Un análisis del uso de Bitcoin en finanzas ilícitas

Por Michael Morell

con Josh Kirshner y Thomas Schoenberger

Abril 6, 2021

Prefacio

Las nuevas tecnologías casi siempre vienen con beneficios significativos para la sociedad, así como externalidades negativas. Es el papel de los funcionarios del gobierno hacer políticas que permitan que los beneficios florezcan mientras nos protegen de las desventajas. Como vi de primera mano en mi carrera de 33 años en la Agencia Central de Inteligencia, el proceso que nuestro gobierno utiliza para lograr este equilibrio a menudo puede ser frustrantemente lento, pero en última instancia y típicamente ha cumplido con el desafío.

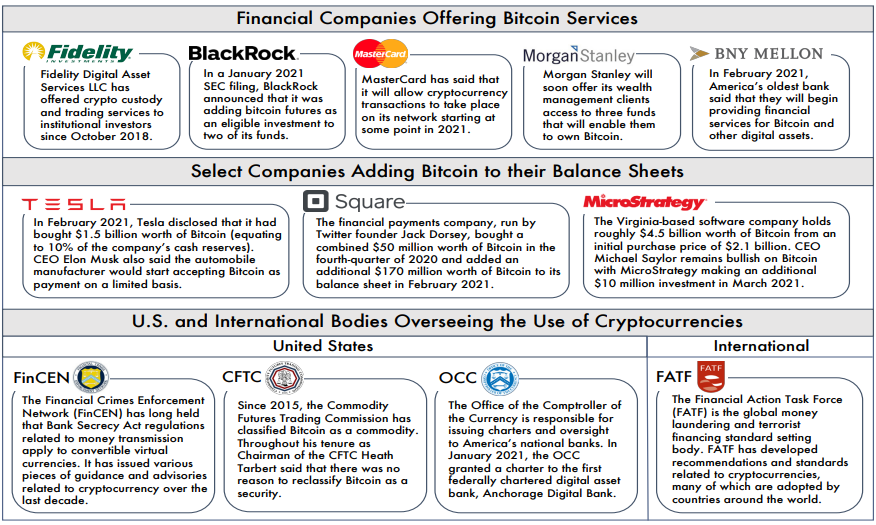
Un ejemplo es cómo nuestro gobierno se ha adaptado a los avances tecnológicos en las redes financieras y de pago, al tiempo que salvaguarda los sistemas vitales. La banca en línea se introdujo en 1994, pero no fue hasta 1999, con la aprobación de la Ley Uniforme de Transferencias Electrónicas (seguida de la aprobación de la Ley federal E-SIGN en 2000), que se establecieron normas para establecer la legalidad de los documentos y firmas electrónicas. La adopción de la banca en línea creció sustancialmente a medida que se promulgaron estas leyes y como un marco regulatorio tomó forma para coincidir con lo que entonces se consideraban avances tecnológicos revolucionarios.

Hoy en día, la rápida adopción de las tecnologías blockchain, y las criptomonedas que admiten, están en camino de revolucionar los sistemas financieros y de pago globales. Y, como era de esperar, estamos comenzando a ver un equilibrio entre innovadores y reguladores, con voces prominentes que intervienen, algunas promocionando la criptomoneda como el futuro de las finanzas y otras planteando preocupaciones sobre las implicaciones financieras ilícitas del ecosistema de criptomonedas.



Habiendo dedicado mi carrera a proteger y promover los intereses de seguridad nacional de los Estados Unidos, reconozco la importancia de garantizar que los avances tecnológicos relacionados con las industrias críticas vayan acompañados de ajustes inteligentes, informados y oportunos a los marcos regulatorios, políticas y leyes. Aquellos que salvaguardan a nuestra nación simplemente deben tener las herramientas adecuadas para hacer su trabajo. Punto.

Es en este contexto que yo, y dos de mis colegas de Beacon Global Strategies, realizamos un análisis sobre el grado de actividad ilícita asociada con las criptomonedas en general y Bitcoin en particular. El proyecto fue patrocinado por un grupo de innovadores e inversores líderes en criptomonedas. Los términos del compromiso eran que lo "llamaría como lo veo", con objetividad y transparencia, tal como lo había hecho a lo largo de mi carrera como analista de inteligencia. Tengo la esperanza de que este análisis ayude a promover un diálogo saludable y basado en hechos a medida que los responsables de la formulación de políticas determinen la mejor manera de garantizar que estas innovaciones financieras sirvan al interés nacional.



Introducción

Hasta ahora, 2021 ha sido un año de desarrollos e hitos significativos para Bitcoin. Su precio superó los $60,000 por primera vez en su historia.**1** Las principales corporaciones, desde Tesla hasta Square y MicroStrategy, lo están agregando a sus balances.**2** Los grandes bancos están brindando servicios relacionados con Bitcoin, y Morgan Stanley dice que pronto ofrecerá acceso a tres fondos de Bitcoin para sus clientes de gestión de patrimonio.**3** Canadá ha aprobado los fondos cotizados en bolsa (ETF) de Bitcoin.**4** Hay un impulso creciente para el uso emergente de Bitcoin como reserva de valor.

Sin embargo, existe la creencia común de que el mercado de Bitcoin está plagado de actividades ilícitas, y muchos sostienen esta creencia que apunta a varios incidentes de alto perfil. Cuando el mercado ilícito de la red oscura de Silk Road (DNM) se cerró en 2013, más de 26,000 Bitcoin fueron incautados por el FBI.**5** AlphaBay, formada en 2014 y ampliamente vista como heredera de Silk Road, fue cerrada por las autoridades internacionales en 2017 después de construir una base de clientes de más de 400,000, con transacciones realizadas en gran parte en Bitcoin.**6** El ataque de ransomware WannaCry de 2017 que infectó a más de 200,000 computadoras requeridas en todo el mundo en Bitcoin.**7** Bitcoin fue incluso utilizado para ayudar a financiar a algunos de los involucrados en la insurrección en Capitol Hill el 6 de enero.**8**

La sabiduría convencional sobre este tema ha sido reforzada por declaraciones públicas de altos funcionarios gubernamentales a ambos lados del Atlántico que han sugerido que Bitcoin se usa principalmente para actividades ilícitas. Los llamativos informes de los medios de comunicación, como un reciente artículo de Buzzfeed titulado, "Documentos secretos muestran cómo los partidarios del terrorismo usan Bitcoin, y cómo el gobierno está luchando para detenerlos", agregan peso a tales comentarios.**9**

Al realizar nuestro análisis, consultamos a un grupo diverso de expertos en los campos de la tecnología e inversión de criptomonedas, servicios financieros, sistemas de pago, inteligencia y seguridad global, regulación financiera y aplicación de la ley. Entrevistamos a ejecutivos de las principales empresas de análisis de blockchain, ex altos funcionarios del Departamento del Tesoro, un alto funcionario de la Comisión de Comercio de Futuros de Productos Básicos (CFTC) y un ex analista de inteligencia de la CIA, así como académicos, inversores de capital de riesgo, ex fiscales federales y un ex líder en la industria bancaria. También consultamos estudios del Departamento de Justicia de los Estados Unidos; la Red de Aplicación de Delitos Financieros (FinCEN); el Grupo de Acción Financiera Internacional (GAFI); las principales empresas de análisis de blockchain; la Brookings Institution; Corporación RAND; BAE Systems; y la Fundación para la Defensa de las Democracias.

Sigal Mandelker, ex Subsecretaria Interina del Tesoro y Subsecretaria del Tesoro para Terrorismo e Inteligencia Financiera, así como ex funcionaria y fiscal del Departamento de Justicia, nos dio una cantidad significativa de su tiempo para aprovechar su gran experiencia en el tema.



Comencé este trabajo esperando encontrar un conjunto de hechos que apoyaran la sabiduría convencional sobre este tema. Después de todo, creía que Bitcoin y otras criptomonedas son una forma en gran parte anónima de transferir fondos a cualquier parte del mundo casi instantáneamente. Y asumí que aquellos funcionarios que han expresado su preocupación por el uso de Bitcoin en actividades ilícitas, con el objetivo de garantizar la vigilancia regulatoria, deben estar entre los expertos mejor informados sobre este tema.

Sin embargo, basándome en nuestra investigación y discusiones con expertos de la industria, confío en dos conclusiones:

• Las generalizaciones generales sobre el uso de Bitcoin en las finanzas ilícitas están significativamente exageradas.

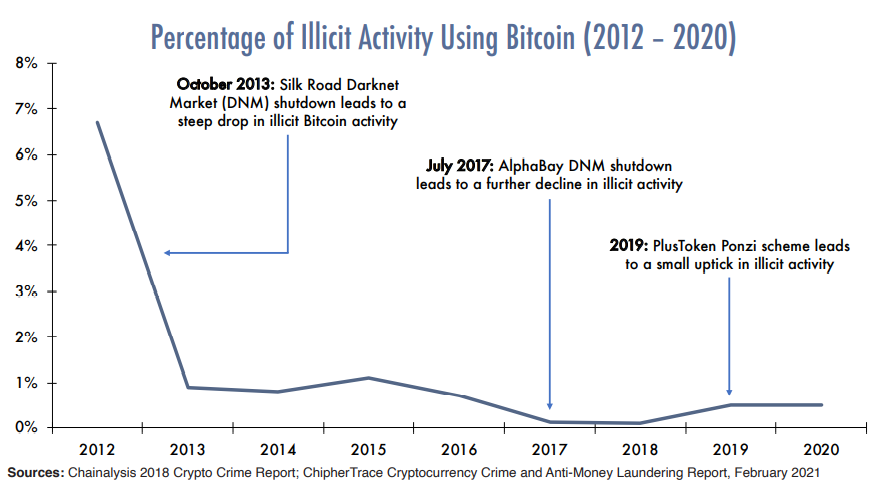
• El libro mayor de blockchain en el que se registran las transacciones de Bitcoin es una herramienta forense subutilizada que puede ser utilizada más ampliamente por las fuerzas del orden y la comunidad de inteligencia para identificar e interrumpir actividades ilícitas. En pocas palabras, el análisis de blockchain es una herramienta altamente efectiva de lucha contra el crimen y recopilación de inteligencia.

**El uso de Bitcoin en actividades ilícitas es relativamente limitado**

Es cierto que la criptomoneda, al igual que otras nuevas tecnologías e innovaciones, ha atraído la atención de actores ilícitos. Y no es sorprendente que, al igual que Bitcoin es la criptomoneda más comúnmente mantenida, también es la moneda que se encuentra con mayor frecuencia en las billeteras DNM por un amplio margen.**10** El hecho de que Bitcoin esté siendo utilizado por actores ilícitos es probablemente la base de comentarios recientes y ampliamente informados por funcionarios gubernamentales y reguladores. Pero profundizando más, sus declaraciones se centran en dos afirmaciones: primero, que Bitcoin se usa "con frecuencia" o "principalmente" para transacciones financieras ilícitas, y segundo, que el uso de Bitcoin en tales transacciones está creciendo.

A pesar de tales declaraciones, un alto ejecutivo de una importante firma de análisis de criptomonedas nos dijo que la creencia común de que Bitcoin se usa principal y cada vez más con fines de finanzas ilícitas está "desinformada y no se basa en datos" y que "no hay números ni metodologías" que lo respalden.

Según un estudio reciente de la firma de análisis de blockchain Chainalysis, la actividad ilícita entre todas las criptomonedas como porcentaje de la actividad total de criptomonedas de 2017 a 2020 fue inferior al 1 por ciento.**11** Para Bitcoin específicamente, la firma de análisis de blockchain CipherTrace estima que la actividad ilícita representa menos del 0.5 por ciento del volumen total de transacciones.**12**



Mientras tanto, las estimaciones de la actividad ilícita en la economía en su conjunto, realizada abrumadoramente a través de intermediarios financieros tradicionales y con monedas fiduciarias tradicionales, son del orden del 2 al 4 por ciento del PIB mundial. De hecho, la base de datos de la Ley de Secreto Bancario (BSA) de FinCEN contiene más de 300 millones de Informes de Actividades Sospechosas (SAR), con 20 millones adicionales agregados cada año.**13** No todos estos SAR equivalen a actividades ilícitas en el sistema bancario tradicional, pero muchos lo hacen.

Un ex analista de la CIA agregó credibilidad a las estimaciones anteriores, diciéndonos que, debido en parte a la diferencia en el volumen general, la mayoría de las actividades ilícitas todavía tienen lugar en el sistema bancario tradicional y no a través de criptomonedas. Un informe de BAE Systems de 2020, encargado por SWIFT, señaló además que "los casos identificados de lavado a través de criptomonedas siguen siendo relativamente pequeños en comparación con los volúmenes de efectivo lavado a través de métodos tradicionales".**14**

Todo esto en conjunto sugiere un punto más amplio: que el uso ilícito de criptomonedas en general y Bitcoin en particular, como proporción de la actividad total del mercado, ciertamente no es más alto que en el sistema bancario tradicional y lo más probable es que sea menor.

Por supuesto, los datos recopilados por las empresas de análisis de blockchain se basan en actividades ilícitas que realmente ven; las estimaciones no intentan cuantificar el tamaño de la actividad ilícita que no pueden ver y analizar.

**"Los casos identificados de lavado a través de criptomonedas siguen siendo**

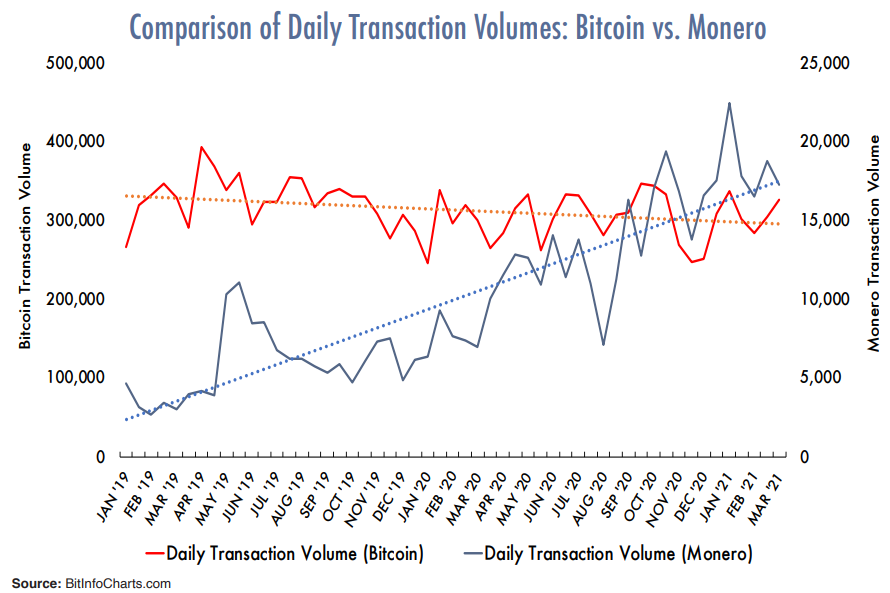
**relativamente pequeños en comparación con los volúmenes de**

**efectivo lavado a través de métodos tradicionales".**

Sin embargo, las empresas con las que hablamos creen que la actividad ilícita invisible es relativamente pequeña. Uno dijo que cree que ve la mayoría de las actividades ilícitas, mientras que otra estima que la actividad invisible no es más de lo que ven. Y, si bien es cierto que no sabemos lo que no sabemos en el mercado de criptomonedas, lo mismo ocurre con la actividad ilícita en el sistema bancario y en efectivo, como lo demuestra la falta de estimaciones firmes para estos sistemas de pago.

Según el estudio de Chainalysis, los dos tipos más significativos de actividad ilícita son los relacionados con estafas "simples" y compras en la web oscura. Los rescates por ataques de ransomware son difíciles de medir, pero los datos sugieren que es la categoría de más rápido crecimiento de delitos de criptomonedas, mientras que la actividad relacionada con el terrorismo y los pagos relacionados con la evasión de sanciones siguen siendo bastante pequeños.**15**

Sobre el tema clave de la financiación del terrorismo, el ex experto en terrorismo de la CIA cree que la exageración es mucho mayor que la realidad y que la criptomoneda aún no es una plataforma importante para las organizaciones terroristas. Agregó que los esfuerzos de crowdfunding de criptomonedas de tales grupos generalmente han traído solo unos pocos miles de dólares antes de ser cerrados. \* Un estudio de 2019 realizado por RAND Corporation concluyó además que el uso terrorista de las criptomonedas es mínimo y que ninguna criptomoneda actual proporciona a un grupo terrorista lo que necesitaría para ser un usuario significativo.**16**



\* El informe de la Red de Aplicación de Criptomonedas 2020 del Departamento de Justicia declaró que "si bien el uso terrorista de la criptomoneda aún está evolucionando, ciertos grupos terroristas han solicitado donaciones de criptomonedas que ascienden a millones de dólares a través de campañas en las redes sociales en línea".

Sin embargo, el ex experto en terrorismo de la CIA también señaló que algunos grupos están comenzando a usar técnicas de anonimización de criptomonedas más sofisticadas para ocultar su flujo de fondos, lo cual es un desarrollo clave para monitorear.

Como se señaló anteriormente, Bitcoin es, con mucho, la criptomoneda más grande utilizada en flujos ilícitos. Sin embargo, dos importantes firmas de análisis de criptomonedas han concluido que esto se debe al dominio de Bitcoin en el mercado y, por lo tanto, a su accesibilidad, no porque tenga atributos que lo hagan más atractivo para los usuarios ilícitos. Bitcoin representa más del 60 por ciento de la capitalización de mercado total de las criptomonedas, con más de 4,000 otras criptomonedas que comprenden el 40 por ciento restante.**17**

Y mientras que Bitcoin es la criptomoneda más utilizada en actividades ilícitas, otras criptomonedas se utilizan con mucha más frecuencia con fines ilícitos como parte de sus transacciones totales. Un importante ejecutivo de una importante firma de análisis de criptomonedas dijo que, para las criptomonedas mejoradas por el anonimato ("AEC" o "monedas de privacidad"), como Monero, que utilizan protocolos incorporados para ocultar información sobre transacciones, la actividad ilícita como porcentaje del volumen total de transacciones es "mucho mayor" que para Bitcoin.

También hay una creciente evidencia de que la actividad ilícita está fluyendo lejos de Bitcoin y hacia los AEC. El informe RAND de 2020 al que se hace referencia anteriormente señaló tal cambio de Bitcoin a las criptomonedas con un anonimato más fuerte.**18** El prominente "Mercado de la Casa Blanca" de DNM se ha movido para aceptar Monero exclusivamente.**19** Del mismo modo, el grupo de ransomware, Sodinokibi, ya no acepta Bitcoin como pago y solo tomará Monero.**20** El creciente uso de AEC para actividades ilícitas se destacó aún más en un aviso de octubre de 2020 emitido por FinCEN que declaró: "[Los actores ilícitos] están exigiendo o incentivando cada vez más a las víctimas a pagar en AEC que reducen la transparencia de los flujos financieros [de criptomonedas], incluidos los pagos de ransomware, a través de funciones de anonimización". El aviso agregó que "los operadores de ransomware incluso han ofrecido tarifas con descuento a las víctimas que pagan sus rescates en AEC".**21**

**La tecnología Blockchain es una poderosa herramienta forense**

La tecnología Blockchain es una herramienta forense poderosa pero subutilizada para que los gobiernos identifiquen actividades ilícitas y lleven a los delincuentes ante la justicia. Un experto en el ecosistema de criptomonedas llamó a la tecnología blockchain una "bendición para la vigilancia".

Un funcionario actualmente en servicio en la CFTC agregó que "es más fácil para las fuerzas del orden rastrear actividades ilícitas utilizando Bitcoin que rastrear actividades ilegales transfronterizas utilizando transacciones bancarias tradicionales, y mucho más fácil que las transacciones en efectivo".

**"[Es] más fácil para las fuerzas del orden rastrear actividades ilícitas usando Bitcoin que**

**rastrear la actividad ilegal transfronteriza utilizando transacciones bancarias**

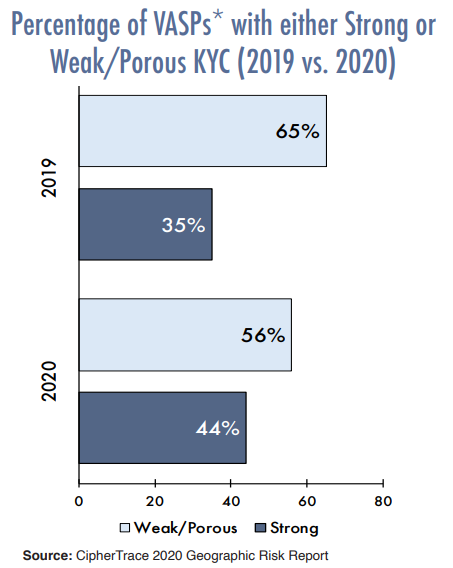
**tradicionales, y mucho más fácil que las transacciones en efectivo".**

El ex alto funcionario del Tesoro Sigal Mandelker estuvo de acuerdo y dijo que esta opinión es compartida por varias personas en este espacio que tienen experiencia trabajando en la aplicación de la ley.

En un testimonio de febrero de 2021 ante el Subcomité de Seguridad Nacional, Desarrollo Internacional y Política Monetaria de la Cámara de Representantes, el ex Subsecretario del Tesoro para el Financiamiento del Terrorismo y delitos financieros Daniel Glaser declaró que, cuando se trata de transparencia en el sistema financiero internacional y el sistema financiero nacional, "las criptomonedas brindan mayores oportunidades de ciertas maneras para que las agencias de aplicación de la ley puedan rastrear transacciones". Glaser agregó que el gobierno de los Estados Unidos debería "traer [criptomonedas] al sistema y regularlas de la manera apropiada".**22**

Un experto nos dijo que la posibilidad de atrapar actores ilícitos es "magnitudes mayores" usando blockchain que en el sector bancario tradicional. Otro llegó a decir que "si todos los delincuentes usaran blockchain, podríamos eliminar la actividad financiera ilícita". De hecho, su naturaleza transparente llevó a un experto en análisis de blockchain a comparar las transacciones en blockchain con tener al "mundo entero" como testigo de pagarle a alguien $ 2,000 en un callejón oscuro.**23** Basándome en nuestra investigación, he llegado a creer que, si hubiera un ecosistema financiero para que los malos actores lo usaran, maximizaría las posibilidades de las fuerzas del orden de identificarlos y sus actividades ilícitas, sería blockchain.

La tecnología Blockchain permite este poder forense porque captura cada transacción para que todos la vean: proporciona a los gobiernos y al público en general un registro permanente e inmutable de las transacciones. Cuando se ve junto con otros datos derivados del análisis de análisis de blockchain, así como herramientas tradicionales de aplicación de la ley como citaciones, la tecnología blockchain puede permitir la identificación tanto de actividades ilícitas como de las identidades de los usuarios finales. La capacidad de detectar actividades ilícitas e identificar a los autores no es perfecta, pero ha crecido significativamente en los últimos años.



\* Los proveedores de servicios de activos virtuales (VASP) son empresas que ofrecen uno de los siguientes servicios: 1) intercambio entre criptomonedas y monedas fiduciarias; 2) intercambio entre una o más formas de criptomoneda; 3) transferencia de criptomonedas; 4) custodia y/o administración o criptomonedas.

Una aplicación más amplia de las regulaciones de Conozca a su Cliente (KYC) y Antilavado de Dinero (AML) mejoraría aún más la capacidad de las fuerzas del orden público para identificar la actividad ilícita de Bitcoin.**24** Si bien una parte creciente de Bitcoin se mantiene en intercambios centralizados, CipherTrace informó que el 56 por ciento de los proveedores de servicios de activos virtuales (VASP) globales\* todavía tienen "procesos KYC débiles o porosos".**25** Dado esto, Espero que la aplicación adicional de las regulaciones KYC y AML, consideradas durante mucho tiempo como efectivas por altos funcionarios del gobierno, ayude a calmar sus preocupaciones sobre las transacciones de Bitcoin.

**"Te pago $ 2,000 en un callejón oscuro, ¿quiénes son los testigos de esa transacción?**

**Solo tú y [yo], ¿verdad? Con criptomonedas...**

**el mundo entero podría ser el testigo".**

Los intercambios descentralizados (DEX), que generalmente no tienen una autoridad central en la que aplicar las regulaciones KYC y AML, también son un desafío emergente. Aunque los DEX son responsables de solo una pequeña parte del volumen total de transacciones de criptomonedas, su naturaleza descentralizada, en su mayoría de código abierto, agrega una capa adicional de anonimato y, por lo tanto, ofrece mayores oportunidades para mover fondos ilícitos.**26**

Por lo tanto, las operaciones DEX seguirán siendo un desafío para los reguladores gubernamentales, particularmente con respecto a su uso para facilitar las transacciones entre billeteras "no alojadas" más anónimas.**27**

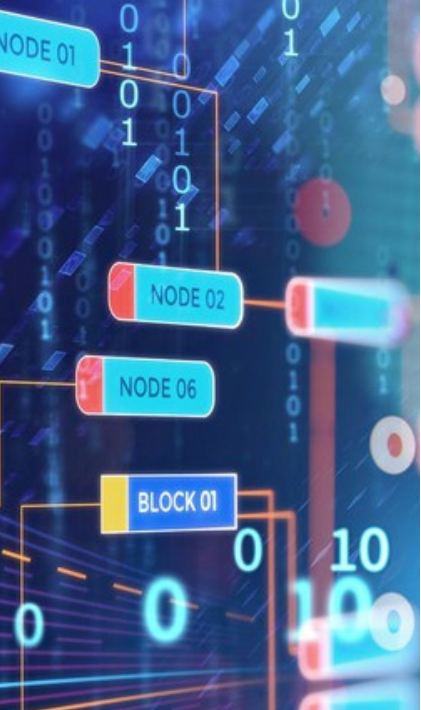
Al igual que otras actividades ilícitas, como el uso de drogas para mejorar el rendimiento en el atletismo, las autoridades trabajan constantemente para ponerse al día con las nuevas técnicas de enmascaramiento utilizadas por los actores ilícitos. En el caso de la criptomoneda, las empresas de análisis de blockchain están desarrollando nuevas herramientas forenses para contrarrestar el uso de tecnologías que crean más anonimato, como monedas de privacidad, mezcladores, vasos, capas y saltos de cadena.

Por ejemplo, en septiembre de 2020, Chainalysis recibió una subvención de $ 625,000 del IRS para desarrollar software de seguimiento de Monero.**28** En noviembre pasado, CipherTrace también presentó dos patentes para tecnologías relacionadas con el rastreo de transacciones de Monero después de trabajar con el Departamento de Seguridad Nacional de los Estados Unidos.**29** Finalmente, en diciembre de 2020, el software forense de criptomonedas incluso pudo rastrear de manera confiable Bitcoin robado que se había pasado a través de varios mezcladores de monedas.**30**

Los servicios forenses de Blockchain pueden ser utilizados de múltiples maneras por las fuerzas del orden y los servicios de inteligencia. En primer lugar, puede utilizarse como instrumento de investigación en casos existentes; La aplicación de la ley puede usar la cadena de bloques para descubrir la actividad ilícita del objetivo de una investigación (e identificar otros posibles malos actores vinculados a través de la cadena de bloques a ese objetivo). En segundo lugar, mediante el uso de algoritmos de inteligencia artificial desarrollados a partir de patrones de cómo se comportan los actores ilícitos en el ecosistema, puede identificar malos actores previamente desconocidos. Con este fin, la cadena de bloques permite a las fuerzas del orden adoptar una estrategia de red proactiva mucho más sofisticada para identificar actividades ilícitas.

Todos los expertos que consultamos creen que los gobiernos han tardado en reconocer el poder forense de la tecnología blockchain. Este retraso refleja una falta de conciencia en los niveles superiores y laborales, así como los desafíos para comprender y trabajar con la extrema complejidad de la informática asociada con la ciencia forense de blockchain. Si bien hay un creciente cuadro de funcionarios gubernamentales que han utilizado con éxito las herramientas analíticas de blockchain para procesar a los malos actores e incautar ganancias ilícitas, relativamente pocos empleados gubernamentales actuales tienen las habilidades para usar esta tecnología en todo su potencial.

Un experto fue aún más lejos, diciendo que la mayor amenaza que involucra a las criptomonedas no son las finanzas ilícitas, sino que los gobiernos aún no entienden completamente el poder de blockchain como una herramienta para las agencias de aplicación de la ley y de inteligencia.



Sin embargo, el experto también señaló que la conciencia de este poder está comenzando a expandirse a medida que los gobiernos se involucran con las tres principales empresas analíticas de blockchain, Chainalysis, CipherTrace y Elliptic. Más allá de los Estados Unidos, los análisis forenses de blockchain están siendo utilizados por agencias gubernamentales en Europa, Japón y Corea del Sur.

Este reconocimiento gradual ayuda a explicar el número de casos legales significativos que se han roto mediante el uso del análisis de blockchain. En noviembre de 2020, el IRS, tras la asistencia de Chainalysis, pudo recuperar $ 1 mil millones en Bitcoin ilícito relacionado con la ahora desaparecida Silk Road DNM.**31**

En la violación de julio de 2020 de la red de Twitter, cuando más de 100 cuentas de alto perfil fueron pirateadas para promover una estafa que pedía a los seguidores Bitcoin, los investigadores tardaron solo dos semanas en identificar a los perpetradores y realizar arrestos. Los investigadores vincularon las direcciones de la billetera a las cuentas de usuario en varios foros. Luego, utilizando análisis de blockchain, rastrearon fondos robados a varios intercambios, trabajaron con esos intercambios para identificar a los usuarios y compararon esa información del usuario con los datos encontrados en los foros. En particular, los investigadores identificaron a un individuo que nunca publicó nada públicamente que pudiera vincularlo a su identidad del mundo real mediante el análisis de transacciones entre direcciones de Bitcoin.**32**

Finalmente, a fines de 2020, el bufete de abogados Kobre & Kim pudo usar el análisis de blockchain para rastrear y recuperar $ 32 millones en criptomonedas que se habían pasado a través de mezcladores de monedas.33 A medida que las herramientas que emplean estas empresas se vuelven más sofisticadas, a los actores ilícitos les resulta cada vez más difícil ocultar su actividad.

Y a medida que se realicen más incautaciones y arrestos, creemos que los actores ilícitos, que son agnósticos de la tecnología, continuarán alejándose del uso de Bitcoin con fines de lavado de dinero a otras vías que les faciliten ocultar sus actividades. Esencialmente será el equivalente antiterrorista de Osama Ben Laden nunca más, por el resto de su vida, usando un teléfono después de enterarse de que el gobierno de los Estados Unidos podía escuchar sus llamadas.

**"El creciente uso de blockchain forense será esencialmente la lucha contra el terrorismo.**

**equivalente a Osama Ben Laden nunca más, por el resto de su vida, usando un**

**teléfono después de enterarse de que el gobierno de los**

**Estados Unidos podía escuchar sus llamadas".**

**Conclusión**

A la luz de las conclusiones a las que hemos llegado, ¿por qué vemos declaraciones y artículos tan alarmistas sobre la amenaza que representa Bitcoin? Hay varias razones. Primero, esta es una nueva tecnología, y es complicada de comprender: las personas suelen temer lo que no entienden.

En segundo lugar, las malas noticias impulsan las percepciones más que las buenas noticias; en resumen, el miedo aparece en los titulares. Una historia sobre un ciudadano francés que envía Bitcoin a personas involucradas en la insurrección en el Capitolio de los Estados Unidos desplaza las historias del uso de forenses habilitados para blockchain para resolver un crimen. Necesitamos reevaluar este tipo de historias reconociendo que fue la naturaleza transparente de la cadena de bloques lo que permitió a las fuerzas del orden identificar tan rápidamente el rastro de los pagos ilícitos, mientras que tales pagos realizados a través del sistema financiero tradicional podrían haber resultado más difíciles de rastrear.

Finalmente, Bitcoin y su naturaleza descentralizada parecen representar una amenaza disruptiva para las instituciones financieras tradicionales. Lo mismo podría haberse dicho de la banca electrónica y las firmas electrónicas hace 20 años, lo que provocó un debate significativo sobre la protección del consumidor y la integridad del sistema financiero. Eventualmente, las instituciones financieras tradicionales encontraron formas de incorporarlo con éxito en sus negocios. Y cualquier nueva tecnología tan innovadora como blockchain representará un riesgo para los métodos establecidos de la industria financiera. Será el papel del gobierno identificar cómo usar y regular mejor la tecnología blockchain para promover el interés nacional.

Toda mi carrera de 33 años en la Agencia Central de Inteligencia fue impulsada por una misión primordial: presentar hechos objetivos y análisis a los responsables de la formulación de políticas para que pudieran tomar la mejor decisión posible para el país. Tales hechos y análisis ayudan a superar el miedo, la percepción errónea y los intereses estrechos (en oposición al interés nacional). Mi esperanza con este documento no es que sea la última palabra sobre el tema de Bitcoin y las finanzas ilícitas, sino más bien, como señalé en la introducción, que conduzca a una discusión más basada en hechos del tema.



**End Notes**

**1**) Monica, Paul R. La. “Bitcoin Tops the $60,000 Mark.” CNN, Cable News Network, 13 Mar. 2021, [www.cnn.com/2021/03/13/investing/bitcoin-prices-60000/index.html](http://www.cnn.com/2021/03/13/investing/bitcoin-prices-60000/index.html).

**2**) Patnaik, Subrat, et al. “A Tesla for a Bitcoin: Musk Drives up Cryptocurrency Price with $1.5 Billion Purchase.” Reuters, Thomson Reuters, 8 Feb. 2021, www. reuters.com/article/us-tesla-crypto-currency/a-tesla-for-a-bitcoin-musk-drives-up-cryptocurrency-price-with-1-5-billion-purchase-idUSKBN2A81CG.

**3**) Manning, Landon. “With Bitcoin on The Rise, Morgan Stanley Joins Institutional Adopters.” Nasdaq, 22 Mar. 2021, www.nasdaq.com/articles/with-bitcoinon-the-rise-morgan-stanley-joins-institutional-adopters-2021-03-22.

**4**) Helms, Kevin. “Canada Has Approved Two Bitcoin ETFs – First One Starts Trading Today.” Bitcoin.com, 18 Feb. 2021, https://news.bitcoin.com/canada-approved-bitcoin-etfs-start-trading/

**5**) Kovach, Steve. “Bitcoin Value Plummeting Following the Silk Road Shut Down.” Business Insider, 2 Oct. 2013, www.businessinsider.com/bitcoin-value-dropsafter-silk-road-shut-down-2013-10.

**6**) Arghire, Ionut. “Dark Web Market AlphaBay Goes Down.” SecurityWeek, 14 July 2017, www.securityweek.com/dark-web-market-alphabay-goes-down.

**7**) Menn, Joseph. “Hackers Mint Crypto-Currency with Technique in Global ‘Ransomware’ Attack.” Reuters, Thomson Reuters, 17 May 2017, www.reuters.com/ article/us-cyber-attack-cryptocurrency-idUSKCN18D00W.

**8**) “Large Bitcoin Payment Made to Far-Right Individuals before U.S. Capitol Attack: Report.” Reuters, Thomson Reuters, 14 Jan. 2021, [www.reuters.com/article/us-usa-election-cryptocurrency/large-bitcoin-payment-made-to-far-right-individuals-before-u-s-capitol-attack-report-idUSKBN29J2PM](http://www.reuters.com/article/us-usa-election-cryptocurrency/large-bitcoin-payment-made-to-far-right-individuals-before-u-s-capitol-attack-report-idUSKBN29J2PM).

**9**) Templon, John. “Secret Documents Show How Terrorist Supporters Use Bitcoin - And How The Government Is Scrambling To Stop Them.” BuzzFeed News, 1 Feb. 10, 2021, [www.buzzfeednews.com/article/johntemplon/bitcoin-cryptocurrency-terrorist-financing-janet-yellen](http://www.buzzfeednews.com/article/johntemplon/bitcoin-cryptocurrency-terrorist-financing-janet-yellen).

**10**) Silfversten, Erik, et al. RAND Corporation, 2020, Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes.

**11**) “Crypto Crime Summarized: Scams and Darknet Markets Dominated 2020 by Revenue, But Ransomware Is the Bigger Story.” Chainalysis, 19 Jan. 2021, blog. chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets.

**12**) “Cryptocurrency Crime and Anti-Money Laundering Report, February 2021.” CipherTrace, 3 Mar. 2021, ciphertrace.com/2020-year-end-cryptocurrencycrime-and-anti-money-laundering-report/.

**13**) “Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium.” Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium | FinCEN.gov, 15 Nov. 2019, www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-chainalysis-blockchain-symposium.

**14**) “New Report Reveals How Cyber Attackers ‘Cash out’ Following Large-Scale Heists.” BAE Systems | Managed Security Services, www.baesystems.com/en-financialservices/insights/news/report-reveals-how-cyber-attackers-cash-out-following-heists.

**15**) Grauer, Kim, and Henry Updegrave. Chainalysis, 2021, The 2021 Crypto Crime Report.

**16**) Dion-Schwarz, Cynthia, and David Manheim. RAND Corporation, 2019, Terrorist Use of Cryptocurrencies.

**17**) “Global Cryptocurrency Market Charts.” CoinMarketCap, coinmarketcap.com/charts/; “Cryptocurrency Prices, Charts and Market Capitalizations.” CoinMarketCap, 22 Mar. 2021, coinmarketcap.com/.

18) Ibid.

**19**) Staff, Decrypt. “Bittrex To Delist Privacy Coins Monero, ZCash and Dash in Two Weeks.” Decrypt, Decrypt, 1 Jan. 2021, decrypt.co/53012/bittrex-to-delistprivacy-coins-monero-zcash-and-dash-in-two-weeks.

**20**) Erb, Kelly Phillips. “IRS Will Pay Up To $625,000 If You Can Crack Monero, Other Privacy Coins.” Forbes, Forbes Magazine, 15 Dec. 2020, www.forbes.com/sites/kellyphillipserb/2020/09/14/irs-will-pay-up-to-625000-if-you-can-crack-monero-other-privacycoins/?sh=32617ccf85cc.

**21**) Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments. Financial Crimes Enforcement Network (FinCEN), 1 Oct. 2020, [www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf](http://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf).

**22**) U.S. House Committee on Financial Services, Subcommittee on National Security, International Development and Monetary Policy, “Dollars Against Democracy” virtual hearing, February 25, 2021.

**23**) Lee, Seulki, and Corinne Redfern. “Sex Criminals Use Bitcoin. So Do the Police.” Foreign Policy, 30 Jan. 2021, foreignpolicy.com/2021/01/30/sex-criminalsuse-bitcoin-so-do-the-police/.

**24**) KYC regulations require financial services companies to acquire sufficient customer information and to perform due diligence. Adequate KYC regulations are integral to AML compliance.

**25**) Silfversten, Erik, et al. RAND Corporation, 2020, Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes; Clegg, Pamela, and Dave Jevans. Cipher Trace, 2020, Cipher Trace Geographic Risk Report.

**26**) Khan, Momina. “DEX Volumes Made up Almost 4% of Centralized Exchange Volumes in July - a Monthly High.” The Block, 4 Aug. 2020, www.theblockcrypto.com/linked/73939/dex-volume-ratio-july.

**27**) Unhosted cryptocurrency wallets are owned and operated by individuals. They do not require a custodian or financial institution in order to conduct transactions.

**28**) Post, Kollen. “Chainalysis and Texas Firm Win Million-Dollar IRS Contract to Crack Monero.” Cointelegraph, Cointelegraph, 30 Sept. 2020, Cointelegraph. com/news/chainalysis-and-texas-firm-win-million-dollar-irs-contract-to-crack-monero.

**29**) Jevans, Dave. “CipherTrace Files Two Monero Cryptocurrency Tracing Patents.” CipherTrace, 21 Nov. 2020, ciphertrace.com/ciphertrace-files-two-monero-cryptocurrency-tracing-patents/.

**30**) “Benjamin Sauter Explains Precedent-Setting Digital Currency Recovery Case.” Benjamin Sauter Explains Precedent-Setting Digital Currency Recovery Case | Kobre & Kim - Disputes and Investigations, kobrekim.com/insights/publications/benjamin-sauter-explains-precedent-setting-digital-currency-recovery-case.

**31**) “United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars.” The United States Department of Justice, 5 Nov. 2020, [www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us](http://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us).

**32**) Barrett, Brian. “How the Alleged Twitter Hackers Got Caught.” Wired, Conde Nast, 31 July 2020, www.wired.com/story/how-alleged-twitter-hackers-gotcaught-bitcoin/.

33) Ibid