidad ni estructura desarrollada y en la que sus miembros no tienen funciones definidas[14].

Aunque no se trata de una definición consensuada, permite establecer una serie de pautas para diferenciar una organización criminal de un grupo terrorista u otro tipo de grupos criminales.

Con el mismo propósito, dada la heterogeneidad que pueden presentar las organizaciones criminales, la Unión Europea a través del Consejo de Europa creó en el año 1997 una lista de criterios para determinar lo que se considera como una organización criminal[15] de una forma mucho más precisa.

La lista en cuestión reúne 11 indicadores estadísticos y para que una agrupación criminal se trate en realidad de una organización criminal tiene que presentar seis de estos criterios siendo obligatoriamente los indicadores 1,3,5 y 11 y otros dos cualquiera. Los indicadores que han de valorarse son:

1. Colaboración de más de dos personas.
2. Cada miembro tiene que tener una tarea propia asignada.
3. Tiene que haber actuado durante un periodo de tiempo prolongado o indefinido (estabilidad del grupo y potencial durabilidad).
4. Uso de algunas formas de disciplina y control.

---

[12] OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, *Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos*, 2004. Obtenido de https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf, p.5: se considera como "delito grave" aquella conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave.

[13] *Ibídem.,* p.5.

[14] *Ibídem.,* p.5.

[15] Dichos criterios se vuelven a presentar en la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave que fueron inicialmente recogidos en el documento 6204/2/97 Enfopol 35, rev 2 de Europol.

5. Haber cometido de delitos graves.
6. Opera a nivel internacional.
7. Empleo de la violencia u otros medios adecuados para la intimidación.
8. Utilización de estructuras comerciales o formales.
9. Implicación en el blanqueo de capitales.
10. Ejercen influencia en política, medios, administración pública, autoridades judiciales o la economía.
11. Búsqueda de beneficios y/o poder.

Junto con estos criterios, se recogen como principales referencias normativas en este ámbito la Decisión Marco 2008/841/JAI del Consejo de la Unión Europea de 24 de octubre de 2008, el Código Penal y la Ley de Enjuiciamiento Criminal.

En relación con lo establecido en la Decisión Marco 2008/841/JAI del Consejo de la Unión Europea de 24 de octubre de 2008, a los efectos de esta se entiende una organización delictiva como:

> Una asociación estructurada de más de dos personas, establecida durante un cierto período de tiempo y que actúa de manera concertada con el fin de cometer delitos sancionables con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos cuatro años o con una pena aún más severa, con el objetivo de obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material[16].

Por lo que se refiere a lo establecido en el Código Penal (CP), la definición de una organización criminal y un grupo criminal fueron introducidas en el Derecho Penal por la LO 5/2010, de 22 de junio, que los tipifica como delitos en el Art.570 bis[17]

[16] Decisión Marco 2008/841/JAI del Consejo, de 24 de octubre de 2008, relativa a la lucha contra la delincuencia organizada, Boletín Oficial del Estado, p.2. Obtenido de https://boe.es/doue/2008/300/L00042-00045.pdf

[17] Según el Artículo 570 bis CP en su segundo párrafo se establece que "A los efectos de este Código se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos".

(organización criminal), el Art.570 ter[18] (grupo criminal) y el Art.570 quater (disposiciones comunes para los delitos de organización criminal y grupo criminal) del CP y además los considera como tipos penales de aplicación extraterritorial siempre que se hayan desarrollado actuaciones relevantes en España aunque el grupo esté asentado en el extranjero[19].

*b) Definiciones académicas*

Con respecto a las definiciones académicas de crimen organizado, tampoco hay consenso para establecer una única definición, sino que diferentes autores han aportado diversas definiciones sobre lo que se puede considerar como una organización criminal. La definición elaborada por las Naciones Unidas en la Convención de Palermo no estuvo exenta de críticas por parte de expertos que consideraban que en una definición de "crimen organizado" era necesaria incluir la violencia y la corrupción como medios para conseguir sus objetivos. Por ello, los autores Corte Ibáñez & Giménez-Salinas Framis han propuesto una definición de «organización criminal» o «grupo de crimen organizado» como:

> Toda organización creada con el propósito expreso de obtener y acumular beneficios económicos a través de su implicación continuada en actividades predominantemente ilícitas y que asegure su supervivencia, funcionamiento y protección mediante el recurso a la violencia y la corrupción o la confusión con empresas legales[20].

De esta forma, aunque no se haya ofrecido una única definición de carácter institucional o académico, cualquiera de las definiciones que se han recogido, especialmente la lista de criterios, pueden ser útiles para seguir unas pautas que diferencien a una organización criminal de cualquier otra agrupación criminal que se haya formado con otros fines y otras características.

---

[18] Según el Artículo 570 ter CP se entiende por grupo criminal "la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos".

[19] FERNÁNDEZ BERMEJO, D. y MARTÍNEZ ATIENZA, G., *Ciberseguridad, ciberespacio y ciberdelincuencia,* Cizur Menor, Navarra, Aranzadi, 2018, p.96.

[20] CORTE IBÁÑEZ, L. y GIMÉNEZ-SALINAS FRAMIS, A., *Crimen.org: evolución y claves de la delincuencia organizada,* Barcelona, Editorial Ariel, 2010, p.21.

## 2. Introducción de las TICs en el crimen organizado

En la actualidad, las características propias del crimen organizado justifican el hecho de que las organizaciones criminales hayan incorporado la tecnología en sus actividades delictivas a la vez que esta tecnología ha producido cambios en este tipo de criminalidad.

Por lo tanto, a continuación se expondrán las características principales del crimen organizado y de sus organizaciones criminales con el objetivo de aportar una explicación a la actualización tecnológica de la criminalidad organizada[21].

En primer lugar, hay que saber que tal y como se recogía en la definición elaborada por las Naciones Unidas, la principal motivación del crimen organizado es la motivación económica, es decir, "el puro y crudo lucro económico"[22], lo que explica su perduración y la pertenencia a una banda.

Esta búsqueda de beneficios como principal motivación permitiría diferenciar a las organizaciones criminales de otras motivaciones que se persiguen en otras tipologías delictivas. Esto tiene como resultado que toda la actividad y decisiones que se toman dentro de la organización se realizarán en torno a la amplificación de las oportunidades de obtener mayores beneficios[23]. Con esto se quiere decir, que este tipo de delincuencia no atiende a doctrinas sociales, creencias políticas o preocupaciones ideológicas (lo que lo diferencia del terrorismo) y que si se involucran en política es para conseguir protección en inmunidad[24].

En segundo lugar, otra de las características relevantes del crimen organizado es su implicación prioritaria en el suministro de bienes y servicios ilegales, mayormente mediante la explotación de mercados delictivos ofreciendo productos y servicios bajo

---

[21] CORTE IBÁÑEZ, L. y GIMÉNEZ-SALINAS FRAMIS, A., *Crimen.org: evolución y claves de la delincuencia organizada,* Barcelona, Editorial Ariel, 2010. Los autores de la obre han recogido como características que son la seña de identidad de los grupos de crimen organizado: la finalidad económica, la implicación prioritaria en la provisión y el suministro de bienes y servicios ilegales, actividades ilegales complementadas con negocios legales, continuidad y medidas de protección y corrupción y violencia.

[22] *Ibídem*, p.225.

[23] *Ibídem.*

[24] ABADINSKY, H., *Organized crime,* Belmont, CA, Wadsworth Cengage Learning, 2013 (10th ed.).

demanda[25]. En otras palabras, la criminalidad organizada depende de la oferta y la demanda de la sociedad de forma que las organizaciones criminales adaptan su oferta a aquellos productos y bienes con los que se podría obtener un mayor número de beneficios.

Como resultado de todo lo anterior, se puede considerar que las organizaciones criminales son comparables con empresas legalmente establecidas ya que gestionan sus actividades criminales de la misma forma que lo haría una empresa al uso. Así mismo, también desarrollan actividades legales junto con negocio ilegales considerando que la financiación de las organizaciones procede de una mezcla de ambos negocios[26].

Por último, las organizaciones criminales cuentan con una serie de estrategias para asegurar su permanencia. Con este objetivo establecen medidas oportunas para que la organización pueda perdurar en el tiempo escapando a la detección por parte de las Fuerzas y Cuerpos de Seguridad. Además, también se valen de la corrupción de empleados públicos y responsables políticos para conseguir sus objetivos evadiendo controles y detección por parte de las autoridades y la violencia como medio de protección y defensa[27].

De esta forma, al considerar las organizaciones criminales como empresas que buscan obtener beneficios económicos o de carácter material mediante la oferta y demanda de productos y servicios, se hace evidente la adaptación de estas a las nuevas tecnologías y al uso generalizado de Internet.

La Red en sí misma es un lugar atractivo para la delincuencia por las propias características de las que consta[28]: ofrece seguridad a la persona que comete el delito, permite cometer delitos aprovechándose de la ingenuidad de las víctimas, hay una gran cantidad de víctimas, permite cometer delitos de forma transnacional y no hay una única

---

[25] CORTE IBÁÑEZ, L. y GIMÉNEZ-SALINAS FRAMIS, A., *Crimen.org: evolución y claves de la delincuencia organizada,* Barcelona, Editorial Ariel, 2010.

[26] CORTE IBÁÑEZ, L. y GIMÉNEZ-SALINAS FRAMIS, A., *Crimen.org: evolución y claves de la delincuencia organizada,* Barcelona, Editorial Ariel, 2010.

[27] *Ibídem*, p.26.

[28] CASAS, E., *La red oscura: En las sombras de Internet. El cibermiedo y la persecución de los delitos tecnológicos,* España, La esfera de los libros, 2017.

legislación que la regule, sino que está supeditada a la interpretación desde muchas legislaciones diferentes.

Como se ya se ha mencionado, la tecnología se sitúa como un medio que ha permitido a las organizaciones criminales tanto la comisión de nuevos delitos cibernéticos (*malware, cryptoware,* ataques a las redes, etc.), como el desarrollo de la delincuencia organizada tradicional de una forma más rápida, eficaz, con menor coste, con mayor número de víctimas y sobre todo, dificultando la detección por parte de las agencias de seguridad y los cuerpos policiales.

Los avances en las Tecnologías de la Información y la Comunicación han permitido una comunicación rápida y efectiva reduciendo las distancias sin la necesidad de que emisor y receptor tengan que encontrarse en el mismo espacio y tiempo. Este avance es sin duda beneficioso para organizaciones criminales ya que les permite comunicarse fácilmente con miembros de la organización de cualquier parte del mundo.

Por otra parte, la aparición de nuevos avances tecnológicos ha provocado la aparición de nuevos mercados delictivos y el desarrollo de los existentes de una forma mucho más segura y directa preservando el anonimato tanto del comprador como del vendedor, que ya no tienen que realizar la compra de forma física. Han surgido nuevos productos fruto de la revolución tecnológica, como los teléfonos móviles de última generación, que son demandados por la sociedad, pero también han surgido nuevos espacios y herramientas que facilitan el desarrollo del negocio. Este es el caso de los mercados delictivos alojados en al *Darknet*[29] en los que se han registrado actividades como la venta de armas y drogas ilegales.

Gracias a esto las organizaciones criminales ha podido ampliar su oferta de bienes y servicios demandados por la sociedad e incluso demandados por otras organizaciones criminales y así tener una mayor oportunidad de conseguir beneficios.

Finalmente, los avances en las nuevas tecnologías han permitido la creación de herramientas y espacios que permiten a las organizaciones obtener un mayor anonimato

[29] CASAS, E., *La red oscura: En las sombras de Internet. El cibermiedo y la persecución de los delitos tecnológicos,* España, La esfera de los libros, 2017: La *Darknet* es la parte de la *Deep Web* dedicada a la venta y oferta de productos y servicios ilegales. Esta zona de la Internet profunda tiene como característica principal que mantiene al usuario en el anonimato haciendo su dirección IP difícil de rastrear. Además, no hay un buscador de páginas web establecido, de forma que también es difícil acceder a los mercados delictivos si no se conoce la dirección en concreto.

y por tanto mayor seguridad de la continuidad de la organización criminal. Este es el caso de la mencionada anteriormente como *Darknet* alojada en la "Internet profunda" que mantiene al usuario en el anonimato ya que hace su dirección IP difícil de rastrear.

En resumen, la adopción de las nuevas tecnologías y el uso de Internet por parte de las organizaciones criminales tiene su razón de ser en los beneficios que pueden obtener para sus negocios delictivos y en la perdurabilidad o continuidad de la organización. En otras palabras, les permite llegar a un mayor número de clientes y de víctimas sin importar el espacio ni el tiempo, les ha permitido ampliar su oferta de bienes y servicios debido tanto a los espacios en la red seguros para anunciarse como debido a la demanda de las herramientas tecnológicas surgidas y por último, les ha permitido contar con herramientas tecnológicas y espacios seguros en la red que han facilitado el desarrollo de sus negocios delictivos dificultando la detección e intervención por parte de las Fuerzas y Cuerpos de Seguridad y los servicios de inteligencia.

Como ejemplo clásico de herramientas fruto de las nuevas tecnologías que han permitido facilitar el desarrollo de la delincuencia se pueden encontrar nuevas formas de pago como las tarjetas prepago, los pagos online y los cupones en Internet[30]. Estas formas de pago permiten realizar pagos a través de Internet dificultado la identificación del usuario que ha realizado la transacción, por lo que se han convertido en una herramienta muy utilizada por las organizaciones criminales en el blanqueo de capitales.

No obstante, el avance tecnológico ha continuado y más tarde surgieron las criptomonedas como un nuevo método de pago a través de monedas virtuales protegidas por criptografía. Esta herramienta ha permitido el pago en mercados delictivos alojados en la *Darknet,* transacciones directamente entre las personas implicadas en el negocio delictivo e incluso el blanqueo de capitales procedentes de la criminalidad organizada.

De esta forma, el hecho de que se hayan registrado casos en los que las organizaciones criminales han utilizado las criptomonedas con fines delictivos, lleva a preguntarse qué ventajas proporcionan estas monedas virtuales al crimen organizado. Este es el propósito que se pretende alcanzar en los apartados siguientes.

---

[30] EUROPOL, *Serious and Organised Crime Threat Assessment* (SOCTA), 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.19.

## III. LAS CRIPTOMONEDAS: BITCOINS.

### 1. ¿Qué son las criptomonedas?

La revolución tecnológica de las últimas décadas ha afectado también al comercio surgiendo nuevas formas de representar el dinero en el entorno online.

De esta forma, antes de definir las criptomonedas sería necesario conocer la diferencia que existe entre las monedas digitales y las monedas virtuales.

En primer lugar, las monedas digitales son aquellas que se usan para pagar algún producto o servicio a través de un medio electrónico sin tener que utilizar el dinero físico[31]. Este dinero se utiliza, por ejemplo, cuando se paga algún producto en comercios online. En este caso no se utiliza dinero físico, sino que se paga a través de la representación digital del dinero de nuestra cuenta bancaria.

En segundo lugar, la moneda o dinero virtual es aquel que solo existen en formato digital sustituyendo al dinero físico[32]. Pudiera parecer similar a la moneda digital, sin embargo, la moneda digital es una representación digital del dinero físico, mientras que la moneda virtual constituye la conversión del dinero físico en un tipo de moneda virtual que no existe en su forma física. Este tipo de moneda es utilizada, por ejemplo, cuando se gasta dinero fiduciario para comprar un tipo de moneda (virtual) utilizada un videojuego y que permite adquirir nuevos niveles, escenarios, personajes, etc.

Por último, están las criptomonedas. Las criptomonedas son un tipo de moneda virtual, es decir, aunque tienen un valor al cambio en algún tipo de moneda física o fiduciaria, en realidad no existen como tal fuera de la red. Sin embargo, lo que diferencia a las criptomonedas de una moneda virtual al uso es la utilización de la criptografía.

---

[31] NIETO, A. (27 de diciembre de 2018). *Cuál es la diferencia entre criptomoneda, moneda virtual y dinero digital,* 2018. Obtenido el 20 de junio del 2018 de https://www.xataka.com/criptomonedas/cual-es-la-diferencia-entre-criptomoneda-moneda-virtual-y-dinero-digital

[32] NIETO, A. (27 de diciembre de 2018). *Cuál es la diferencia entre criptomoneda, moneda virtual y dinero digital,* 2018. Obtenido el 20 de junio del 2018 de https://www.xataka.com/criptomonedas/cual-es-la-diferencia-entre-criptomoneda-moneda-virtual-y-dinero-digital

En definitiva, se puede decir que una criptomoneda es una moneda virtual que no tiene emisor concreto, que está protegida por criptografía[33] y en la que son los propios usuarios en forma de nodos los que de forma masiva y distribuida comprueban las transacciones que se realizan [34,35].

No obstante, en el caso de que hubiera que señalar una única característica de las criptomonedas, se podría decir que lo que verdaderamente las caracteriza es su descentralización. Con este término se hace referencia a que no hay ninguna organización que respalde su valor y controle su emisión, por lo que no se tiene controlada la inflación o deflación y es el propio emisor el que se encarga de la supervisión del blanqueo y de emitir informes sobre su actividad[36].

## 2. Tipos de criptomonedas: bitcoin.

En la actualidad se pueden encontrar más de 1000 criptomonedas diferentes[37]. Hasta la fecha las criptomonedas que se encuentran en el top 10 son: Bitcoin, Ethereum, Ripple, Bitcoin Cash, EOS, Litecoin, Stellar, Cardano, IOTA y TRON[38]. Muchas de ellas

---

[33] BITCOIN PROJECT, *Vocabulario: Bitcoin,* 2018. Obtenido de https://bitcoin.org/es/vocabulario#bitcoin : la criptografía es la rama de las matemáticas que permite crear pruebas matemáticas que proporcionan altos niveles de seguridad. Para el caso del Bitcoin, esto impide que los monederos se puedan corromper y se pueda gastar el dinero de otras personas.

[34] Estas características se explicarán con profundidad cuando se hable de las características de la moneda Bitcoin, que es una de las criptomonedas más utilizada en la actualidad.

[35] NIETO, A. *Cuál es la diferencia entre criptomoneda, moneda virtual y dinero digital,* 2018. Obtenido el 20 de junio del 2018 de la web https://www.xataka.com/criptomonedas/cual-es-la-diferencia-entre-criptomoneda-moneda-virtual-y-dinero-digital

[36] CASAS, E., *La red oscura: En las sombras de Internet. El cibermiedo y la persecución de los delitos tecnológicos,* España, La esfera de los libros, 2017 p. 205.

[37] En la página web https://www.cryptomarketscaps.com/en/live-crypto-currencies-updates se registran el precio, la capitalización de mercado, el volumen generado en 24h en relación con una moneda fiduciaria en concreto, el aumento-disminución de valor en 1h/24h/7d y la oferta disponible para 1771 criptomonedas diferentes.

[38] Debido a que el valor y por tanto la utilización de las criptomonedas puede cambiar mucho en el tiempo, es importante señalar que los datos sobre el top 10 mencionado se han obtenido el 20 de junio del 2018 de la página https://www.cryptomarketscaps.com/en/live-crypto-currencies-updates

cuentan con una serie de mejoras u limitaciones respecto del bitcoin, que es la criptomoneda que ocupa el primer puesto en la lista. Así, por ejemplo, la moneda Ether del sistema Ethereum (en el puesto número tres de la lista) a diferencia de la moneda bitcoin, permite los llamados *Smart Contracts* que son aplicaciones que generan contratos inteligentes que se ejecutan de forma automática[39]. También hay otras criptomonedas como Monero y Zcash que ofrecen un mayor anonimato que el sistema Bitcoin.

Sin embargo, la primera criptomoneda creada con éxito fue el bitcoin[40], propuesta por Satoshi Nakamoto[41] en una lista de intercambio de correos sobre criptografía en el año 2008 y lanzada al mercado en el año 2009 con un límite de 21 millones. Es por esto por lo que el resto de las criptomonedas serían consideradas como "altcoins" (*alternative coins*) o monedas alternativas.

Por lo que se refiere a su definición, la criptomoneda bitcoin consiste en una cadena de firmas digitales *peer-to-peer*, en otras palabras, las transacciones se realizan directamente de persona a persona sin que tenga que intervenir ningún tipo de intermediario.

Este funcionamiento está basado en la filosofía del propio Nakamoto recogida en el primer documento que elaboró para presentar el sistema Bitcoin. En este *whitepaper* Nakamoto exponía que en aquel momento el comercio electrónico dependía demasiado de la confianza depositada en una tercera parte para realizar las transacciones (entidades bancarias, organizaciones, instituciones, etc.). Esta confianza no permitía que las transacciones pudieran ser irreversibles ya que siempre existía la posibilidad de que el intermediario interviniera en el proceso para resolver cualquier disputa, lo que lastraba

---

[39] FERNÁNDEZ, A., *Guía Bitcoin 2018. La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018, pp.140-141.

[40] BITCOIN PROJECT, *Vocabulario: Bitcoin,* 2018. Obtenido de https://bitcoin.org/es/vocabulario#bitcoin : Se escribe Bitcoin con "B" mayúscula para hacer referencia al concepto de Bitcoin o a la totalidad de la red, mientras que con "b" minúscula hace referencia a una unidad del mismo.

[41] "Satoshi Nakamoto" es en realidad el pseudónimo que utilizó su creador para mantener su identidad en el anonimato. Aunque desde su aparición muchas personas se han atribuido el papel de creadores del bitcoin, en realidad hasta la fecha no se conoce la identidad exacta del creador.

el comercio electrónico haciéndolo costoso y dependiente generando a su vez elevados costes [42].

Por todo esto, Nakamoto planteó un sistema de pago electrónico que no depende de la confianza de terceros para el procesamiento de la transacción, sino que esta queda asegurada por el registro en la *Blockchain* mediante la realización de pruebas criptográficas. Así, de este modo se garantiza que la transacción sea irreversible, de bajo coste y además se impide el doble pago y por lo tanto el fraude[43].

Finalmente, como resultado de este sistema Nakamoto no solo conseguía transacciones irreversibles, sino que también evitaba muchos otros problemas derivados de la confianza en terceros como: el elevado coste de las transacciones, la imposibilidad de realizar transacciones de cantidades pequeñas, la posibilidad de que las cuentas del banco sean congeladas y su dinero confiscado o embargado y el rechazo de intermediarios (PayPal, Visa, Mastercard, etc.) a procesar pagos de ciertas cantidades legales[44].

### 2.1. Ecosistema bitcoin.

Hay varios participantes o elementos que componen el protocolo Bitcoin y que hay que considerarlos para saber cómo funciona[45,46]:

*a) Mineros*

Los mineros son las personas encargadas de procesar la transacción realizada y verificarla para que pueda almacenarse en la cadena de bloques o *Blockchain*. De esta forma, mediante esta red de nodos Nakamoto instauró una forma para

---

[42] NAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008. Obtenido de https://bitcoin.org/bitcoin.pdf, p.1.

[43] *Ibidem,* p.1.

[44] PRIETO, A., *¿Qué es el bitcóin?*, 2018. Obtenido de https://www.youtube.com/watch?v=Bt_6JAIXns4&t=687s

[45] FERNÁNDEZ, A., *Guía bitcoin: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018, p.37: participantes que comparten entre sí la utilización del protocolo Bitcoin: mineros, usuarios y *wallets*, *exchanges* o servicios de cambio y comercios.

[46] PRIETO, A., *¿Qué es el bitcóin?*, 2018. Obtenido de https://www.youtube.com/watch?v=Bt_6JAIXns4&t=687s : Alberto Prieto Espinosa señala como elementos del Sistema Bitcoin: la red, los mineros, los bloques y la cadena de bloques o *Blockchain.*

que las transacciones fueran comprobadas y se aseguraran de forma democrática, evitando el doble pago o la ausencia de transacción sin tener que confiar o depender de entidades bancarias que se encarguen de esta tarea[47].

Para minar bitcoins solo es necesaria la instalación de un software específico y abierto en un ordenador conectado a la red Bitcoin y tener una gran capacidad computacional.

El proceso de verificación de las transacciones consiste en la resolución de una serie de puzles criptográficos en forma de "competición". Los ganadores de la competición serán capaces de efectuar la verificación de la transacción y recibir una pequeña compensación. Para que el resultado de esta competición sea justo por así decirlo, las nuevas transacciones se basan en un protocolo de mayorías, de forma que tienen que contar con más de la mitad del apoyo de todos los ordenadores del mundo para que pueda ser incorporada a la cadena de bloques [48]. De esta forma, Nakamoto se aseguraba que la verificación de las transacciones de un nodo se realizase de forma democrática ya que el sistema de votos representaba la decisión de la mayoría. Esto se puede conseguir porque las pruebas de trabajo realizadas equivalen a "una-CPU-un-voto", siendo la cadena de nodos más larga la que tiene un mayor esfuerzo de procesamiento invertido y por tanto la que representaba a la mayoría[49].

*b) Blockchain*

La tecnología *Blockchain* es considerada como una base de datos o un enorme libro de contabilidad en el que se registran todas las transacciones realizadas con bitcoins desde sus inicios hasta la actualidad.

Según algunos autores, es comparable a un libro electrónico de actas público y anónimo. Es público porque pueden consultarse libremente todas las transacciones realizadas y registradas desde sus orígenes, pero a su vez es

[47] NAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008. Obtenido de https://bitcoin.org/bitcoin.pdf, p.1.

[48] FERNÁNDEZ, A., *Guía bitcoin: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018, p.41.

[49] NAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008. Obtenido de https://bitcoin.org/bitcoin.pdf, p.3.

anónimo porque no muestra ningún tipo de información que pueda relacionarse con la identidad de una persona en particular. Únicamente muestran el número del bloque, la fecha y la hora, la persona o grupo de personas que minaron ese bloque [50].

Con esta tecnología, Nakamoto pretendía conseguir la transparencia de las transacciones impidiendo que una misma moneda pudiera ser utilizada en dos ocasiones dejando constancia de la hora y el día en el que se realizó cada transacción.

Además, de esta forma también ofrecía la posibilidad de que todo el proceso pudiera ser libremente consultado y verificado en cualquier momento.

La *Blockchain* se denomina también "cadena de bloques" porque constituye una cadena con todos los bloques en los que se agrupan las transacciones realizadas con bitcoins.

Estas transacciones son irreversibles gracias al sistema "prueba de trabajo" o *Proof-of-work*, en el que una vez se ha consumido toda la energía de la CPU para verificar la transacción, es casi imposible revertir ese bloque o la parte de la cadena de bloques correspondiente hasta llegar a un bloque en concreto. Esta es una buena forma también para confiar en la verificación de las transacciones, ya que la decisión de la mayoría se representa en la cadena más larga o principal, que es la que ha investido un mayor esfuerzo y si un atacante quiere rehacer la prueba de trabajo de un bloque en concreto tendría que rehacer la de toda la cadena hasta llegar a este[51].

Finalmente, aunque esta tecnología fue utilizada por primera vez en el sistema Bitcoin para el que ha alcanzado una gran popularidad, en la actualidad está siendo utilizada con otros fines. Por ejemplo, recientemente se ha incluido

[50] Se puede acceder a la *Blockchain* y consultar los registros almacenados desde la web https://www.blockchain.com/es/explorer

[51] NAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008. Obtenido de https://bitcoin.org/bitcoin.pdf, p.3.

en la industria alimentaria para conseguir la transparencia en la cadena de producción que mantenga la confianza de los consumidores[52].

*c) Usuario y monederos*

El bitcoin en una de las criptomonedas más utilizadas a nivel internacional. No obstante, es difícil determinar esta utilización en término de sujetos que utilizan esta moneda virtual.

Esto tiene su razón de ser en que al inscribirse en la red Bitcoin las personas obtienen una cartera electrónica o *wallet* donde almacenarán sus bitcoins y no una cuenta personal. De esta forma, una misma persona podría tener varias carteras diferentes.

Por lo tanto, para medir el volumen de utilización del bitcoin será más útil estudiar el número de carteras electrónicas que se utilizan en la actualidad.

Con este fin es de gran utilidad la *Blockchain*. Como se ha explicado en el apartado anterior, la publicidad y facilidad de acceso a la misma permite consultar el número de usuarios de carteras electrónicas que hay en un momento dado. Actualmente, hay 31,817.708 usuarios de carteras electrónicas de bitcoins[53].

Obtener un monedero es el primer paso a seguir para cualquier persona que quiera obtener, comprar y almacenar bitcoins.

Cada monedero de bitcoin lleva asociada una clave pública y una clave privada. La primera sería el equivalente al número de cuenta bancaria que se comparte cuando queremos que alguien nos realice un ingreso. La segunda sería el equivalente a la contraseña de la cuenta de correo electrónico, por lo que esta

---

[52] CARREFOUR, *Blockchain alimentario,* 2018. Obtenido de https://actforfood.carrefour.es/Por-que-actuar/BLOCKCHAIN-ALIMENTARIO: tras la pérdida de confianza del consumidor a partir de una serie de escándalos sanitarios, Carrefour decidió implantar la tecnología *Blockchain* inicialmente empleada en la red Bitcoin. Adoptaron la tecnología "Ethereum", que era la tecnología más estable en aquel momento y de esta forma, el "blockchain alimentario" se hace transparente la trazabilidad de los alimentos. Esto se consigue registrando los datos de cada alimento (en un principio era con aves) desde su incubación hasta su distribución, siendo todos estos datos accesibles y públicos de la misma forma que para las transacciones de bitcoins.

[53] BLOCKCHAIN LUXEMBOURG S.A., *Blockchain Wallet Users.* Obtenido el 27 de diciembre de 2018 de https://www.blockchain.com/es/charts/my-wallet-n-users.

clave debe mantenerse en secreto y segura, ya que aquel o aquella que se haga con esta clave será el propietario o propietaria de los bitcoins que contenga ese monedero.

De esta forma, con estas claves no es necesario proporcionar ningún dato de carácter personal u otra información que pueda ser relacionada con una persona en concreto. Por ello, hasta el momento no ha sido posible identificar a una persona en concreto por medio de la clave pública de su cartera electrónica.

Hay muchos tipos de carteras o *wallets* en las que almacenar los bitcoins. Se podría decir que hay dos tipos: fuera de la red y perteneciente a la red. Dentro del primer tipo se encontrarían las carteras instaladas en un ordenador e incluso en un móvil. En el segundo tipo se recogerían las carteras de papel y los dispositivos *hardware* externos que son similares a un *pen drive.*

En lo relativo a la seguridad de cada cartera se podría decir que son más seguras las carteras de papel y las que se encuentran en dispositivos *hardware,* ya que permiten guardarse de forma externa al ordenados/móvil y sobre todo sin conexión a Internet, lo que las mantiene a salvo de posibles hackeos y robo de bitcoins.

En consecuencia, cabe decir que a pesar de la aparente seguridad que alberga la moneda bitcoin, es necesario que el usuario sea consciente de que la seguridad total de la misma depende una utilización adecuada de esta, sobre todo de la clave privada de monedero o *wallet,* ya que los bitcoins de una cartera pertenecen a aquel que conoce la clave privada. Por ello, es necesario que los usuarios, concienciados con la seguridad, adopten las medidas de precaución necesarias.

*d) Servicios de intercambio o Exchanges*

En la actualidad existen varias formas de obtener bitcoins, entre las que se encuentran los servicios de intercambio o *exchanges.*

Los servicios de intercambio son empresas que a través de plataformas electrónicas online y recibiendo una comisión ponen en contacto a personas que quieran comprar bitcoins con personas que quieran venderlos o viceversa[54].

Utilizando estos servicios un usuario del sistema Bitcoin que ya no quiera mantener sus bitcoins puede determinar un precio para estos (en dinero fiduciario) y ponerlos a la venta, de tal forma que es la plataforma la que buscará compradores que estén buscando comprar bitcoins a ese precio.

En cualquier caso, son las personas implicadas en la compra o venta las que deciden si finalmente se llevará a cabo o no la transacción, pero esta no se reflejará en la *Blockchain* (el minado de esos bitcoins ya tuvo lugar y quedó reflejado), sino que se almacena en los sistemas informáticos del servicio de intercambio[55].

*e) Comercios*

Dado que se trata de dinero, de la misma forma que sucede con el dinero fiduciario, las criptomonedas pueden ser utilizadas en determinados comercios para pagar por productos y servicios.

Todavía este método de pago no es muy popular, por lo que no hay una gran cantidad de comercios que permitan esta forma de pago y sobre todo no está introducida en comercios conocidos y relevantes.

Sin embargo, aunque no sea muy popular, el pago de servicios y productos utilizando este tipo de moneda tiene ciertas ventajas con respecto al dinero fiduciario. Entre las ventajas que se podrían encontrar están: evitar las comisiones que se generan en un pago ordinario con tarjeta o la posibilidad de poder pagar con una misma moneda en cualquier parte del mundo sin tener que cambiar al dinero fiduciario en cuestión[56].

---

[54] FERNÁNDEZ, A. *Guía bitcoin: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018, p.41.

[55] *Ibídem*, p.42.

[56] FERNÁNDEZ, A., *Guía bitcoin: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018, p.30.

Aquellos comercios que permiten el pago con criptomonedas son muy variados. Se pueden encontrar comercios en los que el pago puede ser con *fiat* y criptomonedas y otros diseñados únicamente para el pago con criptomonedas. Como ejemplo de los productos legales que se pueden comprar hay joyas de lujo[57], flores[58], pastelería[59], videojuegos[60], etc. Pero también se pueden utilizar para pagar por servicios como reservar viajes[61] o para realizar donaciones[62].

Sin embargo, para el caso de que no se conozcan tiendas online en las que se puedan usar los bitcoins, existen algunos buscadores de tiendas que permiten el pago con bitcoins[63].

### 2.2.Transacciones de bitcoins.

Las transacciones realizadas con bitcoins se caracterizan por registrarse de forma cronológica e irreversible y realizarse de forma asimétrica[64].

Una vez se conocen todos los elementos que forman parte del entorno Bitcoin hay que saber cómo se desarrollan las transacciones de bitcoins.

Imagínese que una persona llamada "B" quiere hacer una transferencia de bitcoins a otra persona llamada "A". Para que se haga efectiva la transacción se siguen una serie de pasos[65]:

---

[57] THE BITCOIN LUXURY BOUTIQUE (2018). Obtenido el 20 de diciembre de 2018 de https://www.bitdials.eu/

[58] APANYMANTEL. Obtenido el 2 de marzo del 2018 de https://www.apanymantel.com/

[59] *Ibídem*

[60] INSTANT GAMING. Obtenido el 2 de marzo del 2018 de https://www.instant-gaming.com/es/

[61] DESTINIA. Obtenido el 2 de marzo del 2018 de https://destinia.com/#_ga=2.189764514.84544423.1551652427-1251879768.1551652426: esta agencia de viajes online permite reservar hoteles, vuelos y transporte utilizando bitcoins, entre otras monedas.

[62] BITPAY, *Contribute to Greenpeace*. Obtenido el 2 de marzo de 2018 de https://bitpay.com/181852/donate

[63] SPENDABIT. Obtenido el 2 de marzo del 2018 de https://spendabit.co/go?q=drug&price=98.00-499.00&price-from=&price-to=&discount=

[64] CASAS, E., *La red oscura: En las sombras de Internet. El cibermiedo y la persecución de los delitos tecnológicos,* España: La esfera de los libros, 2017, p. 213-214: cada usuario tiene dos claves, una pública y otra privada que se corresponden inequívocamente.

En primer lugar, "B" necesita la clave pública del monedero de "A", de forma similar a la cuenta bancaria que se muestra a la otra persona para hacer una transferencia.

En segundo lugar, "B" creará un mensaje en el que incluirá la clave pública del monedero de "A", la cantidad de bitcoins que se quieren transferir y la clave pública de su monedero.

Por último, este mensaje será firmado por "B" utilizando la clave privada de su monedero (que debe de mantenerse segura en todo momento) y esta transacción irá a la red Bitcoin.

Una vez se encuentra en la red, los mineros confirmarán la transacción en los 10 minutos siguientes a su envío y se hará efectiva cuando haya sido confirmada por varios mineros[66]. Esta transacción incluirá una tasa por procesamiento en la red y no podrá ser cancelada o reembolsada.

### 2.3.Obtener bitcoins.

Existen diferentes formas a través de las que una persona puede obtener bitcoins. La forma más conocida sería la que desarrollan los mineros tal y como se ha explicado en apartados anteriores. Esta forma es comúnmente conocida como "minar" bitcoins.

Sin embargo, esta forma de obtener bitcoins no está al alcance de todo el mundo ya que requiere de capacidades computacionales enormes. De esta forma existen otros métodos más accesibles para el resto de la población.

Una de estas formas sería comprando los bitcoins en plataformas electrónicas de intercambio o *Exchange* de las que ya se ha hablado anteriormente como uno de los componentes del ecosistema Bitcoin. En función de la cantidad de dinero que se utilice para comprar las monedas virtuales, la plataforma divide el proceso en etapas diferentes y esta transferencia no quedará

---

[65] PRIETO, A., *¿Qué es el bitcóin?*, 2018. Obtenido de https://www.youtube.com/watch?v=Bt_6JAIXns4&t=687s

[66] *Ibídem:* hay algunas excepciones a este hecho: si se requiere que la transacción sea validada en un tiempo inferior a 10 minutos se deberá de pagar un coste adicional. Además, aquellas cantidades de bitcoins que superen los 1.000$ requerirán de 6 confirmaciones o más para validarse.

reflejada en la Blockchain sino en el sistema informático de la plataforma. Como medida para evitar la delincuencia, para grandes cantidades de dinero sería necesario aportar documentación personal para verificar la identidad[67].

Otra forma de obtener bitcoins sería comprándolos a otra persona directamente, ya sea de forma online o en persona. Ambas formas son más anónimas que la compra a través de un *Exchange* y además tienen menos costes, sin embargo, la primera forma puede conllevar riesgo de estafa por lo que requiere que la persona interesada en la transacción estime las medidas de seguridad oportunas.

Por último, aunque no están tan extendidos como los que se utilizan para el dinero fiduciario, también existe la posibilidad de adquirir bitcoins en cajeros Bitcoin.

## IV. UTILIZACIÓN DE LAS CRIPTOMONEDAS EN EL CRIMEN ORGANIZADO. DELITOS COMETIDOS.

### 1. Características atractivas para el crimen organizado

Con el avance de la era de la tecnología, muchas de las herramientas tecnológicas legales fueron finalmente utilizadas para cometer delitos. Este puede ser el caso del correo electrónico que, aunque fue utilizado como un medio de comunicación que permite salvar las distancias, algunas organizaciones criminales lo han utilizado como un instrumento para amplificar las víctimas de sus delitos (carta nigeriana, *phishing*[68], etc.).

En cualquier caso, hay que dejar claro que, en la gran mayoría de los casos, la herramienta no es ilegal en sí misma, sino que es el uso que se hace de la misma lo que constituye un delito. Esto mismo ocurre con las criptomonedas.

---

[67] FERNÁNDEZ, A., *Guía bitcoin: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018.

[68] EUROPOL, *Serious and Organised Crime Threat Assessment* (SOCTA), 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.32: "Card-not-present fraud is fuelled by the availability of compromised card data resulting from data breaches, information stealing malware and phishing".

En la actualidad, autoridades como Interpol o Europol y medios de comunicación están advirtiendo sobre el uso que organizaciones criminales hacen de las criptomonedas para el desarrollo de sus actividades delictivas.

Para ilustrar mejor esta afirmación se van a mostrar dos casos conocidos de criminalidad organizada en el que tuvieron un papel relevante las criptomonedas.

En primer lugar, hay que hablar de la operación "Tulipán Blanca". En este caso una organización criminal dedicada al narcotráfico en España y Colombia blanqueaba el dinero obtenido de sus actividades delictivas comprando criptomonedas con este dinero. Una vez habían comprado las criptomonedas en España con el dinero de origen ilícito, estas eran enviadas a carteras Bitcoin de miembros de la organización en Colombia. Una vez allí las criptomonedas, fundamentalmente bitcoins, eran transformadas de nuevo a dinero fiduciario o bien se mantenían en criptomonedas[69]. En cualquier caso, de esta forma se hacía difícil de investigar la trazabilidad del dinero procedente de la criminalidad organizada.

El segundo caso conocido fue el del famoso ciberdelincuente ladrón de bancos de origen ucraniano creador del *malware* "Carbanak", que protagonizó uno de los casos de ciberdelincuencia más importantes hasta la fecha tanto por la trascendencia internacional como por las cantidades robadas. El detenido en cuestión era el líder de la banda en su parte técnica junto con dos personas más de Ucrania y otra de Rusia.

En relación con su *modus operandi, e*n primer lugar, los ciberdelincuentes se introducían en la red informática mediante un *malware* que enviaban mediante correos maliciosos a los trabajadores de los bancos. Una vez estaban dentro del sistema informático del banco iban escalando hasta los sistemas de seguridad de cajeros y transferencias[70].

---

[69] EFE y SERVIMEDIA (9 de abril de 2018). Once detenidos de una red que blanqueaba dinero del narcotráfico a través de criptomonedas. *El Mundo*. Obtenido de http://www.elmundo.es/espana/2018/04/09/5acb154ee2704eef6b8b4603.html

[70] HERRAIZ, P. y ALSEDO, Q. (27 de marzo de 2018). Cae en España el "hacker" de los 10.000 millones, el ciberladrón más importante del mundo: Carbanak. *El Mundo*. Obtenido de http://www.elmundo.es/espana/2018/03/26/5ab8bdeb268e3ed01d8b4636.html: aunque la organización compró bitcoins con el dinero de origen ilícito, fue por este mismo motivo por el que su actividad fue detectada, ya que los agentes consiguieron identificar la dirección Bitcoin del líder de la banda.

Una vez la organización había infectado la infraestructura del banco, robaban el dinero de tres formas diferentes: transfiriendo el dinero a cuentas bancarias en bancos extranjeros, aumentando el dinero de las cuentas bancarias para que pudiera ser retirado del cajero automático y controlando los cajeros automáticos para que expulsaran dinero [71]. En los dos últimos casos el dinero de los cajeros automáticos sería recogido finalmente por "muleros" que eran contratados por la propia organización pero que no formaban parte de la cabeza de esta.

Por último, lo que realmente tiene relevancia con el tema en cuestión es que el dinero obtenido de las tres formas anteriormente descritas era convertido a criptomonedas, fundamentalmente bitcoins para dificultar la detección del dinero de origen ilícito[72].

Ambos casos presentados llevan a preguntarse, ¿cuáles son las propiedades de las criptomonedas que han atraído a las organizaciones criminales?

Hay muchos tipos de criptomonedas diferentes que surgieron desde la creación del bitcoin. Sin embargo, dado que el bitcoin es la moneda pionera, con más trayectoria a nivel internacional y para la que más casos de criminalidad organizada se conocen (como en los dos casos presentados anteriormente), este apartado se centrará en las propiedades en concreto de los bitcoins y de su sistema.

Como se ha mencionado ya en apartados anteriores, en sus orígenes el bitcoin fue una de las primeras criptomonedas que se creó con la finalidad de evitar la confianza en terceros para realizar transacciones, reducir el coste de estas y evitar el fraude sin intermediarios[73]. Sin duda sus motivaciones completamente lícitas ofrecen a la sociedad una serie de beneficios respecto de la utilización de otras formas de pago convencionales.

---

[71] Europol. *Internet Organised Crime Threat Assessment*, 2018. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, p.23.

[72] Europol. *Internet Organised Crime Threat Assessment*, 2018. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, p.23.

[73] NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*. Obtenido de https://bitcoin.org/bitcoin.pdf, p.1.

Sin embargo, a su vez, organizaciones criminales han detectado ciertas características en esta criptomoneda que les ha permitido el desarrollo de sus actividades delictivas de una forma más efectiva y al margen de la detección policial:

*a) Descentralización:*

La descentralización de los bitcoins fue la principal motivación que llevó a Satoshi Nakamoto a la creación del sistema Bitcoin. En palabras del propio autor, la confianza depositada en terceras partes para realizar una transacción lastraba el comercio online y no permitía que las transacciones fueran irreversibles.

Como resultado de este pensamiento, el bitcoin es una moneda descentralizada, en otras palabras, no hay ninguna organización que respalde su valor y controle su emisión, de forma que cualquier persona puede instalarse el *software* correspondiente y ser parte de la red[74].

Esta característica ha sido realmente atractiva para las organizaciones criminales que han utilizado esta moneda para comprar productos o servicios ilegales o bien para blanquear dinero escapando del control de los Estados, gobiernos, autoridades, entidades bancarias, etc.

*b) Fácilmente accesible en todo el mundo:*

Los bitcoins al ser unas monedas virtuales que solo existen en su forma digital, pueden ser utilizados en cualquier parte del mundo independientemente del dinero fiduciario del continente o país en cuestión sin necesidad de cambiarlos a dinero físico.

Debido a que la criminalidad organizada ha alcanzado un carácter transnacional, cada vez es menos habitual que las organizaciones criminales se suscriban a un único territorio, sino que actúan en diferentes países o incluso en diferentes continentes.

Es por esto por lo que es atractivo para la criminalidad organizada el hecho de que los bitcoins sean fácilmente accesibles desde cualquier parte del mundo. De esta forma, la organización puede enviar el dinero recaudado con sus actividades ilegales a otros miembros de la organización situados en otras partes del mundo, lo que implica a

[74] FERNÁNDEZ, A., *Guía bitcoin: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018, p.24.

su vez una actividad de blanqueo de capitales. Esto permite el envío de dinero escapando al control de las autoridades de cualquier país.

*c) Coste mínimo de las transacciones:*

En la actualidad, cualquier transacción de dinero realizada mediante una entidad bancaria ordinaria traerá consigo una serie de costes asociados. Esto es incluso más notorio en el caso de que se trate de una transacción de grandes cantidades de dinero.

Incluso puede suceder justo lo contrario, es decir, que los bancos en cuestión se nieguen a realizar determinadas transacciones como aquellas que conllevan una cantidad muy pequeña de dinero.

Estos inconvenientes fueron algunos de los que Satoshi Nakamoto pretendía evitar con la creación del sistema Bitcoin[75]. Como resultado de este pensamiento, en las transacciones con bitcoins solo se pagaría un pequeño coste a los mineros o a los servicios de intercambio, sin importar el tamaño de la transacción de la que se trate.

Esto es beneficioso para las organizaciones criminales que además de escapar al control de los gobiernos y bancos realizando sus transacciones en bitcoins, estas pueden ser de cualquier tamaño, lo que es habitual en la criminalidad organizada que gestiona una gran cantidad de dinero.

*d) Permite realizar transacciones internacionales a través de redes peer-to-peer:*

Las redes *peer-to-peer* son sistemas que permiten a un individuo de la red contactar con otro individuo sin ningún tipo de intermediario o tercera parte[76]. Esto se debe a que los nodos que forman la red se sitúan al mismo nivel constituyendo un colectivo organizado de ordenadores interconectados en el que no hay un "cliente-servidor", sino que todos los nodos actúan como iguales y comparten recursos a cambio de recursos. Algunos de los ejemplos más conocidos de estas redes son eDonkey, Ares, BitTorrent y Bitcoin.

En relación con la red Bitcoin, esta permite la realización de transacciones entre los individuos que pertenecen a la red de una forma directa, sin intermediarios.

---

[75] NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*. Obtenido de https://bitcoin.org/bitcoin.pdf, p.1.

[76] BITCOIN PROJECT., *Vocabulary: P2P*. Obtenido el 23 de febrero de 2018 de la web https://bitcoin.org/en/vocabulary#mining

Este hecho resulta de gran interés para las organizaciones criminales permitiéndoles la realización de transferencias de cualquier tipo entre individuos de forma directa y sin la intervención de entidades bancarias o gobiernos. En consecuencia, las transacciones anónimas con carácter internacional se hacen posibles y resultan atractivas para escapar de la persecución de la ley.

*e) Anonimato:*

Junto con la descentralización, el anonimato es una de las características más significativas de los bitcoins.

Aunque cada transacción queda registrada de forma cronológica, irreversible y pública en la *Blockchain*, ninguna de estas transacciones contiene datos o información que pueda ser relacionada directamente con la identidad de una persona en concreto. En consecuencia, la forma de determinar el dueño o dueña de una cartera depende de aquel o aquella que disponga de la clave privada que le da acceso a la misma. Por ello es tan importante mantener segura la clave privada de la cartera de bitcoins.

De esta forma, los miembros de las organizaciones criminales pueden gestionar sus negocios delictivos seguros de que las transacciones realizadas con este tipo de moneda virtual no los dejará al descubierto. Además, si existiera duda de ello[77] podrían incluso crear varias direcciones Bitcoin para evitar el registro de los movimientos repetidos de una misma dirección.

*f) Posibilidad de cambio de bitcoins a dinero fiat:*

Como se ha mencionado en apartados anteriores, la criminalidad organizada en la actualidad ha adquirido un carácter transnacional, de forma que las organizaciones criminales ya no suelen estar adscritas a un único territorio, sino que sus actuaciones afectan a varios países o incluso varios continentes.

En consecuencia, los miembros de las organizaciones criminales localizados en diferentes países necesitan algún medio para poder enviar o recibir dinero, ya sea de sus clientes o de otros miembros de la organización. Así, utilizando criptomonedas como los bitcoins, pueden enviar el dinero en forma de bitcoins y luego convertirlo a moneda fiat de nuevo (euros, dólares, pesos, etc.).

---

[77] FERNÁNDEZ, A., *Guía bitcoin: La guía más práctica, completa y actualizada para iniciarse y avanzar en el mundo Bitcoin,* 2018, p.24.

Además, la posibilidad de poder cambiar bitcoins a la moneda fíat de un país ha dado lugar a varios casos de lavado de dinero procedente de actividades delictivas de las organizaciones criminales[78].

*g) Operaciones irreversibles:*

La irreversibilidad de las transacciones era una de las principales motivaciones de Satoshi Nakamoto para la creación del sistema Bitcoin. Según Nakamoto la confianza depositada en una tercera parte que actuaba como intermediario impedía que la transacción realizada fuera irreversible porque siempre cabía la posibilidad de que esta parte interviniera. Sin embargo, con la creación del sistema Bitcoin y la implementación de la denominada como "prueba de trabajo" o pruebas criptográficas es imposible revertir una transacción, ya que para ello se debería de revertir el trabajo de toda la cadena de bloques de la *Blockchain* hasta ese momento.

Con este aspecto, las organizaciones criminales se aseguran de que los bitcoins transferidos a las respectivas carteras permanezcan en estas sin que ninguna otra parte pueda revertir esta acción. Esto generaría estabilidad, confianza y seguridad en los negocios que llevan a cabo.

*h) Falta de regulación en la mayoría de los países:*

Este hecho sin duda es realmente beneficioso para las organizaciones criminales ya que muchos de los países o estados que se encuentren con casos de utilización de bitcoins por parte del crimen organizado, no conocerán la forma más efectiva y eficaz para responder ante esta situación.

En España, el Ministerio de Hacienda y Función Pública en su Plan Anual de Control Tributario y Aduanero del 2018 ha hablado del control de criptomonedas como el bitcoin para la prevención y represión del contrabando, narcotráfico y blanqueo de

[78] EFE y SERVIMEDIA (9 de abril de 2018). Once detenidos de una red que blanqueaba dinero del narcotráfico a través de criptomonedas. *El Mundo*. Obtenido de http://www.elmundo.es/espana/2018/04/09/5acb154ee2704eef6b8b4603.html: Esto sucede por ejemplo en el caso "Tulipán Blanca" en el que la organización que operaba en España y Colombia blanqueaba el dinero de origen ilegal obtenido en España utilizándolo para comprar bitcoins. Una vez en las carteras de los miembros colombianos de la organización este dinero era convertido al dinero fíat del país.

capitales[79]. Señala la utilización del bitcoin por los grupos de delincuencia organizada como uno de los desafíos más exigentes de la actualidad para lo que potenciará el uso de unidades de Investigación de la Agencia Tributaria.

A nivel europeo se trabaja para implementar controles a las transacciones con criptomonedas que impidan o al menos dificulten el blanqueo de capitales. Con el objetivo de avanzar en estas cuestiones, la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018[80] ha introducido novedades respecto a directivas anteriores sobre la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.

En relación con estas novedades, en la directiva se recoge que las casas de cambio o *exchanges* y los proveedores de servicios de custodia de monederos estarán obligados a cumplir la normativa y vigilar el uso que se hace de las monedas virtuales a efectos de la lucha contra el blanqueo de capitales y la financiación del terrorismo. Para ello, la directiva recoge que tendrán que colaborar para reducir el anonimato asociado a estas monedas virtuales y además, deberán de estar registrados.

*i) Disponible como forma de pago en muchos mercados delictivos:*

De la misma forma que el dinero digital, las ventajas que pueden ofrecer a la delincuencia las criptomonedas como los bitcoins ha provocado la existencia de mercados delictivos sobre todo en la *Darknet* que permiten el pago con esta moneda virtual.

---

[79] Resolución de 8 de enero de 2018, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se aprueban las directrices generales del Plan Anual de Control Tributario y Aduanero de 2018, p.19. Obtenida de https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-792.pdf

"La utilización por el crimen organizado de la Internet profunda, o «deep web», para el tráfico y comercio de todo tipo de bienes ilícitos, así como el empleo de criptomonedas tipo «bitcoin» o similar como medios de pago, es uno de los desafíos más exigentes en la actualidad. Para afrontar esta amenaza, se potenciará el uso por las unidades de investigación de la Agencia Tributaria de las nuevas tecnologías de recopilación y análisis de información en todo tipo de redes"

[80] Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UR. Obtenido de https://www.boe.es/doue/2018/156/L00043-00074.pdf

Este era el caso de los mercados delictivos "Silk Road", "Alphabay" y "Hansa" que, aunque en la actualidad se encuentran extintos, cuando estaban en funcionamiento permitían la compra de productos como drogas ilegales, armas y herramientas de *hacking*.

Sin embargo, en la actualidad se han registrado nuevos mercados delictivos en la *Darknet* que, aunque no han llegado a la magnitud de los anteriores también cuentan con la posibilidad de pagar sus productos o servicios con estas monedas virtuales.

## 2. Delincuencia organizada en la que intervienen las criptomonedas.

Considerado lo anterior, es indiscutible que las criptomonedas como los bitcoins reúnen una serie de características que resultan atractivas para las organizaciones criminales para cometer delitos o para facilitar la realización de muchos otros.

De esta forma, se pueden encontrar muchos casos de diferentes tipologías delictivas perpetradas por organizaciones criminales y en los que han aparecido las criptomonedas de una forma u otra.

En este apartado, se recogen algunos casos de criminalidad organizada en los que se pueden observar las características anteriormente descritas. Además, también dejan entrever la variedad delictiva en la que son utilizadas las criptomonedas, especialmente los bitcoins y la forma en la que se utilizan.

### *a) Blanqueo de capitales*

Según Europol en su informe del año 2017[81], el blanqueo de capitales se sitúa como uno de los principales motores del crimen organizado junto con el fraude documental y el comercio en línea.

Las criptomonedas como los bitcoins han tenido un gran protagonismo en el blanqueo de dinero permitiendo introducir a la economía legítima dinero obtenido como ganancia de actividades delictivas.

El modo en el que se desarrolla esta actividad delictiva es sencillo. El dinero obtenido de actividades delictivas es utilizado para comprar criptomonedas, en especial bitcoins. Una vez el dinero se ha convertido a criptomonedas, los delincuentes pueden

[81] EUROPOL, *Serious and Organised Crime Threat Assessment,* 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.19.

volver a cambiarlo a dinero fiduciario, enviarlo a las carteras electrónicas de otros miembros de la organización o bien utilizarlo para pagar productos o servicios ileales en los mercados delictivos. De esta forma, se pierde todo rastro del origen ilícito del dinero.

Como muestra de lo anterior basta con recordar casos relevantes de criminalidad organizada como los pertenecientes a las operaciones "Tulipán Blanca" en la que se blanqueaba dinero obtenido en España por tráfico de drogas para enviarlo a Colombia o el caso del *malware* "Carbanak" en el que se blanqueaba el dinero obtenido del robo a diversos bancos.

Este asunto es uno de los que más preocupan a los países y Estados ya que su investigación es muy necesaria de cara al descubrimiento del crimen organizado y de la financiación de grupos terroristas.

*b) Pago en mercados delictivos*

Según un informe de Europol para el año 2017[82], el pago con criptomonedas se presenta junto con las tarjetas prepago y los vales en línea, como uno de los métodos de pago que permite mover grandes cantidades de fondos criminales. Además, presenta las ventajas de que permite transferir dinero internacionalmente, evitando comisiones y regulaciones de los bancos convencionales.

Como resultado, las criptomonedas como los bitcoins son utilizadas por las organizaciones criminales para comprar en la *Darknet* productos como drogas ilegales, armas de fuego, bienes falsificados, documentos fraudulentos, especies en peligro de extinción, etc[83].

Para que los mercados delictivos de este tipo tengan éxito, es necesario que el dinero que se utiliza en estos negocios pase desapercibido. Para ello, debido a que sistemas de pago como Paypal o Western Union ya cuentan con departamentos

[82] EUROPOL, *Serious and Organised Crime Threat Assessment,* 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.19.

[83] *Ibídem,* p.22

especializados en antifraude, las organizaciones criminales y los clientes de sus servicios utilizan los bitcoins[84].

Los primeros mercados delictivos relevantes que aparecieron en la *Darknet* fueron "Silk Road" y "Alphabay", ambos ya extintos. Después del mercado "Alphabay" surgió "Hansa Market", un mercado negro al que migraron muchos usuarios de "Alphabay" y que fue considerado como el tercer mayor mercado de la *Deep Web*. "Hansa" contaba con más de 350.000 productos ilícitos como drogas, armas de fuego y *malware* que podían ser comprados utilizando bitcoins y otras criptomonedas. Sin embargo, al igual que su antecesor este mercado fue desmantelado en una operación policíaca internacional llamada "Bayonet"[85] (Escobar, 2017).

A pesar de las diferentes operaciones llevadas a cabo para desmantelar este tipo de mercados delictivos, las características propias de la *Darknet* unidas a las características propias de las criptomonedas favorecen que estos mercados se extiendan cada vez más.

Esto sobre todo es debido a que en muchas ocasiones, es necesaria la compra de ciertos productos ilegales para el desarrollo de otros delitos de mayor gravedad. Este es el caso del fraude de tarjeta presente o *Skimming*[86], para el que son necesarias materias primas para fabricar las tarjetas de crédito falsas.

De forma similar sucede para el fraude de tarjeta no presente o *Carding*[87], los datos robados sirven para cometer delitos posteriores de mayor gravedad.

Junto con los anteriores, el *Live Child Distant Abuse*[88] o Abuso sexual infantil a distancia en directo ha surgido como una amenaza emergente. Dicha actividad delictiva

---

[84] CASAS, E., *La red oscura: En las sombras de Internet. El cibermiedo y la persecución de los delitos tecnológicos,* España, La esfera de los libros, 2017, p. 139.

[85] ESCOBAR, V. (22 de julio de 2017). Cae Hansa: Operación policíaca internacional desmantela el tercer mayor mercado de la Deep Web. *Criptonoticias*. Obtenido de https://www.criptonoticias.com/sucesos/cae-hansa-operacion-policiaca-internacional-desmantela-tercer-mayor-mercado-deep-web/

[86] EUROPOL, *Serious and Organised Crime Threat Assessment* (SOCTA), 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.32. También denominado fraude de tarjeta presente, este delito consiste en el robo de la tarjeta bancaria de un sujeto para poder utilizarla en su lugar o clonarla. Para su clonación se compran los materiales en mercados delictivos.

[87] *Ibídem*, p.32

es ofertada en la *Darknet* y para acceder a la conexión online en directo el sujeto tiene que pagar una cantidad concreta en criptomonedas. Aunque este tipo de delito todavía no es parte del crimen organizado, hay que tenerlo en cuenta porque si "el servicio" alcanza la suficiente demanda como para obtener una gran cantidad de beneficios, puede que las organizaciones criminales se involucren en esta actividad delictiva[89].

*c) Contratación de servicios delictivos: Crime-as-a-Service.*

En algunas ocasiones, las organizaciones criminales requieren de los servicios de otros delincuentes para cometer delitos complejos y elaborados. Esto sucede sobre todo en la cibercriminalidad ya que, organizaciones criminales de carácter tradicional pueden requerir de ciberdelincuentes para algunas labores relacionadas con el empleo de las TICs en el crimen organizado o para la comisión de ciberataques[90].

Con este objetivo, algunas organizaciones criminales "contratan" a delincuentes profesionales expertos en esta materia que les proporcionen herramientas o los servicios necesarios para cometer dichos delitos o llevar a cabo ciberataques como *cryptoware, ransomware,* ataques DDoS, codificar *malware*, alquilar botnets, etc.

Para poder contratar los servicios de estos ciberdelincuentes, los miembros de organizaciones criminales realizan el pago utilizando criptomonedas como los bitcoins.

*d) Ciberextorsión*

La ciberextorsión consiste en el secuestro de un equipo informático de forma completa o parcial a cambio del pago de una cantidad de dinero o criptomonedas para liberarlo.

---

[88]ECPAT, *Live streaming of child sexual abuse in real-time*, 2018. Obtenido el 23 de diciembre del 2018 de https://www.ecpat.org/wp-content/uploads/legacy/SECO%20Manifestations_Live%20streaming%20of%20child%20sexual%20abuse%20in%20real-time_0.pdf : En el *Live Distant Child Abuse* (LDCA), un sujeto desde cualquier parte del mundo paga por acceder a una conexión en directo en la que un menor es obligado a mostrar comportamientos sexuales delante de una webcam o es forzado a ser víctima de abuso sexual también delante de la webcam y en directo. Tiene lugar a través de aplicaciones de vídeo chat o de salas de chat online e incluso permite al sujeto que ha pagado por la conexión hacer peticiones.

[89] EUROPOL, *The Internet Organised Crime Threat Assessment (IOCTA)*, 2018. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf, p.35 y EUROPOL, *Serious and Organised Crime Threat Assessment* (SOCTA), 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.31.

[90] EUROPOL, *Serious and Organised Crime Threat Assessment* (SOCTA), 2017. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf, p.29.

Los tipos de *malware* más habituales para llevar a cabo este tipo de cibercrimen son los *ransomware* y los ataques de denegación de servicio (DDoS). El primero dirigido a particulares y el segundo dirigido habitualmente a empresas.

En el año 2016 un informe de Europol[91] ya señalaba el r*ansomware* junto a los ataques de denegación de servicio (DDoS) como una de las ciberamenazas en las que la moneda virtual bitcoin era el medio preferido de pago.

Este mismo informe ha señalado a las organizaciones criminales DD4BC (*Distributed DDoS for Bitcoin*) y Armada Collective como unas de las más relevantes en esta tipología delictiva.

El grupo criminal DD4BC (Distributed DDoS for Bitcoin) fue perseguido por Europol y otros cuerpos policiales por ser uno de los grupos dedicados a atacar plataformas web enviando altas cantidades de tráfico a su red e impedir el acceso a la misma a cambio del pago de una determinada cantidad de bitcoins. Este grupo ha sido el responsable de varias campañas de ciberextorsión desde el 2014[92].

El grupo de hackers "Armada Collective" era caracterizado por ciberextorsionar a instituciones u organismos para obtener un rescate a cambio. Este grupo amenazaba con lanzar ataques DDoS contra bancos de Corea del Sur a menos que pagaran el equivalente a 315.000$ en bitcoins[93]. En este caso no se trata de una organización criminal al uso, sin embargo, con el establecimiento de las redes criminales actuales es difícil determinar si el grupo se trata de una organización criminal.

El método que siguen las organizaciones criminales en estos casos comienza por introducir el *malware* en el ordenador de la víctima mediante ingeniería social o aprovechando alguna vulnerabilidad. Una vez introducido, el *ransomware* bloquea el contenido del ordenador o una parte de este de forma que la víctima no puede acceder al

---

[91] EUROPOL, *The Internet Organised Crime Threat Assessment (IOCTA)*, 2016. Obtenido de https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf, p.16.

[92] HERNÁNDEZ, A. (13 de enero del 2016). EUROPOL y otros cuerpos policiales ejecutan operaciones contra un grupo de ataques cibernéticos. *Criptonoticias.* Obtenido de https://www.criptonoticias.com/seguridad/europol-y-otros-cuerpos-policiales-ejecutan-operaciones-contra-un-grupo-de-ataques-ciberneticos/

[93] ARCHILA, D. (23 de junio del 2017). Surcorea en alerta tras extorsión por Bitcoins a siete bancos del país. *Criptonoticias.* Obtenido de https://www.criptonoticias.com/sucesos/surcorea-alerta-amenaza-hackers-siete-bancos-pais/

mismo. Para volver el ordenador a su estado de normalidad, la organización pide a la víctima un "rescate" que se transferirá a través de métodos de pago online como "Paysafecard", "Ukash" o "MoneyPak" [94] y en la actualidad cada vez más a través del pago con criptomonedas.

Hay organizaciones criminales como la del líder ruso Alezander Krasnokutsky que han llegado incluso a conseguir que un sujeto sea víctima de *phishing* copiando la página web de la Policía Nacional y acusando al sujeto de estar en posesión de material de contenido pornográfico. En este correo se le dice al sujeto que para solucionar esa situación tenía que seguir las instrucciones que se indicaban en un enlace en el correo en cuestión. Una vez el sujeto abría el enlace el *ransomware* se introducía en su ordenador bloqueando el equipo informático o parte de este[95].

*e) Sextorsión*

Aunque puede parecer similar a la ciberextorsión, la sextorsión se diferencia de la anterior en que en este caso el delincuente extorsiona al sujeto con mostrar o distribuir fotos de él o de ella de contenido sexual. Se ha dado casos de organizaciones criminales implicadas en este tipo de delincuencia.

En el norte de África una organización criminal engañaba y manipulaba a diversos sujetos para obtener fotos de contenido sexual. Una vez habían obtenido estas fotos amenazaban a las personas en cuestión con distribuirlas a todos sus conocidos si no abonaban la cantidad pedida por la organización criminal que generalmente utilizaba criptomonedas[96].

*f) Robo de criptomonedas*

De la misma forma que el dinero fiduciario o nacional, los bitcoins han alcanzado un valor que es atractivo para las organizaciones criminales.

---

[94] VÁZQUEZ, A. (29 de febrero del 2016). Condenado a seis años de cárcel por hacerse pasar por la Policía con un virus informático. Obtenido de http://www.elmundo.es/espana/2016/02/29/56d48bfc22601d6c5f8b4581.html

[95] *Ibídem*

[96] CASAS, E., *La red oscura: En las sombras de Internet. El cibermiedo y la persecución de los delitos tecnológicos*, España, La esfera de los libros, 2017, p.75.

El valor del bitcoin cambia contantemente siendo en la actualidad de alrededor de 3.680 dólares[97]. Sin embargo, se ha convertido en un patrimonio valioso debido al elevado valor que constituye una unidad de bitcoin y la posibilidad de cambiarlo por la moneda fiduciaria de un país en cualquier parte del mundo.

En consecuencia, los bitcoins no solo se han convertido un medio muy atractivo por las organizaciones criminales para cometer delitos, sino que también se han convertido en un objetivo. En otras palabras, en la actualidad se están viendo casos en los que se roban criptomonedas.

Para llevar a cabo este delito, las personas interesadas en hacerse con las criptomonedas de otras personas han encontrado diversas formas. Habitualmente, los ladrones de criptomonedas utilizan *malware* o *phishing*[98].

Para el caso de que se emplee *malware*, destacan los ladrones de información como "dridex", un tipo de virus que se expandía a través del *spam* y podía llegar a robar credenciales bancarias y claves de carteras de Bitcoin.

Empleando *malware* también se encuentra el denominado como *cryptohacking* que consiste en la infección de ordenadores de terceros con un *malware* que permite usar estos ordenadores para minar criptomonedas sin el consentimiento de estos[99]

En el caso del *phishing* los ciberdelincuentes roban las claves Bitcoin a aquellas personas que han sido víctimas del *phishing* o correo malicioso confiando en la veracidad de la identidad de una página suplantada.

Por último, ajena a la utilización de *malware* y *phishing* para el robo de criptomonedas, se han encontrado casos curiosos en los que se ha amenazado a punta de

---

[97] COINMARKETCAP. *Bitcoin.* Obtenido el 28 de diciembre del 2018 de https://coinmarketcap.com/es/currencies/bitcoin/

[98] PÉREZ, I. (28 de septiembre del 2016). Criptomonedas son favoritas en los crímenes cibernéticos según EUROPOL. Obtenido de https://www.criptonoticias.com/seguridad/criptomonedas-favoritas-crimenes-ciberneticos-segun-la-europol/

[99] VILLAR, E. (12 de junio de 2018). El *malware* "de moda" esta primavera, *La Razón*. Obtenido de https://www.larazon.es/tecnologia/el-malware-de-moda-esta-primavera-CJ18666235

pistola a personas que paseaban por la calle con el objetivo de conseguir las claves de sus monederos electrónicos[100]. Sin embargo, este caso no es lo habitual.

## V. CONCLUSIONES

Llegados a este punto es indiscutible el hecho de que en las últimas décadas el avance de las Tecnologías de la Información y la Comunicación (TICs), el uso generalizado de Internet y el papel de la globalización en la eliminación de fronteras han traído consigo multitud de beneficios para la sociedad, la mayoría de estos relacionados con una comunicación e interconexión de una forma más rápida y efectiva.

Sin embargo, junto con los beneficios anteriores también han aparecido una serie de riesgos e incluso peligros y es que las organizaciones criminales también se han beneficiado del uso de las TICs y de Internet para desarrollar sus actividades delictivas.

De esta forma, criptomonedas como los bitcoins, aunque se crearon con una motivación totalmente lícita, están protagonizando casos relevantes de criminalidad organizada facilitando el éxito de las actividades delictivas. Constituyen un ejemplo más de cómo herramientas tecnológicas legales que se crearon para facilitar la vida de la población, están siendo utilizadas asimismo para ponerla en peligro, de la misma forma que el correo electrónico está siendo utilizado para enviar correo malicioso o *phishing*.

Por consiguiente, no hay que olvidar que las criptomonedas en sí no son ilegales, sino que es el mal uso que se hace de ellas el que es constitutivo de un delito.

El motivo de esta utilización reside en las características de estas criptomonedas como el anonimato o la descentralización, entre otras, que han resultado atractivas para organizaciones criminales que buscan desarrollar sus actividades delictivas escapando a la detección y persecución por parte de las autoridades.

Esta situación ha supuesto un gran obstáculo en la lucha contra la criminalidad organizada de este tipo, instaurando la idea de que la creatividad de los cibercriminales parece no tener límites y cada vez surgen nuevas formas de emplear las nuevas

[100] PASTOR, J. (7 de marzo del 2018). Dame tus bitcoins o te pego un tiro: hay quien roba bitcoins a la vieja usanza. Obtenido de https://www.xataka.com/criptomonedas/o-me-das-tus-bitcoins-o-te-pego-un-tiro-hay-quien-roba-bitcoins-a-la-vieja-usanza

tecnologías con consecuencias igualmente graves para las víctimas y haciéndose cada vez más difíciles de detectar y perseguir.

De esta forma, las Fuerzas y Cuerpos de Seguridad y los servicios de inteligencia se verán obligados a actuar inevitablemente tras conocer algunos casos con víctimas de criminalidad facilitada con este método de pago, ya que es muy difícil conocer con antelación las nuevas herramientas o métodos empleados por el crimen organizado.

Sin embargo, con esto no se quiere poner en duda la rapidez y efectividad de las actuaciones realizadas, sino que se pretende señalar la importancia de la investigación de la criminalidad cometida con esta moneda virtual, su *modus operandi,* las características de la moneda que la hacen atractiva para las organizaciones, los nuevos delitos que aparecen, los perfiles criminales implicados, etc. De forma que se disponga de suficiente información sobre la realidad delictiva que rodea a las criptomonedas, las herramientas puedan igualarse a las del crimen organizado y las actuaciones en este sentido puedan ser mucho más personalizadas ya que, no se puede negar la importancia de conocer un fenómeno criminal para poder elaborar medidas de actuación y prevención adecuadas y eficaces.

Por ello y dado que se trata de un tipo de criminalidad que no se circunscribe a único territorio, sino que tiene carácter transnacional, será necesaria la colaboración de todos los países y Estados implicados. Además, también será necesaria la colaboración de todas aquellas instituciones y empresas implicadas en la gestión y el funcionamiento de las criptomonedas como las casas de cambio o las empresas encargadas de gestionar monederos electrónicos. Así, deberían llevarse a cabo actuaciones coordinadas y de carácter interdisciplinar a nivel europeo dada la confluencia de diversas disciplinas que se produce en este tipo de criminalidad.

Finalmente, para conseguir todo lo expuesto también será de gran importancia la formación de los profesionales encargados de perseguir estas conductas, además de la concienciación y sensibilización de la sociedad en general. El conocimiento esta nueva forma de desarrollar la criminalidad tradicional prepara a la sociedad para que en la medida de lo posible puedan colaborar en la prevención.