Criptomonedas como nueva herramienta en las transacciones financieras cubanas

Articulo arbitrado

Cryptocurrencies as a new tool in Cuban financial transactions

ALEJANDRO GARCÍA FIGAL

Universidad de La Habana, Cuba, agarciaflol@gmail.com

RESUMEN

En la última década se ha presenciado cambios importantes en relación a las finanzas alrededor de todo el globo, uno de estos cambios que más ha impactado es la incorporación de una nueva forma de divisa como medio de pago, estas son las denominadas criptomonedas o criptodivisas. Esta innovadora forma de dinero ha contribuido a la creación de nuevos mecanismos para realizar transferencias financieras, incluso países con importantes economías han optado por utilizar e incorporar estas criptodivisas, sacándole partido a las ventajas que conlleva su uso. Esta investigación tiene como objetivo analizar las características de estas criptomonedas, y cómo incorporarlas como un nuevo instrumento para lograr aliviar las repercusiones del bloqueo existente en Cuba.

Palabras claves: criptomonedas, red de par a par, criptografía asimétrica, llave pública, llave privada, cadena de bloques

Código JEL: G39 Finanzas Corporativas y Gobierno: Otro

Citar como (APA):
García Figal, A. (2021): Criptomonedas como nueva herramienta en las transacciones financieras cubana. *Revista Cubana De Finanzas Y Precios, 5* (1), 102-109. Consultado de http://www.mfp.gob.cu/revista/index.php/RCFP/article/view/08_V5N52021_AGF

ABSTRACT

In the last decade there have been important changes in relation to finance around the globe, one of these changes that has most impacted is the incorporation of a new form of currency as a means of payment, these are the so-called cryptocurrencies or cryptocurrencies. This innovative form of money has contributed to the creation of new mechanisms to make financial transfers, even countries with important economies have chosen to use and incorporate these cryptocurrencies, taking advantage of the advantages that their use entails. This research aims to analyze the characteristics of these cryptocurrencies, and how to incorporate them as a new instrument to alleviate the repercussions of the existing block in Cuba.

Keywords: *cryptocurrencies, peer-to-peer network, asymmetric cryptography, public key, private key, blockchain*

INTRODUCCIÓN

Cuba tiene un área de 109 886 km^2, lo cual aun siendo la mayor de las Antillas no la hace un país grande y de abastos recursos. Otra característica es que se encuentra a 90 millas de Estados Unidos, la potencia más grande del mundo, la cual mantiene un férreo bloqueo que no ha menguado en los últimos años, el cual representa el principal obstáculo para el desarrollo de esta pequeña pero grande isla.

De todas las dificultades que nos presenta el bloqueo económico por parte de Estados Unidos, una de ellas es la entrada de divisas libremente convertibles para Cuba (dígase euro, dólar canadiense, franco suizo, libra esterlina, dólar americano, etc.), lo que dificulta las importaciones de materia prima o capital para el país, puesto que en el mercado mundial se utiliza estas llamadas divisas fuertes para efectuar estas operaciones. Además de que cuando se logra establecer un acuerdo comercial con otro país, las transacciones financieras se encarecen el triple de su valor, e incluso la contraparte la llega a cancelar producto de las sanciones aplicadas por Estados Unidos.

Ante todas estas adversidades, Cuba busca soluciones para lograr un desarrollo próspero e impulsar la economía; buscando aportar y contribuir a la solución, en el trabajo empírico se propone una idea con el fin de lograr esquivar por así decirlo estas trabas, buscando establecer un mecanismo que permita una entrada de divisas fuertes y que evite las sanciones de Estados Unidos en las transacciones financieras, el mecanismo que se propone es el uso de las criptomonedas como instrumento financiero. El uso de estas criptodivisas persigue la idea de permitir a Cuba realizar operaciones financieras directamente con la contraparte, sin la necesidad de que el dinero pase por grandes bancos y que nuestros vecinos no apliquen sanciones ni obstaculicen el proceso.

El estudio empírico que se presenta tuvo como objetivo central las características fundamentales de las criptomonedas, así como la tecnología empleada en sus bases y el análisis de este mercado. Se exponen las bases de la criptografía asimétrica y la evolución de esta nueva forma de pago, ilustrando mediante un ejemplo como se procede en este tipo de transacciones.

La investigación, apoyándose en un análisis del funcionamiento de las criptomonedas, se propone evidenciar como aplicando estos métodos se llega a un mejor resultado financiero, y como

el uso de estas criptodivisas permite a Cuba evitar las trabas del bloque impuesto por Estados Unidos.

METODOLOGÍA

Las monedas virtuales (*virtual currency*), son monedas digitales que se emplean como medio de pago mediante internet (Banco Central Europeo, 2012). Estas no deben ser confundidas con mecanismos representativos de *commodities*. Estos últimos son considerados como dinero basado en mercancía "*commodity money*". Las monedas virtuales tienen denominación propia y no tienen correspondencia en el mundo físico. Estas no se pactan bajo el supuesto de que sean convertibles en dinero fiduciario, aun cuando en mercados secundarios permitan regularmente dicha conversión (Banco Central Europeo, 2012). La función principal de estas es como medio de pago y se determina por lo que se pueda comprar directamente con ellas. (Gas y Halaburda, 2015)

Las criptomonedas son un tipo de moneda virtual con características particulares que les permiten una aplicación más universal y extendida. Una de sus particularidades que las hace especiales es que funcionan sin intermediarios que validen las transacciones, y en sus versiones más populares son descentralizadas, lo que significa que se emiten y cambian de manos de forma descentralizada utilizando criptografía para mantener la fidelidad, además de tecnologías de registros o libros contables que son mantenidos y actualizados por miles de computadoras independientemente para verificar que no existan usos duplicados (Brito y Castillo, 2013; Halaburda Y Sarvory, 2016). Dadas estas especiales características, las criptomonedas aspiran a tener las mismas funciones que el dinero corriente. Son lo que muchos piensan el "próximo paso lógico revolucionario en la historia del dinero".

La historia y los problemas de las monedas virtuales han sido objeto de estudio de muchos académicos, y es que las criptomonedas resuelven en gran parte las trabas de la dependencia de la tasa de intercambio en la demanda, ya que el precio de esta va a fluctuar principalmente por la demanda que presente. Por otra parte, las criptomonedas solucionan de manera definitiva el problema de la centralización con la introducción de mecanismos de registros descentralizados que permiten a las partes transar en forma directa sin preocuparse por los inconvenientes asociados a la existencia de intermediarios.

Para lograr una mejor comprensión del funcionamiento de esta nueva forma de dinero, se exponen algunas nociones de su operatoria que no pretende ser muy profunda desde el punto de vista computacional. Se toma como punto de partida el *White Paper*, que presenta las bases conceptuales del Bitcoin, la más popular y extendida de las criptomonedas.

Para Satosho Nakamoto, Bitcoin es: "Un sistema efectivo electrónico (...) basado en prueba criptográfica (...) que permite a las partes transar directamente entre sí sin necesidad de un tercero, que es reemplazado por una red de par a par (peer-to-peer) descentralizada, que guarda registro cronológico de las transacciones y evita el problema del doble pago. (Nakamoto, 2009)

A esta definición algunos autores agregan características como que Bitcoin es un software de código abierto, que permite un cuasi anonimato y que tiene costos de transacciones menores a otros sistemas de pago. (Brito y Castillo, 2013, Grinberg, 2012)

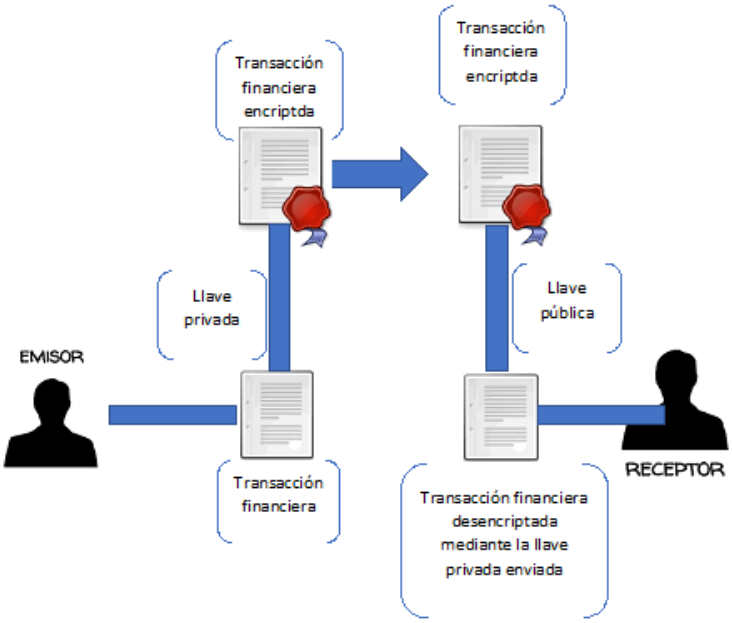
La operatoria de las criptomonedas para una mejor comprensión y siguiendo a Bonneau y sus coautores, es conveniente dividir el análisis en el de tres componentes del sistema:

1. Las transacciones encriptadas que mantienen el historial de cada moneda transada e impiden su falsificación.
2. El protocolo que valida y mantiene el registro cronológico de las transacciones y que evita el problema del doble pago o doble uso simultáneo de una misma moneda.
3. La red de comunicaciones peer-to-peer que guarda las copias de las transacciones y el registro anterior de forma descentralizada. (Bomneau, 2015)

La base para la creación de una criptomoneda se encuentra en su criptografía, y cómo esta aporta que una transacción se pueda realizar entre dos partes de forma anónima y sin necesidad de intermediarios. Un ejemplo sería que una persona A, envíe desde su billetera electrónica un archivo que contiene una llave privada encriptada con datos de una transacción a una dirección o llave pública conocida, contenida en la billetera electrónica de la computadora de una persona B, que recibe la transferencia.

La llave privada enviada por A es una cuerda de 34 caracteres (una serie alfanumérica que técnicamente se denomina hash). Esta se deriva de la dirección pública de la persona A, que también es un hash de 34 caracteres, y que crea constantemente combinaciones matemáticas encriptadas para generar la llave de la transacción efectuada. En el argot de la temática, la operación que A lleva a cabo para generar la llave que le envía a B se denomina “firmar” la moneda que se transfiere, de esta forma la persona B solo puede ver en su billetera la criptomoneda que A le envió porque recibió la llave privada que esta persona le envió, en otras palabras, la moneda con la firma de A en su billetera. De esta explicación es importante destacar que cada llave privada se deriva criptográficamente de la llave pública o dirección de quien la transfiere.

Ilustración 1: Criptografía asimétrica



Fuente: Elaboración propia a partir de (Bomneau, 2015)

Como plantea Roberts: "Uno puede considerar la llave pública como la ranura de alcancía en la que cualquiera puede depositar una criptomoneda, y la llave privada como la forma secreta de abrir la alcancía que solo conoce el dueño."

Esta mecánica se denomina sistema de transferencia bajo doble encriptación, y es distinta de que una persona debite divisa de una cuenta a otra, que es lo que habitualmente sucede con el dinero electrónico y es el esquema al que estamos acostumbrados y vemos en el día a día.

Contrario a lo que sucede con las transferencias mediante dinero electrónico, nadie puede evitar que se produzca estas transacciones llevadas a cabo por dos entidades o dos personas, aun cuando las direcciones públicas contenidas a sus respectivas billeteras son conocidas. Los pagos mediante la red de criptomonedas son irrechazables, y el envío irreversible, aunque el receptor podría hacer la transacción inversa, si ambas partes están de acuerdo y desean hacerlo. También existen "contratos inteligentes", si la operación se quiere hacer mediante ciertas condiciones.

El sistema de criptografía asimétrica (empleado como base del *blockchain*), garantiza la seguridad de una transacción mediante una norma sustantiva y una norma procesal. La norma sustantiva indica que sólo el primer uso de una moneda es válido y todos los demás deben ser descartados conforme lo verifique la mayoría de los miembros de la red de usuarios. Esto deja que el problema sea determinar cuál es realmente el primer uso, y aquí es donde entra en juego el papel de la norma procesal. Como nos encontramos en un escenario donde no existe un validador centralizado, y por tanto el tiempo absoluto no puede ser empleado como parámetro, se emplea un registro ordinal y encadenado, que nadie puede controlar, y que le va informando a la red el orden cronológico de las transacciones desde que estas se iniciaron. Este registro, en el caso del Bitcoin se conoce como "*Blockchain*" o "cadena de bloques", y su mecánica es esencial para entender por qué una red que tenga como base para las transacciones la criptografía puede funcionar sin intermediarios.

El tercer componente es la red de usuario a usuario (peer-to-peer), el cual garantiza el envío de llaves privadas, que se mantengan las llaves públicas, que se anuncien nuevas transacciones y proponen los nuevos bloques que se agregan a la cadena. En su mecanismo logra que mensajes de transferencias no sean alterados por un grupo con exceso de poder computacional, y permite que no existan interrupciones por entidades ajenas.

Las monedas derivan su utilidad de lo que se puede comprar con ellas, y su poder de compra se basa en la fe que tengan las personas que la reciben en poder volver a usarlas. El oro, una de las primeras monedas, dejó esa función hace más de un siglo, y no se usa como respaldo único de moneda hace más de 80 años. El oro dejó de ser unidad de cuenta y medio de cambio, que son dos de las funciones básicas del dinero, porque fue reemplazado por "mejores" y más "eficientes" monedas, y en los tiempos que corren, podemos categorizar a las criptomonedas como esas mondas eficientes.

RESULTADOS Y DISCUSIÓN

Para que un país haga uso de estos instrumentos tiene dos vías, o crea una criptomoneda, o decide usar las ya existentes en transferencias. En el caso de la primera vía, hay que aclarar que

todo creador de una criptomoneda se enfrenta a una cuestión al momento de fundarla: este puede retener el control de la oferta monetaria, o puede abandonar el control de la misma. En el caso de Cuba, como se propone usar estás herramientas como medida de pago y cobro, hay que tener en cuenta la oferta monetaria que tendría dicha criptodivisa, sin embargo, el objetivo del trabajo empírico no es crear una criptomoneda, sino evidenciar como resulta más eficiente la ejecución de una operación financiera a través de este método, el cual permite evadir las sanciones impuestas por el bloqueo y abre camino a una forma más ingeniosa de realizar cobros y pagos sin necesidad de un intermediario, lo cual es una ventaja a tener en cuenta.

Para ilustrar una transacción mediante criptomonedas se apoya en el siguiente ejemplo:

La comercializadora ITH S.A. de Cuba debe importar mercancía de una empresa B en otro país, donde el importe total de la operación equivale a 1 000 000.00 de dólares americanos. Manteniendo estos datos hipotéticos, por la vía convencional del dinero electrónico, a la hora de realizar el pago de esta operación, la empresa ITH a través de su banco gestiona la operación para enviar el dinero hacia la empresa B, sin embargo, por la ley Helms-Burton Cuba no tiene permitido realizar transacciones en dólares, por lo que si se pensaba pagar en esta moneda, Cuba se vería en la obligación de cambiar esos dólares por otra divisa libremente convertible, sea euro, franco suizo, etc., esto da lugar a un coste adicional por las variaciones del tipo de cambio, o por lo menos, a un riesgo que hay que tener en cuenta. Una vez obtenida la moneda para realizar el pago, se procede a realizar la transferencia, resaltando que el sistema de mensajería interbancario que utilizan la mayoría de los bancos del mundo para sus operaciones es el llamado SWIFT, y teniendo en cuenta que Estados Unidos es la primera potencia económica del mundo y su influencia en el SWIFT, a Cuba le resulta muy difícil realizar operaciones mediante este sistema, y muchas veces se recurren a terceos para sortear estas trabas, lo cual repercute en los costes por comisión y en los intereses a pagar, lo que conlleva a que se encarezca el monto de la operación, sumando la posible pérdida de los clientes o proveedores por las sanciones que aplica Estados Unidos a las empresas que realizan transacciones con Cuba.

En el caso del uso de las criptodivisas, la empresa ITH S.A. se ahorraría mucho trabajo, partiendo de que en la negociación previa con el proveedor se estableció de que el pago se iba a efectuar vía Bitcoin (este proceso se realiza en una app la cual se puede descargar o incluso se podría desarrollar una propia), el primer paso, suponiendo que la empresa ITH no posee Bitcoin, sería comprar en el mercado el equivalente de 1 000 000.00 dólares americanos en Bitcoin (la compra de esta criptomoneda se realiza de la misma forma que el pago que a continuación se expone), esto por supuesto obliga a estar analizando el precio internacional del bitcoin y realizar una gestión del riesgo cambiario, aspecto que no se va a abordar en esta investigación.

Como se expuso en páginas anteriores, para realizar una transacción de criptomonedas se necesitan dos cosas: una dirección y una clave privada. En primer lugar, la dirección es lo que se conoce como la llave pública, estas son las claves que dan acceso a los bitcoins, y se muestran mediante una secuencia de letras y números generados por matemática avanzada y aleatoria. Así la llave pública sigue un patrón determinado que empieza por el carácter “1” en cazo del Bitcoin. A su vez, la clave privada se genera a partir de una “semilla” única e irrepetible que la misma empresa establece o genera un software de forma automática. El hecho de que estas “semillas” sean únicas garantiza que no se puedan realizar ataques de fuerza bruta que puedan poner en peligro los fondos.

Siguiendo el ejemplo, cuando ITH le envía Bitcoins al proveedor (empresa B), utiliza su clave privada para firmar cada una de las entradas de la transacción y empleando las herramientas de la criptografía asimétrica de llave pública y privada, los nodos validan rápidamente la transacción y esta se cumple prácticamente al momento.

Utilizando estos métodos de pagos, la transferencia se realiza de forma más fácil, en un corto período de tiempo, sin intermediarios (directamente con el proveedor), no existen pagos por comisiones, ni se corre el riesgo de perder al cliente por sanciones impuestas, puesto que este está operando en una moneda que ningún país ni institución regula, y las operaciones se pueden llevar a cabo de forma anónima.

Teniendo en cuenta lo planteado anteriormente se contextualiza el uso de esta tecnología en distintas fronteras, en primer lugar, Japón, que posee la comunidad más amplia en el uso de criptomonedas, seguidamente de Corea del Sur y Reino Unido, donde este último considera a las criptomonedas como activo personal, y según datos del Banco de Inglaterra, gracias a la incorporación de transacciones con criptomonedas el país logró un aumento de 20 millones de libras esterlinas en su producto interno bruto. En esta lista se encuentra también Dinamarca, Australia, Sudáfrica, Estonia, Rusia, China, entre otros países. En la actualidad estos instrumentas se han consolidado, hasta tal punto que prácticamente en todos los países se utilizan de una u otra forma. Incluso empresas importantes han adoptado esta idea, entre estas se encuentra: Microsoft, Reddit, Shopify, Tesla, Badoo, Uber, IBM, Orange, BBVA, Banco Santander, Bank of America, Goldman Sachs, Royal Bank of Scotlan, VISA, MasterCard, entre otras. Y de ser necesario se puede negociar directamente con el proveedor o cliente para pactar un pago mediante una criptomoneda, esto es una práctica que muchas entidades han ido adoptando a lo largo de los últimos tres años.

Las finanzas en Cuba, en su sentido más amplio, siempre se van a ver afectadas por el bloqueo impuesto por los Estados Unidos, y por más de 60 años muchas transacciones financieras se han visto obstaculizadas y en algunos casos imposibles de realizar, este reto de lograr evitar las trabas del bloqueo se ha convertido en algo imperativo, y el surgimiento de las criptomonedas como un nuevo medio de pago y su constante desarrollo, puede ser la solución o por lo menos un paso hacia una mejora de la economía cubana.

CONCLUSIONES

El éxito alcanzado por las criptomonedas ha sido un acontecimiento de inigualable repercusión a nivel mundial, estableciendo una tendencia en los últimos tiempos donde las expectativas del riesgo hacia los medios de pago convencionales se multiplican en consecuencia a las frustradas políticas económicas de corte neoliberal que trajo consigo las mayores crisis económicas. Las criptodivisas se están convirtiendo en una alternativa más barata para el financiamiento y el ahorro de vendedores y consumidores de todo el mundo, posibilitando el desarrollo de transferencias seguras y un nuevo modelo de registro contable denominado cadena de bloques. Partiendo de los beneficios que trae el uso de las criptomonedas, parece justo destacar que pueden constituir un importante instrumento para mejorar la economía del país, contribuyendo también a la evasión del bloqueo económico, comercial y financiero.

REFERENCIAS BIBLIOGRÁFICAS

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., Felten, E. (2015). *SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies*. En 2015 IEEE Symposium on Security and Privacy. (104-121).http://doi.org/10.1109/SP.2015.14

Banco Central Europeo. (3 de 11 de 2020). Obtenido de Banco Central Europeo Web site: https://www.ecb.europa.eu/ecb/html/index.es.html

Castillo, A., & Brito, J. (2013). B*itcoin: A Primer for Policymakers*. Florida: Mercatus Center at George Mason University.

Halaburda, H. S. (2016). *Beyond Bitcoin The Economics of Digital Currencies*. New York: Journal of Economics & Management Strategy.

Nakamoto, S. (2009). *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario*.

Reuben, G. (2015). *Bitcoin: An innovative alternative digital currency*. Hastings Science & Technology Law Journa.

DATOS DE LOS AUTORES

ALEJANDRO GARCÍA FIGAL

Graduado de honor de la Universidad de La Habana. Licenciado en Contabilidad y Finanzas (2019), Profesor de la Universidad de la Habana con experiencia en docencia, investigaciones y administración financiera. Coordinador de la asignatura de Macroeconomía y Microeconomía, coordinador del programa BlockChain para las finanzas interbancarias. Tiene formación investiga en Chile. Ha impartido docencia, conducido investigaciones o desarrollados trabajos de consultoría en varias universidades y organizaciones de Cuba y Chile.

Fecha de recepción: 5 de diciembre de 2020
Fecha de aceptación: 30 de diciembre de 2020
Fecha de publicación: 30 de marzo de 2021