Aplicaciones ciberdelictivas de criptodivisas como Bitcoin

Autor

Ing. Félix Brezo
DeustoTech Computing (S3Lab)
felix.brezo@deusto.es

Junio 2012

Resumen

Bitcoin es una moneda electrónica concebida a través de un protocolo público que la implementa de una forma completamente descentralizada, de modo que no necesita de ningún emisor central que la gestione. En este informe se recogen las peculiaridades de su diseño, que, junto con un uso cada vez más extendido, convierten a esta criptodivisas en una herramientas útil para la ejecución de todo tipo de transacciones ajenas al control de un organismo regulador, facilitando, entre otras cosas, algunos procedimientos asociados al blanqueo de capitales o al tráfico de sustancias ilegales de diversa índole.

Palabras clave: bitcoin, criptoanarquismo, criptodivisa, dinero virtual, especulación, fraude.

1 Introducción

El fenómeno de las monedas virtuales no es nuevo ni tampoco particularmente reciente, ya que los orígenes del concepto queda situado en algunas listas de distribución de mediados de los 90 [1]. Así, hoy en día, son muchas las monedas virtuales que son utilizadas con mayor o menor éxito en la red: Pecunix[1] hasta e-gold[2], pasando por toda suerte de monedas virtuales asociadas al ocio como los Linden Dollars de Second Life[3] [2, 3] o los Facebook Credits[4] de Facebook.

La novedad que presenta Bitcoin[5] —creada originalmente por Satoshi Makamoto en 2009 [4]— es que se trata de un protocolo público que implementa una criptodivisa basada en una arquitectura *peer-to-peer*. La definición de ésta como una moneda distribuida le viene del hecho de que no existe un organismo central que regule el valor o la cantidad total de monedas existentes, sino que su mantenimiento recae en la capacidad computacional de la red de usuarios en sí misma que gestiona la misma. Esta capacidad de cómputo es utilizada para, entre otras tareas, gestionar el histórico de transacciones —lo que se conoce como la cadena de bloques— y corroborar la validez de todas aquellas nuevas que se vayan a producir en el futuro.

Por protocolo, se establece que la cantidad máxima de unidades monetarias ascienda hasta la cantidad de 21 millones de bitcoins [4] —a veces representados empleando el símbolo de los baht tailandeses (฿) o, en formato de texto, como BTC—, la cual se alcanzará, aproximadamente para el año 2040 tal y como se muestra en la figura 3. Así, la definición de este protocolo hace posible predecir la cantidad total de monedas puestas en circulación en cualquier momento de la historia. A mediados de 2012 ésta ronda la cantidad de los 9 millones de monedas ya repartidas con un valor estimado en el mercado de 52,99 millones de dólares.

1 http://www.pecunix.com/
2 http://www.e-gold.com
3 http://secondlife.com/
4 https://www.facebook.com/credits/
5 http://bitcoin.org

2 Interacción con divisas tradicionales

Son numerosas las formas de comprar o vender bitcoins: desde acceder a páginas de intercambio en las que se pueden hacer transferencias por Paypal, Liberty Reserve, Web-Money u OKPay o transferencias bancarias según el sitio (algunos de los más conocidos son MTGox[6], Bitcoinmarket[7] o BTC-e[8]); hasta la adquisición de bonos o tarjetas de regalo para ser utilizadas en páginas como eBay, Amazon o Steam, pasando por la compra directa de toda clase de bienes o servicios en plataformas de E-commerce que las soporten[9]. En el sitio web Bitcoincharts[10] se listan más de 50 mercados activos en la actualidad en diferentes con movimientos hacia/desde divisas tal y como se muestra en la Ilustración 1.

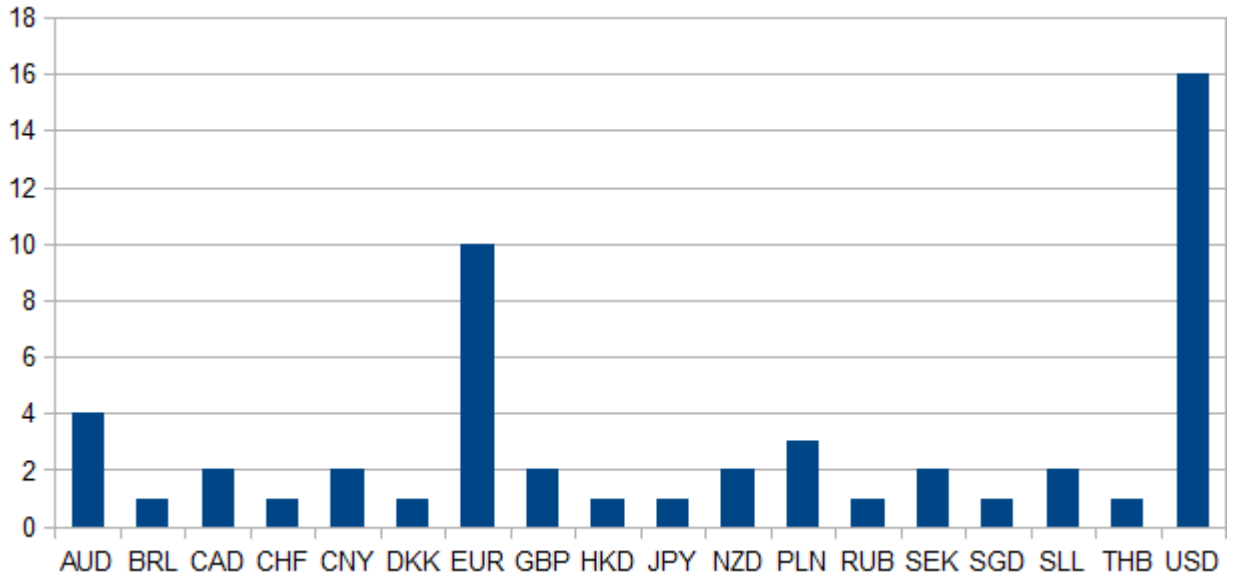

Ilustración 1: Número de mercados disponibles en función de la divisa de cambio.

6 https://mtgox.com/
7 https://www.bitcoinmarket.com
8 https://btc-e.com/
9 osCommerce cuenta con un plugin —descargable en http://addons.oscommerce.com/info/8007— que permite la compra/venta empleando Bitcoin desde mayo de 2011 .
10 http://bitcoincharts.com/markets/list

3 Potenciales usos fraudulentos

El anonimato de las transacciones no es garantizado en sí por el protocolo ya que no es ese el objetivo final del mismo [4]. De hecho, la necesidad de una verificación abierta obliga a la divulgación y publicación de todas y cada una de las transferencias, estudios recientes que emplean herramientas de análisis de tráfico al uso para identificar las llamadas redes egocéntricas, demuestran que ésta no es la realidad de la mayor parte de las transacciones realizadas [5]:

- En el análisis conducido por Reid et ál. se realizaba el seguimiento de una gran cantidad de transacciones realizadas por un autoinculpado como ladrón, al que se le presupone un interés para permanecer anónimo. Los autores, fueron capaces de identificar relaciones de hasta *n=1;2;3* saltos entre la víctima y el supuesto cibercriminal.

- Otro caso planteado por los autores hacía referencia al anuncio de Wikileaks de aceptar donaciones anónimas vía Bitcoin empleando una clave pública única por transacción. Los autores ponen en cuestión el anonimato real del donante.

En resumidas cuentas, se puede afirmar que las transacciones son tan anónimas como imposible sea identificar unívocamente al usuario que las ejecuta [6].

3.1 Movimientos especulativos a gran escala

El intercambio de bitcoins por euros, dólares, libras o incluso por otras criptodivisas es especialmente sensible al movimiento especulativo y a la percepción de su valor. En la ilustración 2 se muestra una la evolución del mercado de intercambio desde el nacimiento de la criptodivisa hasta la situación actual. Como se puede observar, la percepción del valor de los mismos ha oscilado ostensiblemente hasta alcanzar cotas de 25 dólares/bitcoin, cifras muy alejadas de los estabilizados 5,3 dólares/bitcoin actuales; identificándose en torno a junio de 2011 lo que algunos autores como la *Bitcoin Bubble* [7].

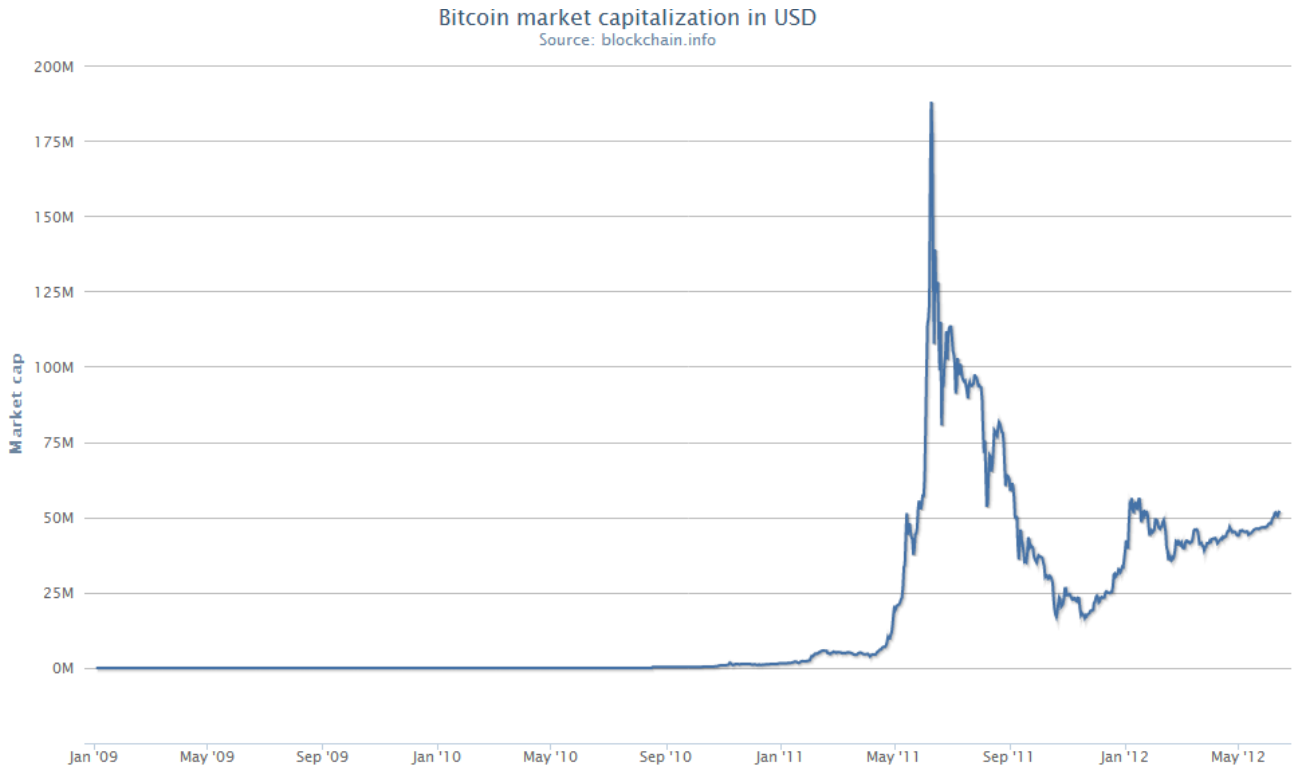

Ilustración 2: Valor del BTC con respecto al USD desde el nacimiento de la divisa.

La especulación también estará presente en el largo plazo. Sabiendo que la totalidad de bitcoins terminará siendo una cantidad finita y si consideramos una población usuaria en crecimiento constante en el tiempo, el valor de 1 BTC tenderá a representar unos bienes con un valor creciente: es decir, la economía de Bitcoin está en la senda de convertirse en una economía potencialmente deflacionaria.

El principal problema operativo que esto conlleva, el de la divisibilidad de la moneda, queda atajado ya que los bitcoins son divisibles en hasta 10^{-8} partes. O lo que sería lo mismo, en partes equivalentes a 10 nanobitcoins, situando la cantidad total de monedas independientes en 2.100 billones de unidades.

De cualquier manera, la circulación real de la totalidad de las monedas es una utopía: diariamente centenares de monedas son asignadas a usuarios que pierden o perderán el control de las mismas por motivos que no tienen por qué estar asociados a prácticas fraudulentas, como su extravío, el olvido de las claves o problemas de índole técnica que afecten a carteras no replicadas.

3.2 Posibilidades para el blanqueo y el tráfico de sustancias prohibidas

A pesar de lo dicho anteriormente, el seguimiento de las transferencias podría terminar dándose por irrastreable con relativa facilidad. A contninuación enumeramos dos supuestos plenamente funcionales a día de hoy:

- La ejecución de transferencias detrás de proxies o sistemas de anonimización como redes tipo Tor[11]. Éste es el caso de la web Silk Road[12]: para acceder a sus servicios es indispensable utilizar la herramienta Tor para preservar el anonimato de sus usuarios. Referenciado por algunos autores como el Amazon de las drogas ilegales [8, 9], en algunos países como EEUU se han llegado a llevar iniciativas políticas para cerrar plataformas similares por el tráfico de drogas [10].

- La ejecución de n transferencias en bloque contra una cuenta que, posteriormente y en un proceso batch u offline auto-gestionado en el que podría tener lugar una comisión, redistribuya el dinero ingresado en m cuentas diferentes, haciendo virtualmente imposible realizar un seguimiento en tiempo real de las cantidades distribuidas. Este proceso, como bien se define en el propio Wiki oficial del proyecto[13] podría tener lugar, bien a través de particulares que ofrecen la posibilidad de incrementar voluntariamente el anonimato de terceros o bien a través de redes organizadas que ofrecen estos u otros servicios a través de mercados de divisas o cibercarteras en la nube —también conocidas como eWallets[14]—.

Algunos de estos enfoques planteam situaciones que requieren de una gestión automatizada de dichas cuentas, sugiriendo un mayor conocimiento y manejo de las herramientas informáticas disponibles. Sin embargo, es tónica habitual en las diferentes comunidades que, de la misma forma que las aplicaciones cliente están distribuidad bajo licencias libres, ocurra lo mismo con aplicaciones paralelas de gestión, facilitando su acceso, replicación y mejora así como diversas características asociadas a su usabilidad.

11 http://www.tor-projet.org
12 http://silkroadvb5piz3r.onion/
13 https://en.bitcoin.it/wiki/Anonymity
14 Dada la irreversibilidad de las transaccciones, no existe verdaderamente ninguna garantía de que las transacciones realizadas hacia o desde un eWallet vayan a ejecutarse más que aquélla que le de el usuario al propio servicio.

3.3 Robo de carteras

Las características del sistema hacen que las monedas se almacenen en forma de ficheros .dat en los equipos de sus dueños. Estos, podrán hacer copias de respaldo que almacenar en equipos alternativos —o en la nube— con el fin de mantener el acceso a ellas aún en caso de fallo en el equipo, lo cual supondría la pérdida automática del control de las mismas ya que no habría forma de recuperarlas. Sin embargo, cualquier usuario —o programa— con acceso lógico a dicho fichero .dat podría ejecutar transacciones por su cuenta si éste no ha sido protegido convenientemente.

Pese a que el uso de estándares de cifrado de los llamados militares —como AES-256[15] por ejemplo— es accesible por parte de cualquier usuario dado que sus protocolos son públicos y están implementados en numerosas librerías y plataformas de código abierto, viene siendo tónica habitual encontrarse con ficheros no protegidos, dando lugar a una corriente de amenazas *malware* dedicadas al robo de estas carteras.

En esta línea, Laboratorios como Kaspersky Labs, desactivaban a finales de marzo el canal de Command & Control[16] de Hlux/Kelihos, una *botnet* especializada en el robo de carteras de Bitcoin [11]. Mientras, las propias Secciones de Ciberinteligencia e Inteligencia Criminal del FBI en un informe de inteligencia recientemente filtrado [12], hablaban de muestras de Zeus[17] pensadas para la extracción directa de los bitcoins de los usuarios infectados con alguna variente de dicho *malware*.

3.4 Uso no autorizado de la capacidad de cómputo

Sin embargo, el uso de redes similares puede también tener otros fines. De forma análoga a como ocurre con los proyectos de computación distribuida, podrían usarse los tiempos muertos de CPU o GPU de las máquinas infectadas para contribuir al proceso de generación de monedas sin el conocimiento del usuario. En las condiciones actuales y con el precío actual del Kwh, la minería de bitcoins no está considerada un negocio rentable si no se dispone del hardware apropiado ya que, en muchas ocasiones[18], los ingresos producidos en el proceso de minería no son capaces de cubrir los costes energéticos de esta generación.

---

15 El Advanced Encryption Standard (AES) es una especificación para el cifrado de datos electrónicos adoptada por el gobierno de los EEUU y que está mundialmente considerado como un estándar criptográfico de facto.

16 Herramienta para el control y gestión de botnets, redes de ordenadores secuestrados con distintos fines.

17 Versión del troyano Zbot especializada en el reclutamiento de equipos como parte de una botnet.

18 https://en.bitcoin.it/wiki/Mining_hardware_comparison

Sin embargo, este extremo es irrelevante en el caso de los escritores de *malware* ya que no harán frente a los gastos de consumo y/o mantenimiento del hardware, por lo que la monetización de la infección será inmediata. Teniendo en cuenta el escenario de una *botnet* de tamaño medio formada por 10.000 ordenadores hábiles y considerando una capacidad de cómputo media de 0,005 bitcoins /día por máquina, el aprovechamiento derivado sería de entorno a 50 bitcoins/día —unos 200 euros/día al cambio en los mercados de compra/venta habituales—. Si se tiene en consideración la desarticulación en 2010 de la *botnet* Mariposa en una acción combinada de Panda Labs junto con la Guardia Civil y cuya dimensión alcanzaba los 13.000.000 de máquinas las cuentas hablan por sí solas del beneficio potencial en el que podría incurrir una red dispuesta para explotar estas características y copar las cifras de asignación diaria de monedas recientemente acuñadas aprovechando una parte aparentemente inofensiva de la capacidad de cómputo de las máquinas infectadas.

4 Tendencias y prospectiva

Para la redacción de este informe se ha podido contactar de forma independiente con negocios europeos que aceptan públicamente esta criptodivisa como elemento de pago y que de hecho utilizan Bitcoin como gancho para atraer a nuevos clientes. En dicho listado[19], en el que principalmente se pueden encontrar locales de hostelería y restauración entre otros negocios, se pone de manifiesto que el uso de esta divisa que en principio podía parecer limitado a las compras por Internet ha traspasado, aunque aún tímidamente, las barreras del mundo real introduciendo un componente adicional del complejidad en la fiscalización del proceso de compra-venta al no haber ningún organismo oficial que reconozca su utilización y, por tanto, no existir un cambio oficial en los diferentes bancos centrales.

El código fuente de Bitcoin puede ser ampliamente estudiada ya que éste está distribuido bajo la Licencia MIT. Esto, casi de forma natural, ha dado lugar a diversas criptodivisas hermanas de la primera pero con características específicas que las diferencian:

- **IXcoin (IXC)**. Se trata de una criptodivisa con un desarrollo paralelo pero programada para tener un período de madurez más breve, ya que el máximo de monedas (también 21.000.000) habrán sido generados para 2015. Esto hace pensar que los movimientos especulativos en el período de maduración de la moneda son potencialmente más violentos.

19 https://en.bitcoin.it/wiki/Real_world_shops

- **Devcoin**. Se trata de una moneda que destina el 90% de los recursos generados a programadores participantes en programas de código abierto para financiar su trabajo, reservando tan sólo el 10% restante a los mineros.
- **Namecoin (NMC)**[20]. También basada en la arquitectura de Bitcoin, los Namecoin son una moneda que trata de crear un sistema de nombres de dominio (DNS) que utilizan el TLD .bit. El objetivo reside en proveer recursos y herramientas a la comunidad para protegerla de la potencial censura que un organismo central (como el ICANN en el caso de los nombres de dominio) tendría la capacidad de efectuar. De esta manera, los dominios .bit son mantenidos por la propia red P2P.

En otro orden de cosas, la filosofía que emplea Bitcoin para evitar el doble gasto y limitar la multiplicación fraudulenta de la moneda ha sido estudiada por algunos autores como Becker et ál. [13] para su generalización y exportación a otros áreas que compartan estas necesidades, mucho más allá de la gestión de dominios que hace Namecoin.

5 Conclusiones

Aunque aún en fases de desarrollo *underground* y desconocidas para el gran público, la proliferación de estas nuevas alternativas de pago trae consigo muchas incertidumbres. Además, la complejidad intrínseca del protocolo y la necesidad de tener unos conocimientos relativamente avanzados para comprender su funcionamiento real, hacen de estas divisas el escenario idóneo para la especulación y la desinformación. Como ya se ha comentado, son muchos los usuarios que piensan que el mero hecho de usarla es una garantía suficiente para ejecutar transacciones anónimas, cuando esto no es así, al menos, por definición.

De la misma manera, la ausencia de un organismo regulador central y la imposibilidad de fijar precios o de hacer uso de otros mecanismos de regulación como ocurre en el caso de las divisas tradicionales, plantea un escenario novedoso: una economía regulada en sentido estricto por los movimientos y sensaciones del mercado. Dicho mercado, autoregulado y actualmente en un proceso de maduración, es susceptible, sin embargo, de ser controlado en el futuro por grandes *fortunas* con la capacidad de mover grandes sumas que terminen por afectar a la percepción del valor de una criptodivisa cuyo valor tangible en sí es nulo.

No hay que olvidar los riesgos de una utilización fraudulenta de la criptodivisa siguen presentes: la gran cantidad de mercados existentes en la red y la posibilidad de cambiar

20 http://dot-bit.org/

bitcoins por euros, libras o dólares con relativa facilidad, hacen de este nuevo método de pago el vehículo perfecto para todo tipo de actividades relacionadas con el blanqueo de capitales, con las complicaciones jurídico-legales que conlleva la delimitación juridisccional de los delitos desarrollados en el ciberespacio. De hecho, uno de los escasos escenarios de fracaso contemplados por sus creadores, salvando una disminución dramática de los usuarios que devaluase la moneda una vez madura, es precisamente una campaña gubernamental a nivel global en contra de su uso. Sin embargo, la diversidad de criterios legales y la pluralidad y complejidad intrínseca de las leyes y acuerdos internacionales en materia de ciberseguridad ya puestos de manifiesto en el pasado, hacen de este extremo un punto de improbable solución inmediata.

6 Referencias

[1] D. Barok, Bitcoin: Financial privacy in a transparent economy, 2011.
[2] P. Ernstberger, Linden dollar and virtual monetary policy, Department of Economics, Economics I, Bayreuth University, 2009.
[3] B. Mennecke, W. Terando, D. Janvrin, and W. Dilla, It's just a game, or is it? Real money, real income, and real taxes in virtual worlds, 2007.
[4] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, http://www.bitcoin.org, 2009.
[5] F. Reid and M. Harrigan, An analysis of anonymity in the bitcoin system, in Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third International Conference on and 2011 IEEE Third International Confernece on Social Computing (SocialCom), pp. 1318–1326, IEEE, 2011.
[6] S. Martins and Y. Yang, Introduction to bitcoins: a pseudoanonymous electronic currency system, in Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research, pp. 349–350, IBM Corp., 2011.
[7] Maurer, B. M., Money nutters, p. 5, 2011.
[8] E. Jacobs, Bitcoin: A Bit Too Far?, volume 12, 2011.
[9] M. BARRATT, SILK ROAD: EBAY FOR DRUGS, volume 107, pp. 683–683, Wiley Online Library, 2012.
[10] Manchin, Joe , Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs, Press Release, 2011:
http://manchin.senate.gov/public/index.cfm/2011/6/manchinurges-federal-law-enforcement-to-shut-down-onlineblack-market-for-illegal-drugs
[11] Kaspersky Lab, How Kaspersky Lab and CrowdStrike Dismantled the Second Hlux/Kelihos Botnet: Success Story, 2012.
[12] Directorate of Intelligence: Cyber Intelligence Section and Criminal Intelligence Section, Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit
[13] J. Becker, D. Breuker, T. Heide, J. Holler, H. Rauer, and R. B¨ohme, Can We Aord Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency, 2012.