Bitcoin y Privacidad 101

Armando Becerra

Consultor en Seguridad de la información, privacidad y protección de datos, México

armando.becerra@ifai.org.mx

Abstract. En este artículo se presenta una visión general de las implicaciones a la privacidad del uso de las llamadas *cripto-monedas*, y su principal representante hasta el momento, el Bitcoin. El artículo pretende destacar algunas consideraciones sobre estas tecnologías: la expectativa razonable de privacidad, la seguridad de la información y el posible abuso por parte de los usuarios.

1 Introducción

El Internet ha transformado la forma en que la macro y microeconomía se desarrollan, hoy en día cerca de dos billones de personas están conectadas a Internet [1] y se estiman intercambios a través de *e-commerce* por ocho trillones de dólares se considera incluso que la madurez en Internet está directamente relacionada al Producto Interno Bruto.

En este entorno es razonable esperar la digitalización de elementos primordiales de la economía como son los sistemas de pago y las divisas, sin embargo muy pocos vislumbraban que el concepto de las *cripto-monedas*, y su principal representante, el *Bitcoin (BTC)*, tuvieran un impacto tan profundo: se le considera la primera moneda digital descentralizada de la historia, su economía es mayor que la de algunos países pequeños y la capitalización de su mercado se estima en más de un billón de dólares.

2 Uso de tecnologías P2P

Ante las amenazas de informáticas, el espionaje gubernamental o simplemente por una noción de *"preservar la privacidad en línea"*, la población ha demostrado inclinación y hasta confianza hacia el uso de las tecnologías de comunicación *peer-to-peer o punto a punto (P2P)*, en un mundo sin *derecho al olvido* [2], muchas personas están optando por estas soluciones para mantener sus actividades en línea fuera de vigilancia, pues actúan como un canal de comunicación instantáneo y a su vez son independiente a terceros que las controlen o monitoreen [3].

La historia de las redes *P2P* puede remontarnos a sitios que han enfrentado serios problemas de derechos de autor (e.g. Pirate Bay [4]), y disidencia civil contra sistemas totalitarios (e.g. TOR [5]): en Arabia Saudita e Irán por ejemplo, la policía religiosa ha encontrado muchas dificultades para evitar que los jóvenes utilicen

mensajería Bluetooth a través de los celulares para llamar y mandar mensajes a completos extraños, ya sea para coquetear o para la coordinación de protestas.

A este punto es difícil entender exactamente quién creo el *Bitcoin*, ya que se hizo bajo el seudónimo de *Satoshi Nakamoto* [6], que podría ser un individuo o un grupo de desarrolladores. En cualquier caso, fue una respuesta a la creciente desconfianza del público hacia la moneda tradicional y a los bancos centrales.

Aprovechando los recursos computacionales existentes, el *BTC* se sostiene en la infraestructura proporcionada por los usuarios y en la comunicación directa entre las partes, bajo la premisa de realizar transacciones anónimas al igual que con las comunicaciones *P2P*.

3 Privacidad en las transacciones

El modelo de banco central tradicional alcanza un nivel de privacidad aceptable en relación de que el acceso a la información está limitado a partes interesadas de confianza. Sin embargo para ciertos usuarios existe la preocupación por reducir el número de entidades que intervienen en estas transacciones:

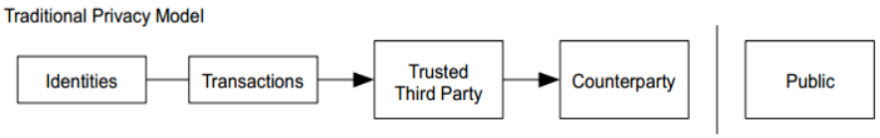

Fig. 1. Modelo tradicional de privacidad en transacciones

A través del cifrado *inherente* en el esquema de funcionamiento de las *cripto-monedas,* se pueden utilizar claves públicas y privadas para la realización de las transacciones, así el público en general puede ver que alguien está enviando una cantidad de *BTC* a otra persona, pero sin información que vincule esta acción a una persona en particular, algo muy similar a la información publicada en las bolsas de valores, donde se conoce el tiempo y el tamaño de las operaciones individuales, sin mencionar las partes que intervienen:

Fig. 2. Modelo de transacciones cifradas

4 Privacidad relativa

Sin bien la concepción del *Bitcoin* contempla un nivel de anonimato similar al de otros esquemas P2P, se podría considerar que a su vez es la red de pagos más transparente jamás creada [7]: todas las transacciones de Bitcoin se almacenan pública y permanentemente en la red, lo que significa que cualquiera puede ver los fondos y transacciones de una dirección Bitcoin.

Si bien el uso de BTC representa beneficios a la privacidad como el hecho de poder crear un número ilimitado de entidades de *Bitcoin* (o carteras, donde se almacena la moneda), cada transacción única es registrada, así por ejemplo alguien podría mandar un BTC a la dirección *"1NiJGiZ2eBvQfKiD7eeG2rtBa6MdHYRXLr"* y saber que esta transacción se hizo pues los "libros" e estas transacciones son públicos, y nada evitaría que alguien realizara una base de datos con el comportamiento de una cartera en particular. Por otro lado, muy pocos bienes lícitos podrían adquirirse por Internet sin que intervenga una forma de identificación [8], como la dirección de envío de la compra. Finalmente, en lugar de prohibir los *BTC*, si estos se vuelven un método de pago de uso corriente entonces seguramente estarán sujetos, quizá no a una regulación específica, pero sí a identificación del comprador. Para fines prácticos y lícitos una moneda no puede garantizar la privacidad de los usuarios.

5 Abuso en la privacidad

TOR es una red de túneles virtuales que permite a los usuarios navegar con privacidad en Internet, a los desarrolladores, crear aplicaciones para el intercambio de información sobre redes públicas sin tener que comprometer su identidad, ayuda a reducir o evitar el seguimiento que hacen los sitios web de los hábitos de navegación de las personas y a publicar sitios web y otros servicios sin la necesidad de revelar su localización.

Los objetivos de TOR como proyecto de software libre son admirables, sin embargo la posibilidad de navegar y crear servicios anónimos ha permitido el desarrollo de actividades a toda luz cuestionables, por ejemplo: pornografía infantil, venta de drogas, tráfico de información sensible o clasificada, lavado de dinero, armas, entrenamiento especializado en temas delictivos, entre otros. El mercado negro tradicional ha encontrado un lugar fértil para expandirse utilizando estas plataformas [9].

Pese a que no hay cifras exactas sobre el crecimiento o popularización de plataformas como TOR para el intercambio de bienes ilícitos, definitivamente hay *un antes y un después* con la utilización *cripto-monedas* como el *BTC* debido a que las transacciones son directas de un usuario a otro, sin ninguna institución mediadora de manera directa.

6 Conclusiones

BTC es una tecnología que ha sorprendido en la sociedad de la información pues está generando grandes cambios en la concepción del dinero y la economía. Existe un desafía inmenso para explotar el potencial minimizando los riesgos existentes: el anonimato relativo, las transacciones internacionales o la consideración de las carteras de *cripto-divisas* como un dato que podrían revelar información de los individuos. El BTC sirve también como referencia respecto a la necesidad del trabajo *inter y trans* disciplinar, pues las tecnologías disruptivas requieren tanto del análisis tecnológico, como del político, legal, económico y por supuesto, el social. Todas las problemáticas identificadas en este artículo, entre otras existentes y por venir, representan un campo fértil para la investigación relacionada al balance *entre la privacidad y la publicidad* de los usuarios al utilizar tecnologías en línea.

Referencias

1. "Internet matters: The Net's sweeping impact on growth, Jobs, and prosperity", 2011, http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters).
2. ROSEN, Jeffrey, "The Right to be Forgotten", Symposium Issue: The Privacy Paradox, 2012. (Consultable en http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten).
3. SCHMIDT Eric, COHEN Jared, "The New Digital Age: Reshaping the Future of People, Nations and Business", John Murray Publishers, 2013, p. 69.
4. El fundador de The Pirate Bay seguirá en prisión preventiva un mes más. (Consultable en http://www.abc.es/agencias/noticia.asp?noticia=1588712)
5. TOR, Overview, "Activist groups like the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online". (Consultable en https://www.torproject.org/about/overview.html.en).
6. NAKAMOTO, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System". (Consultable en: https://bitcoin.org/bitcoin.pdf).
7. Bitcoin.org, "Proteja su privacidad", (Consultable en: https://bitcoin.org/es/proteja-su-privacidad).
8. El lado oscuro del comercio en Internet, El Financiero, 2013 (Consultable en http://www.dineroenimagen.com/2013-08-22/24860).
9. Becerra, A., "Mitos y Realidades de la Internet Profunda", Revista .Seguridad UNAM #20, 2014. (Consultable en: http://revista.seguridad.unam.mx/numero-20/mitos-y-realidades-de-la-internet-profunda)