En contexto

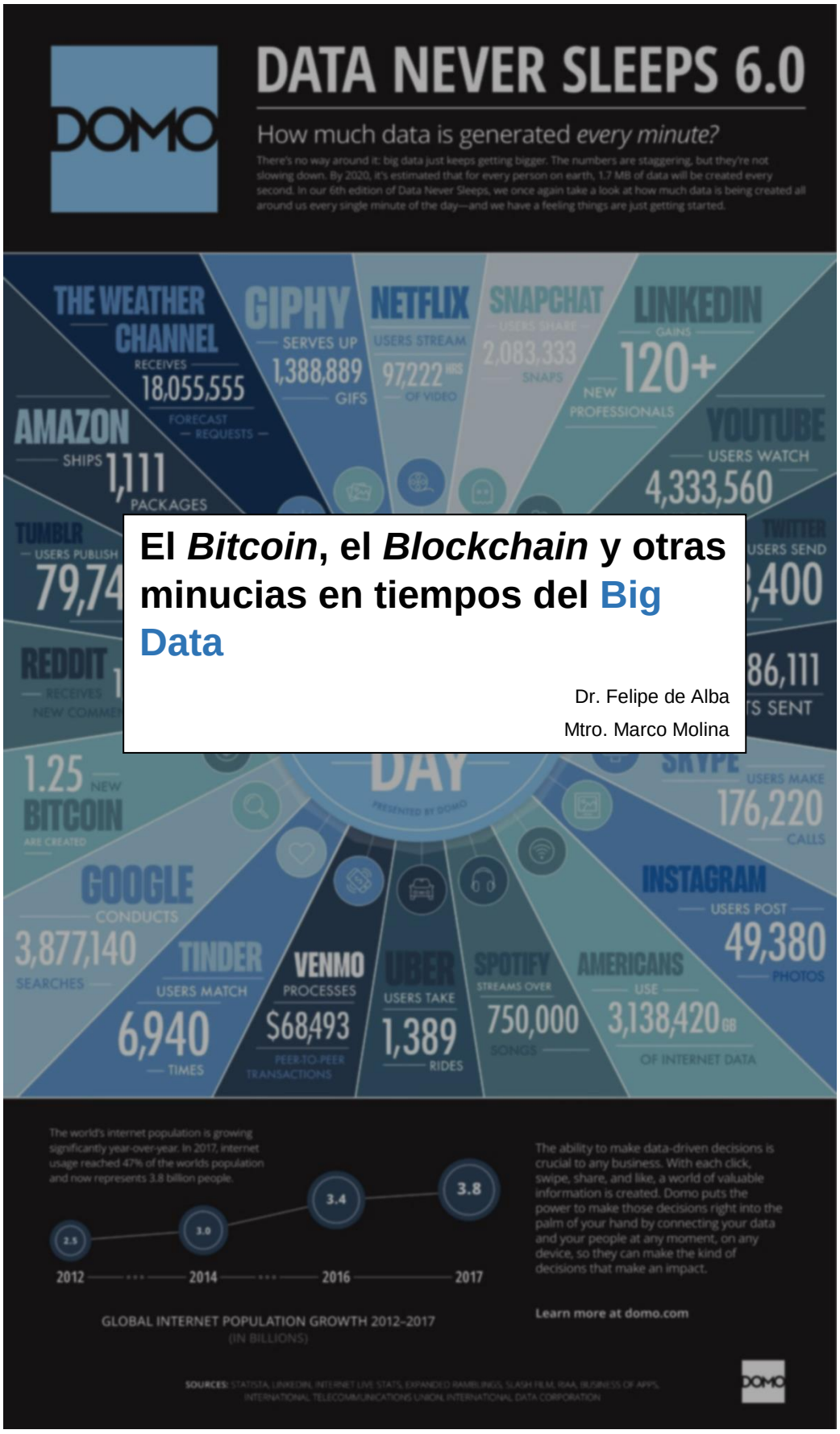
El Bitcoin, el Blockchain y otras minucias en tiempos del Big Data

Julio 2019

CÁMARA DE DIPUTADOS
LXIV LEGISLATURA

CESOP
Centro de Estudios Sociales y de Opinión Pública

www.diputados.gob.mx/cesop @cesopmx cesop01



El *Bitcoin*, el *Blockchain* y otras minucias en tiempos del Big Data

Dr. Felipe de Alba

Mtro. Marco Molina

Introducción

“El sueño de un mundo gobernado por las máquinas, los robots y las supercomputadoras está cada vez más cerca”. Esta frase se escucha con frecuencia en los mundos la informática, la robótica y los pequeños o grandes avances científicos ligados a la automatización de procesos. Los algoritmos son las “entidades”, los conjuntos de instrucciones en los que se define el lenguaje nuevo de estas prácticas de organización del mundo.

Así como los avances del transporte en el siglo XIX e inicios del siglo XX fueron los elementos detonadores de procesos científicos y tecnológicos, los algoritmos serán uno de los ejes, las herramientas que están transformando –a veces de manera imperceptible–, el mundo tal como lo conocemos hasta ahora. Pero, ¿qué son los algoritmos?

Hace poco, en un video del canal TED, especializado en los avances tecnológicos más recientes, un ponente explicaba la definición de “algoritmo”: se trata, decía, de “una detallada explicación de la solución de un problema”. No habíamos encontrado hasta ahora una definición más sencilla de este concepto y de todo lo que significan las ciencias de la información, las ciencias de los datos, como podrá notarse.

Éstas son nuevas áreas de conocimiento (*Data Knowledge*), que registran un vertiginoso crecimiento en vías de la automatización de casi cualquier proceso ligado a la vida cotidiana. Estas áreas de conocimiento representan múltiples especializaciones, como la robótica, la informática, la biotecnología y la geomática, entre otras muchas.

En este texto vamos a tratar específicamente lo relacionado con el desarrollo de la informática, en un área específica dirigida hacia la automatización de procesos mediante técnicas que sugieren un verdadero “aprendizaje de las máquinas” (*Machine Learning*).

El objetivo aquí es llamar la atención sobre un tema que requiere aún del trabajo legislativo en el corto o mediano plazo.

Para ambientar al lector, los cifras sobre el uso de las tecnologías punta en el manejo de varios sectores puede realizarse con detalle en la página “Data Never Sleep 6.0” (“Los datos jamás duermen”, una imagen encontrada en dicha página web fue utilizada en la portada), donde se encuentra un conjunto de infografías en inglés sobre esta “ciencia de los datos” y sus aplicaciones en la sociedad contemporánea (consultar aquí).

El tema de la automatización, la increíble velocidad en el procesamiento de datos con simples algoritmos es por lo demás apasionante. Su conocimiento está cada vez más valorizado en el mundo del desarrollo científico y tecnológico en diferentes áreas de la vida social, pero al mismo tiempo es fuertemente desconocido aún. Conocerlo es también el sueño de muchos operadores, administradores, tomadores de decisiones, que ven la panacea en relación con lo aburrido de la repetición de procesos cotidianos. En México existe aún poca legislación al respecto. El “comercio algorítmico” (que tratamos más tarde como “tradeo algorítmico”, las criptomonedas o los procesos automatizados a través de grandes desarrollos informáticos son aún elementos que requieren de legislaciones en el corto o mediano plazo, en México igual que en diferentes países.

El *Machine Learning* o aprendizaje automático es la rama de la inteligencia artificial que dota a las máquinas de la habilidad de “aprender” a partir del análisis de datos con el fin de identificar patrones y apoyar en la toma de decisiones con la mínima intervención humana; personas y máquinas trabajan de la mano.

Así, esta habilidad permite optimizar los procesos del día a día, hasta el punto de que una máquina puede hacer una llamada para reservar una mesa en un restaurante sin que el interlocutor se dé cuenta de que no está hablando con una persona.

Para ilustrar al lector respecto a lo que se refieren estos “procesos automatizados”, podemos aportar algunos ejemplos de la aplicación de la automatización de procesos que son más o menos conocidos: el envío masivo de e-mails (o la detección de *Spam*), los nodos que activan llamadas múltiples (*Calls Centers*), la selección de productos en un catálogo disponible en línea, la predicción del clima, el autocompletado de un texto; los servicios de voz automatizada (*Siri* o *Alexa*), los servicios de voz de Apple o Amazon, así como el *Google Home*, etc., o los sorprendentes autos “inteligentes” (véase un video al respecto aquí).

Cada vez es mayor la recurrencia que hacemos en la vida cotidiana a modos de operación automatizada sin darnos cuenta. Para ello se utilizan algoritmos de inteligencia artificial o de una rama de ellas que es el *Machine Learning* (“aprendizaje de las máquinas”) (véase el **recuadro**).

Su uso es poco perceptible, aunque existe ya una abundancia de ejemplos. Los datos pueden tener una enorme utilidad en las decisiones de la vida cotidiana para empresas, gobiernos o grandes conjuntos sociales. También pueden tener casos de usos perversos para la vigilancia o el control de masas poblacionales, o el fraude bancario que enseguida veremos.

Dos tecnologías que están cambiando el mundo

Blockchain y la *Inteligencia Artificial* (AI) son dos tecnologías que actualmente han tenido popularidad en internet, particularmente en las redes sociales. Estas dos se han mezclado para crear nuevas herramientas de desarrollo de procesos en la sociedad contemporánea.

Por un lado, *Blockchain* intenta resolver los problemas del "doble gasto" (fraudes en el sistema bancario tradicional) y contar con un sistema gubernamental transparente (los gastos realizados podrán ser registrados en una base de datos).[1] Los nuevos mecanismos económicos a través de los cuales se realizan transferencias de capital utilizando como medio *Blockchain*, son movimientos sin regulación que no respetan fronteras definidas por los gobiernos. En el *Blockchain*, con el tradeo algorítmico se intenta predecir los movimientos de un mercado nuevo (que tiene 10 años, desde la aparición del *Bitcoin*). Se trata de una macroeconomía que trabaja "las 24 horas del día". El *tradeo* algorítmico no es algo nuevo, algunos estudios indican que el *Flash Crash* de 2010 fue causado por *tradeo* realizado por algoritmos creados con *Quants*, usando técnicas de *Inteligencia Artificial*.[2]

Este tipo de eventos son pocos en la historia, pero sus resultados impactan a la economía global. Un algoritmo comenzó a vender millones de contratos futuros en la bolsa de valores con montos que alcanzaron los millones de dólares, y esto comenzó a reflejarse en una caída abrupta en los precios, aunque su recuperación fue pronta, después de 20 minutos.

Por otro lado, tenemos aplicaciones de *Inteligencia Artificial* orientadas a la predicción y a la automatización de procesos. La *Inteligencia Artificial* existe desde la década de 1960,

[1] El problema del "doble gasto" es un tema que ha sido revisado y estudiado por distintos investigadores, puede consultarse, por ejemplo, en: https://www.amazon.com/Truth-Machine-Blockchain-Future-Everything/dp/1250114578. Otra referencia puede encontrarse en: https://www.amazon.com/Bitcoin-Standard-Decentralized-Alternative-Central/dp/1119473861.
[2] Graham Bowley,"Lone $4.1 Billion Sale Led to 'Flash Crash' in May", *The New York Times*, 1 de octubre de 2010 (consulta: 22 de julio de 2019).

aunque durante los últimos años hemos tenido un gran auge en sectores como el financiero para tratar de prevenir fraudes, por ejemplo. Se trata de métodos matemáticos a través de los cuales se llega a predicciones. Se utiliza para la programación de tareas repetitivas, por ejemplo los precios de los mercados internacionales o muchos de los procesos que regulan la vida cotidiana en las grandes ciudades. Actualmente la especulación es creada por algoritmos que trabajan de manera aislada. El *tradeo algoritmico* (también llamado *tradeo* automatizado o *tradeo* en caja negra)[3] utiliza *software* que ejecuta una serie de instrucciones definidas por los creadores.

El *tradeo*, en teoría, puede generar ganancias a una velocidad y frecuencia que un *trader* humano (corredor de bolsa) jamás podría alcanzar. Veamos con más detalle el *Blockchain*.

¿Qué es el *Blockchain*?

El concepto definido en forma simple indica "una cadena de bloques". Dentro de los bloques se almacenan datos de transacciones que son firmadas criptográficamente a través de un proceso llamado "prueba de trabajo" (*Proof of Work*, **PoW**).[4]

La "prueba de trabajo" (**PoW**) es el protocolo introducido por *Bitcoin*, el cual hace posible que miles de nodos se "pongan de acuerdo" o generen un consenso entre sí para definir el estado de la red. Es decir, los nodos que forman parte de la construcción del consenso son llamados mineros (*mining*). De esta forma, cuando un "minero" es capaz de proponer un nuevo bloque y lo puede trasmitir es llamado "minero proponente". De allí que la **PoW** se trata de un número especial que demuestra que el minero proponente encontró la solución a una compleja operación matemática.

La función de esta "minería" no es crear nuevos *Bitcoins*, aunque ésta es una de sus consecuencias. Su función real es la de proveer seguridad y validación a todas las transacciones contenidas en los bloques de acuerdo con reglas de consenso. La

[3] Una traducción de "tradeo" podría ser mercadeo, o simplemente comercio.
[4] La criptografía es la técnica que protege documentos y datos**.** Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet**.**

generación de nuevos *Bitcoins* representa un mecanismo de recompensa que reciben los "mineros" por su trabajo.

Actualmente existen distintas cadenas de bloques, públicas o privadas. Los usos que se les han dado hasta ahora son el almacenamiento de registros de salud, seguimiento de la cadena de suministro de mercancías y, el más famoso de todos, las criptomonedas (el *Bitcoin* es una moneda de este tipo).

> ***Blockchain*** es un libro abierto y distribuido que puede registrar transacciones entre dos partes de manera eficiente y de forma verificable y permanente. El libro mayor también se puede programar para activar transacciones automáticamente. Con ***Blockchain*** podemos imaginar un mundo en el que los contratos están incrustados en código digital y almacenados en bases de datos transparentes y compartidas donde están protegidas contra la eliminación, la manipulación y la revisión. En este mundo, cada acuerdo, cada proceso, cada tarea y cada pago tendrían un registro digital y una firma que podría identificarse, validarse, almacenarse y compartirse. Es posible que ya no sean necesarios intermediarios como abogados, corredores y banqueros. Los individuos, las organizaciones, las máquinas y los algoritmos harían transacciones e interactuarían libremente entre ellos con poca fricción. Este es el inmenso potencial de ***Blockchain***. [1]

En suma, la convención es que la cadena de bloques más larga –más pesada– siempre refleja 'la verdad' del estado de la red, debido a que es probable que en ella se haya invertido más trabajo –capacidad informática que consume mucha energía eléctrica– para resolver las complejas operaciones matemáticas. Las cadenas más cortas –o livianas– serán rechazadas.

El *Blockchain* y el "doble gasto"

Como el término lo sugiere, el "doble gasto" es gastar el mismo dinero en dos ocasiones. Este tipo de problemas se generan porque en la actualidad el dinero que utilizamos son registros almacenados en una base de datos centralizada y gobernada por los bancos.

Miremos el siguiente ejemplo. Antes, cuando uno iba a la tienda más cercana compraba, por ejemplo, una despensa con 500 pesos en moneda o en billetes. Tan pronto se realizaba el pago, la tienda almacenaba ese dinero en sus registros, por lo que nadie podía volver a usar dicho dinero para el mismo fin, salvo al robarlos físicamente de dicha tienda.

En cambio, con el dinero digital la situación se ha vuelto mucho más complicada, o más fácil, si se quiere. Cuando se realiza una transacción con dinero digital, se está enviando esa transacción a todos los nodos que están en la red (los nodos son computadoras que corren el *software* en el cual la moneda está soportada). Esos nodos necesitan recibir y confirmar la transacción, lo cual toma tiempo. Entonces el problema que se presenta es el siguiente: una persona X puede copiar la transacción y reenviarla a dicho nodo antes de que haya sido confirmada por la red; eso es lo que se llama “doble gasto”. La pregunta que aquí intentará resolver el algoritmo es: ¿cómo asegurar cuál transacción es la genuina?

Imagen 1. El funcionamiento del Bitcoin

Fuente: Tomado de "¿Es el Bitcoin la moneda del futuro? En línea.

La invención revolucionaria del *Bitcoin*

Antes de la invención del *Bitcoin* el dinero digital fluía a través de internet. Era todo monitoreado y controlado por los bancos y las instituciones financieras, tal cual y como ocurre hoy en día. El problema de que los bancos actúen como mediadores en las disputas financieras es que las transacciones pueden ser revertidas si la disputa ocurre. Esto lleva a costos más grandes y a desacelerar el tiempo de las transacciones. El *Bitcoin* resuelve estas limitaciones al crear un sistema basado enteramente en pruebas criptográficas, en lugar de estar fundado en la confianza. En efecto, ofrece una manera revolucionaria de que exista el mercado bancario sin los bancos (véase la **Imagen 1**).

Las operaciones bancarias o las operaciones financieras en general cambian de significación con estas tecnologías. El resto de la sociedad y los gobiernos están en poder manejar y someter esto a regulaciones nacionales e internacionales, es decir, que tengan un funcionamiento apropiado para evitar lo que ocurre en algunos casos de operaciones fraudulentas o una economía supranacional que está lejos aún de ser regulada.

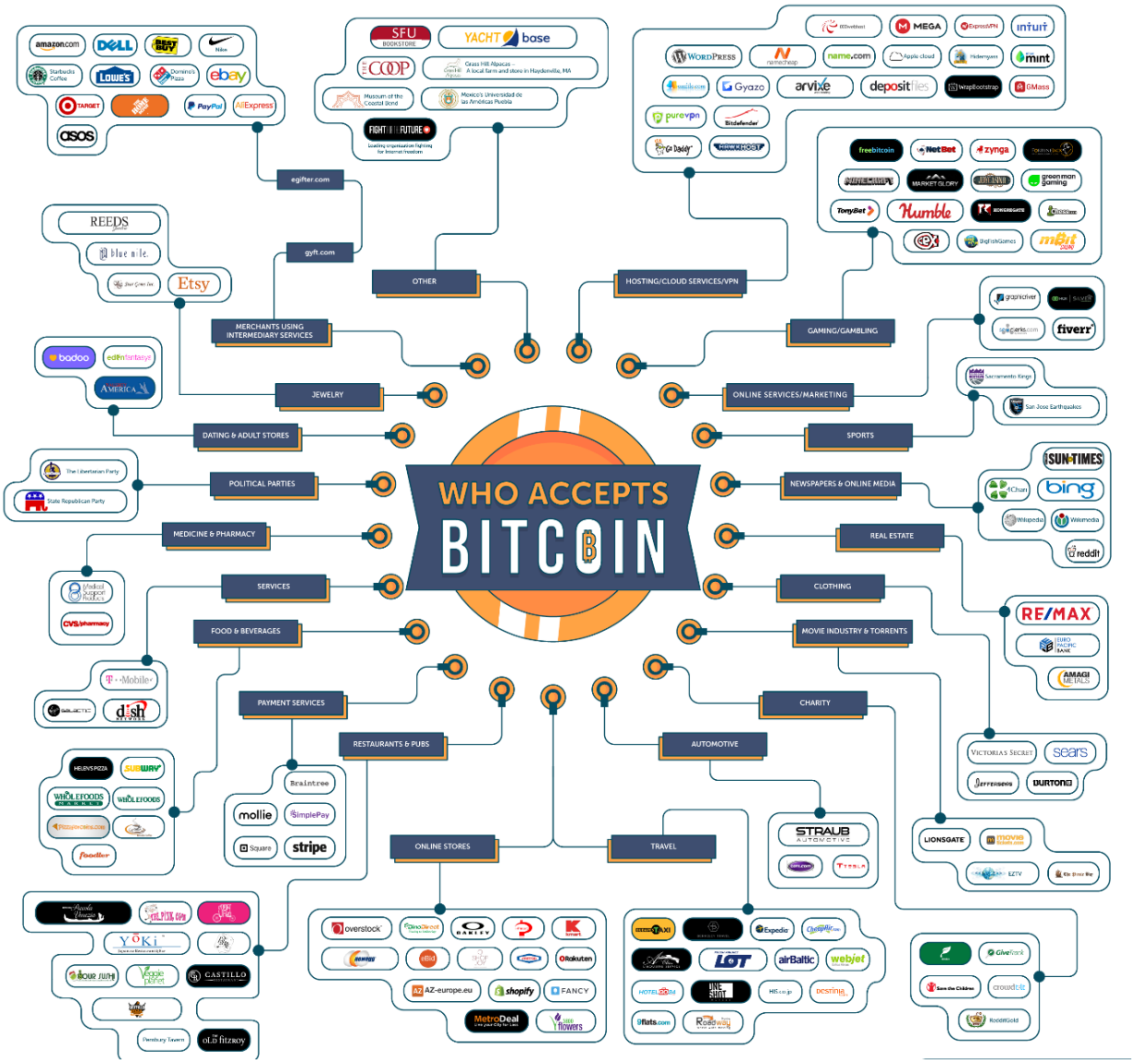
Consideración general

La revolución de las tecnologías y la automatización de los procesos es un fenómeno mundial, presente en la vida cotidiana y que ocupa cada vez mayor espacio en las discusiones del futuro de la economía mundial. Aquí se ha hecho apenas una revisión somera de elementos que definen dos procesos: *Machine Learning* e Inteligencia Artificial.

Igualmente se han explorado los fenómenos económicos definidos por algoritmos, a partir de la aparición en el mundo de las criptomonedas, específicamente del Bitcoin, que tiene cada vez más aceptación en las transacciones (**Imagen 2**). La gran cuestión aquí es que dichas **criptomonedas** permiten imaginar un mundo sin los bancos que, aunque todavía parece imposible, está ya definiendo transacciones millonarias alrededor del mundo.

En todo caso, es evidente que en México aún falta mucho trabajo legislativo por hacer al respecto. El “comercio algorítmico”, las criptomonedas o los procesos automatizados a través de grandes desarrollos informáticos son aún elementos que requieren de legislaciones en el corto o mediano plazo.

Imagen 2. “¿Quién acepta el Bitcoin?”



Fuente: tomado de “Who Accepts Bitcoin”. En línea.