ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

13/2014 19 febrero de 2014

David Ramírez Morán

FUNDAMENTOS DE LAS DIVISAS VIRTUALES: BITCOIN

FUNDAMENTOS DE LAS DIVISAS VIRTUALES: BITCOIN

Resumen:

Las divisas virtuales están ganando popularidad gracias a la publicidad que los medios de comunicación les están proporcionando con las frecuentes noticias sobre el tema. Los beneficios de anonimato y los crecientes intereses financieros que empiezan a rondar a este tipo de activos están dando lugar a un incremento considerable del número de usuarios así como de su precio de mercado. En este documento se hace un análisis de los fundamentos de funcionamiento en los que se basa la más popular de estas divisas virtuales: Bitcoin.

Abstract:

Virtual currencies are experiencing a growth in popularity thanks to the promotion that media is achieving with the numerous news on the subject. The benefits of anonymity and the growing financial interest around this kind of actives is giving place to an increase in the number of users as well as its market price. This brief presents the working fundamentals of one of the most popular virtual currencies: Bitcoin.

Palabras clave:

Divisa virtual, Bitcoin, anonimato, transacciones electrónicas

Keywords:

Virtual currency, Bitcoin, anonimity*, electronic transactions*

El fenómeno del dinero electrónico se está extendiendo para dar soporte a las actividades que se desarrollan en el ciberespacio. Una de las primeras actividades virtuales que incluía el concepto de divisa virtual fue SecondLife, una red social en la que los usuarios podían interactuar entre sí en el mundo virtual que definía. Con la implantación de una moneda virtual, Linden Dollar, los usuarios podían adquirir objetos y posesiones virtuales. Para obtener crédito se podían realizar actividades en el juego o bien recurrir a cambiar dinero real por créditos del mundo virtual. Suponía el primer paso en la creación de productos virtuales por los que los usuarios estaban dispuestos a pagar. Este modelo se popularizó rápidamente y empezaron a surgir juegos multijugador online donde los jugadores podían acceder a objetos, misiones o mejoras mediante la compra de créditos.

Con la explosión del uso de internet, la utilización de medios virtuales de pago también se ha generalizado para facilitar las operaciones y obtener una mayor seguridad en las transacciones. El objetivo es reducir los riesgos asociados a proporcionar a un desconocido los datos bancarios personales. Así, servicios como PayPal o Google Wallet, entre otros muchos, proporcionan un monedero virtual con el que se pueden realizar pagos en infinidad de servicios de todo tipo prestados en la red.

Sin embargo, en ciertos entornos se ha hecho necesario ir un paso más allá con objeto de alcanzar el anonimato total en las transacciones. En este contexto, donde el anonimato de la red resulta imprescindible para los artífices de ciertas actividades, surgen las denominadas divisas electrónicas. Se trata de activos equivalentes al dinero en metálico, dado que no identifican al poseedor y no queda constancia de las operaciones que éste lleva a cabo.

De entre estas divisas destaca Bitcoin, por su creciente popularidad gracias a la aparición en los medios de comunicación y por la capitalización que ha llegado a alcanzar en los últimos meses. A continuación se hace una descripción de los principios de funcionamiento de esta divisa virtual para, en un documento posterior, analizar la evolución, los riesgos y las vulnerabilidades que afectan al sistema.

Origen

Bitcoin se relaciona con el programador Satoshi Nakamoto, quien en 2009 publicó un documento describiendo el funcionamiento de la divisa[1]. La creación de la primera aplicación para operar con Bitcoins también se le atribuye. Sin embargo, existen dudas sobre

[1] Satoshi Nakamoto "Bitcoin: An electronic peer-to-peer cash system." https://www.bitcoin.org/bitcoin.pdf (Consultado el 18/02/2014)

la nacionalidad e incluso sobre la existencia real de esta persona y hay múltiples especulaciones sobre su identidad real.

Bitcoin consiste en un sistema distribuido donde no existe ningún ente central de gestión, sino que se basa en una red entre pares donde todos los nodos pueden contribuir al funcionamiento del sistema. Inicialmente todos los nodos ejercían la doble función de realizar transacciones y de procesarlas. Sin embargo, con la generalización de su uso, aparecieron aplicaciones que permiten únicamente realizar transacciones, mientras que el procesado se está concentrando en sistemas específicos.

Desde que se puso en funcionamiento en 2009 el sistema ha ido ganando popularidad gracias a las características de anonimato con las que permite realizar transacciones comerciales y al interés especulativo que ha despertado la evolución de su cotización al cambio con monedas reales.

FUNDAMENTOS

Para que Bitcoin cumpla su cometido es necesario poder hacer transacciones y para ello, además de existir un elemento a intercambiar, debe ser posible identificar a las partes que intervienen en la transacción. El elemento a intercambiar es el saldo de Bitcoins, mientras que las partes son identificadas mediante los identificadores de usuario. Además, los usuarios deben disponer de procedimientos para realizar las operaciones y para conocer el saldo que tienen disponible.

Seguridad de Bitcoin

La seguridad de Bitcoin reside en la utilización de técnicas de criptografía para la protección del saldo del usuario. La firma y la verificación de las solicitudes de transacción se realizan mediante técnicas de criptografía de clave pública.

Esta técnica consiste en asociar a un usuario dos claves, una denominada pública y otra privada. El conocimiento de una de las claves no permite actualmente obtener el valor de la otra clave por lo que, aunque se distribuya la clave pública, una tercera persona no va a poder deducir, obtener o calcular el valor de la clave privada. Para hacer operaciones es necesario distribuir la clave pública de forma generalizada para que cuando se le remita información a un destinatario éste pueda comprobar que la información es válida, correcta y que corresponde a información que sólo ha podido ser generada por una persona que posee

la clave privada. Por este motivo resulta de importancia vital conservar a buen recaudo la clave privada, dado que toda información que haya sido firmada con la clave privada será considerada como válida y correcta.

El proceso por el que se aplica la clave privada a la información que se va a transferir se denomina firma y consiste en obtener un número que depende de la información a transmitir y de la clave privada. El receptor, a partir de la información recibida y la clave pública del usuario, obtiene un nuevo número que, si coincide con el enviado, permite validar la autenticidad y fiabilidad de la información.

Una vez garantizada la seguridad del saldo del usuario, el sistema también debe asegurar que las transacciones son correctas y que el poseedor de un saldo no puede gastarlo más de una vez. Para ello se utilizan técnicas de sellado temporal con las que se registra el momento exacto en el que se solicita una transacción de bitcoins. Los nodos de procesado tienen en cuenta estos valores para determinar cuándo una transacción es válida o no.

Identificador de Bitcoin

A un usuario de Bitcoin se le asigna una dirección formada por una cadena entre 27 y 34 caracteres alfanuméricos, que empieza por 1 o por 3, y que incluye varios caracteres que permiten, como el dígito de control de las cuentas corrientes o la letra del DNI, verificar que la dirección es válida para evitar errores al teclearlas. Este valor es equivalente a un número de cuenta o a un número de teléfono, e identifica unívocamente al usuario. La cadena contiene la información sobre la clave pública del usuario, lo que permite validar las transacciones firmadas mediante la clave privada de este usuario cuando llegan a un nodo de la red.

La obtención de un identificador de Bitcoin es gratuito y se puede obtener tanto en los servicios que están surgiendo en la red como en las aplicaciones monedero que utilizan los usuarios. Con un ordenador actual, un usuario puede obtener varios miles de identificadores con sus claves asociadas en cuestión de minutos.

Monedero de bitcoins

Un monedero de Bitcoins es una aplicación, que con frecuencia se denomina cliente Bitcoin, que permite al usuario realizar operaciones. La aplicación puede estar en el ordenador del usuario, en su teléfono móvil o en uno de los múltiples servicios que están surgiendo en la red que proporcionan la opción de alojar el monedero de un usuario.

Las informaciones que maneja el monedero son el o los identificadores del usuario y las claves correspondientes a cada una de las identidades.

Mediante la aplicación, el usuario puede consultar el saldo de Bitcoins de cada una de sus identidades y ordenar la realización de transacciones. Una vez introducidos los valores de remitente, destinatario e importe, la aplicación realiza la firma de la solicitud de transacción y la remite a los nodos de minería, que se describen más adelante.

Cadena de bloques

La cadena de bloques es el núcleo central de Bitcoin y consiste en la lista de todas las operaciones realizadas con Bitcoins hasta la fecha una vez validadas. Se trata de un fichero que con el tiempo se va haciendo cada vez más largo a medida que se incorporan nuevas transacciones.

La cadena de bloques es el único elemento a partir del cual se puede determinar el saldo de un usuario. Para ello se debe recorrer la cadena buscando la última transacción validada de ese identificador.

La cadena de bloques es uno de los aspectos más cuestionados en lo que respecta al anonimato de este sistema, dado que la información de absolutamente todas las transacciones se almacena sin ningún tipo de cifrado y de forma accesible para todos los usuarios.

Transacciones

La información requerida para llevar a cabo un transacción, o intercambio de Bitcoins entre dos o más personas, se compone del identificador del remitente o remitentes, el identificador del destinatario o destinatarios, el importe o importes de la transacción y el instante en el que se ordena la misma.

Cuando un usuario desea llevar a cabo una de estas transacciones, genera una petición con estos datos y la firma con su clave privada. Esta información se envía a los nodos que las tramitan y, tras cierto tiempo, los datos se incorporan a la cadena de bloques de forma definitiva. A partir de ese momento, el destinatario ya puede comprobar cómo el saldo asociado a su identificador se ha incrementado mientras que el del remitente habrá disminuido.

Obtención de Bitcoins

Los mecanismos por los que se pueden obtener Bitcoins son varios:

- Compra en servicios de intercambio que están apareciendo en la red.
- Intercambio entre particulares.
- Compensación por la venta de productos o servicios.
- Minería de Bitcoins.

En la red están surgiendo intermediarios que permiten que la oferta y la demanda de Bitcoins coincidan en un lugar común para poder hacer intercambios. Estos servicios son muy importantes porque constituyen el nexo con la economía real. Permiten adquirir Bitcoins a cambio de dinero y, lo más importante, permiten convertir los Bitcoins en dinero en metálico. Estas operaciones pueden estar sujetas a una comisión para el prestador del servicio.

Un particular también puede hacer un intercambio sin necesidad de recurrir a un servicio específico. Sólo requiere conocer el identificador del destinatario de la transacción y ordenarla mediante su monedero de Bitcoins. Como contraprestación puede recibir dinero, servicios o cualquier otro beneficio que hayan acordado las dos partes como si se tratara de dinero en metálico.

Las empresas también están utilizando el Bitcoin como medio de pago de sus servicios. El tipo de negocio que empezó a aceptar el pago en Bitcoins estaba relacionado con actividades ilícitas como armas, drogas, etc. Sin embargo, la economía real también está empezando a tenerlo en cuenta como medio de pago y ya hay incluso una agencia de viajes que permite el uso de Bitcoins[2].

Para fomentar que los usuarios colaboren de forma activa en el funcionamiento del sistema, la colaboración en el procesado de transacciones es una actividad remunerada que permite a la persona que proporciona sus recursos e infraestructuras obtener lucro de las operaciones necesarias para incorporar transacciones a la cadena de bloques. Este procesado, que se denomina minería, es un mecanismo relativamente complejo que se trata con más detalle a continuación.

[2] "Los primeros turistas del mundo en comprar viajes con «bitcoins»" Diario ABC 30/01/2014. http://www.abc.es/viajar/20140130/abci-turistas-bitcoins-201401291903.html (Consultado el 18/02/2014)

Minería de Bitcoin

La minería constituye un mecanismo imprescindible para el funcionamiento de esta divisa virtual. Se denomina así al procedimiento por el que las transacciones se incorporan a la cadena de bloques, y resulta imprescindible para que se puedan realizar transacciones. A su vez, constituye el mecanismo único por el que se ponen en circulación los nuevos Bitcoins.

La denominación proviene de la similitud con la labor desarrollada en una mina de oro, donde por cada hora de trabajo se consigue una porción del preciado metal.

La minería de Bitcoins se puede comparar con realizar la compra en un supermercado en el que no se conocen los precios de los productos. La labor que tiene que hacer el minero es encontrar el producto adicional de la tienda que, añadido a un carro de la compra de valor desconocido, hace que el número de ceros finales del importe total sea igual o superior a cierto número. La dificultad de la operación estriba en que obtener el importe total es una tarea que requiere realizar cierto número de operaciones con el precio de cada producto, y que esta operación hay que volver a realizarla desde el principio cada vez que se comprueba que el producto adicional que se ha añadido no da un resultado correcto y hay que probar con otro.

El carro de la compra es equivalente a lo que en Bitcoin se denomina “bloque”; los productos que incluía el carro de la compra son las nuevas transacciones de Bitcoins entre usuarios; y el producto añadido por el minero para conseguir el importe total deseado es lo que se conoce como “nonce”, que no es más que un número que se añade a los datos de las transacciones y que produce el cambio del resultado a medida que se incrementa o varía. Técnicamente, la operación de calcular el importe total del carro de la compra es, en realidad, una operación de doble *hashing* SHA256 en cadena, que, a partir de una secuencia de valores de longitud arbitraria, proporciona un resultado de 256 bits, denominado “hash”, que debe ser menor de cierto umbral.

Obtener el valor hash a partir de la secuencia de datos es una operación relativamente sencilla. Sin embargo, la operación inversa, consistente en determinar los datos que producen un valor de hash determinado, es muy compleja, por lo que no es posible determinar de forma analítica el valor del “nonce” necesario para validar el bloque y hay que hacerlo por prueba y error.

El primer usuario que consigue encontrar el "nonce" que da lugar al resultado deseado lo comunica al resto de la red para que se actualice la cadena de bloques y se le adjudica la recompensa por haber encontrado la coincidencia. A partir de ese momento, todas las transacciones incluidas en el bloque quedan consolidadas en la cadena de información de Bitcoin y, desde ese momento, el resto de mineros que estaban haciendo pruebas con los datos contenidos en ese bloque deben vaciar el carro de todos aquellos productos ya procesados y llenarlo con el resultado del bloque anterior y las nuevas transacciones que realizan los usuarios.

Se puede dar la situación de que dos usuarios obtengan una solución de forma simultánea. El carro de cada uno de los usuarios contendrá diferente número de transacciones, por lo que la infraestructura de Bitcoin sólo recompensará al usuario que haya incluido un mayor número de ellas en su carro. De esta forma se consigue que los mineros vayan incorporando las nuevas transacciones con cierta frecuencia, dado que si se quedan calculando los mismos productos mucho tiempo, otro minero puede encontrar una solución que, además de esas transacciones, incluya alguna más.

La dificultad de la operación de minería se puede ajustar modificando el umbral que se debe satisfacer. Cuanto más pequeño se hace el umbral de validación del hash, el número de valores "nonce" que proporcionan un valor correcto disminuye y, por tanto, hay que probar más valores diferentes para encontrar uno válido. Mediante el ajuste del valor es posible controlar la velocidad a la que se validan bloques. Este valor se va ajustando para que se valide un bloque cada 10 minutos y el valor del umbral se corrige cada 2160 bloques, lo que equivale, idealmente, a 15 días.

El tiempo que se tarda hasta que un minero consigue validar un bloque determina la velocidad con la que se pueden realizar transacciones con Bitcoin. Una transacción no está completa hasta que el bloque que la incluye no se ha validado e incorporado a la cadena de bloques.

La recompensa a la minería de datos consiste en otorgar al usuario que encuentra la solución a un bloque cierta cantidad de Bitcoins. Inicialmente esta cantidad era de 50 Bitcoins, aunque el funcionamiento del sistema contempla ir reduciendo esta cantidad a la mitad cada vez que se añadan 210000 bloques a la cadena. Actualmente la recompensa se encuentra en 25 Bitcoins e irá disminuyendo a lo largo del tiempo como se muestra en la Ilustración 1.

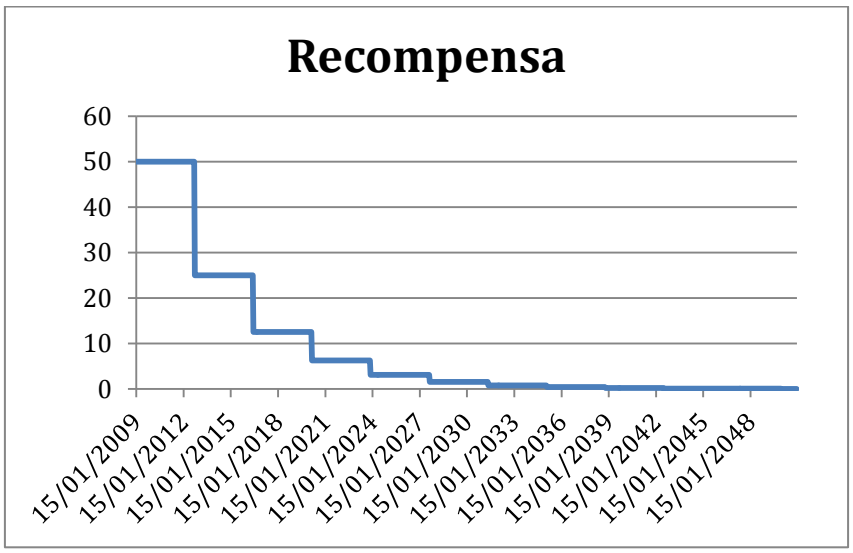

Ilustración 1 Evolución de la recompensa por minería (Fuente: elaboración propia)

Además de la recompensa asociada a la minería de datos, los usuarios también pueden hacer un pago a los mineros para priorizar la inclusión de sus operaciones en el proceso de minería. De hecho, a medida que la recompensa vaya disminuyendo, el pago por transacción se va a tener que generalizar para cubrir los costes asociados a la realización de las operaciones necesarias para incorporar los nuevos bloques a la cadena.

Las recompensas otorgadas por las tareas de minería son el único procedimiento por el que aumenta la cantidad de Bitcoins en circulación. El algoritmo en el que se basa el funcionamiento impone un límite a la cantidad máxima de Bitcoins en circulación, que tiende asintóticamente a alrededor de 21 millones de unidades, como se representa en la Ilustración 2. Este valor se corresponde con la suma de todas las recompensas que se van a adjudicar a medida que se vayan incorporando los bloques de transacciones a la cadena. Actualmente el número de Bitcoins en circulación asciende a alrededor de 12 millones y medio.

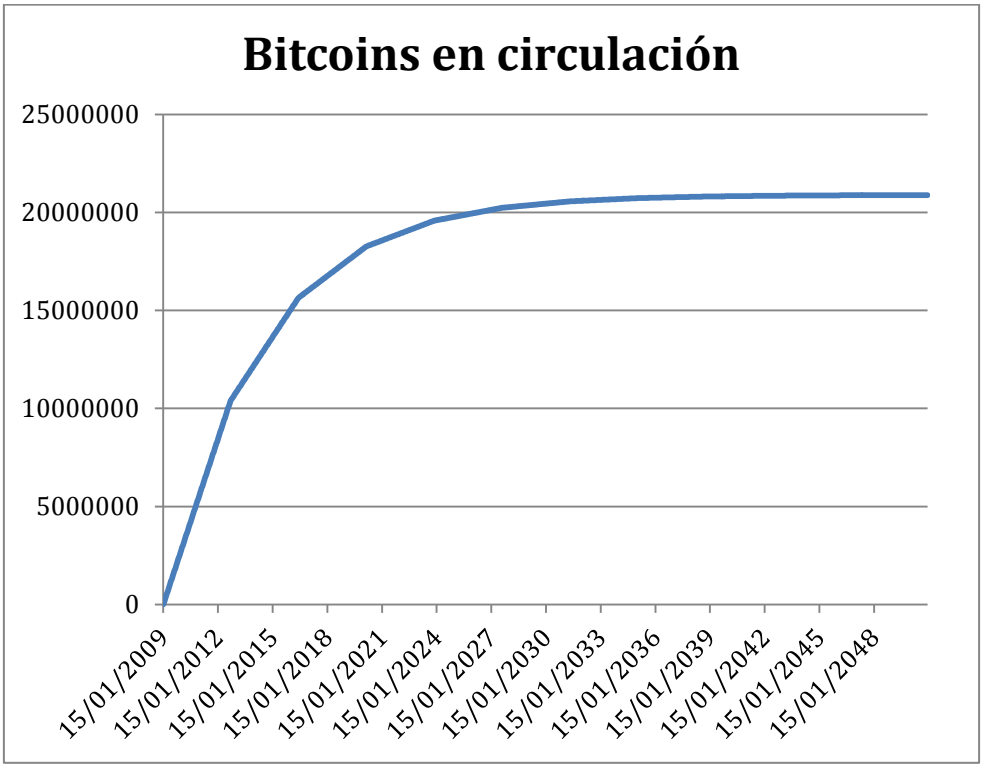

Ilustración 2 Evolución del número de Bitcoins en circulación (Fuente: elaboración propia)

Cotización

En ausencia de un organismo que respalde el valor del Bitcoin, el precio que toma viene dado exclusivamente por el precio al que los usuarios estén dispuestos a intercambiarlo. El tipo de cambio se está determinando a partir de las operaciones que se realizan en los servicios que permiten adquirir Bitcoins o venderlos y, por tanto, convertirlos en efectivo de cualquier otra moneda.

A partir de la cotización es posible obtener la capitalización total, que resulta de multiplicar el número de Bitcoins en circulación por su cotización, y asciende a alrededor de 3750 millones de euros (a fecha de 18/02/2014), pese a haber alcanzado un máximo alrededor de 12.500 millones de euros cuando su cotización tomó valores por encima de los 1.000 euros.

Anonimato

Una vez que se dispone del equivalente al dinero en efectivo en la red, sólo queda un paso más para conseguir el total anonimato en las transacciones virtuales: eliminar la relación entre el identificador de Bitcoin y la dirección IP del ordenador desde el que el usuario

realiza las operaciones. Para hacer una transacción el usuario tiene que enviar a los nodos que dan soporte a Bitcoin los datos de la operación. Mediante el uso de tecnologías de "anonimización" como TOR[3] es posible ocultar la dirección IP desde la que se está realizando la transacción, lo que constituye, al fin y al cabo, el único método por el que poder identificar a la persona u organización que la está realizando. Esta práctica es la que establece y fortalece la relación existente entre Bitcoin y lo que se denomina como *web profunda*.

Otra forma de contribuir al anonimato de las transacciones consiste en hacerlas de forma que en la misma transacción se transfiera todo el importe del remitente. El importe pactado se envía al destinatario deseado, mientras que el resto del importe se destina a un nuevo identificador que el remitente haya creado. De esta forma, el identificador original del remitente queda sin saldo y puede dejar de utilizarlo sin problema. Esta práctica también es recomendable para la renovación periódica de las claves de firma del usuario, dado que con la creación de un nuevo identificador se crean una nuevas claves, tal y como se recomienda hacer en general con las contraseñas.

La práctica del *tumbling* se da a menudo entre los usuarios de Bitcoin y consiste en realizar transacciones entre un número elevado de identificadores diferentes con importes que van variando para incrementar la dificultad a la hora de rastrear el camino que ha seguido el saldo de Bitcoins. A partir, por ejemplo, de una cuenta de origen, el saldo se va distribuyendo entre muchas más cuentas de distintos importes. A su vez, el importe de estas cuentas se va juntando y separando con diferentes importes a lo largo de múltiples operaciones consecutivas.

En los dos casos anteriores quedan registradas todas las operaciones en la cadena de bloques por lo que, con los recursos adecuados, podría llegar a ser posible desentrañar estas operaciones.

[3]Luis de Salvador, REDES DE ANONIMIZACIÓN ENINTERNET: CÓMO FUNCIONAN YCUÁLES SON SUS LÍMITES, Documento de Opinión 16/2012. Instituto Español de Estudios Estratégicos http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf (Consultado el 18/02/2014)

CONCLUSIÓN

Las divisas virtuales se están popularizando gracias al anonimato con el que los usuarios pueden realizar sus transacciones. Fruto de esta popularización, también están surgiendo riesgos en la utilización de este tipo de divisas.

Como con todo activo que gana popularidad y despierta interés, están apareciendo prácticas fraudulentas que pueden afectar a su funcionamiento actual y a los intereses de aquellas personas que recurren a este tipo de divisas virtuales.

El aumento de la dificultad para conseguir Bitcoin por procedimientos formales está dando lugar a múltiples técnicas por las que apropiarse de los Bitcoin ajenos. Como todo sistema basado en nuevas tecnologías e internet, está sujeto a ataques de origen difícil de determinar y que en un breve lapso de tiempo pueden tener graves consecuencias, en este caso para los usuarios.

Los estados no son ajenos al progreso que están tomando las divisas virtuales y empiezan a tomar decisiones con las que regular su utilización y funcionamiento.

Los riesgos y vulnerabilidades de este tipo de divisas virtuales y la regulación que se está desarrollando respecto a estas iniciativas serán tratados con detalle en un futuro análisis.

David Ramírez Morán
Analista del IEEE