

Eco. Rafael Correa Delgado  
**PRESIDENTE DE LA REPÚBLICA DEL ECUADOR**  
En su Despacho.-

De nuestra consideración:

La Comunidad Bitcoin Ecuador nace a finales del año 2013 como un grupo de ciudadanos interdisciplinarios, interesados en la adopción de métodos alternativos como las criptomonedas descentralizadas.

El principal objetivo de la Comunidad es investigar y dar a conocer, en nuestro país, las bondades tecnológicas de Bitcoin; un protocolo que ha logrado despertar inusitado interés mundial debido a su particular aplicación como moneda; contando además con características únicas que permiten que a su alrededor se desarrollen nuevos servicios con variadas aplicaciones tales como: almacenamiento descentralizado de información, servicios notariales, contratos inteligentes, etc.

El escenario de creación de una moneda electrónica ecuatoriana planteado a través del proyecto de Código Orgánico Monetario y Financiero, ha despertado evidente interés en nuestra comunidad debido a que guardamos estrecha relación con el tema; razón por la cual hemos planteado inquietudes respecto de la privacidad del sistema de moneda electrónica así como el estatus legal de Bitcoin y sus tecnologías derivadas en el Ecuador.

#### **ANTECEDENTES**

El "Proyecto de Código Orgánico Monetario y Financiero", propone la creación de una nueva moneda electrónica centralizada que operaría a la par con el dólar físico según lo determinan los siguientes artículos:

*Artículo 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."*
- 39. "Establecer unidades de cuenta".*

*Artículo 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;"*

*Artículo 94. "...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 moneda tiene poder liberatorio y curso legal en la República del Ecuador en el marco de las regulaciones que emita la Junta de Política y Regulación Monetaria y Financiera."*

Queda claro que se emitirá una nueva moneda de carácter electrónico, que será regulada por la Junta de Política Monetaria y Financiera, y gestionada por el Banco Central del Ecuador.

La creación de una moneda electrónica trae incuestionables beneficios tales como la reducción de costos para el sistema y de practicidad para el usuario; pero también plantea interrogantes respecto de la privacidad de los ciudadanos que usarán dicha moneda electrónica y también en lo referente al estatus legal para las personas que han adoptado el uso de Bitcoin en el Ecuador.

## **OBSERVACIONES**

### **1. Sobre el respeto de la privacidad**

La intimidad es un derecho humano universalmente reconocido por múltiples tratados y convenciones, varios de ellos ratificados oficialmente por nuestro país y recogidos en la Constitución de la siguiente manera:

Derechos de Libertad

*Artículo 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 dinero es uno de los instrumentos más íntimos que tenemos. La vida cotidiana incluye actividades de compra – venta de bienes y servicios en hechos tan sencillos como viajar en bus o adquirir alimentos. La moneda electrónica vendría a facilitar la experiencia o relación entre comerciante y consumidor; sin embargo, una implementación inadecuada del sistema podría derivar en la creación de un instrumento con la capacidad de rastreo de las actividades económicas de sus usuarios, pudiendo incluso determinar la ubicación de los mismos. 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 moneda física, debido a su propia naturaleza no tiene la capacidad de revelar información de sus usuarios; empero, la moneda electrónica debido a su naturaleza digital y centralizada es completamente programable, el sistema puede ser fácilmente modificado teniendo como límite exclusivo el marco legal vigente. Un sistema de moneda electrónica que no tome en cuenta estas observaciones podría ser utilizado como un medio de vigilancia masivo.

Adicionalmente, aunque el artículo 92 del proyecto “Código Orgánico Monetario y Financiero” 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 los Estados Unidos de América”*; la capacidad de acceso al circulante físico que tiene el ciudadano podría verse limitada por los siguientes artículos de dicho proyecto:

*Art.94. “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.97. “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 un escenario en el cual la capacidad de acceso del ciudadano al circulante físico pudiera verse limitado y que debido a la practicidad de la moneda electrónica, esta se propague con mayor facilidad y que por lo tanto se vuelva de uso masivo.

Por ello, la implementación de la moneda electrónica debería considerar las ventajas de privacidad que ofrece el medio físico, e incorporarlas a los algoritmos que estructuran este sistema. Esto es técnicamente factible debido a que existen algoritmos criptográficos que permiten mantener cierta independencia entre los datos personales del ciudadano y los datos propios de la transacción, pudiendo mantener incluso la trazabilidad de la moneda, es decir mantener el historial de transacciones monetarias sin la necesidad de asociar los datos personales de los ciudadanos. Prueba de ello es el protocolo Bitcoin, en donde las transacciones guardan independencia de los datos de identidad de los usuarios.

## **2. Sobre el uso de Criptomonedas Descentralizadas**

A finales del año 2008 se publicó un documento titulado “Bitcoin: Un Sistema de Dinero Electrónico Par a Par”; el mismo describe el funcionamiento de una moneda electrónica que actúa en Internet sin la necesidad de un agente central de coordinación. La publicación dio 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. Esto permite que el protocolo pueda ser utilizado en aplicaciones de distinta índole como sistemas de DNS descentralizados, notaría descentralizada, contratos inteligentes, propiedad inteligente y varias aplicaciones tecnológicas aún en proceso de desarrollo.

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 acorde con el decreto ejecutivo 1014 del 2008 que establece al Software Libre como Política de Estado.

Por su concepción, utilidad y probadas posibilidades consideramos que el protocolo Bitcoin merece ser estudiado e investigado desde el punto de vista académico y que debería permitirse el desarrollo de un escenario adecuado hacia las criptomonedas en el Ecuador. Por ejemplo, el Instituto Tecnológico de Massachusetts (MIT) ha permitido el desarrollo de un ambiente viable hacia Bitcoin en el 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.

Siguiendo con esta línea, proyectos como Yachay, que buscan impulsar el desarrollo tecnológico y el cambio de la Matriz Productiva podrían ser espacios en donde las criptomonedas se investiguen y desarrollen formalmente. Esta tecnología disruptiva permite la creación de una nueva manera de relacionarse económicamente, de manera descentralizada y entre iguales (Par a Par), acorde con los preceptos y directrices de desarrollo de las políticas de economía popular y solidaria delineadas en el Plan Nacional del Buen Vivir.

## **PROPUESTA DE LA COMUNIDAD BITCOIN ECUADOR**

### **1. Sobre el respeto a la privacidad**

Solicitamos se incluya en el 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,

*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. Se deberán implementar todas las seguridades necesarias que reflejen el estado actual de la técnica, con el objetivo de, a nivel de algoritmo, limitar la asociación entre los datos personales de los usuarios, el lugar y la información propia de la transacción. Su código de implementación será auditable y de código abierto."*

Consideramos es una cuestión de tiempo para que la moneda electrónica sea la norma monetaria cotidiana y debido a su practicidad sea de uso masivo. El Ecuador, al ser pionero en creación de una moneda electrónica de origen estatal, debe utilizar una metodología que respete los derechos humanos fundamentales. 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.

"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

### **2. Sobre las Criptomonedas Descentralizadas**

Para evitar poner en riesgo de ilegalidad a Bitcoin en el Ecuador y permitir el desarrollo de emprendimientos en torno a las criptomonedas descentralizadas, proponemos,

- Incorporar la palabra “nacional” a continuación de la palabra “electrónica”, redactándose el artículo 94 de la siguiente manera:

Art. 94 “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 artículo 98.
- Incluir al artículo 99 las criptomonedas descentralizadas como un medio de pago de carácter voluntario.
- Añadir la palabra “nacional” a continuación de la palabra “electrónica” al numeral 21 del artículo 14, de la siguiente manera:

Art. 14 (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,”

Con estos antecedentes, solicitamos Sr. Presidente se considere el análisis de las propuestas presentadas, y en caso de ser necesario se nos conceda una audiencia formal a fin de aclarar inquietudes o cuestionamientos que pudieren presentarse al respecto. La respuesta a este petitorio la recibiremos en el correo [comunidad@bitcoinecuador.org](mailto:comunidad@bitcoinecuador.org) y en el sistema de gestión documental Quipux.

Esperando poder aportar hacia la mejora del actual proyecto de Ley, agradecemos de antemano su atención.

Atentamente,

Comunidad Bitcoin Ecuador  
[www.bitcoinecuador.org](http://www.bitcoinecuador.org)  
[comunidad@bitcoinecuador.org](mailto:comunidad@bitcoinecuador.org)