Quito, 16 de julio del 2014

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

Estimados Asambleístas,

Por este medio queremos solicitar audiencia en la comisión donde se discute el Código Orgánico Monetario y Financiero. Somos un grupo de ciudadanos interdisciplinarios en el área de economía, sistemas informáticos, electrónica y comerciantes interesados en el respeto a la privacidad de los ciudadanos y en la adopción de sistemas monetarios alternativos como las criptomonedas descentralizadas.

Respecto de la Privacidad
El derecho a la intimidad y a la privacidad es un derecho universalmente establecido, también presente en el Pacto de San José del cual Ecuador es parte y está bellamente reconocido en nuestra Constitución:

> *Derechos de Libertad*
> *Art.66 Se reconoce y garantizará a las personas:*
> *20."El derecho a la intimidad personal y familiar."*
> *21 "El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual [...] Este derecho protege cualquier otro tipo o forma de comunicación."*

El Proyecto de Código Orgánico Monetario y Financiero plantea la creación de una nueva moneda electrónica centralizada, que operará a la par par del dólar físico, así lo determinan los siguientes artículos:

> *Art.14. Funciones: La Junta tiene las siguientes Funciones:*
> *19. "Establecer Medios de Pago",*
> *21. "Regular la gestión de moneda electrónica [...] de acuerdo con lo dispuesto en este código.",*
> *38. "Establecer unidades de cuenta".*
>
> *Art.36. Funciones: El Banco Central del Ecuador tiene las siguientes funciones:*
> *20. "Proveer de forma exclusiva moneda metálica nacional, así como moneda electrónica, en el marco de la política dictada por la Junta de Política y Regulación Monetaria y Financiera;"*

> *Art.92. "... El Banco Central del Ecuador es la única entidad autorizada para proveer y gestionar moneda metálica nacional o electrónica en la República del Ecuador, [...] de acuerdo a las disposiciones de este código [...]". "La moneda determinada en este artículo es medio de pago."*

La creación de una nueva moneda electrónica trae incuestionables beneficios técnicos, como la reducción de costos para el sistema y practicidad para el usuario; pero también existe el riesgo de violar la privacidad de los ciudadanos debido a una inadecuada implementación técnica.

El dinero es uno de los instrumentos más íntimos que tenemos, la actividad cotidiana incluye actividades de compra y venta, al pagar un bus, al adquirir víveres, bienes o servicios, etc. Dependiendo del algoritmo de implementación, la moneda electrónica podría invadir la privacidad de los ciudadanos, ya que a partir de las transacciones digitales se puede realizar la asociación entre identidad, lugar, monto, establecimiento y tiempo de la transacción. La inadecuada implementación del sistema podría derivar en la creación de un instrumento con la capacidad de rastrear la actividad de sus usuarios e incluso la ubicación de los mismos.

La moneda física debido a su propia naturaleza no tiene la capacidad de revelar información de sus usuarios, y aunque el Art.92 del proyecto de ley determina que: *"En ningún caso el Estado podrá obligar a una persona natural o jurídica de derecho privado a recibir moneda distinta del dólar de lo Estados Unidos de América."* La capacidad de acceso del ciudadano al circulante físico podría verse limitada por los siguientes artículos del mismo proyecto:

> *Art.92. "...el canje... de dólares de los Estados Unidos de América,... corresponden exclusivamente al Banco Central del Ecuador... de acuerdo con las disposiciones de este código y con la regulación que emita la Junta de Política y Regulación Monetaria y Financiera."*

> *Art.95. "El canje de la moneda... será realizada por el Banco Central del Ecuador, al portador y a la vista, sin cargo de ninguna naturaleza. Las entidades del Sistema Financiero Nacional estarán obligadas a prestar los servicios de canje de moneda de conformidad con los términos que disponga la Junta Política y Regulación Monetaria y Financiera, con las excepciones que se determinen."*

Estos artículos podrían crear los antecedentes necesarios para que el acceso a la moneda física sea limitado y que la moneda electrónica se propague con mayor facilidad. La moneda electrónica, debido a su naturaleza digital y centralizada, es completamente programable y el sistema puede ser fácilmente modificado teniendo como límite el marco legal vigente, un sistema de moneda electrónica incorrectamente implementado puede ser utilizado como un medio de vigilancia masiva.

La implementación de la moneda electrónica debería considerar las ventajas de privacidad que el medio físico tiene para el usuario, e incorporarlas a los algoritmos del sistema de moneda electrónica. Conocemos que esto es técnicamente factible puesto que existen protocolos como

Bitcoin, que haciendo uso de algoritmos criptográficos permiten la independencia de los datos personales del usuario y de lugar, de los datos propios de la transacción. Es posible incluso mantener la trazabilidad de la moneda, sin asociar los datos personales de los ciudadanos. Existen alternativas tecnológicas, sólo hace falta la voluntad política.

Respecto de las Criptomonedas Descentralizadas

A finales del año 2008 se publicó un paper titulado “Bitcoin: Un Sistema de Dinero Electrónico Par a Par”. Este documento describe el funcionamiento de una moneda electrónica que funciona en Internet sin la necesidad de un agente central de coordinación. La publicación dió origen a las criptomonedas descentralizadas, es decir monedas digitales implementadas sobre algoritmos criptográficos que trabajan sobre la red sin la necesidad de tener un núcleo rector centralizado, sino que entrega las funciones de control y coordinación a algoritmos matemáticos que operan de forma distribuida entre los nodos de la red.

La red/protocolo Bitcoin fue concebida originalmente como una criptomoneda digital descentralizada, pero su diseño planteó una elegante solución al problema de los Generales Bizantinos, un problemas de los sistemas de computación distribuida que se creía sin una solución escalable.

Esta solución, permite que la red/protocolo pueda ser utilizada en aplicaciones de distinta índole como sistemas de DNS descentralizados, notarización descentralizada, contratos inteligentes, propiedad inteligente y varias aplicaciones tecnológicas aún en proceso de desarrollo.

No se conoce cuál será el futuro de la red/protocolo Bitcoin, de la misma manera en la que no se conocía cuál sería el futuro de Internet en 1990, sin embargo su tecnología promete mucho, y una tecnología que ha sido inventada, no puede desinventarse.

Bitcoin es software libre, su distribución es gratuita y el código fuente es abierto, por lo que cualquier persona puede acceder a esta tecnología, y si posee los conocimientos necesarios puede participar directamente en el desarrollo de la misma. En ese sentido, Bitcoin es corde con el decreto ejecutivo 1014 del 2008 que establece al Software Libre como Política de Estado.

Las criptomonedas pueden abarcar el concepto económico de moneda tradicional, pero a nivel de desarrollo los servicios también son considerados como un tipo de moneda.

Bitcoin es una tecnología innovadora e incluso con más trascendencia que los drones, cuadricópteros, impresión 3D, automoviles autoconducidos, etc. Por ello consideramos que la tecnología merece ser estudiada e investigada desde el punto de vista académico y que se debe permitir el desarrollo de un ecosistema de criptomonedas en el Ecuador. Por citar un ejemplo, el Instituto Tecnológico de Masachusets ha permitido el desarrollo de un ecosistema Bitcoin al interior de su campus con el objetivo de impulsar la investigación y actividades de emprendimiento en torno a esta tecnología por parte de sus alumnos. En ese sentido,

proyectos como Yachay, que buscan impulsar el desarrollo tecnológico y el cambio de la Matriz Productiva pueden ser espacios en donde el protocolo Bitcoin y las criptomonedas puedan ser investigadas y desarrolladas formalmente.

Además, existen antecedentes de grandes empresas como Overstock, Dish y Expedia, etc. Que han logrado aumentar su nivel de ventas incorporando a Bitcoin como un medio de pago. En ese sentido el Ecuador podría ser pionero en permitir que Bitcoin sea un medio de pago.

Ecuador es la mayor economía dolarizada, por lo que actualmente depende de una autoridad extranjera para el manejo de su política monetaria; permitir el uso de criptomonedas descentralizadas no supone menoscabo alguno de su soberanía o del manejo de la economía, sino que podría situar al Ecuador en la vanguardia de las políticas monetarias a nivel mundial.

Bitcoin es la criptomoneda más desarrollada del mundo. Pero además, es toda una tecnología disruptiva que permite la creación de una nueva manera de relacionarse económicamente de manera descentralizada y entre iguales (Par a Par).

Esta tecnología puede verse limitada con el planteamiento actual del proyecto de Código Orgánico Monetario y Financiero. Bitcoin es una tecnología emergente y disruptiva por naturaleza; que ha demostrado estar en la capacidad de tolerar ataques de distinto tipo a su protocolo y funcionamiento, sin embargo ha logrado mantenerse, seguir de pie y continuar su expansión alrededor del mundo, en donde cada día es más notoria su presencia.

El proyecto de Código Orgánico Monetario y Financiero, tal como se encuentra planteado puede impedir el desarrollo de un ecosistema y de emprendimientos en torno a Bitcoin, una tecnología emergente de carácter mundial.

PROPUESTA

Respecto de la Privacidad

Se tomen en cuenta las observaciones hechas y se incorpore al Nuevo Código Orgánico Monetario y Financiero un artículo que a nivel de algoritmo ordene separar los datos personales y de lugar, de los datos del sistema de transacciones de la moneda electrónica. Para ello proponemos la incorporación de un artículo en el nuevo Código Orgánico Monetario y Financiero que indique:

> *Art. "Se mantendrá la privacidad de los usuarios de la moneda electrónica bajo los principios de inviolabilidad y secreto establecidos a tal efecto en la Constitución del Ecuador. Además se incorporarán al sistema de moneda electrónica y a su algoritmo de implementación todas las seguridades técnicas necesarias que reflejen el estado actual de la técnica, con el objetivo de limitar la asociación entre los datos personales de los usuarios, el lugar y la información propia de la transacción. Su implementación será de código abierto."*

Consideramos que es una cuestión de tiempo para que la moneda electrónica sea la norma monetaria y que debido a su practicidad sea de uso masivo. El Ecuador se ha caracterizado por defender los derechos humanos y los principios de libertad, y al ser pionero en crear una moneda electrónica de origen estatal, es necesario que lo haga de una forma técnica que respete derechos fundamentales.

Así como se debe garantizar la privacidad de los ciudadanos, también se debe garantizar la transparencia del Estado. El sistema de dinero electrónico debe ser auditable y su código fuente debe ser publicado como software libre. Con el fin de asegurar la privacidad del sistema por diseño del algoritmo, más que por política de funcionamiento. El decreto ejecutivo 1014 del 2008 donde establece al software libre como una política de Estado.

"La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secretismo. Una cuestión privada es algo que no queremos que todo el mundo sepa, pero una cuestión secreta es algo que no queremos que nadie sepa. La privacidad es la capacidad de revelarse selectivamente al mundo." Eric Hughes, 1993

Respecto de las Criptomonedas Descentralizadas
Para permitir el desarrollo de un ecosistema de criptomonedas descentralizadas, proponemos los siguientes cambios al Proyecto de Código Monetario y Financiero,

- En el Art. 92 incorporar la palabra nacional tras la palabra electrónica así quedaría el artículo redactado de la siguiente manera:

  > Art. 92 El Banco Central del Ecuador es la única entidad autorizada para proveer y *gestionar moneda metálica nacional o electrónica nacional* en la República del Ecuador, equivalente y convertible a dólares de los Estados Unidos de América, de acuerdo con las disposiciones de este Código y con la regulación y autorización de la Junta de Política y Regulación Monetaria y Financiera.

- Excluir a las criptomonedas descentralizadas de las prohibiciones del Art. 96.

- En el Art. 98, incluir a las criptomonedas descentralizadas como un medio de pago de carácter voluntario.

- En el Art. 14, numeral 21 incorporar la palabra nacional delante de la palabra electrónica de la siguiente manera:

  > 21. Regular la gestión de moneda electrónica *nacional* y disponer al Banco Central del Ecuador su implementación, monitoreo y evaluación, así como de la moneda nacional metálica, de acuerdo con lo dispuesto en este Código,

Esperamos esta carta tenga acogida en el seno de la Asamblea Nacional, confiamos en la voluntad política de nuestros representantes para escuchar estas propuestas y nos ponemos a su disposición con el fin de despejar cualquier duda que pudieran tener.

Atentamente,

Bitcoin Comunidad Ecuador