



# CRIPTOMONEDAS GRUPO V



JAVIER ESPADAS

JULIO MORÁN

VERÓNICA POO

ROCÍO POZO

JARVEIR RODRÍGUEZ

ANTONIO RUÍZ





## ÍNDICE

<b>1. INTRODUCCIÓN</b> .....	<b>3</b>
<b>2. CONSIDERACIONES INICIALES SOBRE LAS CRIPTOMONEDAS</b> .....	<b>4</b>
<b>2.1. Criptomonedas o criptoactivos</b> .....	<b>4</b>
<b>2.2. Tecnología Blockchain</b> .....	<b>5</b>
<b>2.3. Riesgos (Debilidades)</b> .....	<b>6</b>
<b>3. TIPOS DE CRIPTOMONEDAS</b> .....	<b>10</b>
<b>1. BITCOIN (BTC):</b> .....	<b>11</b>
<b>4. MINERÍA DE CRIPTOMONEDAS</b> .....	<b>16</b>
<b>5. ENEMIGOS Y ALIADOS DE LAS CRIPTOMONEDAS</b> .....	<b>18</b>
<b>5.1. El Salvador: La apuesta de Bukele por el Bitcoin</b> .....	<b>20</b>
<b>5.2. Irán: electricidad subsidiada – paraíso de minado</b> .....	<b>25</b>
<b>5.3. Corea del Norte: país promotor de la ciberdelincuencia</b> .....	<b>28</b>
<b>6. TENDENCIAS CRIPTOMONEDAS Y SANCIONES</b> .....	<b>31</b>
<b>7. Bibliografía</b> .....	<b>36</b>

# 1. INTRODUCCIÓN

Las criptomonedas son un activo digital surgido en el 2009 que ha llegado para quedarse. La idea original de un sistema financiero descentralizado, con sus partidarios y detractores, ha ido implantándose en diversas esferas gracias a sus características: agilidad de transacciones, transparencia e inmutabilidad.

Las criptomonedas han dejado de ser un mero activo financiero volátil en el que invertir y es ya un fenómeno global con consecuencias para las economías de muchos países, como por ejemplo, en la factura energética.

La Unión Europea o EEUU han comenzado a regular el mercado de las criptomonedas con el objeto de mejorar su transparencia, combatir el fraude fiscal, y proteger a sus ciudadanos y sus economías de la volatilidad. Otros países, como El Salvador han ido más allá al implementar un peligroso experimento cuyas consecuencias ya están sufriendo sus arcas. Por su parte, países no occidentales bajo sanciones han visto en las criptomonedas y su minado una oportunidad para, ora mitigar el efecto de las sanciones sobre sus economías, ora eludir directamente las sanciones.

En este trabajo, nos proponemos dar una panorámica sobre la situación actual en la relación que determinados países han desarrollado con las criptomonedas gracias a sus políticas, más o menos inclusivas. Por un lado, analizamos la situación en El Salvador, el primer país del mundo en autorizar el uso de Bitcoin para el pago de productos y servicios dentro de su territorio. Por otro, hemos puesto la lupa sobre países bajo sanciones como la República Islámica de Irán y Corea del Norte. Finalmente, analizamos ciertas tendencias relacionadas con el uso de criptomonedas, tanto por actores estatales como cibercriminales apoyados por los primeros.

No obstante, antes de entrar al análisis, el lector encontrará una propedeútica introducción a conceptos como ‘criptomoneda’, ‘blockchain’ -la tecnología tras las ‘criptomonedas’ y el ‘minado’. Conceptos que cada vez ocupan más espacio informativo y, sin embargo, pocas personas han aprehendido correctamente, a pesar, de que ya forman parte de nuestras vidas.

## 2. CONSIDERACIONES INICIALES SOBRE LAS CRIPTOMONEDAS

### 2.1. Criptomonedas o criptoactivos

En primer lugar, es necesario indicar que se entiende por moneda. Tradicionalmente se ha entendido como moneda (dinero) a los activos físicos, billetes o monedas que los bancos centrales de los estados o la autoridad competente de estos ha emitido de manera oficial. Esta emisión oficial tiene el objeto de acreditar la legitimidad y valor del soporte físico dotándolo de una confiabilidad, esto asegura al usuario de divisa que el billete o moneda que poseía tenía un valor determinado y este será reconocido por el resto del mercado, permitiéndole realizar transacciones comerciales.

Por tanto se observa que el dinero, es un instrumento para la gestión de la confianza. Las personas físicas y jurídicas necesitan realizar transacciones económicas para permitir la correcta continuidad de su actividad vital. Para poder realizar esas transacciones se necesita transferirse entre las partes un valor y para ello necesitan un método de referencia que hasta ahora ha sido el dinero emitido por los gobiernos, depositando los usuarios la confianza en estos.

A este dinero se le denomina FIAT o dinero fiduciario, cuya característica es que el estado es el que ordena expedir y se encuentra respaldado por este.

Para evitar el poder de los gobiernos se crean las criptomonedas. La motivación para su desarrollo es la falta de confianza en los gobiernos, por lo que se crea un sistema en el que la confianza en el valor de la moneda no depende de actores estatales. La primera criptomoneda es el “Bitcoin” creada en 2008 por Satoshi Nakamoto, teniendo el objetivo mencionado.

**Las criptomonedas no forman parte del dinero fiduciario** ya que ni se encuentran respaldados por activos físicos como oro o plata, ni se encuentran respaldadas por los gobiernos. Su principal característica es que se basan en la confianza que los usuarios depositan en ella. Esta se articula sin necesitar de un tercero ajeno al sistema que intervenga para fijar el valor o la autenticidad del dinero, evitando mediante este diseño un sistema centralizado y desarrollando un sistema descentralizado dónde la confianza se garantiza por la arquitectura de la propia red.

Para conseguir el objetivo de tener un sistema descentralizado, las criptomonedas implantan su arquitectura de red bajo el sistema “peer to peer” de forma que se crea una cadena de bloques entre distintos nodos enlazados criptográficamente en la que todos los usuarios confían. La tecnología para desarrollar este sistema es el Blockchain.

Como se ha indicado la definición de moneda, es aquel activo físico emitido por una entidad estatal para acreditar el valor determinado del dinero. Pero esta definición no puede ser aplicada a las criptomonedas, ya que estas no tienen fijado un precio determinado, por lo que es más correcto denominarlas criptoactivos. Sin embargo, nos referiremos a estas como criptomonedas en el presente trabajo, al ser un término con el que el lector está mucho más familiarizado.

Debido a que no tiene un precio fijado por el cual se asocia un valor fijo a un determinado activo, el valor que tiene el activo dinero es el que quiera darle el usuario que lo compra. Comportándose por tanto como un activo financiero y no como una moneda que tiene un precio fijo el cual el usuario no puede modificar, el comportamiento de las criptomonedas es más similar a un activo de renta variable que al de una moneda fiduciaria.

## **2.2. Tecnología Blockchain**

Como se ha indicado el blockchain es la tecnología que permite la creación y operación de las criptomonedas, sin esta tecnología no se podría obtener la confianza requerida para el funcionamiento de estos activos financieros.

Blockchain es un protocolo o infraestructura que permite crear una red descentralizada de nodos que comparten un registro común de transacciones de cualquier tipo, basados en una cadena de bloques enlazados criptográficamente. Sus principales características son: inmutabilidad, trazabilidad, resiliencia y tokenización.

El registro es una cadena de bloques enlazados criptográficamente. Esta cadena de bloques está creada a partir de un proceso de consensos en el que todos los nodos están de acuerdo en seguir ese proceso para asegurar la fiabilidad y veracidad de ese registro.

Las transiciones que se realizan dentro del sistema (ej: Bitcoin) son validadas por todos los nodos de la red, al crearse un orden concreto a partir de enlaces criptográficos. La validación de la cadena de bloques es lo que se conoce como la “Minería de criptomonedas”.

Esta tecnología es usada por las criptomonedas ya que garantiza tener un registro distribuido e inmutable. Si se tratase de modificar un bloque sería detectado por el propio sistema ya que la cadena es redundante en múltiples nodos que forman la red, por lo que al estar replicada aun modificando una cadena y un nodo, esta modificación sería detectada por el resto de nodos indicando a la red que dicho activo no es de confianza y ha sido alterado. No solo permite detectar que el activo ha sido modificado y su valor no corresponde con el que le ha asignado la red, sino que la tecnología blockchain también permite realizar una trazabilidad de identificar quien ha realizado dicha modificación.

La tokenización es la característica de esta tecnología que permite interactuar la tecnología con un activo físico. De forma, que se asocia un token a un determinado activo físico, siendo este token una referencia blockchain, permitiendo introducirlo en el sistema de manera que convertimos un objeto físico en accionable dentro del sistema. Esta capacidad permite realizar transacciones con activos físicos dentro de la infraestructura blockchain.

## 2.3. Riesgos (Debilidades)

### 1. Minería Egoísta

Esta vulnerabilidad es una amenaza directa a la descentralización de las criptomonedas. Los mineros participan en las criptomonedas con la motivación de adquirir beneficios económicos y para ello realizan una inversión en infraestructura y recursos. La forma mediante la que obtienen los beneficios es introduciendo bloques en las cadenas de blockchain de las distintas criptomonedas, reciben una recompensa económica por cada bloque introducido.

Se encuentran dos tipos de mineros, aquellos que actúan de forma honesta poniendo en la cadena cada bloque en el momento que lo calculan y los “Egoístas”. Los mineros egoístas actúan principalmente en grupo o en diferentes grupos coordinados, aunque también actúan de manera individual.

Por el diseño de la red de blockchain de las principales criptomonedas, se puede dar la situación en el que la cadena de blockchain se divida en dos ramas similares que confluyen. Al objeto de resolver este cálculo los protocolos establecidos por la mayoría de criptomonedas disponen la cadena de bloques más desarrollada ( la más larga) como la correcta. En el momento que se válida la cadena de bloques más larga, el resto de cadenas desarrolladas en paralelo que son

más cortas quedan eliminadas y por tanto el beneficio económico se lo adjudicó aquel minero que ha desarrollado la cadena larga.

Esta característica es aprovechada por los mineros “egoístas”, explotan la vulnerabilidad de la siguiente forma: En primer lugar, incitan al resto de mineros a desarrollar cálculo de ramas de bloques antiguas o sin capacidad de crecimiento. Mientras el resto de mineros cuando calculan un bloque lo ponen a disposición de la red para poder construir la cadena, estos mineros “egoístas” cuando encuentran un bloque se lo quedan en privado y no lo comparten. De manera que desarrollan una cadena de bloques más larga que la del resto de mineros ya que son los únicos que poseen los bloques previos necesarios para realizar el cálculo. Por último, esperan a liberar su cadena de bloques en el momento que más pueden impactar en el resto de mineros, de forma que la ponen en la red cuando los mineros “honestos” van a alcanzar el cálculo de una cadena. Con esta acción no solo consiguen obtener ellos todo el beneficio económico, sino que eliminan a la competencia, ya que el resto de mineros no obtiene ningún beneficio económico y su gasto en infraestructura y recursos no se amortiza , provocando que tenga que abandonar el minado.

Esto provoca que una de las principales características de las criptomonedas que es la **descentralización** se vea amenazada, ya que el proceso de validación de bloques se queda centralizada en unos pocos mineros.

Se han desarrollado criptomonedas que evitan esta vulnerabilidad, como es el caso de “Ripple” que no permite la minería de su activo.

## **2. Escalamiento.**

Las características de configuración de las criptomonedas no permiten su implantación a gran escala. Esto es debido a que la tecnología de blockchain está diseñada para ser una herramienta segura pero no una tecnología rápida, debido a los cálculos necesarios para realizar una transacción se requiere de una cierta cantidad de minutos para poder validarla. Esta característica impide que por el momento se pueda implantar una criptomoneda como moneda principal de un país ya que no sería operable a gran escala.

## **3. Wallet/Cartera.**

Tradicionalmente uno de los puntos más vulnerables de la gestión de activos fiduciarios ha sido su depósito y custodia, esto también sucede con las criptomonedas. Para poder gestionar

las criptomonedas, es decir, para mantenerlos en depósito o realizar transacciones con ellos, los propietarios de estos necesitan de una cartera o monedero.

Actualmente se encuentran disponibles 5 tipos diferentes de carteras:

1. Hardware. Son aquellas carteras tipo memoria “USB”. El propietario guarda las claves que le permiten operar sus criptomonedas en dicha memoria física.
2. Software. Son soluciones de custodia no física. Dentro de esta modalidad se pueden distinguir tres tipos: 1-web dónde se depositan las claves en una página web ajena al usuario o en una nube virtual propia. 2-Escritorio, se guardan las claves en el escritorio (memoria interna) de un ordenador del titular y por último 3- móvil, en esta modalidad de cartera se custodian las claves en el dispositivo móvil del usuario.
3. Monedero de papel. Se denomina de esta forma al procedimiento de custodia, en el que el propietario escribe en un papel físico las claves de operación de sus criptomonedas, no depositando las claves en ningún medio tecnológico.

Se debe tener en cuenta que las claves de operación son las que permiten disponer de los activos y operar con ellos, por lo que sería necesario encriptarlas o realizar copias de seguridad. Estas claves son el principal objeto de ataque de los criptohackers ya que son el punto más débil de la cadena y el más fácil de explotar. La encriptación es necesaria para que en el caso de ser robadas o hurtadas las claves no puedan ser operables. Las copias de seguridad son necesarias debido a que la mayoría de carteras se encuentran respaldadas en medios físicos que en el caso de sufrir un ataque, accidente o pérdida si no se tienen en redundancia, se perderían los activos.

Los principales ataques que se han producido contra las “wallet” y que han conseguido sustraer grandes cantidades económicas, no se han realizado mediante complejos ataques informáticos, sino mediante ingeniería social. Por lo que no solo se debe disponer de un sistema de depositado correctamente encriptado y redundante, sino que debe ir aparejado con una correcta concienciación del usuario, a pesar de ser activos virtuales el eslabón más débil sigue siendo la persona física.

#### **4. Ataque 51%**

Como se ha indicado con anterioridad una de las principales características de las criptomonedas es su descentralización, es decir, que la confianza en el sistema no depende de

un único organismo o grupo y radica en la integridad de todos los usuarios de la red. Impidiendo mediante este protocolo que un grupo pueda tomar decisiones que alteren el mercado buscando objetivos particulares.

Las primeras criptomonedas como el “Bitcoin”, al objeto de intentar garantizar su descentralización implementaron en su red un protocolo “Prueba de trabajo” (“POW”). Este protocolo consiste en que el usuario que quiere introducirse en la red en este caso para minar debe realizar una prueba de trabajo, en concreto, una prueba de cálculo compleja. Se implantó el “POW” para evitar ataques de denegación de servicio y la introducción en la red de usuarios maliciosos, pero debido a la alta potencia de cálculo requerida se limita el acceso a usuarios pequeños. Debido a ello se han ido creando agrupaciones de mineros o “pool” tienen el objetivo **de agrupar potencia de cálculo de distintos mineros y procesan bloques de código de manera conjunta**. Esto crea la vulnerabilidad de dar un control amplio a determinados grupos de minero, teniendo estos la capacidad de influir en la criptomoneda si consiguen superar la barrera del 51% de potencia de computación total de la criptomoneda, perdiendo por tanto el activo su descentralización.

No es necesario que la agrupación de mineros llegue al 51%, con un control superior al 25% ya podrían limitar cadenas de códigos de competidores o bloquear transacciones no realizando su validación.

Para evitar esta vulnerabilidad determinadas cripto criptomonedas activos desarrollaron el protocolo “prueba de participación” (“Proof of Stake (POS)”). Este protocolo no requiere una gran potencia de cálculo ya que no solicita realizar operaciones de cálculo, sino que requiere de un compromiso del minero con la red. De forma que para poder validar operaciones o participar en la red se requiere mantener los activos durante un determinado número de tiempo, lo que evita las vulnerabilidades del 51% ya que no es sostenible para un minero o agrupación mantener en propiedad esa cantidad durante el tiempo requerido. A la vez, la configuración del propio protocolo establece la validez de los activos para impedir que se pueda alcanzar una acumulación superior al 51%. Este protocolo también evita la vulnerabilidad de los mineros “egoístas”, al no depender únicamente de la potencia de cálculo de código.

## 5. Identidad /anonimidad (Mezcladores)

A pesar de la creencia popular de que las criptomonedas facilitan la anonimidad del propietario de los activos, la realidad es completamente opuesta. Como se ha indicado las criptomonedas

se basan en blockchain y en protocolos de confianza , esto supone que el propietario de una criptomoneda se encuentra perfectamente identificado por el resto de la red. Las criptomonedas van asociados a un código cifrado único para cada propietario por lo que toda la red conoce a quien corresponde cada activo y una de las bases de la red es que terceros validen que dicho activo está asociado a un propietario concreto.

Debido a esta característica estados que quieren eludir sanciones internacionales, y a su vez determinados actores no estatales como grupos criminales utilizan tecnología que dificulta conocer la identidad del propietario de las criptomonedas. Para ello utilizan los mezcladores de criptomonedas.

**Los mezcladores de criptomonedas tienen la finalidad de ocultar la propiedad real de estos.** Para ello realizan un protocolo de mezcla que funciona de la siguiente manera; los usuarios que tiene la intención de ocultar la propiedad de sus criptomonedas los depositan en una cuenta, en esta cuenta se encuentran criptomonedas de distintos usuarios y de distinto tipo. Para lograr la anonimidad de los titulares el protocolo de mezcla intercambia la titularidad de los activos entre los usuarios y a la vez troca los distintos tipos de criptomonedas entre ellos, de manera que las criptomonedas que recibe el usuario al finalizar el proceso son distintos a los que deposito, mitigando de esta forma su huella de identidad en las criptomonedas.

Estos mezcladores, si bien proporcionan anonimidad tienen riesgos ya que para poder realizar la operación es necesario que los usuarios depositen sus criptomonedas en una cuenta externa y otorguen el control de los mismos a un tercero desconocido, creando una ventana de oportunidad para su sustracción.

Entre los más destacados se encuentra “Tornado Cash” que opera con Ethereum y el Tesoro Americano identificó que fue usado por un grupo de criptohackers asociados a Corea del Norte. Otro de los protocolos de mezcla más usado es “Wasabi Wallet” que utiliza la red Tor para mezclar las criptomonedas.

### 3. TIPOS DE CRIPTOMONEDAS

Actualmente existen **casi 10.000 monedas virtuales** a nivel mundial. Una cifra que no cesa de crecer, pues surgen nuevas criptodivisas cada cierto tiempo, creadas mediante el proceso ICO. La diferencia entre estas divisas radica en su tecnología, la encriptación y la filosofía utilizada. Si bien, la mayoría usan la tecnología Blockchain, aunque no es la única.

---

Número de divisas: 9.497

Capitalización de mercado total: \$922,98B

Volumen 24 h: \$45,61B

---

La creación de estas criptomonedas implica la aparición de plataformas para enviar, recibir y comprar las criptomonedas (p.ej.: Bitcoin, Bitcoin Cash y Ethereum) y los wallets o monederos de criptomonedas, que son el puente que nos permiten administrar nuestras criptomonedas, es decir, una pieza de software o de hardware con los que realizar las operaciones de recepción y envío a través de la red blockchain de cada criptomoneda.

**El auge del Blockchain augura la consolidación de las divisas virtuales** y la llegada de más inversores, incluyendo los Gobiernos.

Una de las principales críticas radica en la huella de carbono de estas criptomonedas, dada la elevada cantidad de energía necesaria para su minado y para confirmar transacciones en la cadena de bloques. Si Bitcoin y Ethereum fueran un país separado, Bitcoin y Ethereum combinados tendrían el 12º mayor consumo de energía de cualquier país, solo detrás del Reino Unido y Francia. Con emisiones de 50 a 60 millones de toneladas de CO<sub>2</sub> al año, Ethereum es casi el doble de dañino para el clima que la central eléctrica de carbón más grande de Europa.

A continuación se exponen las 3 criptomonedas más relevantes según el capital de mercado.

## 1. BITCOIN (BTC):

Lanzamiento y adopción (2008-2010):

El Bitcoin ha sido la criptomoneda pionera. El 1 de noviembre de 2008 fue creada por varias personas bajo el pseudónimo Satoshi Nakamoto. En su origen se describió como «un nuevo sistema de efectivo electrónico» llamado Bitcoin «que es totalmente peer-to-peer y que no está basado en terceros de confianza», además, se hace referencia a un documento técnico titulado *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, s/f), y en el que se explica el funcionamiento del protocolo propuesto.

El 3 de enero de 2009 entra en funcionamiento la primera red peer-to-peer basada en dicho protocolo (también bajo el nombre de «Bitcoin»). Ello supuso la creación de los primeros bitcoins y el inicio de la minería de esta criptomoneda. El bloque de génesis de Bitcoin fue minado por el propio Satoshi Nakamoto.

El 9 de enero de 2009 se lanza el primer cliente de software de código abierto para correr nodos de la moneda a través de la plataforma SourceForge.

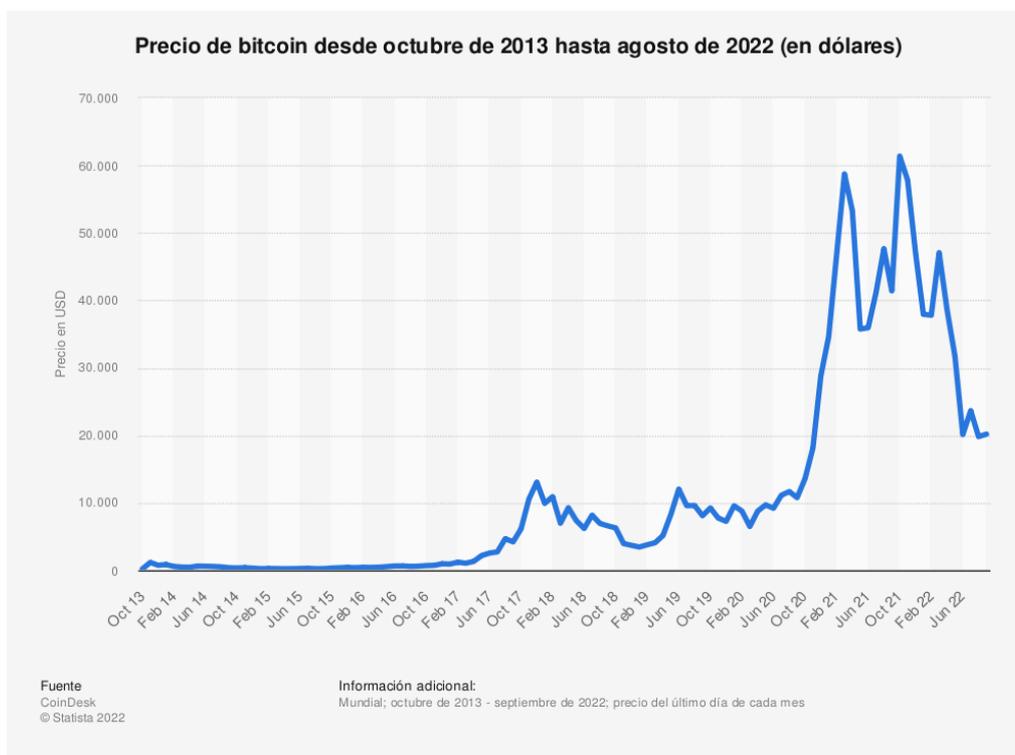
Bitcoin es la primera y principal criptomoneda del mercado. Se considera la referencia del mercado, destacando que la capitalización de mercado de Bitcoin es superior a la de la suma del resto de criptomonedas. Su precio máximo histórico hasta la fecha es de 68.789,63 USD, alcanzado en noviembre de 2021.

Bitcoin se emplea también como valor refugio, llegándose a comparar con el oro; si bien la volatilidad de Bitcoin es muchísimo más elevada. Para conseguir ese valor refugio, la emisión de Bitcoin está limitada a 21 millones de BTC, lo que implica una “escasez” similar a la del oro.

En España se pueden comprar Bitcoin a través de diversas plataformas o agencias de cambio acreditadas, denominadas exchanges, que pueden ser físicas o digitales. Es por ello que invertir en Bitcoin es igual de viable que hacerlo en cualquier divisa de curso legal.

Al almacenar los Bitcoins en un wallet o monedero se garantiza la custodia del activo, lo que permite protegerse frente a hackeos o la quiebra del exchange o plataforma donde se adquirieron.

Cabe destacar que de la criptomoneda principal surgió Bitcoin Cash tras una bifurcación en diciembre de 2017. El objetivo es aumentar el número de transacciones que soporta la red, dado que la tecnología blockchain hoy en día tiene ciertos problemas de escalabilidad y de procesar muchas transacciones a la vez. Existen similitudes entre ambas criptomonedas, si bien Bitcoin cuenta con un tamaño del bloque de 1MB y Bitcoin Cash de 32MB, lo que implica que las transacciones con Bitcoin Cash se procesan con una comisión más barata. Además, al usar más bloques (32 MB) la seguridad de la Bitcoin Cash se reduce.



Fuente: [Statista](#)

## 2. ETHEREUM (ETH):

Ethereum no es una divisa, sino una plataforma de código abierto, que sirve para ejecutar contratos inteligentes. Ethereum se considera como una blockchain de 2º generación, donde su principal característica es ser programable, lo que significa que los desarrolladores pueden usarlo en la creación de aplicaciones descentralizadas.

Estas aplicaciones descentralizadas (abreviado en inglés como *dapps*) se valen de la capacidad de transaccionar de las criptomonedas, la programabilidad de un contrato inteligente y la tecnología de cadena de bloques. Son confiables y predecibles, lo que significa que una vez que se cargan (minan) en Ethereum, siempre se ejecutarán según lo programado.

Pueden controlar los activos digitales para crear nuevos tipos de aplicaciones financieras.

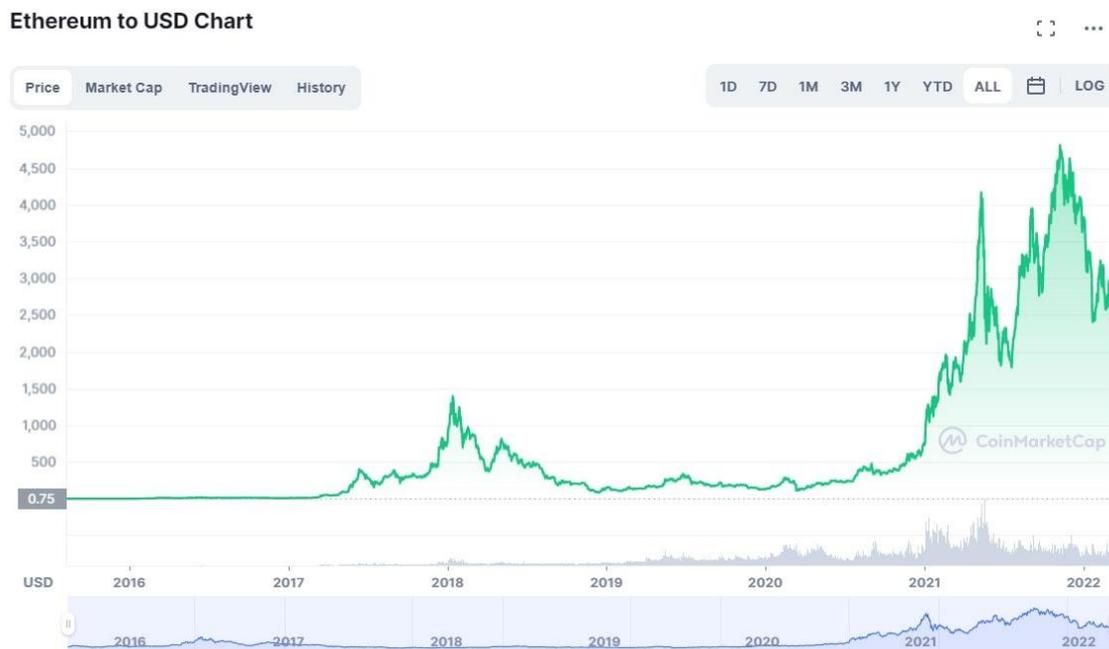
En este momento, miles de desarrolladores de todo el mundo están creando aplicaciones en Ethereum e inventando nuevos tipos de aplicaciones, muchas de las cuales pueden usar hoy en día:

- Carteras de criptomonedas que le permiten realizar pagos baratos e instantáneos con ETH u otros activos (tókenes).

- Aplicaciones financieras que le permiten pedir prestado, prestar o invertir sus activos digitales.
- Mercados descentralizados, que permiten intercambiar activos digitales, o incluso intercambiar "predicciones" sobre eventos en el mundo real.
- Juegos donde tienes activos en el juego e incluso puedes ganar dinero real.
- Tókenes no fungibles.

Después de una bifurcación de la blockchain en julio de 2016, hay dos cadenas de bloques de Ethereum activas: Ethereum y Ethereum Clásico.

### Gráficos de precios de Ethereum desde su creación



Fuente: [Stormgain](https://stormgain.com)

### 3. TETHER:

Tether es una moneda estable o stablecoin, a la par que una criptomoneda. Lo que diferencia a esta divisa digital con el resto de monedas, como bitcoin o ethereum, es que todas las stablecoin en circulación están respaldados por una cantidad equivalente de las monedas fiduciarias tradicionales, como el dólar, el euro o el yen japonés. En el caso de Tether está vinculado al dólar estadounidense y mantiene una relación de 1 a 1 en términos de valor. Es decir, 1 Tether equivale a 1 Dólar. Esto significa que originalmente un USDT (nombre del token) se diseñó para que valiera siempre un dólar, manteniendo un dólar en reservas por cada Tether emitido.

Tether fue diseñado específicamente para construir el puente necesario entre las monedas gubernamentales y las criptomonedas y ofrecer estabilidad, transparencia y cargos mínimos por transacción a los usuarios. Al ser una stablecoin, no se mina. Simplemente se va creando más monedas y va variando su precio en función del dólar americano. Con todos los pros y los contras que ello conlleva, como por ejemplo que no es una divisa para salvar la inflación que se dé en los Estados Unidos.

Entre las ventajas de Tether destaca que su precio es estable, que el envío de dinero no supone costes por la transacción y puede suponer un refugio de capital para los traders o inversores que deciden desinvertir de una criptomoneda no estable sin cambiar sus activos por dinero gubernamental. Pueden convertir sus criptomonedas en Tether y posteriormente en otro criptoactivo en el que quieran invertir.

Aunque no todo son ventajas y existe gran preocupación en cuanto a la gestión y tesorería de Tether Ltd. El 14 de marzo de 2019, Tether Ltd. cambió el respaldo del dólar exclusivo para incluir préstamos a empresas afiliadas. Y el 30 de abril de 2019, el abogado de Tether Ltd. afirmó que cada Tether estaba respaldado por solo \$0,74 en efectivo y equivalentes de efectivo.

Ahora bien, la utilidad del USDT es su principal atractivo. Es una de las divisas más utilizadas, incluso a veces supera a Bitcoin. El motivo es que cuenta con los beneficios de ser una criptomoneda y con ser equivalente al dólar. Tether también se emplea para las transferencias internacionales con la ventaja de reducir los tiempos a minutos y sin apenas comisiones.

Otra ventaja radica la mayor accesibilidad al USDT que a la moneda de dólar física. Si un país con inflación alta o hiperinflación, como el caso de Argentina, desea poseer dólares, pues es algo preciado, puede tener problemas para acceder a los dólares o deben recurrir al mercado paralelo para intercambiar las divisas. Sin embargo, con USDT es más accesible.

Existe una cara oculta de esta criptodivisa al encontrarse problemas en sus auditorías y problemas a la hora de verificar las cuentas, personas y organizaciones que usan Tether para ocultar su rastro.

Desde el punto de vista inversor, Tether no es un activo tan interesante como los anteriores, ya que no se va a revalorizar, sino que fluctúa en consonancia con el dólar americano.

## 4. MINERÍA DE CRIPTOMONEDAS

Como hemos dicho, se llama minería al proceso necesario para validar las operaciones que se llevan a cabo mediante este tipo de activos digitales. Por ejemplo, en el caso de un bitcoin: su minería se basaría en la validación y el registro de las transacciones en el registro *blockchain*.

Los mineros que llevan a cabo este proceso obtienen a cambio criptomonedas.

Para la minería se requiere una gran cantidad de potencia informática, y muchos recursos, además de una red eléctrica estable. La minería requiere un *software* específico para la resolución de problemas matemáticos, la verificación de la transacción legal que confirma que un bloque, que se va agregando al libro mayor público, es realmente un bloque.

Cuanto más rápido el hardware del minero pueda procesar estos problemas matemáticos, más probable es que verifique las transacciones y se lleve la recompensa.

La minería de criptomonedas normalmente requiere dejar encendido un equipo las 24 horas del día, los 7 días de la semana para que a través de un programa informático se realice automáticamente la tarea de ‘extraer’ bloques en una Blockchain. Por tanto, la determinación de la ubicación de los mineros en un país u otro depende principalmente de tres factores:

- el coste energético de tener los equipos funcionando
- el hardware a utilizar
- el software para funcionar.

El “*hashrate*” es la unidad de medida de la potencia de procesamiento de la red Bitcoin, o dicho en otras palabras, lo que determina su capacidad para producir nuevas monedas.

El precio de **Bitcoin** se ha multiplicado los últimos años y esto está provocando un aumento en el consumo de la energía eléctrica. Los equipos de minería están formados por CPUs y tarjetas gráficas muy potentes que tienen que resolver problemas matemáticos complejos. Además, a medida que los mineros resuelven los problemas reciben recompensas en la criptomoneda minada, lo que hace que a su vez haya mas gente compitiendo para extraerla necesitando más y más energía.

Según un análisis realizado por el *New York Times*

- **La minería de bitcoin consume alrededor de 91 teravatios hora de electricidad al año.**

- Eso **supera al consumo anual de electricidad de Finlandia**, que tiene 5,5 millones de habitantes.
- Este volumen de gasto **diez veces superior al de hace cinco años** y representa, casi el **0,5% de todo el consumo de electricidad en el mundo**.
- Tiene un consumo energético siete veces superior al que realiza Google en sus operaciones en todo el mundo en un año.

Debido al gran consumo de energía necesaria en la minería de criptomonedas, esta actividad suele concentrarse en países menos desarrollados y con bajos precios de electricidad. Pero esto está suponiendo que se disparen los consumos provocando problemas de suministros y un alza de los precios. Muchas regiones que antes recibían a los mineros con los brazos abiertos ahora han cerrado las puertas a la actividad llegando incluso a prohibirla.

Este ha sido por ejemplo el caso de China. Hasta junio de 2021, China, que cuenta con una red eléctrica barata, fue el principal destino de las minas de datos concentrando el 34% del hashrate. En septiembre del mismo año, Pekin declaró ilegal las transacciones con criptomonedas, incluido el minado alegando un problema de seguridad nacional debido a los problemas de suministros provocados en el sur del país por el alto consumo energético.

El principal destino pasó a ser Estados Unidos dominando con un 35% y llegando a controlar más de un tercio del poder computacional del Bitcoin, seguido de Kazajistán con un 18%, Rusia con un 11%, Canadá con un 10%, Irlanda con un 5%, Malasia con otro 5% y Alemania con un 4%.

Muchos de los mineros de China, ante la prohibición del gobierno, se fueron a países como Kazajistán debido a los bajos precios de la energía en el país. El país asiático ha llegado a concentrar el 18% de toda la minería de las criptomonedas del mundo, lo que ha supuesto un coste energético inasumible para el país llegando a provocar revueltas ciudadanas debido al aumento del precio de la electricidad. El Gobierno Kazajo ya ha impuesto limitaciones provocando que los mineros se desplacen a otras regiones.

En el caso de Islandia, a finales del 2021 La escasez de energía en la isla provocó que Landsvirkjun, la principal empresa de servicios públicos de la isla redujera los suministros a algunos clientes industriales, obligando a la empresa a rechazar a nuevos mineros de Bitcoin que se habían establecido en el país atraídos por los bajos precios de la energía. Es el mismo

caso el de Kosovo que siendo uno de los países más pobres de Europa se ha visto afectado por varios cortes de energía lo que ha derivado en la prohibición de minar criptomonedas en la región. Por su parte Suecia ha sugerido a Europa la posibilidad de prohibir la extracción de los criptoactivos ya que requiere grandes cantidades de energía y genera grandes emisiones de CO2 que amenazan el cumplimiento de los Acuerdos de París.

Sin embargo, como imaginará el lector, existe una gran diversidad de opiniones a nivel subestatal respecto a la conveniencia y riesgos de adoptar las criptomonedas como monedas de cambio, o simplemente de invertir en ellas.

## **5. ENEMIGOS Y ALIADOS DE LAS CRIPTOMONEDAS**

El auge de las criptomonedas ha obligado a Estados de todo el mundo a debatir y tomar una determinación sobre el nivel de “tolerancia” que se tendrá con ellas. En países de nuestro entorno, en mayor o menor medida, se ha comenzado a regular los criptoactivos con el objetivo de combatir el fraude fiscal. No obstante y a pesar de lo que pudieran sugerir los titulares, existen serias dudas y diferencias sustanciales de opinión entre diversos actores estatales y gubernamentales sobre los riesgos de un sistema financiero descentralizado.

Tradicionalmente, los Bancos Centrales han sido los enemigos de las criptomonedas. Sus presidentes han denunciado en innumerables ocasiones los elevados riesgos asociados con las mismas para los ciudadanos de sus países y para la economía en general. La volatilidad de su valor y la falta de herramientas para controlarla son, desde el prisma de las autoridades monetarias, una amenaza para la estabilidad económica de un país.

Además, las criptomonedas suponen una amenaza a la mera existencia de los Bancos Centrales. Una de las funciones principales de un Banco Central es controlar la inflación de la moneda a través de los tipos de interés. Si los ciudadanos de un país dejaran de usar la moneda regulada por su banco central para usar criptomonedas, los Bancos Centrales y, los Ministerios de Economía de ese país perderían su capacidad de implementar una política monetaria efectiva para proteger la economía.

Estas reticencias han sido habituales entre los bancos centrales de países occidentales y no-occidentales de igual manera. Incluso en países como Irán, donde el minado de criptomonedas

está actualmente regulado y se emplea para eludir sanciones (véase sección sobre Irán), se prohibió su uso en 2018 en el interior del país.

En contra de las autoridades monetarias han estado a menudo los Ministerios de Finanzas y agencias fiscales. La razón es que, desde la perspectiva de estas últimas autoridades, mediante la prohibición y la política de no regulación de los criptoactivos, el Ministerio estaba perdiendo una fuente de ingresos muy importante derivada de la aplicación de impuestos a dichas transacciones.

Los servicios de inteligencia y las fuerzas del orden, por su parte, también alertan de los riesgos para la seguridad del país que suponen las criptomonedas. Por un lado, el crimen organizado, el lavado de dinero y la contratación de servicios ilegales en la deep web es algo que, si bien sigue siendo mucho menor que el volumen de moneda FIAT usado para actividades criminales, está creciendo rápidamente. Por otro lado, en países menos democráticos, como en la Federación Rusa, entran en juego otras consideraciones. Por ejemplo, el FSB se opuso durante meses a la aprobación del uso de criptomonedas debido al uso de estas por activistas políticos para financiar las actividades de políticos como Alexei Navalni.

A pesar de estos aspectos generales compartidos por todo tipo de Estados, observamos una clara bifurcación entre los intereses y preocupaciones de los organismos pertenecientes a países occidentales y aquellos de países no occidentales. Esta diferenciación es más pronunciada si cabe entre democracias occidentales y países menos democráticos y bajo un régimen de sanciones, para los que las criptomonedas abren un amplio abanico de posibilidades.

Países de la Unión Europea, por ejemplo, ven en la tecnología blockchain que sostiene las criptomonedas una potencial oportunidad para mejorar la seguridad y velocidad de las transacciones, así como la identidad de las partes en esa transacción. Por el otro lado, países sancionados como Corea del Norte han encontrado en las carencias en materia de seguridad de algunos criptoactivos una oportunidad inigualable para conseguir realizar robos por valor de cientos de millones de dólares. Otros, como la República Islámica de Irán, han visto en el sistema de minado de Bitcoin una forma de eludir sanciones.

Esto supone una clara bifurcación en el desarrollo no solo de minado o uso de criptomonedas, sino en las futuras regulaciones que estos Estados de los activos digitales y que traerán como consecuencia un contrapeso que socavará la efectividad de las regulaciones propuestas recientemente por, entre otros, la Unión Europea.

A continuación, ahondamos en la situación en distintos países, comenzado por El Salvador, pionero en la adopción del Bitcoin como moneda de curso. Para entender cómo ha llegado el país centroamericano a esta situación, es preciso viajar a una pequeña localidad en el Oeste del país.

### 5.1. El Salvador: La apuesta de Bukele por el Bitcoin

En el año 2019, en la localidad de El Zonte, un pueblo costero al occidente de El Salvador, el estadounidense Mike Peterson, quién dirige la *Hope House* —una organización sin ánimo de lucro en pro del desarrollo de la zona— fue contactado por un donante anónimo que quería contribuir con bitcoin (BTC) a la labor altruista. La condición: que los BTC no fueran cambiados a dólares (USD), sino que se emplearán en proyectos locales y se les enseñara a los residentes sobre el uso y funcionamiento de la criptomoneda; con el fin de establecer un modelo de economía circular en la zona (González Díaz, 2021). En un inicio la tarea fue principalmente pedagógica porque se dieron charlas y cursos, pero pronto se comenzó a pagar en BTC a los más jóvenes. Desde entonces, el empleo de la criptomoneda se ha ido extendiendo en la comunidad y se estima que hasta la fecha El Zonte ha recibido alrededor de 350.000 USD de su benefactor anónimo (Tidy, 2022).

Según los residentes locales, tras la introducción de BTC por parte de donantes anónimos, el volumen de transacciones aumentó en un 30%, ya que muchos turistas de BTC y amantes de las criptomonedas se sintieron atraídos por la novedad de usar la moneda digital allí (El Zonte, pueblo de El Salvador pionero en el uso de Bitcoin, 2022). Tal fue el auge de la medida que incluso la localidad empezó a ser conocida como *Bitcoin Beach* o Playa Bitcoin.

Inspirado por el proyecto y los resultados alcanzados en la región de El Zonte, el presidente Nayib Bukele sugirió al Congreso salvadoreño la “Ley Bitcoin”, según la cual la criptomoneda se legalizaría con el dólar como monedas de curso legal en El Salvador a partir del 7 de septiembre del 2021 (Tidy, 2022). Las disposiciones legales del Capítulo I, Artículo 1, que tienen por objeto regular a BTC como una moneda de curso legal, con poder liberatorio, sin limitación en cualquier transacción y en capacidad de ser efectuada por una persona natural o jurídica, pública o privada, sin afectar la aplicación de la Ley de Integración Monetaria (Dictamen Comisión Financiera N.º 3 - Ley Bitcoin, 2021).

Otros puntos importantes de la ley son: la determinación de la tasa de cambio entre BTC y el USD será determinada libremente por el mercado; los impuestos y tarifas se pueden pagar en BTC y todos los comerciantes deben aceptar BTC o su equivalente exacto en USD cuando los clientes ofrecen BTC como forma de pago; todos los precios pueden expresarse en BTC; todas las obligaciones adquiridas en USD que existían antes de la fecha de vigencia de la Ley pueden ser en BTC. Finalmente, cabe señalar que El Salvador ofrecerá permitir a los usuarios pagar en BTC o USD y el Gobierno proveerá alternativas que permitan al usuario llevar a cabo las transacciones, asimismo, promoverá la capacitación necesaria para que las personas puedan comerciar con BTC (Marín, 2021).

Para facilitar las transacciones diarias y el uso de BTC, el Gobierno de El Salvador desarrolló *Chivo Wallet*, una billetera digital oficial de El Estado. *Chivo Wallet* permite enviar y recibir BTC y USD entre salvadoreños, y también cambiar BTC a USD y viceversa, todo esto sin comisión (Chivo Wallet, 2022). Chivo también es compatible con otras billeteras digitales. La billetera está conectada al sistema bancario de El Salvador y a la red de cajeros automáticos de Chivo para depositar y retirar efectivo en USD. También tiene una versión empresarial que le permite cobrar tarifas, asignar terminales de pago a los empleados y pagar impuestos de forma rápida y sencilla (Chivo Wallet, n.d.).

Para incentivar la utilización de BTC, el gobierno ha ofrecido un bono de 30 USD a cada nuevo usuario que descargue y use la billetera. No obstante, un año después de la entrada del BTC como moneda de curso legal, los salvadoreños no emplean la criptomoneda más allá de cobrar el bono incentivo de la Chivo (Alfaro, 2022). Además, también hay discrepancias en la cantidad de usuarios de la Chivo. Según la BBC, más de 4 millones de usuarios de BTC han descargado la billetera virtual, en un país donde solo unos 3 millones de habitantes tienen acceso a internet, es decir, en El Salvador hay más cobradores de bonos que usuarios reales de BTC (Tidy, 2022).

A pesar de las medidas gubernamentales para promover el uso de BTC, actualmente no está muy extendido, ya que la Cámara de Comercio e Industria de El Salvador (CAMARASAL) afirmó en un estudio publicado en marzo de 2022 que el 86% de las empresas encuestadas nunca habían efectuado transacciones con BTC, lo que indica que son muy pocas las empresas que utilizan la moneda (Alfaro, 2022).

Otra piedra en el zapato de Bukele ha sido la alta volatilidad del Bitcoin; es decir, las fluctuaciones en el rendimiento de la moneda. Actualmente, el precio de BTC ha caído tanto que para mayo de 2022 ha perdido aproximadamente un 56 % de valor en lo que se refiere a su precio máximo histórico en noviembre de 2021. Desde la primera compra de BTC el 7 de septiembre de 2021 hasta el 7 de septiembre de 2022, la pérdida estimada es de alrededor de 50 millones USD (Diario Bitcoin, 2022). En los menos de 10 meses desde que El Salvador convirtió BTC en moneda de curso legal y hasta la última compra de BTC, los precios han oscilado bastante; el precio ha variado entre los 64.400 USD y los 19.000 USD. El siguiente gráfico muestra los cambios de precio de BTC (Deutsche Welle, 2022).



(Gráfico tomado de Deutsche Welle, 2022)

Como se puede ver en el gráfico, las fechas en que El Salvador compró BTC muestran un cambio de precio significativo. Esta inconsistencia en los criterios de compra revela la intención que aunque se tuviese por objeto comprar BTC a un precio bajo para obtener ganancias a medida que sube su rendimiento, en la práctica, la compra ha sido en periodos prósperos, por lo que la tendencia general apunta a pérdidas asociadas a la depreciación de BTC frente al USD (Bitcoin en El Salvador: un ejemplo para el mundo, 2022).

La variación en los tipos de cambio son un factor de incertidumbre económica y, según varios expertos, lo que ha causado pérdidas de alrededor de 50 millones USD para El Salvador. Si bien, 50 millones USD equivalen a menos del 0,2% del PIB del país, si se comparara el total



de BTC expresado en USD con el presupuesto del país para 2022, es posible notar que este dinero corresponde a cerca del 1,31% del presupuesto nacional salvadoreño (Diario Bitcoin y Deutsche Welle, 2022). Un monto de más de 100 millones USD que, según detractores de la medida, podría haberse invertido en otros sectores de gran importancia para El Salvador, como la salud, la educación o la seguridad ciudadana. Además, se debe recordar que el dinero que se usó para construir la infraestructura tecnológica, los fondos convertidos de USD a BTC y los bonos de incentivo entregados para la Chivo corresponden a algo más de 203 millones USD. Capital que sumado al monto de pérdidas, según expertos, hubiera podido implementarse en proyectos que respondieran a necesidades de El Salvador y sobre todo considerando que dichos montos son propiedad del erario público salvadoreño (Bitcoin en El Salvador: un ejemplo para el mundo, 2022).

Solo el 20% de la población del salvador emplea BTC a diario, y un estudio de la Universidad Centroamericana (UCA) muestra que 7 de cada 10 salvadoreños no están de acuerdo o se oponen rotundamente a BTC. Además, la misma encuesta muestra que el 82,8% de la población tiene poca o ninguna confianza en BTC (El Salvador adopta el bitcoin: ocho claves para entender su uso como divisa legal, 2021). Es probable que esta desconfianza se deba a acciones como la calificación crediticia emitida por la firma *Fitch*, la cual ha situado a El Salvador como un país con un perfil financiero altamente vulnerable; con riesgo de impago y bonos muy especulativos (Plaza, 2022).

Esta degradación crediticia significa que El Salvador es más proclive a incumplir los compromisos financieros adquiridos, y que además otorgarle un crédito es de alto riesgo, afectando severamente la confianza en la economía local y reduciendo la inversión extranjera. Adicional a la desconfianza y degradación de la calificación financiera del país, actualmente, El Salvador es, después de Venezuela, el país con más riesgo para inversión en Latinoamérica, según el indicador de *Emerging Markets Bond Index* (EMBI), prueba de este mal desempeño es la devaluación de los bonos soberanos de países en vía de desarrollo los cuales pasaron de un precio de 62,24 USD a 38 USD, es decir un retroceso cercano al 55% (Álvarez, 2022).

El Fondo Monetario Internacional (FMI) ha instado a derogar la Ley Bitcoin en El Salvador y ha avisado de los riesgos de la adopción de la criptomoneda como moneda de curso legal, considerando que esta medida puede incrementar los riesgos regulatorios para instituciones financieras, incluyendo la posibilidad de violar leyes contra el blanqueo de capitales y financiación del terrorismo. Y, el Instituto Centroamericano de Estudios Fiscales (ICEFI)

llamó a anular el uso de BTC en El Salvador debido a los grandes costos generados y la falta de beneficios reales para la población (La Vanguardia, 2022).

Si bien BTC actúa como moneda de curso legal en El Salvador, no se debe olvidar que las criptomonedas no tienen un banco central que las regule, ni una autoridad para determinar su uso o precio. En otras palabras, BTC, al igual que otras criptomonedas, es un sistema de código que se distribuye entre miles de usuarios, la mayoría de ellos de forma anónima, en la denominada tecnología blockchain. Así, se crea un tipo de activo puramente digital que permite, entre otras muchas cosas, subvertir las restricciones y regulaciones estatales en un modelo P2P —*peer to peer*— en el que los individuos pueden negociar entre sí (Sánchez Porras, 2022).

Al funcionar en un blockchain que no hace necesario identificarse para efectuar transacciones con Bitcoin, causa que los poseedores de las claves privadas sean personas anónimas, de tal forma que esta situación dificulta en gran medida una efectiva regulación jurídica, por ejemplo frente a temas tributarios, pero también facilita la comisión de algunos delitos tales como lavado de activos, ya que la identidad de los dueños de los BTC puede mantenerse en reserva, las transacciones pueden ser anónimas y en muchos casos no se puede rastrear el origen de los activos. Sin embargo, no se limita a los delitos de lavado de activos, también se extiende a delitos como extorsión y financiación de la actividad delictiva. El jefe de la Unidad de Inteligencia Financiera (UIF) de México dijo que los narcotraficantes a menudo dividen su dinero ilícito en pequeñas cantidades en múltiples cuentas bancarias para luego comprar BTC, y nublar el origen del dinero, permitiéndoles pagar a sus colaboradores en todo el mundo (Blandón Ramírez, 2022). Por otro lado, el uso de criptoactivos puede derivar en el financiamiento irregular de campañas electorales, ya que dichos fondos pueden provenir de otros países, de actividades de lavado de dinero o de grupos de presión con intereses políticos; de modo que la falta de regulación del blockchain facilitaría que los delitos electorales pasaran desapercibidos (Rodríguez, 2022).

Aunque la utilización de BTC en el Salvador pretendía ayudar en la digitalización de la economía del país, particularmente mediante la reducción de las tasas a las remesas, que representan alrededor del 20 % del PIB del país, y la atracción de inversión extranjera, la realidad es que el uso de BTC no ha sido tan efectiva, pues a la fecha no hay infraestructura tecnológica suficiente ni proyectos que impulsen el desarrollo económico del país de la mano del uso del BTC. Al 5 de abril de 2022, hay 204 cajeros automáticos BTC instalados en el país,

pero su empleo es mínimo, ya que menos del 20% de la población de El Salvador confía y usa BTC (Statista, 2022). Además, para poder utilizar BTC correctamente, se necesita usar un dispositivo electrónico con acceso a internet, pero en El Salvador solo el 55% de la población tiene acceso a internet y la mayoría no tiene un teléfono inteligente (Min Shum, 2020).

Finalmente, se debe recalcar que la utilización de BTC en territorio salvadoreño ha tenido influencia en las dinámicas macroeconómicas, pues más allá de las degradaciones en los índices de confianza crediticia o la reducción de inversión extranjera, la criptomoneda no es moneda de curso legal en ningún otro país salvo en la República Centroafricana (Bangui, 2022). Por lo que si el Estado salvadoreño decidiera emplear la divisa como método de pago solo podría hacerlo con este país o a usuarios particulares como empresas o individuos, pues hay países donde inclusive el empleo de BTC está prohibido, por lo que se hace imposible comerciar con la criptodivisa (Orellana, 2022).

## **5.2. Irán: electricidad subsidiada – paraíso de minado**

El Banco Central de Irán prohibió comerciar con criptomonedas dentro del país en 2018, debido a los riesgos de lavado de dinero y financiación del terrorismo. Sin embargo, el minado de monedas ha seguido creciendo en el país, ahondando la existente crisis energética y obligando a las autoridades a perseguir a los mineros sin licencia. Sin embargo, en 2019, tras la imposición de sanciones contra Irán por parte de EEUU y el impacto que estas tuvieron en su divisa, el gobierno iraní cambió de idea y comenzó a explorar las criptomonedas como una alternativa al dólar estadounidense.

En enero de 2019, el Banco Central iraní autorizó el minado de criptomonedas. Para ser autorizado a ejercer esta actividad, se exigía identificarse y pagar más por la electricidad. No obstante, se han descubierto miles de casos de minado ilegal en el país, incluso en mezquitas, que no pagan por el suministro eléctrico.

Irán anunció el mismo mes el lanzamiento de una criptomoneda nacional. 4 bancos iraníes se unieron para lanzar ‘PayMon’, una moneda digital sustentada por las reservas nacionales de oro. Estrictamente hablando, no se trata de una ‘criptomoneda’ en la medida en que no hay un proceso P2P en las transacciones, sino que, como en otras monedas digitales nacionales, existirá un intermediario que en este caso será el Banco Central de Irán. En abril de 2021, el



Banco Central de Irán autorizó a bancos y otros agentes el pago en criptomonedas por importaciones por primera vez.

En agosto de 2022, Irán aprobó el uso de criptomonedas para pagar por importaciones, con el objetivo explícito de evitar las sanciones de EEUU que bloquean el acceso iraní a las instituciones financieras internacionales. El líder de la Organización para la Promoción del Comercio en Irán, Alireza Peymanpak, dijo en agosto de este año que, para finales de septiembre, el uso de criptomonedas y “smart contracts” sería ampliamente usado en el comercio exterior con ciertos países. El mismo mes, Irán realizó la primera importación oficial pagada con criptomonedas. Sin especificar cuál se utilizó, la agencia de noticias Tasnim informó de que coches por valor de USD 10 millones se habían importado en el país gracias a esta transacción.

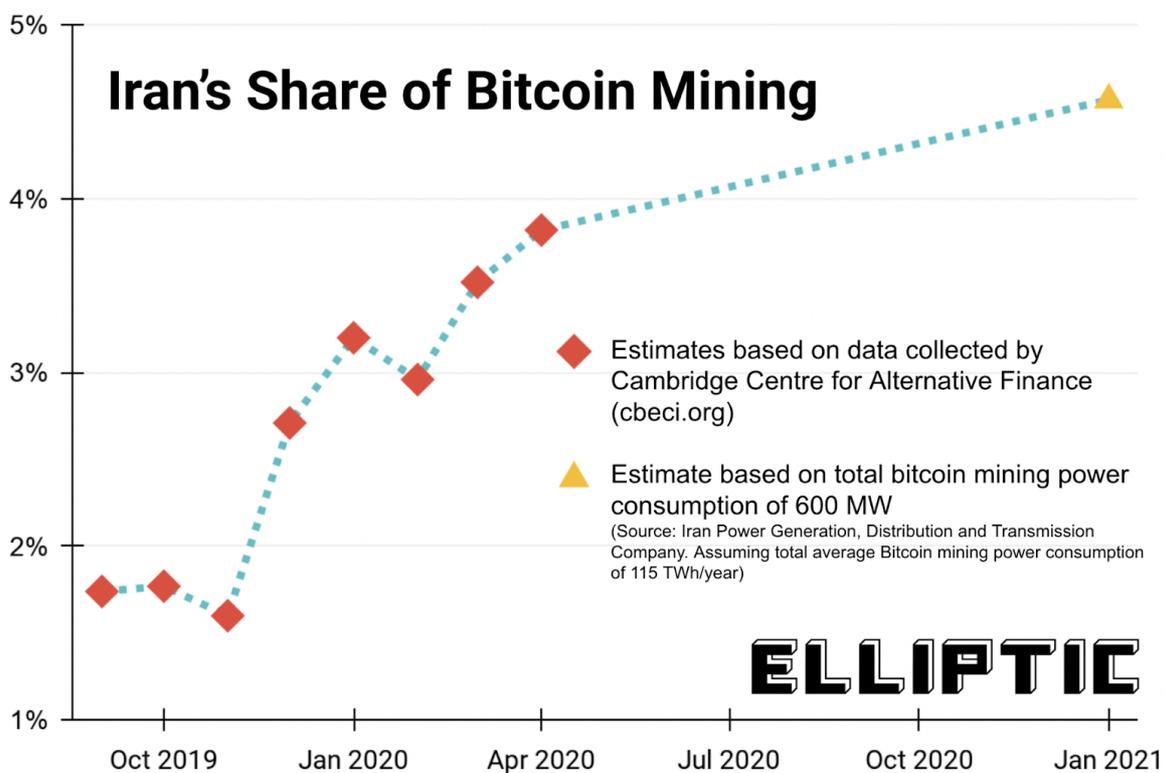
A pesar de lo que pudiera parecer, la política de minado de criptomoneda está provocando graves problemas económicos a la República Islámica. Debido al alto requerimiento energético del minado de criptomoneda, Irán se ve obligada a cortar la electricidad a los operadores de minado autorizados por el gobierno en el país cuando se espera una alta demanda. En los primeros meses de 2021, el aumento de la minería ilegal de criptomoneda, unida a las sequías, provocaron apagones en diversas partes del país. De acuerdo con oficiales iraníes, en el país hay alrededor de un millón de usuarios nuevos cada año, pero solamente un 16% del aumento de la demanda se debe a las nuevas licencias de minado de criptomoneda.

Irán dedica USD 60.000 millones al año en subsidios indirectos para el suministro eléctrico a negocios y personas físicas, lo que garantiza precios bajos en el país. Sin embargo, la incapacidad de las autoridades para alcanzar los objetivos de aumento de la producción eléctrica y esta política de subsidios, están provocando un aumento considerable de la deuda del país. En el último año fiscal, la República Islámica de Irán logró un aumento de 1,2 gigawatios (GW) en su generación de energía, apenas un tercio del objetivo del Ministerio de Energía de 3,5 GW. Este fue el tercer año consecutivo que no se alcanza el objetivo de crecimiento, una racha que comenzó con la sequía de 2018, la peor que ha sufrido el país en 50 años según sus registros.

La falta de inversión pero también las sequías, son una de las razones principales razones de los malos resultados: la producción hidroeléctrica cayó un 36% el año pasado. En 2021, estas produjeron 15 terawattios/hora (TWh), mientras que en 2019 se produjeron 31TWh.

Según información recogida por el Cambridge Center for Alternative Finance e información revelada por autoridades iraníes, como anticipábamos, se estima que en 2021 Irán constituía el 4,5 % del minado mundial de Bitcoin. Irán admitió que el minado de criptomonedas suponía unos 500/600MW de electricidad, lo cual significaba que al país llegan aproximadamente unos USD 1.000 millones en criptomonedas anualmente. Sin embargo, las autoridades reconocían que solamente la mitad de estos operadores estaban autorizados, por lo que los fondos que organizaciones estatales iraníes se embolsan anualmente de esta forma podría ser menos de la mitad.

### Porcentaje de minado de Bitcoin realizado en Irán, del total en el mundo



Fuente: [Elliptic](#)

De acuerdo a la misma organización que estimó el beneficio, para generar esa electricidad, Irán necesitaría 10 millones de barriles de petróleo anuales, o el 4% de su producción. Es decir, gracias al minado de criptomonedas, Teherán logra sacar partido a productos sancionados como el petróleo e incluso pagar por importaciones, por ahora a pequeña escala. En primer lugar, Irán puede utilizar su petróleo y gas para producir electricidad adicional. Esta energía puede ser usada para el minado de criptomonedas, y las criptomonedas se emplean para las importaciones de productos como vehículos. De esta manera, se saca partido a productos afectados por sanciones o embargos comerciales.

Aunque es difícil estimar el impacto que la política de minado ha tenido en los problemas económicos del país, disociándolo de la influencia de las sanciones económicas, es innegable que estas políticas no han contribuido a solucionarlos. La deuda pública iraní, de acuerdo a estimaciones del Fondo Monetario Internacional (FMI), ascendió en 2021 a USD 591.000 millones. En 2019, la deuda era de USD 214.000 millones y, el año siguiente, de USD 351.000 millones. La inflación se encuentra por encima del 50% desde junio.

El caso de las criptomonedas sustentadas por recursos naturales como las reservas de oro (PayMon iraní) o de petróleo (Petro venezolano) conlleva la introducción de un nuevo elemento: la confianza en los datos oficiales de ese Estado sobre las reservas reales.

Por otro lado, existe otra consecuencia muy importante para occidente derivada del minado de criptomoneda en Irán. El sistema de tarifas de la tecnología blockchain fue creado no solamente para evitar el spam de transacciones que ralentizara el sistema, sino también para incentivar a los mineros a validar las transacciones. Esto significa que transferencias de bitcoins realizadas, por ejemplo, en la UE o en EEUU, podrían conllevar el pago de comisiones a mineros en Irán. Si tal como se estima, el 4.5% del minado de Bitcoin a nivel global se produce en Irán, esto significa que casi una de cada 20 transacciones en Bitcoin incluye pagos en comisiones a operadores iraníes. Esto supone un riesgo de violación de sanciones muy alto para entidades financieras ofreciendo servicios con criptoactivos.

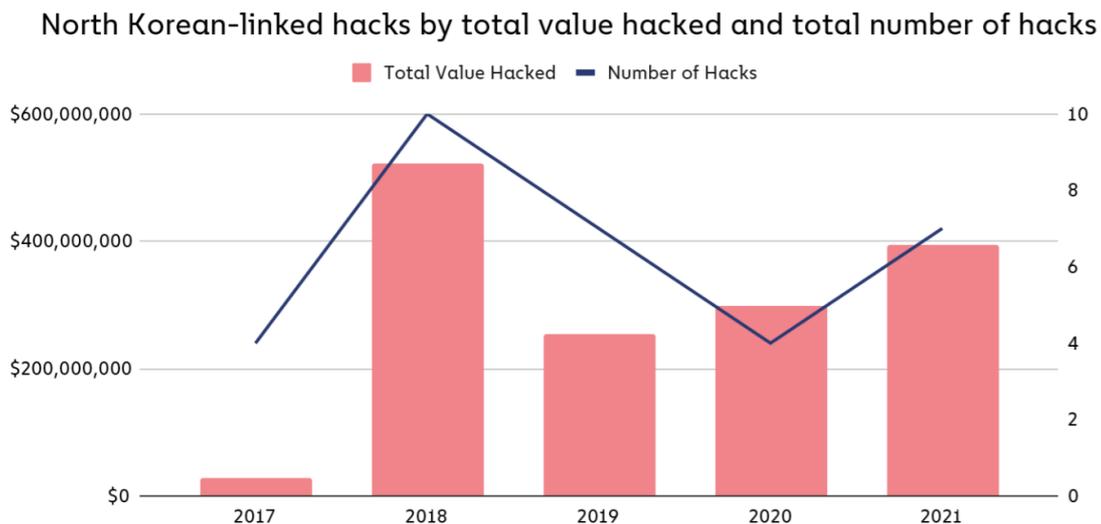
### **5.3. Corea del Norte: país promotor de la ciberdelincuencia**

Corea del Norte es una jurisdicción cuya opacidad hace mucho más difícil encontrar datos fiables para realizar un análisis sólido sobre el impacto que actividades relacionadas con las criptomonedas tienen en la economía o en la distribución y coste de la energía. No obstante, debido al interés que provoca el país asiático, existen numerosas investigaciones publicadas sobre sus actividades delictivas que detallan el *modus operandi* de estos grupos a la hora de robar y lavar criptomonedas.

Corea del Norte ha visto en las criptomonedas una oportunidad para sus propios grupos de cibercriminales. El país asiático ha sido acusado por el Consejo de Seguridad de las Naciones Unidas de estar detrás del robo de USD 571 millones en criptodivisas entre enero de 2017 y septiembre de 2018. Entre 2019 y noviembre de 2020, el país también ha sido acusado de robar

de plataformas de intercambio de criptodivisas al menos USD 316 millones. En 2021, según ChainAnalysis, estos grupos son responsables del robo de USD 400 millones.

### Valor de criptoactivos hackeados y número de hackeos ejecutados por actores asociados con Corea del Norte

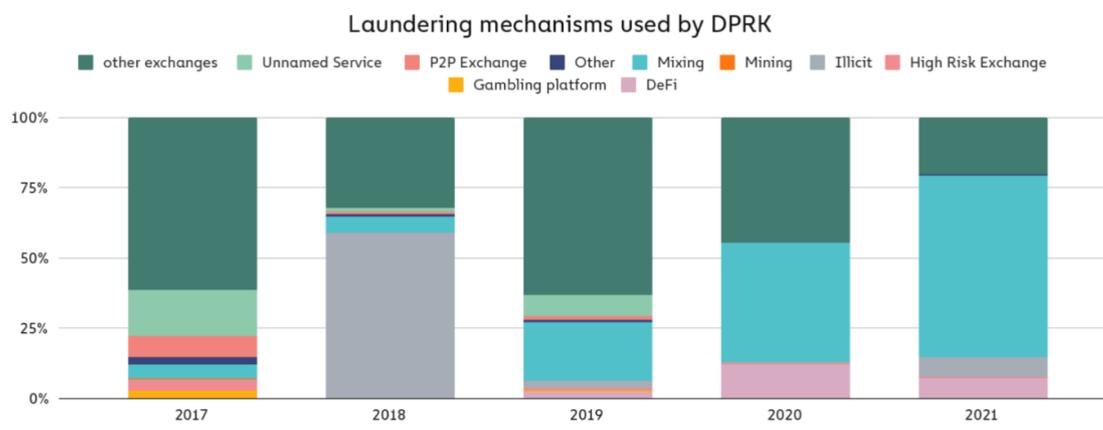


Fuente: [ChainAnalysys](#)

No obstante, en lo que llevamos de 2022, los cibercriminales norcoreanos ya han superado esta cifra con creces. En marzo de este año, el Grupo Lázarus (APT 38) robó USD 621 millones en Ethereum del videojuego Axie Infinity. Este videojuego, basado en tecnología blockchain, premia a sus jugadores con tokens que, posteriormente, pueden intercambiar por criptomonedas. La cifra es muy significativa, ya que coincide con el gasto estimado de las pruebas con misiles realizadas por Corea del Norte durante la primera mitad del año, según el Instituto Coreano para los Análisis de Defensa.

Además, si tomamos en consideración que en 2021, Corea del Norte exportó oficialmente productos por un valor total de USD 150 millones, el valor de las criptomonedas robadas como fuente de divisa extranjera en el país adquiere unas dimensiones mucho mayores. No obstante, la tecnología blockchain y el mercado de criptomonedas, tal como hemos visto, la información es inmutable, transparente y validada. Por lo tanto, las criptomonedas robadas por grupos de criminales han de ser “lavadas” antes de poder ser usadas para pagos o intercambiadas por dinero fiat en puntos de “cash-out”.

## Mecanismos de lavado de criptomonedas usados por grupos asociados con Corea del Norte



Fuente: [ChainAnalysis](#)

Como demuestra la labor de investigación realizada por ChainAnalysis sobre la forma de operar de estos grupos en Corea del Norte, los mezcladores (mixers) han ido adquiriendo peso entre las formas preferidas para lavar estos fondos.

Los mezcladores son herramientas de software que mezclan las direcciones de diversas criptomonedas para dificultar la identificación de las mismas, su origen y, por tanto, la identidad de sus propietarios. A cambio de una comisión de en torno al 1-3% de la criptomoneda mezclada, estos softwares funcionan habitualmente de la siguiente manera: primero, mediante ‘smart contracts’, se permite aceptar tokens de una dirección que, posteriormente, serán extraídos desde otra. Ese smart contract alberga cientos o miles de depósitos de distintos clientes, que se unen en él, se despedazan y se entremezclan. Finalmente, cuando el usuario retira un activo digital por el mismo valor que introdujo (menos la comisión del mezclador) desde una dirección distinta, se rompe la cadena de información, y por tanto, la posibilidad de identificar su origen. En general, se ha asociado el lavado de criptoactivos robado por grupos norcoreanos con el mezclador Tornado Cash.

El siguiente es un método habitual de lavado de criptomonedas robadas por Lazarus en 2018:

1. Corea del Norte roba ERC-20 tokens y Altcoins que quieren “lavar”.
2. Los intercambian por Ether usando una plataforma de intercambio descentralizada (DEX).



3. Se mezcla el Ethereum obtenido con un mezclador.
4. El Ethereum mezclado se intercambia por Bitcoin con un DEX.
5. El Bitcoin se mezcla con un mezclador.
6. El Bitcoin mezclado se coloca en nuevas carteras.
7. El Bitcoin se envía a puntos de intercambio de criptomonedas por dinero fiat (o dinero por decreto).

En particular, China es uno de los países preferidos por los cibercriminales norcoreanos para retirar los fondos obtenidos al finalizar el proceso de lavado mencionado. Solamente 2 hombres de nacionalidad china llamados Tian YinYin y Li Jaidong (ahora bajo sanciones de la OFAC) lavaron más de USD 100 millones de criptomonedas robadas por el Grupo Lazarus en 2018. Para ello, emplearon técnicas similares a las mencionadas en el proceso anterior, además de fraccionar los pagos llegando a realizar miles de transferencias de pequeñas cantidades, o adquiriendo productos con Bitcoin, como tarjetas de regalo de Apple, por valor de más de USD 1 millón.

## 6. TENDENCIAS CRIPTOMONEDAS Y SANCIONES

Bancos Centrales de países de todo el globo, incluyendo a EEUU y Federación Rusa, están explorando la viabilidad de versiones digitales de sus monedas. La digitalización de la economía es un fenómeno en gran medida global. No obstante, como hemos visto, algunos Estados sancionados han visto en las criptomonedas una oportunidad para mejorar su situación económica e incluso eludir dichas sanciones.

Países como Rusia o China tienen sus propios sistemas para transferencias internacionales, reduciendo así la dependencia del dólar y ofreciendo a los bancos adscritos una alternativa al sistema SWIFT. China cuenta con el 'Cross-Border Interbank Payment System' (CIPS), y Rusia con el 'Financial Messaging System' (SPFS).

Cuando en febrero de 2019, SWIFT volvió a desconectar a los bancos iraníes del sistema SWIFT, Irán se conectó al SPFS (Sistema de Transferencias del Sistema Financiero, en ruso), la alternativa de la Federación Rusa creada tras las sanciones que siguieron a la anexión de Crimea y Sevastópol en 2014. No obstante, son en general pocos los bancos fuera de sus respectivos países que se han unido a dichos sistemas y, algunos de ellos, han dejado de aceptar dichos pagos a raíz de las sanciones contra Rusia desde el comienzo de la invasión de Ucrania en febrero de este año.

En el contexto actual de sanciones y de aislamiento internacional que países como Rusia, Irán y en menor medida China están sufriendo, los activos digitales ofrecen, como hemos visto, una lucrativa fuente de ingresos y una manera de eludir sanciones en aquellos casos en los que socios comerciales están dispuestos a aceptar pagos con criptomonedas. No obstante, el uso de criptomonedas a nivel estatal a gran escala para socavar el régimen de sanciones requeriría de una enorme infraestructura de minado de la que Rusia no dispone en la actualidad. El crecimiento exacerbado de la deuda iraní, así como los continuos problemas de suministro energético, dan cuenta de los problemas asociados con la minería.

Además, la cantidad de electricidad necesaria para minar criptomonedas es muy elevada con lo que únicamente puede ser lucrativa y sostenible si los precios de la electricidad se mantienen bajos. La dependencia energética para la producción de criptomonedas afecta directamente al medio ambiente y a los sistemas eléctricos tradicionales. En algunas ciudades el consumo de luz ha aumentado hasta en un 30% pero además en el proceso de minado se producen altas cantidades de residuos electrónicos físicos. Se calcula que sólo la minería de Bitcoin produce una huella de carbono de 17.000 kilo toneladas de dióxido de carbono al año, lo que implica que la minería de criptomonedas tiene un papel muy importante en la emisión de gases de efecto invernadero afectando al medio ambiente y al clima.

Una solución para disminuir el impacto de la minería en el medio ambiente sería rehacer de nuevo el proceso creando una alternativa más sostenible. El protocolo Proof of Stake no tiene una huella de carbono tan elevada y muchas criptomonedas están migrando sus procesos hacia este protocolo para dirigirse hacia una red Blockchain más verde. En el futuro, el argumento ecológico irá perdiendo peso.

Por otro lado, las criptomonedas servirían para evitar el bloqueo de activos en una nueva ronda de sanciones. Es decir, podrían emplearse por empresas, individuos, y potencialmente por el Estado, para proteger sus fondos. Sin embargo, no todas las criptomonedas valdrían para este

propósito. Aquellas que son emitidas por empresas, como Tether (USDT) o Circle (USDC) están sujetas a los mismos riesgos que activos que las cuentas bancarias. Las criptomonedas empleadas han de ser, por tanto, descentralizadas y lo menos volátiles posible.

En resumen, los principales problemas de esta estrategia son que:

- Se necesita un enorme volumen de transacciones de Bitcoin (u otras criptomonedas) para evitar las sanciones, y existe un número limitado de criptomonedas. Además, el valor de estos activos es muy volátil y será afectado por un gran número de transacciones realizadas en un corto periodo de tiempo.
- La moneda digital puede utilizarse para futuras transacciones pero, si lo que se pretende es obtener fondos en una cuenta bancaria, la transacción será mediada por instituciones financieras, bancos, etc. lo cual aumenta el tiempo y los riesgos de ser detectada como ilegal o sospechosa.

A esto se añade que las autoridades de EEUU y la UE llevan años investigando y actuando contra actividades criminales relacionadas con las criptomonedas. El 28 de noviembre de 2018, la Oficina de Control de Activos Extranjeros de EEUU (OFAC) incluyó por primera vez en la lista de “Specially Designated Nationals” (SDN) dos operadores de Bitcoin. Se trataba de Ali Khorashadizadeh y Mohammad Ghorbaniyan, brokers de criptomonedas residents en Irán que tramitó USD 17 millones de fondos provenientes de la campaña SamSam ransomware.

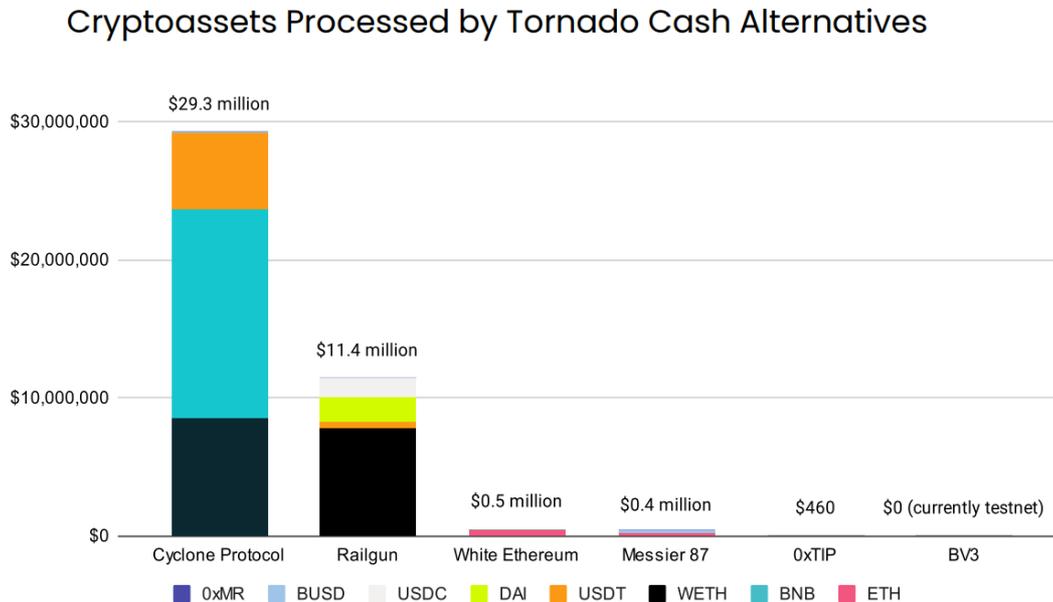
Las pesquisas están dando sus frutos. De hecho, en septiembre de este año, el Gobierno de EEUU, en colaboración con ChainAnalysis logró recuperar 30 de los 620 millones de dólares robados por cibercriminales norcoreanos al videojuego Axie Infinite. Esto constituye el 12% de los fondos robados.

Los mezcladores suponen aún una gran amenaza para la seguridad de las criptomonedas y su empleo por parte de cibercriminales. Antes de que Tornado Cash, uno de los servicios de mezclado más importantes, fue sancionado por los EEUU en agosto de este año, esta empresa había lavado ya más de USD 1.500 millones. Entre sus clientes, cibercriminales del Grupo Lazarus norcoreano.

No obstante, ya se han detectado seis servicios diferentes compitiendo por la base de clientes que Tornado Cash ha dejado. Una clara alternativa es “Cyclone Protocol”, un mezclador que funciona utilizando exactamente el mismo mecanismo que Tornado Cash y que está aumentando rápidamente su número de clientes. Además, existen numerosas otras plataformas

que otorgan anonimidad a sus usuarios en el uso de criptomonedas basadas en blockchain, y contribuyen así a su “lavado”. Railgun, es un popular sistema que elimina las direcciones asociadas con transacciones realizadas.

### Criptoactivos procesados por alternativas a Tornado Cash



Fuente: [Tornado Cash Alternatives. Elliptic Briefing Notes.](#)

En cuanto a la legalización de criptomonedas como el Bitcoin como moneda de curso, el caso de El Salvador ofrece numerosas problemáticas. A pesar de que El Salvador quisiera atraer inversión extranjera, digitalizar su economía y reducir las tasas a las remesas que representan el 20% de su PIB al volverse el primer país del mundo en convertir el BTC en moneda de curso legal, este no ha logrado su objetivo.

La implantación de la criptodivisa ha degradado la calificación crediticia de riesgo de El Salvador y ha convertido al país en el segundo estado latinoamericano con más riesgo de inversión. Además, ha provocado una devaluación de cerca del 55% de los bonos de países en vía de desarrollo. Por otra parte, el anonimato que ofrece el blockchain no ha permitido una efectiva regulación jurídica y probablemente ha facilitado la comisión de delitos. Asimismo, por causa de la volatilidad de la divisa, se calculan pérdidas por más de 50 millones de USD, pues el precio del BTC ha perdido cerca del 56% de su valor.

El Fondo Monetario Internacional, el Instituto Centroamericano de Estudios Fiscales (ICEFI) y otros organismos han pedido derogar la Ley Bitcoin en El Salvador y ha avisado de los riesgos



de la adopción de la criptomoneda como moneda de curso legal, causando desconfianza e incertidumbre. Por si no fuera poco, se debe tener en cuenta que El Salvador no hizo un análisis situacional de su capacidad de infraestructura tecnológica antes de la adopción de la medida, pues el acceso a internet es primordial si se quiere usar los BTC eficazmente, y con una cobertura de red no mayor al 55% esto es casi imposible.

En consecuencia, pese a las medidas del gobierno por incentivar el uso de BTC, y el enorme monto de capital público invertido en la implantación de la criptomoneda, menos del 25% de empresas hace empleo de esta y poco menos del 20% de la población emplean los BTC en sus transacciones diarias. Además, 7 de cada 10 salvadoreños están en desacuerdo o muy en desacuerdo con el empleo del BTC.

El Salvador podría convertirse en un ejemplo de los riesgos que acarrea la implantación de una criptomoneda como moneda corriente sin haber realizado un buen análisis previo. Es poco probable que lo acontecido en El Salvador tras la puesta en marcha de la Ley Bitcoin genere una tendencia entre otros estados a evitar las criptomonedas como monedas de curso legal o a ser más cautos a la hora de hacerlo, contemplando los diversos escenarios y capacidades jurídicas, económicas y tecnológicas para una implantación beneficiosa. No obstante, la tendencia global a la digitalización de las economías augura un futuro en el que, como mínimo, la tecnología blockchain y los criptoactivos centralizados transformarán la forma en la que nuestras instituciones financieras funcionan.

## 7. Bibliografía

1. Alfaro, K. (2022). El uso del bitcoin en El Salvador no trascendió del bono de bienvenida. Recuperado el 4 de octubre de 2022, en <https://www.eleconomista.net/cripto/El-uso-del-bitcoin-en-El-Salvador-no-trascendio-del-bono-de-bienvenida-20220907-0001.html>
2. Álvarez, J. (2022). Venezuela y El Salvador lideran los países con más riesgo para inversores en LatAm. Recuperado el 4 de octubre de 2022, en <https://www.bloomberglinea.com/2022/06/14/venezuela-y-el-salvador-lideran-los-paises-con-mas-riesgo-para-inversores-en-latam/>
3. Anónimo. ¿Qué es la minería de Bitcoin y otras criptomonedas? (s. f.). *Criptonoticias*. Recuperado 12 de octubre de 2022, de <https://www.criptonoticias.com/criptopedia-old/que-mineria-bitcoins-criptomonedas/>
4. Bangui. (2022). La República Centroafricana, segundo país que adopta el Bitcoin como moneda oficial. Recuperado el 4 de octubre de 2022, en [https://www.eldiario.es/tecnologia/republica-centroafricana-segundo-pais-adopta-bitcoin-moneda-oficial\\_1\\_8949952.html](https://www.eldiario.es/tecnologia/republica-centroafricana-segundo-pais-adopta-bitcoin-moneda-oficial_1_8949952.html)
5. Baker, J. (2021, 17 diciembre). *Bitcoin miners lose power in Iceland*. IceNews. Recuperado 21 de septiembre de 2022, de <https://www.icenews.is/2021/12/17/bitcoin-miners-lose-power-in-iceland/>
6. Bitcoin en El Salvador: un ejemplo para el mundo. (2022). Recuperado el 4 de octubre de 2022, en <https://www.chiapasparalelo.com/opinion/2022/09/bitcoin-en-el-salvador-un-ejemplo-para-el-mundo/#:~:text=En%20principio%2C%20se%20comprar%C3%ADa%20a,criptomonedas%20con%20relaci%C3%B3n%20al%20d%C3%B3lar>
7. Bitcoin: cajeros instalados por ciudad en El Salvador en 2022 | Statista. (2022). Recuperado el 4 de octubre de 2022, en <https://es.statista.com/estadisticas/1267356/cajeros-bitcoin-instalados-por-ciudad-el-salvador/>
8. Blandón Ramírez, D. (2022). Economía - Bitcoin: así lo usan carteles del crimen para lavar dinero (y las autoridades para desmantelarlos). Recuperado el 4 de octubre de 2022, en <https://www.france24.com/es/programas/econom%C3%ADa/20201211-bitcoin-as%C3%AD-lo-usan-carteles-del-crimen-para-lavar-dinero-y-las-autoridades-para-desmantelarlos>

9. Chivo Wallet. (2022). Recuperado el 4 de octubre de 2022, en <https://www.chivowallet.com/>
10. Deutsche Welle. (2022). Bitcoin en El Salvador: doce meses no son suficientes | DW | 07.09.2022. Recuperado el 4 de octubre de 2022, en <https://www.dw.com/es/bitcoin-en-el-salvador-doce-meses-no-son-suficientes/a-63047762>
11. Diario Bitcoin. (2022). Bukele escribió un artículo contra quienes lo reprocharon por comprar Bitcoin con dinero de la nación y defiende su decisión. Recuperado el 4 de octubre de 2022, en <https://www.diariobitcoin.com/paises/centro-america/el-salvador/bukele-critico-en-un-articulo-a-quienes-lo-reprocharon-por-comprar-bitcoin-con-dinero-de-la-nacion-y-defiende-su-decision/>
12. Dudley, D. (2021, 28 mayo). *After Years Of Warnings, Iran Finally Clamps Down On Power-Hungry Bitcoin Miners*. Forbes. Recuperado 14 de octubre de 2022, de <https://www.forbes.com/sites/dominicdudley/2021/05/28/after-years-of-warnings-iran-finally-clamps-down-on-power-hungry-bitcoin-miners/?sh=73cbabf41229>
13. El Salvador adopta el bitcoin: ocho claves para entender su uso como divisa legal. (2021). Recuperado el 4 de octubre de 2022, en <https://elcomercio.pe/economia/mundo/el-salvador-adopta-el-bitcoin-ocho-claves-para-entender-su-uso-como-divisa-legal-fotos-mndc-noticia/>
14. El Zonte, pueblo de El Salvador pionero en el uso de Bitcoin. (2022). Recuperado el 4 de octubre de 2022, en <https://mycryptoway.com/el-zonte-pueblo-de-el-salvador-pionero-en-uso-de-el-bitcoin/>
15. *Ethereum (ETH) Price Live | Etereum Chart, Value Today*. (2022, 25 febrero). StormGain. Recuperado 12 de octubre de 2022, de <https://stormgain.com/cryptocurrencies/ethereum>
16. *FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea*. (2022, 21 julio). Federal Bureau of Investigation. Recuperado 14 de octubre de 2022, de <https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea>
17. Fernández, Y. (22 de julio de 2022). *Criptomonedas: qué son, cómo funcionan y qué otras existen además de Bitcoin*. Xataka. Recuperado 14 de octubre de 2022, de <https://www.xataka.com/basics/criptomonedas-que-como-funcionan-que-otras-existen-bitcoin>

18. Financial Tribune. (2021, 23 abril). *Banks and Forex Shops Can Use Digital Assets to Pay for Imports*. Recuperado 14 de octubre de 2022, de <https://financialtribune.com/articles/business-and-markets/108313/banks-and-forex-shops-can-use-digital-assets-to-pay-for-imports>
19. Gobierno de El Salvador. Dictamen No. 3 Comisión Financiera - Ley Bitcoin (2021). Disponible en <https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/27F0BD6F-3CEC-4F52-8287-432FB35AC475.pdf>.
20. González Díaz, M. (2021). El Zonte, el pueblo de El Salvador pionero en el uso de bitcoin - BBC News Mundo. Recuperado el 4 de octubre de 2022, en <https://www.bbc.com/mundo/noticias-america-latina-57579861>
21. Gonzáles V., C. (1 de enero de 2022). Las consecuencias indirectas que provocan las criptomonedas al medio ambiente. Computer Hoy. Recuperado 15 de septiembre de 2022. <https://computerhoy.com/noticias/tecnologia/consecuencias-indirectas-provocan-criptomonedas-medioambiente-993455> I
22. Goodin, D. (2022, 9 septiembre). *Feds claw back \$30 million of cryptocurrency stolen by North Korean hackers*. Ars Technica. Recuperado 14 de octubre de 2022, de <https://arstechnica.com/information-technology/2022/09/feds-claw-back-30-million-of-cryptocurrency-stolen-by-north-korean-hackers/>
23. Iran International. (2022, 29 agosto). *Iran Approves Use Of Cryptocurrency For Imports To Bust Sanctions*. Recuperado 14 de octubre de 2022, de <https://www.iranintl.com/en/202208293261>
24. *Investing.com UK - financial news, shares, quotes & charts*. (s/f). Investing.com UK; Investing.com. Recuperado el 12 de octubre de 2022, de <https://uk.investing.com/>
25. Ittay Eyal and Emin Gün Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable. Department of Computer Science, Cornell University.
26. Jones, H. (2022, 11 octubre). *Regulators propose first global rules before «crypto winter» thaw*. Reuters. Recuperado 14 de octubre de 2022, de <https://www.reuters.com/technology/regulators-propose-first-global-rules-before-crypto-winter-thaw-2022-10-11/>
27. Kaushal, R.: Bitcoin: Vulnerabilities and attacks. Imperial Journal of Interdisciplinary Research 2(7) (2016), <http://www.imperialjournals.com/index.php/IJIR/article/view/1238>.

28. Khatri, Y. (2019, 5 febrero). *Gold-Backed Cryptocurrency Launched by Iranian Banks: Report*. CoinDesk. Recuperado 14 de octubre de 2022, de <https://www.coindesk.com/markets/2019/02/05/gold-backed-cryptocurrency-launched-by-iranian-banks-report/>
29. King, S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake (2012).
30. La mayor minera de bitcoin de EEUU sale a bolsa por 3.800 M de euros. (2022, 12 enero). *El Confidencial*. Recuperado 12 de octubre de 2022, de [https://www.elconfidencial.com/mercados/2022-01-20/la-mayor-minera-de-bitcoin-de-eeuu-saldra-a-bolsa-por-3-800-m-de-euros\\_3361688/](https://www.elconfidencial.com/mercados/2022-01-20/la-mayor-minera-de-bitcoin-de-eeuu-saldra-a-bolsa-por-3-800-m-de-euros_3361688/)
31. La Vanguardia. (2022). ICEFI recomienda derogar la Ley Bitcoin en El Salvador por 'grandes costos'. Recuperado el 4 de octubre de 2022, en <https://www.lavanguardia.com/vida/20220907/8509619/icefi-recomienda-derogar-ley-bitcoin-salvador-grandes-costos.html>
32. Marín, M. (2021). Así funciona el 'bitcoin' legal en El Salvador. Recuperado el 4 de octubre de 2022, en <https://lexlatin.com/entrevistas/bitcoin-el-salvador>
33. Martín, A. (2022). Cómo afectan las criptomonedas al medio ambiente. OVACEN. Recuperado 16 de septiembre de 2022. <https://ovacen.com/criptomonedas-medioambiente/>
34. Merino, Á. (2022, 13 enero). ¿Cuáles son los países que más bitcoin minan en el mundo? *El Orden Mundial*. <https://elordenmundial.com/mapas-y-graficos/paises-minado-bitcoin-mundo/>
35. Min Shum, Y. (2020). Situación digital, Internet y redes sociales El Salvador 2020. Recuperado el 4 de octubre de 2022, en <https://yiminshum.com/social-media-salvador-2020/>
36. Miranda, D. (11 de agosto de 2022). *¿Qué son las criptomonedas y el blockchain? Así funciona esta nueva tecnología*. [www.nationalgeographic.com.es](http://www.nationalgeographic.com.es). Recuperado 14 de octubre de 2022, de [https://www.nationalgeographic.com.es/mundo-ng/que-son-criptomonedas-y-como-funcionan\\_16981](https://www.nationalgeographic.com.es/mundo-ng/que-son-criptomonedas-y-como-funcionan_16981)
37. Nakamoto, S. (S/f). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. Recuperado el 12 de octubre de 2022, de <https://bitcoin.org/bitcoin.pdf>
38. Oquendo, A. (2022, 1 agosto). *Minería de bitcoin arroja datos «perturbadores» de su consumo eléctrico, según políticos*. CriptoNoticias - Noticias de Bitcoin, Ethereum y criptomonedas. Recuperado 14 de octubre de 2022, de

<https://www.criptonoticias.com/mineria/mineria-bitcoin-arroja-datos-perturbadores-consumo-electrico-politicos/>

39. Orellana, R. (2022). Criptomonedas: en qué países son legales y dónde están prohibidas | Digital Trends español. Recuperado el 4 de octubre de 2022, en <https://es.digitaltrends.com/tendencias/criptomonedas-legales-prohibidas/>
40. Penner, J. D. (2022, 19 abril). *Why central banks dislike cryptocurrencies*. IBM Business Operations Blog. Recuperado 14 de octubre de 2022, de <https://www.ibm.com/blogs/internet-of-things/why-central-banks-dislike-cryptocurrencies/>
41. Plaza, N. (2022). Fitch degrada calificación crediticia de El Salvador, mientras Bukele busca la reelección. Recuperado el 4 de octubre de 2022, en <https://www.criptonoticias.com/finanzas/fitch-degrada-calificacion-crediticia-el-salvador-bukele-busca-reeleccion/>
42. *Precio, cotización en tiempo real y noticias de Tether (USDT)*. (s. f.). Google Finance. Recuperado 14 de octubre de 2022, de <https://www.google.com/finance/quote/USDT-COP?hl=es&ucbcb=1>
43. *PoW* (s. f.). Diario Bitcoin. Recuperado 28 de septiembre de 2022, de <https://www.diariobitcoin.com/glossary/pow/>
44. Reuters. (2021, 2 junio). *Navalny ally urges donors to use cryptocurrency due to crackdown*. Recuperado 14 de octubre de 2022, de <https://www.reuters.com/world/europe/navalny-ally-urges-donors-use-cryptocurrency-due-crackdown-2021-06-02/>
45. Rodríguez, M. (2022). Expertos advierten: Financiar campaña con bitcoin abre vía a lavado de dinero. Recuperado el 4 de octubre de 2022, en <https://www.elsalvador.com/noticias/nacional/bitcoin-tse-campanas-electorales/968239/2022/>
46. Reuters. (2022, 9 agosto). *Iran makes first import order using cryptocurrency - report*. Recuperado 14 de octubre de 2022, de <https://www.reuters.com/business/finance/iran-makes-first-import-order-using-cryptocurrency-tasnim-2022-08-09/>
47. Robinson, T. (s. f.). *How Iran Uses Bitcoin Mining to Evade Sanctions*. Recuperado 14 de octubre de 2022, de <https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions>
48. Roth, E. (2021, 28 noviembre). *Cryptocurrency miners grapple with major energy crunch in Kazakhstan*. The Verge. Recuperado 14 de octubre de 2022, de

<https://www.theverge.com/2021/11/27/22805033/kazakhstan-cryptocurrency-miners-suffer-energy-shortages>

49. Sánchez Porras, C. (2022). Criptomonedas: un activo seguro que requiere la regulación del Estado para evitar su uso en la comisión de delitos. Universidad Santo Tomás, Tunja. Disponible en <https://repository.usta.edu.co/bitstream/handle/11634/44195/2022.carlos%20sanchez.pdf?sequence=1&isAllowed=y>
50. Santander. (25 de mayo 2022). *¿Qué son las criptomonedas y cómo funcionan?* Recuperado 14 de octubre de 2022, de <https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas>
51. Sigurdsson, G., Giaretta, A., & Dragoni, N. (2020). Vulnerabilities and Security Breaches in Cryptocurrencies. In M. Mazzara, A. Messina, A. Sillitti, G. Succi, & P. Ciancarini (Eds.), *Proceedings of 6th International Conference in Software Engineering for Defence Applications - SEDA 2018* (pp. 288-299). Springer. *Advances in Intelligent Systems and Computing* Vol. 925 [https://doi.org/10.1007/978-3-030-14687-0\\_26](https://doi.org/10.1007/978-3-030-14687-0_26)
52. Simões, C. (2022). *¿Qué son los bloques en la tecnología Blockchain?* Blog ITDO - Agencia de desarrollo Web, APPs y Marketing en Barcelona. Recuperado 14 de octubre de 2022, de <https://www.itdo.com/blog/que-son-los-bloques-en-la-tecnologia-blockchain/>
53. S., J. (14 de mayo de 2022). *¿En qué consiste la minería de criptomonedas y qué usos tiene?* *Economia3*. Recuperado 14 de octubre de 2022, de <https://economia3.com/que-es-mineria-criptomonedas-y-que-usos-tiene/>
54. Staff, R. (2018, 22 abril). *Iran central bank bans cryptocurrency dealings*. U.S. Recuperado 14 de octubre de 2022, de <https://www.reuters.com/article/us-cryptocurrencies-iran/iran-central-bank-bans-cryptocurrency-dealings-idUSKBN1HT0YN>
55. The White House (2022, 9 marzo). *Executive Order on Ensuring Responsible Development of Digital Assets*. The White House. Recuperado 14 de octubre de 2022, de <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/>
- 56.
57. Tidy, J. (2022). *Cuál es el uso real del bitcoin en El Salvador a 9 meses de adoptarse (y cómo le afecta la crisis actual de la criptomoneda)* | DPL News. Recuperado el 4 de



octubre de 2022, en <https://dplnews.com/cual-es-el-uso-real-del-bitcoin-en-el-salvador-a-9-meses-de-adoptarse-y-como-le-afecta-la-crisis-actual-de-la-criptomoneda/>

58. Timejacking & bitcoin. <http://culubas.blogspot.dk/>.
59. *Two Chinese Nationals Charged with Laundering Over \$100 Million in*. (2022, 23 julio). Recuperado 14 de octubre de 2022, de <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>
60. Vishnumurthy, V., Chandrakumar, S., Sirer, E.G.: Karma: A secure economic framework for peer-to-peer resource sharing. In: Workshop on Economics of Peerto-Peer Systems. (2003).
61. Vyas, C.A., Lunagaria, M.: Article: Security concerns and issues for bitcoin. IJCA Proceedings on National Conference cum Workshop on Bioinformatics and Computational Biology NCWBCB (2), 10–12 (May 2014).
62. Wright, T. (2022, 10 octubre). *European Parliament Committee passes MiCA crypto framework in landslide vote*. Cointelegraph. Recuperado 14 de octubre de 2022, de <https://cointelegraph.com/news/european-parliament-committee-passes-mica-crypto-framework-in-landslide-vote>