Bitcoin, criptomonedas, blockchain y regulación

Por Carlos Fernández

GRUPO PRIDES

2022

¿Qué es el Bitcoin?

Es la primera criptomoneda mundial. Funciona gracias a la primera red blockchain pública mundial.

Permite que usted envíe o reciba un “valor” de cualquier persona en el mundo, usando nada más que un computador y una conexión a internet.

¿Cómo se asegura el Bitcoin en el Blockchain?

El Bitcoin está asegurado por criptografía.

Criptografía. La ciencia de usar teorías matemáticas y computación para codificar y decodificar información.

¿Porqué es revolucionario el Bitcoin?

Porque a diferencia de cualquier otra herramienta para enviar dinero por internet, funciona sin la necesidad de “confiar” en un intermediario.

La ausencia de una empresa intermediaria significa que Bitcoin es la primera infraestructura “pública” mundial de pagos digitales.

Pública significa que esta disponible para todos y no es propiedad de ninguna entidad individual.

¿Cuáles otras infraestructuras existen?

- Internet que es una infraestructura pública para la información, para los sitios web, para los correos electrónicos.
- Pero la única infraestructura pública de pagos que tenemos es el efectivo, es decir el papel moneda, pero solo funciona en transacciones cara a cara. Antes de Bitcoin si usted quería pagarle a alguien en forma remota por el teléfono o por internet usted no podía usar una infraestructura pública de pagos, solo podía hacerlo mediante un banco privado.
- El Banco privado abría sus libros y agregaba un registro en el libro mayor (ledger) para debitar su cuenta y acreditar la de la otra persona.
- Si usted y esa persona no tenían las cuentas en el mismo banco entonces era necesario utilizar varios bancos y hacer varios registros en varios libros mayores en el proceso. (SWIFT)

¿Qué es el blockchain en Bitcoin?

- En Bitcoin el libro mayor es un blockchain público.
- Cualquiera puede agregar un registro en ese libro mayor para transferir sus bitcoins a otra persona.
- Cualquiera, sin importar su nacionalidad, raza, religión, género, sexo y solvencia crediticia, puede, sin absolutamente ningún costo, crear una dirección de bitcoin para recibir pagos digitalmente.
- Bitcoin es la primer moneda pública accesible globalmente.

¿El Bitcoin es perfecto?

- No lo es.
- Tampoco lo era el email cuando fue inventado en 1972.
- Tampoco es el mejor dinero, todavía no es aceptado en toda parte, no se usa a menudo para cotizar precios y no es siempre un depósito de valor estable.
- Pero está funcionando y el solo hecho de que funcione sin intermediarios de confianza es extraordinario, es un logro de las ciencias de la computación y será tan significativo para la libertad, la prosperidad y progreso humano como lo fue el nacimiento de la internet.
- Bitcoin es solo el comienzo. Si podemos reemplazar la infraestructura privada de pagos, podemos también reemplazar otros cuellos de botella privados.

¿Pero porqué cambiar?

- ¿ Porqué querríamos construir más infraestructuras públicas?
- ¿Porqué deberíamos aceptar el blockchain en lugar de intermediarios privados?
- ¿Porqué deberíamos tolerar sus ineficiencias e invertir en hacerla mejor?
- ¿Porqué deberíamos querer que los pioneros de estas tecnologías se queden en nuestros países y no se vayan a otros?
- Simple… porque los intermediarios privados que hoy proveen infraestructura crítica, pero que son dueños de la misma, son cada vez menos, más grandes y más poderosos y sus fallas son cada vez más graves

¿Hay ejemplos de esas fallas?

En Estados Unidos más de 143 millones de números de seguro social fueron expuestos por los hackers debido a una fuga de información de Equifax.

La red SWIFT ha tenido cientos de millones de dólares en transacciones fraudulentas debido a bancos hackeados en Bangladesh, Vietnam, Rusia y otros países.

El BFI sospecha que los hackeos más grandes de esos bancos fueron hechos por hackers de Corea del Norte.

Empleados de bajo nivel corruptos en el Punjab National Bank de la India fueron capaces de certificar mensajes SWIFT fraudulentos y se robaron 1.8 billones de dólares, el robo electrónico de bancos más grande de la historia, el robo de banco más grande de la historia.

¿Hay más?

- Muchos más…
- En octubre de 2016 un estimado de 1.2 millones de dispositivos conectados a internet fueron hackeados y convertidos en una red “robot” que por varias horas volvió innacesibles sitios web prominentes a lo largo de Europa y America del Norte incluyendo CNN, Fox News, New York Times y Wall Street Journal.
- Cada vez más máquinas físicas son conectadas a la internet a través de servidores que son propiedad y son mantenidos por intermediarios privados de confianza en lo que se llama la Internet of Things.
- Marcapasos del St Jude Hospital han sido hackeados, monitores de bebés han sido hackeados, autos Jeep han sido hackeados al extremo de ser gobernados remotamente y sacados del camino.
- En octubre de 2021 hackers rusos atacaron la red eléctrica Colonial en USA.

¿Algún ejemplo reciente y cercano?

- Si claro…
- Hace unos meses el Ministerio de Hacienda de Costa Rica y la Caja Costarricense de Seguro social fueron hackeados. Los empresarios no pudimos pagar los impuestos en las fechas establecidas, los pacientes no pudieron ser atendidos en sus citas, se suspendieron cirugías, hospitalizaciones.
- Varios meses después aún no hemos podido restablecer los sistemas al 100%.
- El inventario de los datos que se perdieron para siempre, el costo de las reparaciones y de los datos perdidos para la sociedad no se conocen aún pero de seguro son enormes.
- ¿Y podremos evitar el siguiente ataque o ataques a otras empresas e instituciones?…lo podemos atenuar…pero no podemos asegurar que no volverá a pasar.

¿Pero porqué sucede esto?

- Por los puntos únicos de fallo.
- Todas esas vulnerabilidades son inevitables en sistemas que tienen un punto único de fallo.
- No importa si el punto único de fallo es una empresa o el gobierno, lo que importa es que no debería existir un punto único de fallo.
- Estos puntos únicos de fallo ya existían antes de la internet. Si usted quería transmitir un mensaje tenía que acudir a una de las tres cadenas de televisión de los Estados Unidos o a un puñado de periódicos.
- Las empresas privadas son esenciales pero ninguna estructura crítica debería depender de una o dos empresas.
- El Internet eliminó los puntos únicos de falla en la infraestructura de comunicaciones y marcó el inicio de la competencia entre nuevas corporaciones de medios que se construyeron sobre esa infraestructura pública.

¿Pero estamos condenados o esto se puede evitar?

- El blockchain puede igualmente eliminar la intermediación en los pagos y en la infraestructura IoT.
- La tecnología aún no está preparada para responder a todas las preguntas pero es nuestra mejor esperanza.
- Es por eso que al igual que para la internet en los 90’s necesitamos un marco regulatorio blando y una política pro innovación para garantizarnos que estas innovaciones prosperarán en nuestros países para el beneficio y seguridad de todos los americanos.

La economía del Bitcoin

¿Cómo surgió el Bitcoin?

- En 2008 durante la crisis financiera. Satoshi Nakamoto (un pseudónimo) escribió un ensayo de tan solo nueve páginas que denominó “Bitcoin: Un sistema de Efectivo Electrónico Usuario-a-Usuario”. Satoshi mismo transformó ese ensayo en un programa de computadora que hoy conocemos como Bitcoin.

¿Cuánto vale el Bitcoin?

En el 2010 valía US$ 0,003. Se usó para comprar dos pizzas por 10.000 BTC. US$30.00 en ese momento)

Esas dos pizzas costaron entre US$240 y US$250 millones al precio actual del BTC.

¿Qué pasó con Satoshi?

- Nadie sabe quien es o fue Satoshi. Desapareció en el 2011.
- Se dice que una billetera que él usaba tiene 1 millón de Bitcoins que no se han movido desde que se crearon.
- Cuando el Bitcoin alcanzó su máximo histórico de US$68.000 en el 2021, el millón de BTC de Satoshi lo colocaron entre las 20 personas más ricas del mundo.

¿Cómo se emiten nuevos Bitcoins?

Lo emite un programa de computadora.

Las transacciones se agrupan en un bloque que se pone a disposición de mineros para su validación.

Los mineros usan computadoras super potentes y que consumen mucha electricidad.

El minero que resuelve primero un acertijo matemático se gana los bitcoins.

¿Cuál es la capacidad de minería del Bitcoin?

- Al 10 de agosto habían más de un millón de mineros.
- La capacidad de procesamiento de los mineros es astronómica, son 201.87 Exahashes/s. EH/s = 1.000.000.000.000.000.000 de hashes por segundo (un millón de millones de millones en español es decir un trillón en español o un quintillón en inglés).
- Un hash = operación matemática compleja.
- Solo con el 51% de la capacidad de cómputo se puede hackear.

¿Qué tanto ha avanzado la adopción de monedas digitales?

- En Estados Unidos son parte de los fondos de pensión y se usa para ETFs con autorización de la SEC
- Ya es **moneda de curso legal en El Salvador.**
- En 2021 se volvió institucional. Microstrategy, Tesla
- Ya hay monedas virtuales creadas por bancos centrales. Dólar de Arena, Yuan Digital, eNaira.

¿Qué dicen de las criptomonedas algunos líderes mundiales en materia financiera?

- Christine Lagarde dice que no valen nada pero que deben ser registrados (Mayo de 2022).
- Gary Gensler, presidente de la SEC: en junio 2022 dice que es una “mercancía”. En agosto: que son “valores” no registrados y se basa en la prueba del pato (Si camina como un pato…)
- Warren Buffet dice que es “veneno de ratas al cuadrado”.
- Bill Gates dice que el Bitcoin está 100% basado en la teoría del “tonto mayor”
- Otros dicen que es un esquema Ponzi.
- Y otros como Elon Musk lo atacan por su excesivo consumo de electricidad.

¿Qué dicen otros empresarios líderes?

- Michael J. Saylor CEO de Microstrategy ha comprado más de 121.000 Bitcoins (US$2.9 billones). Dice que es más seguro que el oro.
- Tesla ha comprado más de 40.000 Bitcoins (US$960 millones) y Elon Musk dice que es mejor que el efectivo en el balance.
- Otros dicen que el Bitcoin es la invención más importante de la última década.
- Otros hablan de la Internet del dinero: dicen que el Bitcoin nos permitirá intercambiar dinero a nivel global.
- Otros indican que aún no se ha develado su verdadero potencial.

¿Qué dicen los “fundamentalistas” del Bitcoin?

- Atacan la emisión de dinero por antidemocrática. Que la ventaja del BTC es que no puede ser emitida por el Estado.
- Que la emisión fiat financia el déficit de países grandes.
- Que la emisión de fiat se usa para financiar las guerras sin usar los impuestos, que produce inflación y empobrece al mundo entero.
- Que el dólar se devalúa mientras que el BTC vale más ahora que antes.
- Que el fiat no tiene valor intrínseco tampoco, pues los billetes son solo papel. Que su valor descansa nada más en la confianza que la gente tiene y en las leyes que obligan a aceptarlo para impuestos y pago de deudas.
- Que Bitcoin y Ethereum no son “valores” que deban ser registrados ni regulados pues no cumplen la parte de la prueba de “Howey” que dice que un “esquema de financiamiento es un valor registrable si el retorno de los inversionistas depende del trabajo de un grupo pequeño de personas”.

¿Sirve el Bitcoin para hacer pagos como propuso Satoshi?

¿Por qué la gente sigue comprando y reteniendo los Bitcoins a pesar de sus fluctuaciones, su poca eficiencia en pagos y los comentarios tan negativos?

Lo usan para defenderse de la inflación.

El Bitcoin es deflacionario. Solo se emitirán 21 millones de Bitcoins, la emisión es cada vez más pequeña. Ya se han emitido 19 millones de Bitcoins solo quedan 2 millones. El ultimo se emitirá en el 2140, dentro de 118 años.

La gente lo compra hoy para acumular valor pues piensa que valdrá mucho más en el futuro. La historia del Bitcoin les da la razón como se muestra a continuación.

¿Qué tan buena inversión ha sido el Bitcoin ?

Bitcoin & Traditional Assets ROI (vs USD)

	Bitcoin	Gold	S&P 500
1 year:	+288%	-13%	+32%
2 year:	+301%	+15%	+53%
3 year:	+638%	+43%	+56%
4 year:	+1,195%	+35%	+81%
5 year:	+7,706%	+29%	+103%
6 year:	+16,892%	+56%	+112%
7 year:	+8,077%	+32%	+128%
8 year:	+47,188%	+31%	+162%
9 year:	+386,618%	+7%	+215%
10 year:	+437,171%	-0.25%	+277%

(Data Source: Messari.io, bitcoincharts.com)

1) Datos a Noviembre del 2021

¿Qué es el blockchain o cadena de bloques?

Es el corazón de Bitcoin. Es un libro mayor distribuido (no centralizada), los datos se organizan en bloques que se encadenan por lo que su orden no puede ser alterado.

La criptografía garantiza la inmutabilidad de los datos.

El hackeo es imposible pues se requieren capacidades de computo astronómicas.

Es descentralizado. No hay una institución o empresa que lo controle, lo modifique o niegue el acceso.

La seguridad es mayor que la de cualquier base de datos.

La transparencia de los datos en un blockchain está garantizada pues cualquiera puede ver los datos.

¿Para que podemos usar el blockchain?

Para fortalecer la democracia. Con un blockchain se puede hacer un sistema electoral que impide el fraude, brinda transparencia, evita la discriminación, es accesible y de bajo costo.

Para mejorar los sistemas de pagos. Los bancos centrales puedan emitir monedas digitales.

Para mejorar la identificación de las personas. Cédulas, licencias, pasaportes, certificados de vacunación, etc. sin que ni el Estado ni los hackers puedan alterar los datos.

¿Para que otras cosas podemos usar un blockchain?

- Para logística.
- Para propiedad intelectual.
- Para tokenizar propiedades.
- Para cualquier otra cosa en la que sea necesario eliminar el punto único de fallo y que además sea inmutable, transparente, validado por varias personas, empresas o países usando consenso y no una autoridad central o tercero de confianza.

¿Cuáles son los riesgos de las criptomonedas para el lavado de dinero y financiamiento del terrorismo?

- Las transacciones son anónimas así que se pueden usar para comercio ilícito (Lavado, terrorismo, narcotráfico, etc.).
- Michael Camdessus, ex director gerente del FMI, ha calculado la magnitud del lavado de dinero entre un 2 y un 5% del producto bruto interno mundial que en 2022 se estima en 104 Trillones. Es decir el lavado de dinero será de entre 2 y 5 trillones de dólares (en este caso hablamos de trillones en inglés es decir 1.000 billones de dólares).
- Si consideramos que se estima que el total de transacciones de lavado de dinero que se hacen utilizando criptomonedas es de un 0,62% y el monto de esas transacciones se estiman entre 8 y 30 billones de dólares, entonces entre un 0,4 y un 0,6% (menos de un 1%) del lavado se hace usando cripto.
- No olvidemos que las transacciones en cripto, si bien son anónimas, quedan registradas en el blockchain y eso es algo que puede desestimular a los delincuentes a usar las criptomonedas para el lavado de dinero.

¿Cuáles son los desafíos de las regulaciones para Fintechs?

Es una industria nueva, poco comprendida y altamente cambiante. Las regulaciones se enfrentan al desfase y la complejidad.

Los mercados y las industrias son imperfectos por lo que es necesario regularlos para hacerlos justos, transparentes y evitar los riesgos sistémicos.

Las empresas son aliados de los reguladores. No quieren estafas, hackeos, engaños ni actividades ilegales ni muchos menos fallas sistémicas que afecten la economía de un país o de todo el mundo.

La regulación debe ser equilibrada. Consumidores vs innovación.

Debe ser coordinada a nivel global. Las tecnologías son trans fronterizas.

¿Cómo estamos en América Latina en regulaciones de Bitcoins y Fintechs?

Bahamas. Tiene una CBDC.

El Salvador. El Bitcoin es moneda de curso legal.

Panamá. Ley 697 que regula los criptoactivos y el uso de blockchain, vetada en junio pasado. Hay un banco que acepta depósitos en criptomonedas.

México. Ley Fintech publicada en 2018. Marco “permisivo” para la empresas que manejen criptoactivos.

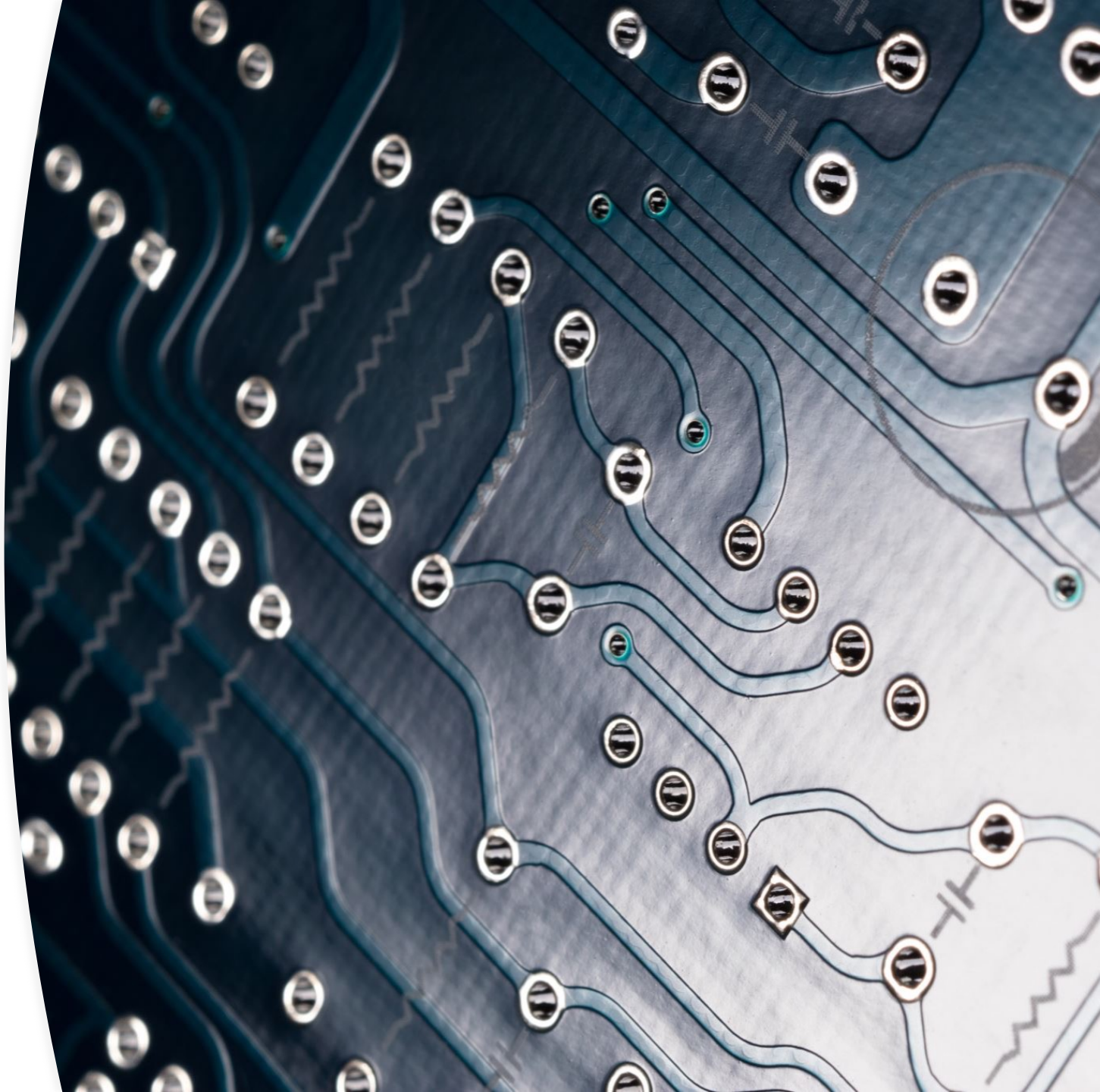
Brasil. Ley Bitcoin en proceso y prevista para ser aprobada este año.

¿Que tanto ha avanzado la regulación en USA?

- La principal discusión es definir que son las criptomonedas para determinar si y quien las regula.
- Para la SEC es un valor no registrado.
- Para la Reserva Federal no es una moneda legalmente establecida.
- Se permite la minería (hoy es el país con más mineros en el mundo).
- Las empresas pueden incluir criptomonedas en sus balances y pagan impuestos sobre las ganancias de capital.
- Algunos estados y ciudades están promoviéndose como “amigables” para la industria cripto (Miami por ejemplo).

Conclusión

- Conclusión: Las criptomonedas como el Bitcoin y el Ethereum llegaron para quedarse. El blockchain es una tecnología que nos permite evitar los riesgos de los sistemas centralizados y sus puntos únicos de falla. La regulación es indispensable, pero debe hacerse con la ayuda de las empresas y procurando no afectar negativamente la innovación.



Muchas gracias a todos y muy especialmente al Diputado Leandro Avila, Secretario Alterno de Comisiones y al Dr. Elias Castillo, Director Ejecutivo por la invitación.

Reconocimiento:

Parte de los conceptos e ideas de esta presentación fueron tomados de la comparecencia, ante el comité del Senado de los Estados Unidos de Banking, Housing and Urban Affairs, del 2018 del Señor Peter van Valkenburg Director of Research de Coin Center.

Este es el link a al video de esa audiencia:

https://www.c-span.org/video/?452837-1/senate-banking-panel-explores-cryptocurrencies-blockchains