

# Criptomonedas, y marcas de código abierto

## v-1.1

Prodezzargenta

21 de junio de 2022

### Resumen

Propuesta de un emprendimiento con un modelo de negocio *alternativo*, con el fin de crear mercados paralelos, al fabricar bienes valuados en criptomonedas, e independizarse del sistema *fiat*.

## Índice

<b>1. Introducción</b>	<b>2</b>
1.1. Situación actual . . . . .	4
1.2. Acerca de la legalidad . . . . .	5
<b>2. Emprendimiento</b>	<b>8</b>
<b>3. Marca de código abierto</b>	<b>9</b>
3.1. Ventajas . . . . .	10
3.1.1. Transparencia de los procesos de trabajo . . . . .	10
3.1.2. Escrutinio público de la marca . . . . .	11
3.1.3. Salto del control estatal . . . . .	13
3.2. Desventajas . . . . .	14
3.2.1. Falsificación . . . . .	15
3.2.2. Incentivo económico . . . . .	18
<b>4. Comprobación</b>	<b>23</b>
4.1. Procedimiento . . . . .	25
<b>5. Ramificaciones</b>	<b>25</b>

<b>6. Liquidez</b>	<b>27</b>
6.1. Local . . . . .	27
6.2. Mundial . . . . .	28
<b>7. Diagrama de flujo</b>	<b>30</b>
<b>Referencias</b>	<b>31</b>

## 1. Introducción

La creación de las criptomonedas ha representado, en mayor o menor medida, una ruptura en la concepción de la economía. Desde la creación del Estado, las economías han sido progresivamente administradas por estas entidades; y a lo largo de la historia, se evidencia cómo los Estados han ido legitimizando el monopolio del dinero.

De acuerdo con lo expuesto en su artículo *El origen del dinero*, Carl Menger detalla:

Suponer que ciertas mercancías habían sido promovidas como medio de cambio por una convención o ley general solucionó la dificultad, y lo hizo aparentemente con gran facilidad y naturalidad, porque la forma de las monedas pareció ser un signo de regulación por parte del Estado. Ésta es la opinión de Platón, Aristóteles y los juristas romanos, seguidos muy de cerca por los escritores medievales. (Menger, 1892, págs. 240-241)

Dar por sentado que el dinero *es y sólo es* una creación estatal, como medio de cambio para diferentes bienes y servicios, es absurdo. La experiencia económica sobre el intercambio directo (trueque) y su evolución al intercambio indirecto (dinero) data desde que el ser humano descubre que los metales como el cobre, bronce, plata, y el oro, pueden atesorarse y sobrevivir al paso del tiempo. Es más, como explica Ludwig von Mises en su libro *La Acción Humana*:

Algunos autores han intentado explicar el origen del dinero por decreto o convención. Una decisión del gobernante o un acuerdo entre los ciudadanos, de modo deliberado y consciente, habría implantado el cambio indirecto y creado el dinero. El principal fallo de esta doctrina no radica en la suposición de que [...] desconocían el cambio indirecto y el dinero pudieran llegar a proyectar

un nuevo orden económico totalmente distinto de las condiciones reales de su propia época y comprendieran la importancia de semejante plan.

Si admitimos que los interesados mejoran sus respectivas posiciones, a medida que van sustituyendo el cambio directo por el indirecto, [...] no hay porqué recurrir [...] a una imposición autoritaria o a un expreso pacto entre ciudadanos.

[...] Ante este hecho, es innecesario apelar a interferencias gubernamentales ni a convenciones entre los ciudadanos para explicar la aparición del cambio indirecto. [...] Resulta mucho más plausible suponer que esas inmediatas ventajas del cambio indirecto fueron percibidas por los propios interesados, que imaginar que hubo un ser genial capaz de organizar mentalmente toda una sociedad traficando con dinero y [...] de explicarla luego convincentemente al resto de la población. (von Mises, 2011, pág. 488)

En resumen, el dinero es una creación de la misma interacción entre seres humanos a lo largo de la historia, en donde descubren que existen mayores ventajas al *trueque* (o intercambio directo) para poder comerciar.

El Estado, en este contexto, toma posesión de la administración del dinero y, luego, de su acuñación. Esta situación, sumado al monopolio *legitimado* de la violencia sobre un territorio, conduce a una situación en donde los incentivos no son favorables para el libre comercio. Es decir, por un lado, es el Estado la *única* entidad, legitimada por sí misma, para administrar la creación de dinero; y, por otro lado, es la entidad que ejerce la violencia sobre el territorio.

Así, a lo largo de los milenios, los Estados han incrementado su poder de forma *violenta*<sup>1</sup>, de forma directa (a través de las fuerzas armadas) e indirecta (a través del dinero). Mediante la aplicación de *impuestos*<sup>2</sup>, esta entidad ha podido sobrevivir al paso del tiempo; y quién no paga los impuestos en tiempo y forma, será sancionado de alguna forma.

En los últimos siglos, cuando los Estados comenzaron a administrar la educación sobre el territorio, el contenido teórico ha sido reformado para justificar su propia existencia, financiando, entre otras cosas, teorías que avalan su accionar violento. Es así como, por ejemplo, en países como Argentina

---

<sup>1</sup>En el momento de escribir este artículo, existe actualmente el desarrollo de la invasión de Rusia a Ucrania, por razones tales que han variado significativamente a lo largo de los meses. Y esta invasión supone, también, una ocupación del territorio ucraniano para ser anexado a Rusia.

<sup>2</sup>La palabra en español delata fácilmente su naturaleza violenta, a diferencia del inglés, que se traduce como *tax*.

todavía se enseña que los desequilibrios macroeconómicos y la depreciación de la moneda local (por nombrar algunos de los problemas actuales) se deben pura y exclusivamente al sector privado y no a las políticas económicas creadas por el mismo Estado. No solamente eso, sino que también se enseña esta idea fundamental en *todos* los órdenes educativos (desde jardín de infantes, hasta las universidades), negando cualquier refutación empírica ya comprobada. Esto demuestra que el incentivo *principal* del Estado es incrementar su poder; y para realizarlo, deberá ejercer, progresivamente, más violencia contra las personas.

Desde el lanzamiento de Bitcoin por Satoshi Nakamoto en el 2009, a pesar de los «altibajos» técnicos que ha tenido, la naturaleza de su *código abierto* ha demostrado ser una implementación exitosa para que personas a lo largo del mundo, de forma voluntaria, contribuyan a re-escribir el código, mejorando el protocolo original; o creando nuevas criptomonedas basadas en el mismo principio. Y dado que utilizan sistemas criptográficos y protocolos de seguridad, las criptomonedas (como su nombre lo indica) han podido establecerse como candidatos a ser medios de intercambio de bienes y servicios *por fuera* del control Estatal. Es más, actualmente existen unas pocas monedas estatales con la tecnología *blockchain*, con el fin de reemplazar el dinero *fiat* actual en una «divisa 2.0».

## 1.1. Situación actual

A pesar de la creación de múltiples criptomonedas, donde actualmente existen registradas 717 criptomonedas (Mining Pool Stats, 2022), existe una tendencia *general* a concebir las criptomonedas como un simple activo financiero para ganar más dinero *fiat*. Esto implica que las criptomonedas no se consideran como un medios de intercambio de bienes y servicios *por fuera* del control Estatal; sino más bien un mero activo financiero para comprar «a un precio bajo» y vender «a un precio alto», en base a criterios completamente arbitrarios y subjetivos, o en base a algún tipo de análisis técnico de su precio.

Este cambio de concepción puede justificarse por las múltiples publicidades en los diferentes medios de comunicación y redes sociales, en base al historial de navegación, interacción de sitios de internet, etcétera; las recomendaciones de *youtubers* especializados en finanzas (aunque también los que *no* se especializan en dicha disciplina); o las noticias acerca de diferentes personas que «se volvieron millonarios» o «han perdido todo su dinero». No obstante, no hay que ignorar el hecho que no hay escrito suficiente teoría económica acerca de las criptomonedas para ofrecer una lectura más detenida del fenómeno, como también hay un impulso emocional de introducirse

en el mundo de las criptomonedas para ganar más dinero local (o dólares, euros, etcétera) de forma rápida.

Más allá de las múltiples interpretaciones que podrían escribirse sobre esto (desde la ignorancia de los usuarios, hasta aquellas teorías (hasta ahora) conspirativas acerca del incentivo por parte del Estado a que los usuarios pierdan su dinero, para que luego el mismo Estado ofrezca «seguridad financiera» a cambio de la reducción de las libertades individuales), lo cierto es que existe una concepción *errada* de las criptomonedas. Los desarrolladores tampoco están exentos de este problema. En Monero, por ejemplo, los proyectos de desarrollo más importantes son *exchanges* descentralizados (aunque existe cierta controversia aún en discusión acerca de los protocolos internos). Podría justificarse que esto permitiría liquidez en el mercado; pero ya existen alternativas descentralizadas para cambiar el dinero *fiat* por Monero.

El punto de esta última declaración refiere al punto central de este documento: dejar de concebir las criptomonedas como un mero activo financiero para adquirirlo cuando la tasa de cambio a dinero *fiat* es bajo, y vender parcial o totalmente la cantidad de criptomonedas adquiridas cuando es alto (y así ganar más dinero *fiat*). Así, la acción humana tenderá a ver las criptomonedas como un medio de intercambio por fuera de las regulaciones y el control estatal, y producir bienes y servicios bajo un mercado *paralelo*.

## 1.2. Acerca de la legalidad

Esto podría ser un tema controvertido para discutir sobre la naturaleza de las criptomonedas. Sin entrar en detalle sobre el tema, dado los incentivos en el mercado, el criterio *general* acerca de las criptomonedas es el siguiente: cualquier denominación de criptomoneda que sea «aceptada» por los Estados implica que estas entidades ya pueden controlar de forma indirecta el poder adquisitivo de las personas (ya sea de forma parcial o total).

Los *exchanges* que tienen personería jurídica en los países son controlados por los Estados. Esto quiere decir que deben informar acerca de su situación patrimonial y la de sus clientes. Por ejemplo, en el caso de Bitcoin, a pesar que las transacciones registradas en la *blockchain* son pseudo-anónimas (es decir, no aparecen los datos legales de la persona como el nombre y el apellido), dadas ciertas condiciones, se puede conseguir tales datos. El modelo de negocio de los *exchanges* es el siguiente: es una entidad financiera, un tercero, que atrae a nuevos clientes en utilizar su plataforma; y son estas entidades las que proveen de una cuenta privada para ofrecer liquidez y facilidad de intercambio entre diferentes criptomonedas y dinero *fiat* (a cambio,

por supuesto, de una comisión por utilizar sus servicios)<sup>3</sup>. Así, estos negocios se encargarán de atesorar diferentes criptomonedas para que los usuarios puedan intercambiarlos rápidamente. Sin embargo, para que los usuarios comiencen a operar, es requisito por los *exchanges* que se les suministren sus datos legales. Binance, el *exchange* internacional más reconocido en el mundo de las criptomonedas, requiere de los siguientes datos para poder utilizar sus servicios sin ninguna restricción:

- País de residencia, y nacionalidad.
- Nombre y apellido, y fecha de nacimiento.
- Dirección, ciudad y código postal.
- Imagen escaneada del anverso y reverso del documento nacional, pasaporte o licencia de conducir.
- Imagen frontal de la persona para reconocimiento facial.
- Verificación de los datos suministrados (varios días luego de la primera carga de datos).
- Imagen escaneada de cualquier servicio que compruebe el lugar de residencia.

Quitando de lado el peor de los casos donde la base de datos del *exchange* es robada y publicada libremente en internet, si los *exchanges* son personas jurídicas que están reguladas por el Estado, ¿qué le impide al Estado obtener dichos datos, dada una situación arbitraria? Si la consecuencia de no acatar las órdenes estatales es la de su cierre operativo (o su juicio) en donde se pone en riesgo su propio capital, el *exchange*, claramente, se verá más beneficiado en proporcionar los datos legales de las personas. Es por ello a lo que se refiere como «*exchanges* centralizados».

Expuesto ya este paradigma sobre los incentivos en el mercado, ¿por qué hay criptomonedas «aceptadas» y otras «criminalizadas»? En el caso de Bitcoin, éste ha sido adoptado como dinero de curso legal en El Salvador y en la República Centroafricana. Monero, por citar un contra-ejemplo, suele asociarse a noticias relacionadas con ciberataques (*hacking*, *ransomwares*, etcétera) o rodeado de algún tipo de controversia sobre alguna actividad ilícita. Por citar una noticia del portal Cointelegraph:

---

<sup>3</sup>De lo contrario, las personas deberán encontrar físicamente a otras personas que esté dispuesta a realizar dicha transacción.

Cointelegraph reportó previamente que las monedas privadas han estado surgiendo últimamente, ya que parece que los fondos familiares y los inversores individuales tienen cada vez más XMR como cobertura en medio de las recientes turbulencias del mercado. El tópico de las monedas privadas han sido controversiales entre la comunidad *crypto*. Algunos señalan de su habilidad para asegurar un mayor anonimato durante las transacciones, mientras que otros levantan preocupaciones acerca del uso de XMR para escudarse de transacciones ilícitas y su alegada aceptación por parte de grupos extremistas. El año pasado, Kraken sacó de su lista a XMR por sus clientes ingleses, citando presiones de regulación [estatal]. (Sun, 2022)

Más allá de la obvia aclaración que un bien no posee ningún tipo de moralidad<sup>4</sup>, la criminalización de Monero puede deberse a la imposibilidad actual de rastrear las transacciones en la *blockchain*; y dado sus protocolos internos de seguridad para evitar cualquier tipo de ataque es lo que, a diferencia de Bitcoin, hace que los Estados los prohíba (no puede ser controlado directa ni indirectamente).

Para responder a la cuestión central de esta sección: la legalidad no implica moralidad. En las discusiones académicas *acerca de la ética* (*precisamente, sobre el imperativo categórico* expuesto por Immanuel Kant) y la legalidad, se suele citar el caso de un individuo arbitrario que ayuda a refugiar a una persona judía en la Alemania Nacional-Socialista de los años 40. Ayudar a una persona, sea de la religión que sea, es un acto moralmente «bueno», pero en este caso va en contra de las leyes y del deber que tiene el individuo. No obstante, entregar a la persona a las autoridades, es un acto moralmente «malo» (la persona será torturada, desaparecida, fusilada, etcétera), aunque implica el respeto por las leyes y del deber que tiene el individuo. Por más banal que sea este ejemplo, este es un contra-ejemplo que el cumplimiento de las leyes y los actos moralmente buenos no son compatibles.

En conclusión: al usuario no debería importarle si su acción es *legal* o *ilegal*; sino si es moralmente *bueno* o *malo*. Esta distinción se podrá hacer en la medida que no afecte la vida y/o la propiedad privada de un tercero. Sin ir más lejos, el Estado funciona a través de la violencia (un acto moralmente *malo*) mediante las restricciones de la libertad individual, sea tanto en su plano económico (impuestos, regulaciones, depreciación de la moneda oficial) como en la libertad misma (entiéndase esto como, por ejemplo, las

---

<sup>4</sup>En este caso, Monero no es «inmoral» porque lo utilizan los criminales. La inmoralidad reside en la acción de los individuos que atentan contra la vida y/o la propiedad privada de otros. El bien *per se* no tiene ninguna moralidad intrínseca.

restricciones arbitrarias impuestas durante la pandemia del COVID); incluso atentando expresamente contra la vida de las personas (la actual invasión de Rusia a Ucrania, por ejemplo).

## 2. Emprendimiento

Crear un emprendimiento es un proceso complejo. Esto comienza desde la idea inicial de lo que se quiere ofrecer, pasando por la imagen de la nueva empresa, hasta su publicidad. En cuanto al proceso de fabricación o servicio, se debe considerar la materia prima y los insumos disponibles para su ejecución, es decir, el capital inicial para emprender (incluyendo el material y el intelectual). Y en cuanto a su aplicación, se debe pensar, con dicho capital inicial, en los procesos de fabricación o de servicios para lograr así una *estandarización* de los procesos de trabajo.

En el marco *legal*, es difícil establecer parámetros «equitativos» para cada persona que vive alrededor del mundo, porque los requerimientos legales son diferentes para cada uno de ellos. Algunos países son más flexibles para emprender; y otros requieren de un largo proceso burocrático y tedioso<sup>5</sup>, en el que involucra un gran gasto de dinero para su validación (hasta, incluso, en actos de corrupción). Dado el *ethos* agorista que suele haber, generalmente, en las comunidades de las criptomonedas donde se asume este activo como un bien de intercambio, el emprendimiento se realiza para crear mercados *paralelos*<sup>6</sup> y sobrepasar toda esta serie de controles estatales.

En este sentido, el acto de emprender para ofrecer bienes o servicios en el mercado *legal* o en el *paralelo* es «lo mismo». Obviamente que, para la fabricación de ciertos bienes específicos, existirán mayores controles y restricciones estatales para con los privados, dependiendo de la magnitud del capital invertido para fabricarlo (no será lo mismo cocinar pan casero y venderlo; que fabricar un automóvil de código libre y venderlo al mercado paralelo). Aún así, más allá de estas diferencias, no se requiere de ningún proceso u homologación especial para emprender y vender en el mercado paralelo: de hecho, conceptualmente hablando, habrá *siempre* un mayor libertad en éste mercado que en el primero.

---

<sup>5</sup>Desde la decisión de realizar el proceso legal hasta poder, finalmente, emprender con el permiso del Estado, puede pasar medio día, como sucede en Nueva Zelanda (Doing Business, 2020a, pág 4), o 230 días en Venezuela (Doing Business, 2020b, pág 4).

<sup>6</sup>Es decir, un mercado *independiente* de la economía basada en dinero *fiat*, que funciona con criptomonedas. Se usa la palabra «paralelo» y no «ilegal» porque existe una rápida connotación negativa a la palabra «ilegal»; pero, como ya se ha mencionado en la sección anterior, la legalidad no es un parámetro para determinar la moralidad de la acción.



### 3. Marca de código abierto

Las *Marcas de código abierto* (u *Open Source Brand* en inglés) serían, en simples palabras, emprendimientos ya creados: tanto la imagen de la marca como todos los procesos estandarizados de fabricación/servicio están asentados en documentos digitales. Este tipo de emprendimiento no es, para nada, un requisito necesario para crear tal mercado paralelo. En este documento, se propone *otra* forma más de incentivar al mercado para desligarse de la cotización de la criptomoneda valuado en moneda *fiat*<sup>7</sup>. Básicamente, se trata de ofrecer un *modelo de empresa*, de forma libre, a cambio de una comisión por cada venta (esto es análogo, en la economía actual, a crear una patente de un bien para que cualquier empresa pueda tomar dicha patente y fabricarlo por su cuenta).

¿Por qué hablar, entonces, de una *marca de código abierto*? Dada la experiencia con respecto al desarrollo de *software* libre, la metodología de trabajo detrás de este proceso (el escrutinio público y la renovación de los procesos) podrían ser, también, aplicado a proyectos *por fuera* del ámbito digital. Así como se ha tomado a Bitcoin como un modelo estándar de criptomoneda, y se han realizado diferentes modificaciones del código para lanzar nuevas criptomonedas, lo mismo sucedería con las marcas de código abierto. Es decir, no solamente se podría ofrecer marcas del mismo rubro, compitiendo entre sí; sino que también podrían surgir marcas que ofrezcan productos *muy* similares entre sí, compitiendo en base al precio y la comisión que ofrecen al mercado (este último punto estará desarrollado más adelante).

Se pretende que, en el largo plazo, exista una situación en la que las personas alrededor del mundo, que quieren comenzar *inmediatamente* a emprender, puedan elegir diferentes marcas dentro de un «catálogo de marcas». Así, la marca que les sean de su agrado, o la que les resulten económicamente más viable en la locación donde se encuentren, pueda ser tomada y utilizada, bajo los procesos estandarizados de trabajo que la misma marca estipula, para venderlos en el mercado paralelo local. Esta idea supondría, inmediatamente, un rechazo debido a los incentivos económicos por parte del inventor de la marca para ser comercializado; pero también será expuesto más adelante.

Se espera, también, que la fabricación y venta de estos productos puedan ser valuados en diferentes criptomonedas (y no en una *única*, aunque esto dependerá de las preferencias subjetivas del vendedor); dando lugar, así, a

---

<sup>7</sup>Sobre esto se refiere al acto de comprar criptomonedas «cuando el precio es bajo» y venderlas «cuando el precio es alto». En este intercambio, se utilizan las criptomonedas como un activo financiero para ganar más dinero; y esto, si bien podría aportar una liquidez al mercado, no contribuye para nada a la creación de un mercado paralelo.

una mayor liquidez en el mercado. Y esto provocará diferentes oportunidades de mercado para que surjan nuevas marcas y competidores para que se regule automáticamente el precio de los bienes ofrecidos en el mercado.

### 3.1. Ventajas

¿Qué ventajas tiene una marca de código abierto con respecto a un emprendimiento común? A decir verdad, una marca de código abierto *es* un emprendimiento; y no supone un cambio de paradigma que «deje obsoleto» el emprendimiento. Como no difiere demasiado de la concepción de un programa de código abierto, sí se puede mencionar una serie de ventajas a la hora de crear una marca de código abierto:

1. Transparencia de los procesos de trabajo.
2. Escrutinio público de la marca.
3. Salto del control estatal.

#### 3.1.1. Transparencia de los procesos de trabajo

Así como en el mundo digital, los programas se encuentran bajo una licencia de código abierto, en el que cualquier persona puede acceder al código y realizar un escrutinio de su funcionamiento, lo mismo se propone con los emprendimientos y sus procesos de trabajo. ¿En qué se diferenciaría una empresa de esta característica de una empresa tradicional? La diferencia radicaría en la *transparencia* de los procesos de trabajo (pues éstos están descritos públicamente).

Dado que, en el entorno de las criptomonedas, la palabra *transparencia* está referida a la visualización y el rastreo de las transacciones del usuario, aquí la palabra refiere a los procesos de trabajo. Nada tiene que ver con demostrar públicamente el estado de la cuenta a la que pertenece la marca, sino que se especifican los *procesos* de trabajo, la materia prima e insumos.

Esta *transparencia* de los procesos de trabajo no es algo exclusivo del ámbito digital, sino que también existe en la vida real. Un ejemplo cotidiano sucede en el mundo gastronómico, donde en internet y en impresiones en diarios, revistas, y libros, se encuentran las materias primas y los procesos de trabajo para crear una comida específica. Cuando uno consulta una receta del libro *Gino's Italian Express* del cocinero italiano Gino D'Acampo, se está trabajando con la materia prima y el proceso de cocina que ha sido estipulado por el mismo Gino D'Acampo. En vez de cocinar la comida personalmente para el usuario que lo desee, deja asentado el proceso de trabajo en un libro

para que el usuario compre dicho libro y pueda realizarlo (y obtener un porcentaje de la venta del libro).

El modelo de negocio de la marca de código libre, conceptualmente hablando, refiere a lo mismo<sup>8</sup>. Al detallar los procesos de trabajo para elaborar ciertos bienes u ofrecer servicios, un tercero no sólo podrá tener un grado mayor de seguridad al saber *cómo* se realizó, sino que también se podrá replicar en otros lugares para ofrecer el mismo producto.

### 3.1.2. Escrutinio público de la marca

Al igual que sucede con el *software* libre, en este caso también se puede realizar una revisión de todos los procesos de trabajo, materias primas e insumos (vale aclarar que el escrutinio público es posible cuando existe *transparencia*). Esta revisión podría derivar en casos en donde las personas interesadas corrigen ciertos errores pasados por alto por el inventor. En el caso de no ser modificados, dada la naturaleza *libre* de la marca, podrían surgir marcas *alternativas* con un proceso similar<sup>9</sup>.

El escrutinio público, aplicado a las marcas que ofrecen bienes no digitales, podría servir para replicar los procesos de trabajo y objetar públicamente si es realizable o no (y si el producto fabricado es *legítimo* o no). Además, también serviría en casos donde el inventor ha diseñado y creado un bien, pero no tiene el capital necesario para fabricarlo. El ejemplo más sencillo, para entender esta idea, podría ser el del mercado de impresiones 3D, en donde, tal vez, una persona ha diseñado una máquina manual, pero no posee una impresora 3D debido su alto costo (y su bajo poder adquisitivo para adquirirlo). Dado que es una marca de código libre de impresiones 3D, siendo una máquina manual compleja, se podría dejar al escrutinio público para que se analice

---

<sup>8</sup>Otro ejemplo de transparencia sería cuando los padres, al elegir una escuela privada para enviar a su hijo, desean ver el currículum que se enseña allí. Dependiendo de las preferencias subjetivas, y la comparación con otras escuelas privadas, los padres podrán tomar una decisión al respecto y elegirán una institución por sobre la otra (cuando el factor económico queda descartado). La estandarización del proceso de enseñanza está materializado en el currículum: puede que se cumpla todo el proceso como no; pero esto es una guía para que los padres sepan *a priori* qué contenidos se verá en las escuelas. Caso contrario, el contenido que su hijo verá será revelado *a posteriori*: los padres únicamente sabrán cuál es el currículum del día, luego de habérselo enseñado a su hijo. Por lo tanto, en este caso, la transparencia es beneficiosa tanto para la escuela como para los padres. La institución se asegurará un ingreso mensual a largo plazo, y los padres se asegurarán de pagar por un buen servicio a largo plazo. Además, existe la ventaja adicional que este esquema permite la competencia entre las diferentes escuelas mediante el currículum de estudio.

<sup>9</sup>A esto se refiere a lo que, por ejemplo, sucedió con Bitcoin y sus criptomonedas derivadas del mismo código.

el diseño, se lo replique y se haga las revisiones necesarias en el caso que existan fallas<sup>10</sup> (y que las personas sepan si estos diseños funcionan o no). Una vez comprobado el diseño, se podría utilizar la marca para fabricar dicha máquina.

Este concepto del escrutinio público, también, puede ser de gran ayuda a la hora de fabricar bienes que requieren de un enorme capital inicial, pero que, por ejemplo, la locación donde se encuentra el inventor, dado un mayor grado de autoritarismo y control estatal, no le es posible realizarlo (tanto legalmente como económicamente). Aquí, el control de calidad del diseño se realizaría *por fuera* de la vigilancia estatal (es decir, en otras locaciones más «libres»); para que el inventor sepa si su proyecto tiene fallas, o si es viable para su fabricación.

Por ejemplo, una persona ubicada en Guinea Ecuatorial, quien está interesado en crear una marca de código libre de fabricación de vehículos (con un logo y un proceso estandarizado de fabricación), diseña digitalmente un automotor. Su problema radica en no poder materializarlo por falta de recursos y una enorme cantidad de trabas legales para fabricarlo y probarlo. Al publicar su diseño y estipular que es un diseño de código abierto, un argentino podría fabricarlo, y realizaría un control de calidad. Un mexicano podría revisarlo y llegar a la conclusión que existen ciertas inconsistencias en los datos publicados, pudiendo hacerse unos ligeros cambios en el diseño para ser más eficiente. Dado el escrutinio público de este diseño para mejorarlo, el ecuatoguineano podría asentar el diseño final en una nueva versión de su diseño; y lo publicaría para su fabricación (a cambio, por supuesto, de una comisión por cada venta del auto fabricado).

El ejemplo anterior podría ser fácilmente rechazado por su «idealismo» al pretender crear un automotor y creer que se podría circular libremente por las ciudades, lejos del control policial y de tránsito. Si bien es cierto en las circunstancias actuales, el tema aquí se basa en el escrutinio y control de calidad del diseño de un bien que requiere de un gran capital, cuyo creador no puede pagar por sus propios medios. No obstante, el ejemplo del diseño de un automóvil de código libre está inspirado en el caso real de *Hyperloop*, una propuesta diseñada por Elon Musk de un sistema de trenes de alta velocidad, que viaja a través de un tubo al vacío, publicado como diseño de código libre el 9 de octubre de 2013 (Gray, 2013).

Entonces, ¿cuál sería el beneficio de un escrutinio público? Continuando con el ejemplo, si existen interesados en adquirir un automotor valuado en criptomoneda, ellos mismos serán quienes querrán dicho vehículo con las

---

<sup>10</sup>Esto es similar a tener una empresa en donde los nuevos diseños son enviados al Departamento de Desarrollo.

mejores condiciones (claramente, para su propia seguridad y especialmente su propio interés), las prestaciones que deseen, y la adquisición de un bien por fuera de todo tipo de control estatal<sup>11</sup> (con la ventaja que aporta a la fabricación y circulación de bienes en el mercado paralelo).

En resumen: el escrutinio público permitiría un control de calidad más riguroso para todos los interesados en adquirir dicho bien, en vez de confiar o depender de una empresa regulada por el Estado, o una entidad estatal, en un país específico.

### 3.1.3. Salto del control estatal

Este punto sea el que diferenciaría una marca de código abierto con respecto a un emprendimiento común. Antes de comenzar, el control estatal no se podrá evitar *por completo* en el emprendimiento, sino que se podrá intentar reducirlo a su mínima expresión; y mientras más autoritario es el gobierno, más difícil será evitar este control estatal<sup>12</sup>. Habiendo dicho esto, un emprendedor podría dudar de la legitimidad de la marca de código abierto; y que sea el mismo emprendedor quien fabrique bienes y los comercialice a nivel local. No obstante, el problema, aquí, es la comercialización a una escala más grande.

Un emprendimiento en el mercado paralelo podría verse restringido por la locación geográfica en la que se encuentra. El emprendedor, por lo tanto, podrá comercializar su producto de forma local pero con la dificultad de expandirse y evitando los controles estatales. Si, por ejemplo, una persona decidiese comprar un bien X, residiendo en un país lejano, una alternativa podría ser la del envío por medio de algún medio transporte (por ejemplo, aéreo o náutico). El gran problema al que se enfrentará el vendedor serán los siguientes puntos:

- Burocracia estatal y permisos necesarios.
- Corrupción aduanera.
- Pago del servicio de envío con dinero *fiat*.

---

<sup>11</sup>Como el control de calidad y la homologación del auto está puramente en manos del Estado, dado los incentivos que posee, puede incurrir en trámites burocráticos costosos y extensos en el tiempo, impedimentos legales y/o fiscales arbitrarios para la fabricación, como también en todo tipo de acto de corrupción en el proceso (soborno, investigación fiscal, multas arbitrarias, persecución sindical, etcétera).

<sup>12</sup>Aunque esta declaración podría estar sujeto a debates, dado que podría justificarse que cuanto más grande es el Estado, más ineficiente se vuelve para controlar todas las actividades humanas.

El primer punto refiere a todo el proceso de homologación del bien y su aprobación para certificar que dicho bien cumple con las normas nacionales e internacionales. Es decir, aparte de realizar todos los trámites, la entidad estatal aduanera valorará, clasificará y verificará el bien en cuestión para aprobar su envío a otro país; o prohibirlo si este bien es considerado «peligroso» o «ilegal» por la entidad reguladora.

El segundo punto, como se menciona, trata sobre los actos de corrupción que puede tomar la aduana, que puede tomar diferentes formas: demoras muy extensas para entregarlo; pedidos de sobornos para que el cliente pueda retirarlo; traspapelado de permisos que impiden su retiro; exigencia de pagos de aranceles o multas arbitrarias por el servicio; entre otras cosas.

El tercer punto engloba a los anteriores, y refiere a que el envío internacional, al estar controlado por el Estado, suele ser un servicio que se paga con dinero *fiat*; y esto se contrapone con la idea de crear mercados *paralelos*, con el fin de comerciar con criptomonedas y abandonar el dinero *fiat*. Aquí, el problema yace en que la valuación en criptomoneda de un bien perderá importancia, ya que todos los procesos intermedios entre el vendedor y el cliente estarán valuados en otra moneda. Esto implica que, ante la situación de elevar el costo en otra moneda, terminará resultando más práctico venderlo en dinero *fiat* (pues todo el proceso de fabricación hasta la venta se encuentra en dicha denominación), que realizar los procesos de conversión de criptomoneda.

La marca de código abierto permitiría replicar la fabricación de un bien en una locación a otra, saltando todo el control estatal de transporte, pero también permitiendo al inventor de la marca ganar dinero con ello. De esa forma, la restricción geográfica se verá resuelta; y si bien no podrá fabricar y enviar el bien a una locación específica, sí podrá ganar dinero a través de la comisión para «certificar» que el producto corresponde a su creación (pero el tema del incentivo económico será explicado en la siguiente sección).

### 3.2. Desventajas

Se debe señalar dos puntos *fundamentales* acerca del concepto de *marca de código abierto* planteado en este documento. Para comenzar, este modelo de negocio difiere de proyectos de código abierto basados en donaciones, es decir: un desarrollador o grupo de desarrolladores que reciben dinero de forma voluntaria por parte de los demás miembros de la comunidad por su trabajo; y que dichas donaciones no interfieren con su uso. Por otro lado, también difiere en el modelo de negocios basado en CCS (Community Crowdfunded System), en el que se propone una idea para que la comunidad de dicha criptomoneda acepte o rechace financiar el trabajo. Aquí se plantea que una

persona desarrolle una marca, y ésta sea «cedida» a la comunidad a cambio de una comisión por la venta de cada bien. Es por ello que se pueden enumerar dos *grandes* problemas a la hora de crear un emprendimiento con estas características:

1. Falsificación del producto.
2. Incentivo económico.

Dado que la marca de código libre establece el procedimiento para fabricar un producto, con la materia prima y los insumos necesarios, una persona podría simplemente buscar dicho procedimiento, crear el producto estipulado; y no pagar ninguna comisión al inventor. Este escenario «forzaría» al inventor en *confiar* en la moral del fabricante anónimo para que pague la comisión por utilizar su marca. En este artículo se presentarán sus respectivas soluciones que, en definitiva, serán el punto de partida para el emprendimiento. La experiencia, al fin y al cabo, determinará las mejores soluciones para llevar a cabo dicha empresa.

### 3.2.1. Falsificación

Vale aclarar que existe una diferencia *sustancial* entre la falsificación y la réplica. No es lo mismo ofrecer al mercado una réplica de un bien, que una falsificación de la misma.

En cuanto a las réplicas, estos casos suceden en la vida real. Por ejemplo, a la hora de crear la receta de Baileys Irish Cream, existe una enorme cantidad de recetas diferentes en internet que replican la bebida alcohólica. Todas ellas con las materias primas necesarias (crema, leche condensada, chocolate, vainilla y whiskey irlandés) en diferentes proporciones. No obstante, en todos estos casos se está logrando un producto muy parecido al original (al punto de ser comercializado como una bebida símil Baileys), pero ninguna de ellas pertenece a la marca original que ha creado dicha receta. Aquí es donde se podría considerar la idea de «valor agregado», al comprar una bebida homologada por la misma marca y comprar una réplica de la misma.

Por citar otro caso de mayor tamaño, en el mercado de pedales de efectos para guitarra existen cientos de réplicas de pedales para guitarra que son considerados «clásicos»<sup>13</sup>. La empresa Behringer, por ejemplo, es conocida por tener una línea de pedales de efectos de muy bajo precio, y replican modelos de pedales de marcas «importantes» pero más caros. El fabricante de pedales

---

<sup>13</sup>Algunos ejemplos de estos pedales, considerados «clásicos», pueden ser: Dunlop *Fuzz-Face*; Vox *Wah*; Univox *Uni-Vibe*; MXR *Dyna Comp*; MXR *Phase 90*; Boss *DS-1*; Ibanez *TubeScreamer 808*; ProCo *Rat*; etcétera.

JHS Pedals, Josh Scott, en su canal de Youtube realizó una comparación entre éstos pedales y sus réplicas. A continuación, una tabla comparativa de algunos de los pedales que Josh considera como una «réplica idéntica», con sus respectivos precios de mercado:

Original	Precio	Behringer	Precio	Dif.
Ibanez CP-9	USD 170	CL-9	USD 25	x6,80
Boss TR2	USD 114	UT300	USD 25	x4,56
Boss GE7	USD 137	EQ700	USD 25	x5,48
Boss VB2	USD 254	UV300	USD 25	x10,16
Boss CH1	USD 137	UC200	USD 25	x5,48
Ibanez TS808	USD 165	TO800	USD 25	x6,60
Boss FZ2	USD 370	SF300	USD 25	x14,80

Extracto del video *What's the Deal With Behringer?* (JHS Pedals, 2019)

A pesar de replicar los circuitos originales, consiguiendo un sonido *idéntico* en mucho de los casos, los pedales son vendidos con la marca Behringer. La diferencia *radical* con respecto a la falsificación sería que la misma empresa Behringer fabricase las réplicas, vendiéndolas como si fuesen los originales<sup>14</sup>. En este caso, se estaría engañando al cliente al venderle una réplica como si fuese un original. Diferente sería ofrecerle un pedal que, a pesar de ser una réplica del modelo original, se le hace notar al cliente que es una «copia idéntica» al original. Aquí, por lo tanto, la persona sabrá que estará comprando una copia, no un *original*.

Dado que los procesos en la marca de código libre ya están transparentados (es decir, «están a la vista de todos»), tal vez no habría incentivos para crear falsificaciones del mismo producto<sup>15</sup>. En todo caso, se podría ofrecer una bien similar. Sin embargo, se asumirá que un mercado de «falsificaciones» de bienes será inevitable<sup>16</sup>.

En resumen, la primera y más obvia desventaja de este modelo de emprendimiento podría ser la *falsificación*. Llevado a un paso más adelante, el actor malicioso podría realizar, por ejemplo, una campaña publicidad sobre una marca específica como aquella que fabrica un producto «defectuoso», «peligroso», «engañoso», etcétera (asociando, así, la marca a alguna de estas características para «removerlo» del mercado). No obstante, dado que la

<sup>14</sup>Es decir, que Behringer fabrique su pedal UV300, pero, en vez de utilizar su propia carcasa, utilice la de Boss VB2, replique exactamente el mismo color y la tipografía, y lo venda al mercado a \$ 254.

<sup>15</sup>Suposición creada a partir del caso mencionado de los pedales de efectos para guitarra.

<sup>16</sup>Véase el caso del modelo de negocio de los *softwares* privativos; y los *cracks* de su código para descargarlos y utilizarlos sin pagar un centavo por ello.



marca y el proceso de fabricación se encuentra en escrutinio público (y es, por lo tanto, de fácil acceso), esta situación podría ser fácilmente objetada: bastaría, simplemente, con revisar los materiales e insumos utilizados y los procesos de fabricación para determinar si el producto final es legítimo o no.

Si bien lo siguiente sucede por fuera del ámbito económico (y que excede las propuestas de este artículo), podría existir el caso de actores maliciosos que, para quitar del mercado a una marca, injurian al inventor de la marca para desincentivar su producción (y las ganancias que recibe a través de la comisión). Podría suceder el caso en que, por ejemplo, Juan no le agrada Antonio, el inventor de una marca. Su resentimiento es tal que decide boicotear la marca al denunciar falsamente, en las redes sociales y los espacios de interacción social, que Antonio es un *nazi*; exigiendo a la comunidad que deje de utilizar dicha marca (para no financiar a una persona «con una ideología nefasta»), y, además, promover la censura y el rechazo de cualquier nueva marca que él invente<sup>17</sup>.

Un caso que sí compete a este artículo es aquel en donde un actor malicioso, con ansias de eliminar una marca en particular, en vez de ofrecer un producto similar y competitivo, fabrique el bien ofrecido por la marca pero con diferentes materiales (o con un proceso de fabricación diferente) con el fin de crear intencionalmente un producto «defectuoso». Así, podrá insertar en el mercado un producto falsificado; para que los usuarios consuman dicho bien y asocien la marca a productos «de muy baja calidad», «peligrosos», «tóxicos», «no confiables», etcétera.

¿Cómo el cliente podría asegurarse que el producto que desea comprar es «auténtico» y no una falsificación? En un principio, podría considerarse la creación de una empresa que ofrezca certificaciones de calidad del producto. Esto es: una empresa *autónoma* que verifica tanto el proceso de fabricación del producto como el producto final, y otorgue una certificación de calidad al fabricante y al producto. Por otro lado, podría ser el mismo inventor quien supervise el proceso de fabricación y el producto final, para ser la misma persona quien otorgue la certificación de calidad.

Sin embargo, en estos dos casos, aparecería un nuevo problema (que no es para nada «nuevo»): se debe recurrir a un *tercero de confianza* para determinar la autenticidad del producto. Aquí es donde aparece, una vez más, la tecnología *blockchain* y el desarrollo teórico de Satoshi Nakamoto en su artículo *Bitcoin: A Peer-to-Peer Electronic Cash System*:

Lo que se necesita es un sistema de pagos electrónicos basado

---

<sup>17</sup>Esta situación podría ser el puntapié inicial para la formación de una *Justicia privada*, con el fin de resolver disputas y agravios contra la propiedad privada de un tercero (entendiéndose la *integridad* y el *honor* como parte de la propiedad privada de una persona).

en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas en realizar transacciones directamente sin la necesidad de un tercero confiable. Las transacciones que son computacionalmente poco factibles de revertir protegerían a los vendedores de fraude, y mecanismos de depósitos de fideicomisos de rutina podrían ser fácilmente implementados para proteger a los compradores. (Nakamoto, 2008, pág. 1)

En este paradigma, la «certificación» es diferente al de la vida real, y tiene que ver con este tema fundamental: todos los procesos de trabajo están a libre disposición de los usuarios (y este proceso estará firmado digitalmente por el creador, para garantizar la autenticidad de todos ellos). Por lo tanto, no habría necesidad de solicitar un tercero de confianza para que garantice que los procesos de trabajo sean los que corresponden. Bajo el paradigma actual, las patentes están ocultas al escrutinio público; y esto hace que sí se necesite un tercero de confianza para certifica que se utilizan materias primas y procesos de trabajo adecuados para la fabricación de un producto. En la propuesta de este artículo, el inventor no debe por qué estar pendiente si cada uno de los fabricantes respetan los procesos estipulados, ni esperar que haya un tercero de confianza para garantizar que los procesos de trabajo sean legítimos. En definitiva, *todos* los agentes involucrados son los certificadores de calidad del producto: desde el fabricante (que desea ganar dinero al vender su producto fabricado), hasta el vendedor (que desea ganar dinero al vender el producto desde la fábrica hasta el cliente), y el cliente (que desea comprar dicho producto). Y todos ellos, ante la duda, podrán comprobar por sí mismos si el producto es *legítimo* o no en base a los procesos determinados por el inventor.

Dada la noción de un *sistema sin confianza*, en la sección *Comprobación* se incluirá una posible forma de certificación (con sus ventajas y desventajas); pero esto no implica que se descarte cualquier surgimiento de nuevas aplicaciones, métodos o tecnologías de verificación de calidad, dada la misma interacción entre los agentes económicos que están interesados en comprar un producto «confiable».

### **3.2.2. Incentivo económico**

Este punto quizás sea el más controversial y la piedra angular de todo este modelo de negocios. Hasta ahora, se ha dado por sentado que aquellos que deseen fabricar los bienes de la marca de código libre estarán dispuestos a pagar voluntariamente una comisión al inventor por cada venta. Pero esto implica que el fabricante tenga que realizar la acción de vender el producto

y *elegir* no pagarle al inventor (y al ser una marca de código libre, no existe ninguna privación por parte del fabricante en realizar esto). Esto genera una situación que no es económicamente favorable para el inventor<sup>18</sup>.

Al no poder asegurar un ingreso constante o «esperable» a lo largo del tiempo, este modelo de negocio parecería no proveer de ningún incentivo económico para crear una marca; y, así, un tercero fabrique ese bien, y lo venda para que ambas partes ganen dinero. La única situación en donde el inventor podría ganar dinero sería en el caso de pedir donaciones al resto de los usuarios de la comunidad (como se ha mencionado al principio de la sección).

Para solventar este problema desde el punto de vista *puramente* económico, se podría referenciar el modelo de negocio que tienen las *pool* de minado<sup>19</sup>. Por un pequeño porcentaje como comisión, las *pool* ofrecen servidores para que diferentes personas, en cualquier parte del mundo, se «reúnan» para minar una criptomoneda; y así aumentar las posibilidades de obtener la recompensa (que, luego, será repartido para cada uno de los participantes, dependiendo del sistema de recompensa ofrecida por la misma *pool*).

Ahora bien, ¿qué parámetros podrían tomarse en cuenta para elegir una por sobre otra, si, en definitiva, todas ofrecen el mismo servicio (minar los bloques)? En principio, la comisión entre las mismas *pools*<sup>20</sup>. Si todas ellas ofrecen la posibilidad de minar una misma criptomoneda, en cuanto a su incentivo económico, será el porcentaje de comisión por cada vez que el usuario desee retirar su dinero de allí. A continuación, se mostrará un listado de varias *pools* con su porcentaje de comisión y el límite inferior para poder retirar XMR:

<b>Pool</b>	<b>Comisión</b>	<b>Pago min.</b>
MineXMR	1,10 %	4,00 mXMR
Nanopool	1,00 %	110,00 mXMR
XMRPool	0,90 %	70,00 mXMR
Hashvault	0,90 %	1,00 mXMR
SupportXMR	0,60 %	100,00 mXMR
MoneroOcean	—	3,00 mXMR
P2Pool	—	0,30 mXMR

Nótese que MoneroOcean y P2Pool no cobran comisiones a los usuarios.

<sup>18</sup>A menos, claro, que ofrezca una marca de código libre y explicita que no desea obtener ninguna ganancia al respecto.

<sup>19</sup>De hecho, algunas de las *pools* son *marcas de código abierto* porque, literalmente, su código para funcionar se encuentra en escrutinio público.

<sup>20</sup>Existen, por supuesto, *excepciones* a esto, como la *pool* llamada P2Pool.

Aún así, se diferencian en que el primero admite el retiro de XMR cuando el usuario llega a un mínimo de 3 mXMR; y el segundo, a 0,3 mXMR.

Aparte de la competencia que existe entre estas *pools*, ésto puede tomarse como ejemplo para el modelo de negocios. El vendedor, cuando ofrece su producto al mercado, podría dar un código QR para que el cliente pueda escanear dicho código y pagarlo; con la diferencia que, dentro del mismo código QR, el cliente, al realizar la transferencia, esté enviando su dinero a dos direcciones diferentes. Por ejemplo, dada una marca de licores, el vendedor podría etiquetar la botella con el código QR, para que el cliente, con su aplicación correspondiente, pueda transferir su dinero en criptomonedas de su billetera a dos cuentas a la vez. Si la marca de licores pide un 1 % de comisión por cada venta, contablemente hablando, se vería de la siguiente manera<sup>21</sup>:

Agente	Debe	Haber	Porc.
Comprador	—	25,000 mXMR	100,00 %
Vendedor	24,750 mXMR	—	99,00 %
Inventor	0,250 mXMR	—	1,00 %

Si el vendedor ofreciese el código QR al comprador para realizar la transacción, éste se vería así:



Con sólo una sola imagen, el código QR mostrará:

- El monto del producto.

---

<sup>21</sup>Vale la pena aclarar que aquí no se cuenta la comisión por la transacción asentada en la *blockchain*.

- La dirección del vendedor, con el monto correspondiente.
- La dirección del inventor, con el monto correspondiente.
- El detalle de la compra.

¿Que pasaría si el vendedor, maliciosamente, engañase al comprador al dar tres direcciones diferentes, pero que todas ellas corresponden al mismo vendedor? Para reducir este grado de confianza y evitar este acto, tanto el inventor como el vendedor deberán ofrecer públicamente sus direcciones en un archivo `.asc`, firmados con sus respectivas claves privadas GPG, y utilizar un protocolo para verificar que las direcciones incluida sen el código QR correspondan con las partes involucradas. De esta forma, el comprador, mediante una comparación visual o a través de una simple aplicación, podrá verificar que las dos direcciones corresponden al vendedor y al inventor.

Siguiendo con el ejemplo anterior, ahora con direcciones reales y con órdenes creadas a partir de la opción *Payment request* en el programa Monero GUI (aunque con una modificación en la sintaxis), el código QR podría verse de la siguiente manera:



Este código se desglosa de la siguiente manera:

- Datos del *vendedor*:
  - **Dirección de Monero:** 8BB dgnA ckd2 DWfX qHcc 2466 v19d VeWv hgAt jSm1 hZGP xe6C BkPg Dxqa BLbr D9NL K8re WLFf oUtd pg18 rzkT DC2i BJMe rKDv
  - **Cantidad:** 0.024750000000
  - **Nombre:** Vendedor
  - **Descripción:** Botella de licor
- Datos del *inventor*:
  - **Dirección de Monero:** 887 UEV7 9zZT KeKb tGjT 2GUe 6P6H aFLn DF52 KibH PL2C yZUp isgA 2EyN anJh LXRf oJW6 FNhX Q7sd h9SE K8YX u7ZX 8JKL YADh
  - **Cantidad:** 0.000250000000
  - **Nombre:** Inventor
  - **Descripción:** Li'monero

Entonces, el cliente podrá tener los siguientes parámetros:

- La suma total de las tres transacciones da como resultado 0.025 XMR (o 25 mXMR), precio que coincide con el precio de venta del producto, por lo que podrá asegurarse que el precio está bien.
- El desglose de los 25 mXMR en 24,75 mXMR (99 %) para el vendedor y 0,250 mXMR (1 %) para el inventor, ambos porcentajes coincidentes con las comisiones propuestas por la marca de código abierto y el vendedor, respectivamente.
- Mediante una comprobación con las claves públicas GPG, podrá comprobar que las direcciones son *legítimas* (y esto podrá ser únicamente comprobable si los dos recipientes de XMR han dado públicamente su dirección, firmados con sus claves privadas).
- Podrá ver el nombre de la dirección y la descripción a la que corresponde el monto en la transacción.

De esta manera, el comprador podrá hacerlo rápidamente (ya sea desde la computadora o desde cualquier dispositivo móvil), sin la necesidad de realizar demasiados pasos para su comprobación. Además, esto mismo podrá realizarlo el inventor.

En resumen, este ejemplo contiene las siguientes ventajas:

- El comprador tendrá la facilidad de pagar por el producto, sin la necesidad de tener que realizar el pago correspondiente a dos agentes económicos diferentes por separado: lo hará, simplemente, con un solo pago.
- El vendedor tendrá un incentivo económico, pues obtendrá una gran suma de dinero por cada venta (en este ejemplo, un 99 %).
- El inventor podrá ganar una pequeña suma de dinero de forma *pasiva* con cada venta, al ofrecer su idea al mercado. Esto incentivará a competir en el mercado para que más personas puedan fabricar su producto; y obtener, así, mayores ingresos pasivos.
- Todos los agentes económicos podrán verificar, a través del código QR, que las direcciones con su correspondiente comisión sean *fidedignas* en base a las claves GPG proporcionadas. Caso contrario, alguno de ellos podrá demandar a la otra parte el cumplimiento del acuerdo; o, simplemente, el producto no se venderá pues no cumple con el estándar de venta.

## 4. Comprobación

La comprobación de bienes no tangibles, dada la naturaleza *digital* de las criptomonedas, es muy sencillo.

Por cada bien digital creado, el productor podría realizar una comprobación *hash* del archivo<sup>22</sup>, y ofrecer la facilidad al usuario que compruebe la integridad del archivo (y no comprometer la «salud» de la computadora). Por dar un ejemplo, el *hash* del programa de minería XMRig, en su versión 6.17.0 para Linux x64, comprimido en un archivo .tar.gz es:

```
75ce 5d4d 52c4 6a7c 8c60 4e1d e354 9cba 9dc4 b074 05d6 598e
12b6 f21f 5024 7739
```

Mediante el uso de un programa como, por ejemplo, GtkHash<sup>23</sup>, se puede cargar el archivo descargado y la comprobación *hash*. De ser correcto, el pro-

<sup>22</sup>Comúnmente, se utiliza SHA-256; pero puede realizarse con cualquier otra función, como BLAKE2, BLAKE3; o la nueva familia de algoritmo SHA3, siendo SHA3-256 o SHA3-512. Incluso, se puede ofrecer varias comprobaciones hash para una «doble comprobación».

<sup>23</sup>Los programas que se escriben para realizar las diferentes comprobaciones *hash* (en vez de escribirlo mediante la terminal del sistema operativo), tal vez podrían considerarse como una especie de «tercero de confianza». El grado de confianza dependerá si el programa es de código abierto o no, para realizar un escrutinio público del código.

grama tildará como válida la comprobación mediante el algoritmo SHA-256. De lo contrario, no marcará ninguna casilla; y el usuario deberá comprobar por su cuenta si el archivo se ha descargado con errores, o ha escrito o copiado mal el *hash* provisto por XMRig.

Esta práctica, por lo tanto, puede realizarse fácilmente, y no dependerá de ninguna empresa o tercero para la comprobación de los archivos digitales: incluso, este documento que se distribuye en GitHub figura la comprobación *hash*, para que el usuario se cerciore de la autenticidad de este artículo.

¿Cómo se puede, entonces, expandir esta idea en la compra de bienes tangibles? La utilización del algoritmo SHA-256 en los archivos existe para comprobar que el *hash* del archivo coincida con lo que la organización o la persona muestra públicamente. Sin embargo, como esto puede estar sujeto a un *hacking* (es decir, un *hacker* puede interceptar el sitio de internet donde se almacena este hash, o la comunicación entre el cliente y el servidor) la seguridad debe ser aún más fuerte. Dado que se ha propuesto que las diferentes partes involucradas en la transacción deban compartir la dirección de su monedero, cualquier actor malicioso podría interceptar esta comunicación y «engañar» al cliente. Y al no existir un tercero de confianza, si el cliente envía sus fondos a una cuenta equivocada, éste perderá dichos fondos de forma irreversible. En resumen: una situación en donde las partes involucradas provean, en texto plano<sup>24</sup>, no es condición suficiente como para *asegurarse* que la dirección provista sea legítima. Es aquí donde aparece el protocolo GPG.

Dado que no existe un tercero de confianza para mediar las transacciones entre las personas, todas las partes involucradas podrían publicar su dirección de su monedero mediante el protocolo GPG. Así, todas ellas podrán compartir públicamente su clave pública; y las personas que deseen realizar la transacción se asegurarán que la dirección corresponde con la persona u organización involucrada. Esto, quizás, representaría una «desventaja» pues las personas, al comprar por primera vez, deberá tomarse el tiempo de buscar la firma GPG de la otra parte. No obstante, esto representará otro paso de seguridad más; pero que no representa un enorme contratiempo. Es más, una vez registrada la llave pública en el dispositivo digital, este paso no será necesario realizarlo de nuevo.

Claro está que este procedimiento deberá realizarse en el momento *anterior* del pago. A través de la aplicación para transferir criptomonedas, el programa deberá tener, primero, las llaves públicas GPG de todas las partes involucradas (vendedor, inventor, etcétera). Luego, el programa deberá verificar que el archivo `.asc` que contiene la dirección firmada de una de las

---

<sup>24</sup>Es decir, un texto sin ningún tipo de encriptación.



partes, coincide con la llave pública que ha proporcionado. Si todo esto es correcto, aquí ya se podrá habilitar la opción de pago.

Además, se podría usar el protocolo GPG para especificar el porcentaje de comisión correspondiente a cada una de las partes. Si mediante una simple cuenta matemática, por ejemplo, la comisión para el inventor es del 0,1 %, cuando la marca públicamente establece que es del 1 %, la operación será rechazada. El cliente, por lo tanto, actuaría como mediador al ver que los términos entre el vendedor y la marca no coinciden (situación por la cual el cliente podría sospechar de la autenticidad del producto y, por ende, del vendedor). Así, se elimina un grado más de confianza entre el vendedor y el inventor, al ser el cliente un actor *pasivo* de mediación.

Al final de este artículo se anexará el diagrama de flujo *básico* de esta propuesta; como también se añadirá a la carpeta de la cuenta de GitHub la clave pública en formato `.asc` y un archivo de texto con la comprobación *hash* de este documento, con la firma correspondiente, para que el lector pueda verificar la autenticidad de este documento.

## 4.1. Procedimiento

Para aquel lector que no sabe comprobar una clave GPG, será necesario tener un programa que pueda descifrar y verificar las firmas GPG. El programa más conocido es *Kleopatra* (aunque también existen otras alternativas como *GPA* en Linux), y es un gestor de claves GPG. Por lo tanto, el usuario si quiere comprobar la autenticidad de algún mensaje, como se ha dicho, deberá tener la clave pública de una de las partes. Así, el archivo de texto firmado que fue proporcionado por una de las partes podrá ser fácilmente verificado. Simplemente, se deberá seguir los siguientes pasos:

- Importar la clave pública al programa correspondiente.
- Seleccionar el archivo de texto que contiene el mensaje firmado.
- Verificar que la firma corresponde con la clave pública importada.

De ser inválida la firma (es decir, no se reconoce de quién es la firma) el archivo de texto estará adulterado.

## 5. Ramificaciones

El incentivo para crear más emprendimientos para ofrecer bienes y servicios al mercado paralelo, al demandar materia prima y/u otros servicios,

provocará una oportunidad de mercado local para que *otros* emprendimientos surjan para suplir dicha demanda. Por ejemplo, en el caso de una marca de licores, la demanda por las materias primas (tales como las botellas de vidrio, la bebida blanca, y la fruta) permitirá la oportunidad para que surjan en el mercado fabricantes de botella de vidrios, fabricantes de bebida blanca, y productores agropecuarios que germinen y cosechen tales frutas. A su vez, éstos demandarán insumos para crear sus productos: fabricantes de botella de vidrios necesitarán vidrio (su materia prima), pero también hornos y combustibles; los fabricantes de bebida blanca necesitarán de su materia prima, como también de insumos para su fermentación y almacenaje; los productores agropecuarios necesitarán de agua, agroquímicos (si su forma de producción no es «libre de agroquímicos»), fertilizantes (químicos o naturales), y máquinas agropecuarias; etcétera.

Se estima que, en un principio, habrá muy pocos emprendimientos (y, en menor medida, marcas de código abierto) que tendrán que lidiar con la tasa de cambio «volátil» de las criptomonedas<sup>25</sup>, el poco margen de ganancias por las ventas, y la incomodidad de lidiar contablemente con dos tipos de monedas diferentes para la obtención de materia prima. Ante esto, la respuesta estará en la decisión de cada agente económico en tomar el riesgo de emprender o no.

No obstante, vale la pena destacar que estas marcas podrían ser mejores aplicadas en países con grandes inestabilidades económicas, debido a que, generalmente, esto viene de la mano de la poca flexibilización de monedas extranjeras y una rápida depreciación de la moneda local. Las criptomonedas, por lo tanto, supondrán un bien de intercambio de «menor» volatilidad en comparación con el dinero *fiat* local; ya que la tendencia a largo plazo del dinero estatal tiende a depreciarse, mientras que la tendencia a largo plazo de las criptomonedas en general, tienden a apreciarse<sup>26</sup>.

Retomando el ejemplo de la marca de código abierto que ofrece el licor, sí: al principio podría haber un margen de ganancia bajo o nulo debido a la compra de botellas de vidrio, sus tapas correspondientes, y la impresión de las etiquetas para las marcas. Pero aquí puede darse una «vuelta de tuerca»: en un comienzo, las botellas podrían ser recicladas de otras botellas vacías que las personas hayan arrojado a la basura. Se puede remover la etiqueta y usar el envase, correctamente esterilizado, para rellenarlo, taparlo y venderlo al público.

---

<sup>25</sup>De nuevo, por la concepción extendida de ver las criptomonedas como un activo financiero para hacer *forex trading*, en vez de ser utilizado como *dinero par-a-par*.

<sup>26</sup>En el 2009, Bitcoin no valía absolutamente nada; pero hoy, en el 2020, es la criptomoneda de mayor cotización de todo el mercado. Lo mismo sucede con las otras criptomonedas en sus inicios, con respecto a ahora.

El hecho de recolectar estas mismas botellas vacías, separándolas en sus diferentes tonalidades, podría dar lugar a la creación de una fábrica de botellas de vidrio, cuya materia prima es, justamente, las botellas arrojadas a la basura. Dado que el vidrio puede ser reutilizado, esta fábrica de botellas se ahorraría en el pago de materia prima en dinero *fiat* para, únicamente, obtenerlo de la recolección de la basura. En resumen: debido a la demanda de botellas de vidrio valuado en criptomoneda, una fábrica de botellas de vidrio podría suplir esto, al obtener su materia prima recolectada de la basura.

Explorando más allá de esta situación, puede que, en una región donde exista la circulación de autos eléctricos, un usuario que genera su propia electricidad para cargar la batería del auto, pueda tener la oportunidad de transportar las materias primas. En este contexto, dicho usuario podría valorar su servicio de transporte en criptomoneda, lo que ocasionaría una ventaja competitiva tanto para el fabricante de licor como el de botellas de vidrio, pues podrán abarcar un área mayor de ventas.

Se podría continuar con los ejemplos; pero como comentario final, basta con decir que la producción de una marca de código abierto (siendo un modelo específico de emprendimiento) daría, también, lugar a la competencia entre diferentes usuarios: si los precios ofrecidos por cada una de las marcas anteriormente mencionadas son altos, podrían surgir otros usuarios que fabriquen productos similares al mercado con un precio más bajo. De aquí, la idea de la *ramificación* de una actividad económica en otras actividades económicas que se complementan entre sí.

## 6. Liquidez

### 6.1. Local

Otro factor positivo de las *marcas de código abierto* es que permitirían una circulación mayor de las criptomonedas. Esto implicaría que, por un lado, habría oferentes de bienes y servicios (que, en países donde hay menor libertad económica, esto implicará una solución a los problemas del tipo de cambio de la moneda local, con respecto a la extranjera, y a su depreciación); y, por otro lado, existirían demandantes de dichos bienes y servicios. Así, las transacciones económicas entre los diferentes agentes permitirá que éstos mismos tengan mayor accesibilidad de criptomonedas al haber un mayor volumen de circulación.

Este escenario provocaría que las personas ya no necesiten depender de las casas de cambio centralizadas (en especial, aquellas que son del tipo *KYC*) para cambiar dinero *fiat* por criptomonedas: recurrirían a los mismos agentes

económicos de la nueva economía *paralela*. Y no solamente eso, las personas dejarían de atesorar, únicamente, las criptomonedas o utilizarlas como un mero activo financiero para ganar más dinero *fiat*: podrán ser utilizadas como dinero *par-a-par* (tal y como se estableció en el *white paper* de Bitcoin). Cabe mencionar que, de acuerdo con la teoría económica, esto también incrementaría su valor, siendo que aumentará, naturalmente, su *utilidad* en el mercado. Si esta apreciación se traslada a su cotización, cada unidad de criptomoneda valdrá aún más (y el dinero *fiat* quedará relegado al pago de impuestos).

Esta práctica podría ser, además, trasladado a otras criptomonedas, provocando una competencia de criptomonedas. En otras palabras, la economía paralela podría no estar relegada a una única criptomoneda, sino a diferentes criptomonedas. La valuación de los diferentes bienes quedará sujeta a los agentes económicos, quienes decidirán con qué criptomoneda comprar o vender ciertos bienes (o todas ellas).

## 6.2. Mundial

En la sección anterior se mencionó un escenario *local*; pero, siendo que las marcas de código abierto son libres, ésta será accesible a cualquier parte del mundo. La única barrera<sup>27</sup>, no obstante, que tendrá será la del idioma (y, por ende, la educación).

Por ejemplo, un venezolano podría crear una marca de código abierto sobre una serie de recetas de comida, con un proceso de fabricación específica. Dado que no puede acceder a una cuenta bancaria, y no puede comprar criptomonedas con la moneda local debido a su extrema depreciación en el corto plazo, tal vez un uruguayo podría utilizar esta marca para vender su comida; y por cada venta, el venezolano recibirá una comisión, dado que ha provisto de su dirección en criptomoneda para cobrar por cada venta (aunque, esto dependerá del modelo de negocios que el venezolano elija ofrecer<sup>28</sup>). Así, el venezolano podrá ganar dinero, al haber ofrecido una marca de código abierto, sin tener que recurrir a una cuenta bancaria y a una casa de cambio para obtener las criptomonedas. Y si este modelo se replica en la región donde vive el venezolano, los demás habitantes de esa zona podrán obtener el dinero suficiente como para que pueda circular localmente dicha criptomoneda.

Esto supone una ventaja más grande que la de, simplemente, emprender *localmente*. Los creadores recibirán una mínima comisión por las ventas que

---

<sup>27</sup>Asumiendo que las personas tendrán acceso a internet.

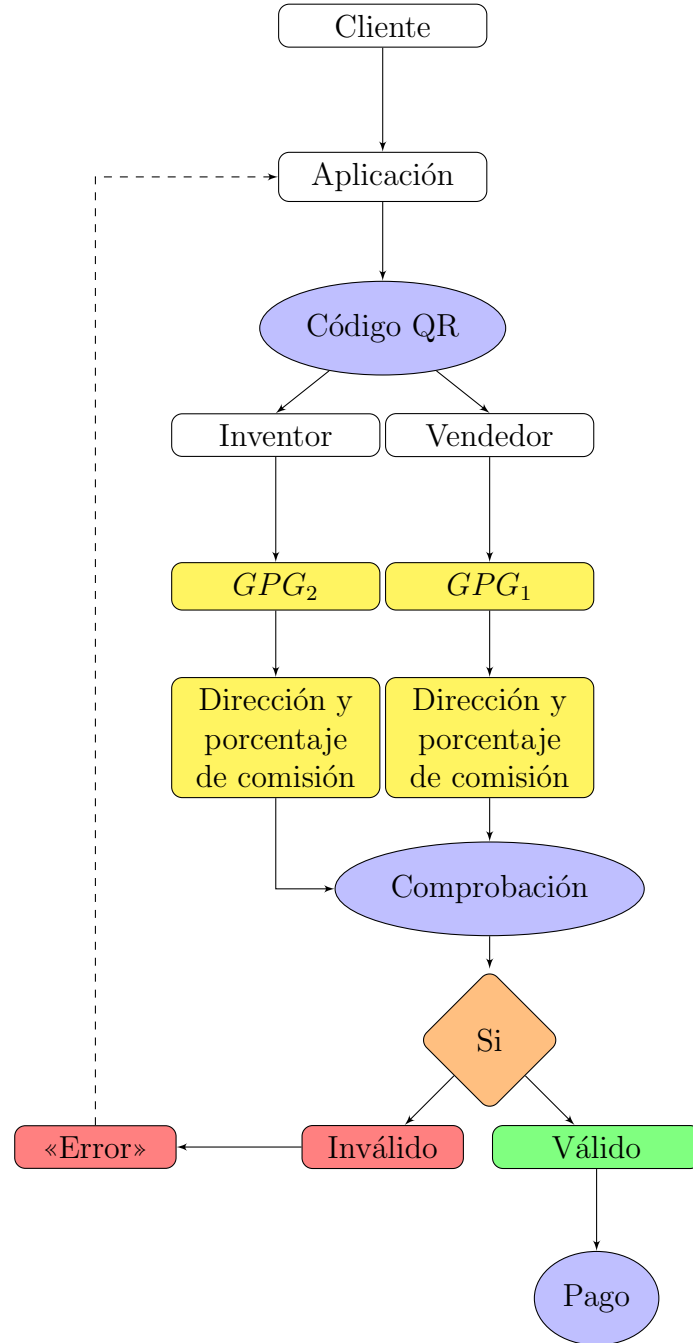
<sup>28</sup>Con respecto a esto, tiene que ver con respecto a si ofrece una marca en la que la persona que decide fabricar dicho producto, debe pagarle por cada venta; o simplemente realizar un único pago para obtener un «permiso» por parte del creador.

sucedan en otras regiones o países; y el vendedor podrá obtener una ganancia por sus ventas (por eso, la importancia del incentivo económico). Si se desea implementar una criptomoneda en un país o región determinada, la comunidad podría incentivar al usuario que vive en dicha región para que cree una marca de código abierto<sup>29</sup>, y sea implementado en otras regiones y países (saltando todas las barreras financieras y controles estatales).

---

<sup>29</sup>Solución más eficiente que, tan solo, pedir donaciones.

## 7. Diagrama de flujo



Válido  $\rightarrow ADDRESS_{GPG} = ADDRESS_{QR} \wedge \%_{GPG} = \%_{QR}$   
 Inválido  $\rightarrow ADDRESS_{GPG} \neq ADDRESS_{QR} \vee \%_{GPG} \neq \%_{QR}$

## Referencias

- Doing Business. (2020a). Economy Profile New Zeland. *World Bank Group*.
- Doing Business. (2020b). Economy Profile Venezuela, RB. *World Bank Group*.
- Gray, J. (2013, 09 de octubre). *Hyperloop in OpenMDAO*. Descargado 6 de junio, 2022, de <https://openmdao.org>
- JHS Pedals. (2019, 11 de abril). *What's the deal with behringer?* Descargado 29 de mayo, 2022, de <https://www.youtube.com>
- Menger, C. (1892, Junio). On the origin of money. *The Economic Journal*, 2(6), 239-255.
- Mining Pool Stats. (2022). *Trust pool*. Descargado 21 de mayo, 2022, de <https://miningpoolstats.stream/>
- Nakamoto, S. (2008). Bitcoin: Un sistema de efectivo electrónico usuario-a-usuario (Ángel León, Traduc.). *Bitcoin.org*. Descargado 31 de mayo, 2022, de <https://www.diariobitcoin.com/>
- Sun, Z. (2022, 18 de abril). *Monero community reaches consensus for july hard fork*. Descargado 21 de mayo, 2022, de <https://cointelegraph.com>
- von Mises, L. (2011). *La acción humana* (10.<sup>a</sup> ed.; J. Reig Albiol, Traduc.). Madrid: Unión Editorial.