

# Artículos BBO

Esta sección contiene una colección de todos los artículos escritos por miembros de la comunidad y publicados por BBO. Comuníquese con nosotros si desea escribir algo para esta sección.

- [Store of Value](#)
- [Bitcoin y la Macro](#)
- [Systems falln't](#)
- [Cypherpunks | El origen y la filosofía detrás de Bitcoin](#)
- [Bitcoin ya existe](#)
- [Rutas de distribución e incentivos](#)
- [Situacionismo](#)

# Store of Value



[Begleri \(@begleristirner\)](#)

Publicado: 02/08/2022

Tags: Economía / Política / Hyper-bitcoinización

Bien, tengo problemas con el concepto de Store of Value. Puede que sea por mi opinión sobre esa creencia de la mayoría de Bitcoiners de creer que el proceso de adopción de Bitcoin sigue unas reglas al pie de la letra. Me gustaría culpar de ello a la interpretación que ha hecho Saylor de The Bullish Case of Bitcoin y a la influencia de este en el ecosistema Bitcoin.

En el libro se expone que un bien monetario no puede convertirse en método de pago antes de ser ampliamente valorado y considerado depósito de valor. Muchos lo han tomado al pie de la letra y han criticado que se esté usando Bitcoin como método de pago con unos precios basados en la paridad Fiat. Si bien es cierto que un bien monetario que no sea valorado por gran parte de la

población no puede convertirse en método de pago, que se use como método de pago solo puede ayudar a su adopción, nunca la perjudica.

Para poder expresar bien la idea quisiera aclarar un par de conceptos que la mayoría de plebs no tienen interiorizados. Lo primero es aceptar que la hyperbitcoinización supone la caída de la propiedad privada como la entendemos. Esto es así debido a la pérdida de la violencia blanda por parte del estado. Existen la violencia blanda (confiscación del dinero) y la violencia dura (monopolio de la fuerza) para mantener la propiedad privada, base de la organización de nuestro modelo. Con un dinero inconfiscable abandonamos la propiedad privada enfocada desde un marco legal y la entendemos desde un enfoque Stirneano (Max Stirner). Ya no es un derecho natural del individuo sino que se considera que es de mi propiedad aquello que poseo y puedo defender. La violencia blanda era la que permitía al estado tener subyugada a la población y el monopolio monetario se encargaba de brindarle recursos ilimitados para ejecutarlo.

Lo segundo que en un escenario de hyperbitcoinización, el estado desaparece automáticamente. Pues si no tiene poder confiscatorio, por definición ya no es el estado. Aunque nos imaginemos a los boomers contribuyendo voluntariamente a una forma de gobierno local, estarán haciéndolo de forma voluntaria a cambio de recibir unos servicios: protección, sanidad, carreteras...etc. Eso, queridos amigos, se llama empresa privada y tiende a quebrar si no es rentable en el largo plazo. La desaparición del estado como tal supone la privatización forzosa de la seguridad y del poder militar. Por lo que al solo existir la violencia dura de forma privada, deja de tener validez la Ley escrita en los tiempos en que aún existía el estado y entramos a un escenario donde la fuerza manda y ejecuta la voluntad de los agentes privados. En ese momento, dejan de tener validez el registro de la propiedad. Por mucho que un terrateniente argumente que firmó unos documentos que acrediten su propiedad, si no tiene recursos para defenderla no lo será de facto. En algunos países como España donde los precios de las viviendas se han disparado, la ocupación de los inmuebles se ha vuelto un conflicto. Sin una policía desalojadora, los propietarios están desarmados frente a los violentos ocupas que no respetan su documento firmado por la Ley. Esto sin mencionar que sin un estado, ya no existe la narrativa central que otorgue legitimidad a ningún documento.

En el momento en que los terratenientes dejan de tener el poder suficiente como para exigir unos cobros a sus inquilinos de forma periódica, estos pierden la razón de cumplir con sus pagos. Algunos podrán alegar que la mayoría lo seguirá haciendo por tradición, buena fe o civismo pero la verdad es que si estos cumplen con esos pagos de forma voluntaria será debido a la intimidación. Marx ya señalaba que los terratenientes eran el problema pero no había forma de acabar con su poder sin un bien monetario inconfiscable. En un escenario donde solo existe la violencia dura, la parte dominada se puede sentir más tentada a armarse y revelarse que cuando no podía hacer nada frente a la violencia blanda y la violencia dura suponía un riesgo muy alto a sumir. Por no hablar de que un dinero universal e inconfiscable iguala las condiciones entre las partes, permitiendo que la parte dominada pueda acceder a armas con mayor facilidad.

La hyperbitcoinización es inevitable, debido a sus propiedades Bitcoin se impondrá como moneda de reserva mundial. El problema de muchos plebs es pensar que van a coexistir diferentes formas de dinero, cuando en verdad sabemos que a largo plazo solo la forma de dinero más dura sobrevivirá. Demasiados autores han tratado este tema por lo que no entraré en detalle, pero me

atrevería a decir que esto ha sido legado de Friedrich Hayek por su libro La Desnacionalización del Dinero. Entonces tenemos claro que en el largo plazo Bitcoin se impondrá como unidad de cuenta y los productos y servicios que haya en el mercado serán expresados en sats. Es actualmente que expresamos los precios de dichos bienes y servicios en dólares por su papel de moneda de reserva mundial y sacamos la paridad en Satoshis. Dicha paridad la obtenemos a partir del precio de Bitcoin expresado en dólares, el cual depende a largo plazo de una única variable: cantidad de bitcoin en manos de holders. En el momento en que el presidente de El Salvador aceptó Bitcoin como moneda de curso legal puso al mundo entero en un escenario de Teoría de juegos que incentivaba a los jugadores a acumular el máximo de bitcoin posible. Esto es así porque si hay jugadores como él o Saylor que están comprando bitcoin sin planes de venderlo están vaciando los exchanges. Aceptar Bitcoin como dinero incentiva a cambiar bitcoin por productos y servicios, no a guardarlo para posteriormente volver a venderlo a FIAT. Tenemos por un lado al dólar con problemas de inflación (hiperinflación dependiendo de cuando lea esto) y por otro la forma de dinero más dura que ha existido, Bitcoin. Si los holders están solo comprando y los traders siguen jugando con el precio, vemos como el bitcoin está pasando de manos de traders a holders a medida que más jugadores adopten esta postura, la entrada de República Centro Africana a mitad de 2022 es una demostración de que más jugadores lo están entendiendo. Si sigue la tendencia, no habrá bitcoin en manos de traders y no habrá vendedores, lo que significa que no existirá el precio. Sin fallos en el protocolo de Bitcoin, no parece haber motivo para que los usuarios abandonen la red por lo que asumiremos que esta tendencia se va a mantener y más jugadores adoptarán una posición hold y no de trader.

Entonces la crítica de estar usando Bitcoin como método de pago se basa en que estamos usando bitcoin en unos precios FIAT. Si bien es cierto que no tiene sentido para el que tiene una cuenta FIAT paralela, para el que está all-in es la única opción. Aquellos que usan bitcoin en su día a día están contribuyendo a la posición holder y no a la posición trader ya que esos bitcoins no vuelven al exchange a ser vendidos, por lo que no tiene ningún sentido la crítica más allá de que estos bitcoiners no están empleando bien su bitcoin. Podríamos decir lo mismo de aquellos que holdean el bitcoin en un Hot Wallet, no es lo más inteligente pero al mercado no le afecta. Un pensamiento que te puede llevar a creer que gastar tu Bitcoin no es la mejor opción es el de creer que los precios de los productos y servicios tienden a bajar expresados en una contabilidad Bitcoin. El claro ejemplo es el del pleb que nos enseñó que una Pizza en aquella época podía ser intercambiada por 10.000 bitcoins. Lo mismo pasa si miramos el precio de un Iphone expresado en bitcoin durante los últimos 10 años, vemos que baja a medida que el precio de Bitcoin expresado en dólares sube. Es evidente que la cantidad de bitcoin que hay en circulación y la cantidad de usuarios en el mundo que lo usan sugieren una revalorización al alza del bien monetario, lo que significa que un bitcoin hoy lo puedo intercambiar por menos productos y servicios que en el futuro. Es por eso que vemos como el valor de 1 bitcoin hoy es mayor que al valor de 1 bitcoin en el 2012, es intercambiable por más lo que nos lleva a decir que el valor ha aumentado. El concepto "Store of Value" expresa esta relación. Es por eso que estos críticos de usar bitcoin como método de pago creen que debemos esperar a que los precios de los productos y servicios estén más bajos (precio de Bitcoin se mantenga al alza) para que el valor de este bitcoin sea mayor, siendo la decisión a simple vista más racional.

Debemos sumar a esta creencia el poder de una oferta limitada, lo que nos lleva a un descubrimiento de precios real donde gracias a la competencia los precios tienden a los costes

marginales. Si los precios tienden a la baja a medida que entra más competencia, lo normal sería que nuestro bitcoin pudiera comprar más productos y servicios ahora que los precios caen. Eso permitiría cambiar 1 bitcoin en el futuro por más productos y servicios que en la actualidad, incentivando al ahorro de ese bitcoin. En este caso también se cumple la relación para que el concepto de "Store of Value" tenga sentido. Pero para que eso sea cierto debe haber más competencia que disminuya los precios, de lo contrario la oferta se reducirá y el precio aumentará. Es este escenario el que rompe la relación entre el bien monetario y los precios provocando que pueda cambiar mi bitcoin por menos productos y servicios en el futuro que en el presente, incentivando a consumir en el presente donde el valor del bien monetario es mayor. Es por la existencia de este escenario que me incomoda la palabra "Store", cuya naturaleza es estática creando un símil a acumular, solo tiene sentido al alza. Pero la verdad es que el valor es un equilibrio que varía constantemente dependiendo de los precios, y estos dependen de cómo interactúan oferta y demanda. Quisiera poner un ejemplo donde se podría dar este escenario donde los precios expresados en Sats son mayores en el futuro que en el presente.

Actualmente un refresco cuesta 3000 sats, obtenemos este precio por la paridad del bitcoin al dólar. En un futuro hyperbitcoinizado donde no exista el precio ni unos precios dependientes del dólar, puede que el refresco pueda ser intercambiado por 300 sats o por 30. Esto dependerá de con qué facilidad lleguen los refrescos (oferta) y cuánto estén dispuestos a pagar los consumidores que los quieran (demanda). Queda muy bonito cuando estos precios son inferiores a los actuales porque se cumple la regla y vemos que bitcoin ha servido como "Store of Value" si queríamos comprar refrescos. Pero en un mundo sin estado ni propiedad privada, no sabemos el poder que tendrán los terratenientes, esto dependerá de su capacidad para conservar la propiedad a base de poder militar. En un escenario sin terratenientes, la población tendrá menos obligaciones de pago que cumplir cada mes. Por lo que sin la necesidad de producir para pagar, veremos como gran parte de la población pierde incentivos para generar más allá de lo que necesita para subsistir, dependiendo de sus preferencias. Sin una población necesitada de producir para pagar, se reestructura el mercado laboral pudiendo significar mano de obra más cara en muchos sectores donde veremos subidas de precios en los productos y servicios que ofertan. Si ahora los trabajadores de la fábrica de refrescos no deben pagar un alquiler a fin de mes, puede que decidan no cambiar su tiempo por el dinero que ya no necesitan. Un escenario así provocaría una propuesta salarial más alta por parte de la empresa aumentando costes y por lo tanto precios de venta. La rentabilidad de esta empresa la dictará la demanda, que puede estar de acuerdo en pagar a 4000 sats por el refresco o dejar de consumirlo. El error de los plebs que usan el término "Store of Value" se basa en creer que la oferta de productos y servicios se va a mantener una vez hyperbitcoinizada la economía. Los equilibrios a los que nos llevará Bitcoin no pueden ser anticipados ya que veremos grandes variaciones en las preferencias de los consumidores (demanda) y veremos como los incentivos para los productores y la mano de obra también varían (oferta). Lo que sí podemos saber es que los mercados con una alta demanda verán una gran competencia entre productores para saciar ese mercado y los precios tenderán a la baja, por lo que Bitcoin serviría como "Store of Value" en el mercado de esos productos.

Es por esa mala comprensión del valor que vemos a plebs decir que Bitcoin no debe ser tratado para realizar pagos aún y debemos esperar a que sea aceptado como depósito de valor por la mayoría. Este suele ser el argumento de muchos para decir que el precio de Bitcoin en algún momento se estabilizará. Si bien usarlo como método de pago incentiva la adopción, lo que la

precipitará de forma exponencial será el mal funcionamiento de las cadenas de suministro y la consecuente muerte del dólar. Todo ha ido siempre de recursos y cómo se reparten entre los agentes, el dinero solo juega como mediador y hay agentes que no venden sus preferencias.

“ □ [Begleri \(@begleristirner\)](#)

# Bitcoin y la Macro



[Begleri \(@begleristirner\)](#)

Publicado: 21/09/2022

Tags: Economía

Me sorprende mucho oír a bitcoiners hablar sobre escenarios “when lambo” para los próximos años o décadas. A mi gusto estos están tan perdidos como los no-coiners que no conciben que el dinero más duro desplaza a los demás. Y es que si hablamos de dinero todo depende del diseño. En este artículo quería comentar los dos grandes cambios que veo entre el diseño Fiat y el de Bitcoin.

La carrera de Economía la resumí en mi mente como Micro, Macro y Econometría. La econometría es una herramienta, sirve para analizar modelos creados por el humano para intentar sacar conclusiones de la data. La micro estudia el intercambio P2P y explica las decisiones de los agentes según sus incentivos. Por último la macro me explica a nivel nacional como justificar las políticas económicas que se están tomando. Y aquí las importantes son las políticas fiscales y las monetarias.

Como cualquier niño que le gusta entender lo que le están explicando me perdí en el keynesianismo sin poder entender cuál era la propuesta. El gasto público siempre por encima de sus posibilidades y la deuda pública creciendo de forma estructural. Recuerdo preguntar en clase cual era el valor promedio en el que debía estar la deuda pública de un país y recibir por respuesta que no se sabe del todo. La siguiente pregunta fue si algún día la veríamos en 1000% del PIB. Creo que ya imaginan la respuesta.

Esas dudas del modelo actual me llevaron a Hayek y a Mises y a sus ideas de desnacionalización del dinero, pero sus diseños carecían de una tecnología a la altura, por eso encontrar Bitcoin después me hizo cerrar la profecía. Es gracias a su cifrado criptográfico con lo que Bitcoin se convierte en la única forma de dinero inconfiscable. La privacidad que se puede conseguir en Bitcoin dificulta el rastreo e imposibilita la confiscación por parte del estado, lo que acaba con las políticas fiscales con las que contábamos a nivel macroeconómico para jugar con nuestro modelo económico. Por otro lado, si la oferta monetaria en Bitcoin es fija, se sabe desde el día 0 la cantidad de bitcoins que habrá en circulación, no tenemos políticas monetarias. Para mi mente eso fue fumarse las cuatro asignaturas que me habían hecho entender la política.

Estos dos cambios solucionan dos problemas diferentes por separado, con una influencia diferente en el diseño de nuestro sistema. Una política monetaria fija deja fuera de juego la figura del banco central, pero aún más importante, imposibilita la ejecución de malabares keynesianos con el gasto público. Por su diseño basado en la escasez, Bitcoin desmonetiza el resto de activos competidores como reserva de valor y esto muchos economistas no lo consiguen entender por ruido como el valor intrínseco o el concepto comunidad. Siendo Bitcoin el diseño de dinero más duro del mercado, está destinado a convertirse en moneda de reserva mundial pero el diseño final de cómo interactuará el usuario sigue siendo cuestión de debate y arena de batalla ideológica. A partir de estos dos cambios propuestos en el ámbito fiscal y monetario me gustaría profundizar en algunos escenarios y en algunas teorías. En los artículos derivados de este, daré mis puntos sobre los conceptos, modelos y mitos que entiendo se rediseñan.

# Systems falln't



Begleri (@begleristirner)

Publicado: 21/09/2022

Tags: Filosofía

La idea de una oferta monetaria fija le suele gustar a todo el mundo, excepto a los que se benefician de la impresión de dinero. Lo más similar a esto es el diseño del oro como activo monetario, no se puede crear más oro para ponerlo en circulación. Por ese motivo se hace la comparativa entre lo que significaría que Bitcoin se posicione como moneda de reserva mundial y el Gold Standard. El resto de propuestas cuentan con un Banco Central o un agente que tiene la capacidad de alterar la masa monetaria en un futuro.

En primer lugar las propuestas más sencillas de descartar: CBDCs, FIAT y Altcoins. En todas ellas contamos con un Banco Central o un Agente con Mayor poder sobre la red que el resto. En el caso del FIAT y las CBDCs entendemos que son prácticamente lo mismo: el estado recupera el poder sobre el dinero en el ámbito fiscal y monetario. Puede tomar impuestos a su población a su antojo y puede decidir emitir moneda para rescatar los sectores que necesita. Más allá del debate

“Democracia vs Monarquía”, que la oferta monetaria dependa de una decisión humana es una fisura en el modelo de estos competidores. Lo mismo ocurre en el caso de una Altcoin que busque competir con Bitcoin o con el oro como reserva de valor, pero en este caso es un agente privado y no el estado quien tendería a aumentar la oferta monetaria.

Como siempre, los incentivos para llevar a cabo estas políticas son diferentes en cada caso pero la mera existencia de esa acumulación de poder en la red pone en peligro la promesa de una oferta monetaria fija. Recordemos que todos hacen la promesa de una oferta monetaria fija porque una oferta monetaria creciente provoca una inflación estructural en la economía. Bajo una oferta monetaria fija veríamos cómo desaparecen fuerzas en el mercado que permitían unos equilibrios deseados por la sociedad. Algunos ejemplos en mi opinión son la carne, el litro de gasolina y los precios de los pasajes de avión. Ya sea para mantener una producción que le convenga o ya sea para contentar a las masas con unos recursos a unos precios por debajo de su coste real (subvenciones). Si en una contabilidad donde no se puede imprimir no hay rescates del sector privado puede que veamos una gran destrucción de oferta lo que presione los precios en el corto plazo aún más a la alza. Este fenómeno es conocido como “Descubrimiento de precios” y traerá consigo un aumento de populismos muy deseado en varios conflictos occidentales. Un mercado sin intervención estatal es lo que yo entiendo como Economía Austríaca, donde solo los principios microeconómicos y la teoría del valor marginalista se imponen sobre todo. Es aquí donde los bitcoiners del “when lambo” no han llegado y se imaginan una economía produciendo al ritmo actual donde la impresión de dinero ha creado equilibrios absurdos a los que se han acostumbrado.

La misma discusión me he encontrado con la Monero Gang (XMR) que tienen buenos puntos sobre la fungibilidad y la privacidad. Sin embargo el no poder llegar a definir la oferta de Moneros en circulación demuestra que no han comprendido las cualidades que requiere un diseño monetario para imponerse como moneda de reserva. Todo se podría definir bajo la expresión: el valor reside en la escasez. Por mucho que no sea lo privado que desearían algunos cypherpunks, por su diseño basado en la escasez Bitcoin se posicionará como competidor monetario más fuerte. El único que puede competir a nivel práctico es el oro, a nivel teórico Bitcoin es perfectamente escaso. Por lo que debemos estudiar los diseños que se basen en un Bitcoin Standard y un Gold Standard, como únicos modelos donde podemos hablar de una oferta monetaria fija.

Entramos ahora a otra dimensión, esta no tiene que ver con las matemáticas como la monetaria. Esta dimensión es la fiscal, Bitcoin se proclama como el primer activo monetario inconfiscable, lo cual cambia las reglas del contrato social al desaparecer una de las dos formas de violencia que tiene el estado contra el individuo. Esta dimensión depende del humano y de cómo entienda el equilibrio al que tiende en el largo plazo. Entendemos que las dos formas de violencia del estado son la violencia contra la libertad del individuo y la violencia contra la propiedad de este individuo.

En el primer caso, esta violencia la aplican las armas, los soldados, los tribunales y las prisiones. Que aplican castigos y amenazas para incentivar el comportamiento del individuo, con esta forma de violencia puedes confiscar todo aquello tangible que posea el individuo: oro, cosecha, ropa, tierras... En el segundo caso, debemos definir qué entendemos como propiedad: abandonamos la idea de propiedad como derecho natural que nos presenta Rousseau en el Contrato Social y volvemos a la idea de propiedad que defiende Max Stirner. Propiedad es aquello que está bajo nuestra posición o dominio y lo podemos proteger. En el momento en que me di cuenta de que lo

único que entraba bajo esta definición de propiedad era Bitcoin entendí que este había creado el superlativo de propiedad que exponía como falsa propiedad aquella aceptada por el sistema: activos Inmobiliarios. Si el estado no puede confiscar lo que se empieza a considerar reserva de valor, como va a financiarse? Hasta ahora podía imprimir para financiar sus déficits pero ahora depende únicamente de rescates privados si son deficitarios. Sin una seguridad organizada, no se puede garantizar la propiedad privada como está entendida en nuestro sistema. También hay que entender que si ahora la financiación de la seguridad depende completamente del voluntarismo, podemos hablar de que solo existe seguridad privada.

Por lo que la inconfiscabilidad nos lleva a dos conclusiones: mueren los agentes públicos en todos los modelos macroeconómicos y se rediseña el contrato social y el concepto de propiedad privada por una tecnología que imposibilita la violencia sobre la propiedad. Antes de Bitcoin, no existía ningún activo que cuadrara a la perfección con la definición de propiedad, únicamente activos que nos hubiera gustado que de verdad cumplieran las condiciones, pero los estados siempre han tenido la propiedad de todo lo que pueden confiscar con su violencia organizada. Si adoptamos una nueva contabilidad basada en Bitcoin muere la confiscabilidad sobre el dinero y eso imposibilita la financiación de los soldados que garantizan la seguridad, ya sea con intenciones públicas o admitiendo que es privada. Es por esta falta de seguridad que deja de tener sentido la propiedad como la entiende Rousseau, desaparece la violencia contra la propiedad y solo queda la violencia contra el individuo.

Ante un escenario donde todos los agentes son privados y ninguno puede confiscar el dinero a los demás, la financiación de la seguridad se vuelve lo más importante para reestructurar el contrato social. Esta dimensión asusta mucho más a los amantes del orden y a los vencedores del sistema FIAT que ven como toda su tranquilidad y lujos dependen de esta violencia estructural. Es en este punto donde tanto no-coiners como bitcoiners demuestran como de beneficiados han salido del sistema FIAT, por eso hay algunas propuestas tan absurdas dentro del ecosistema. Recordemos que para volver a construir un sistema basado en propiedad, necesitamos poder aplicar la violencia contra ésta, por lo que la arquetípica disputa "orden-caos" o "fascismo-anarquismo" se libra en la cualidad de confiscabilidad sobre el diseño final.

Escenario I: CBDC pinned to Gold Escenario II: CBDC pinned to Bitcoin Escenario III: Smart Contract world on Bitcoin Escenario IV: Bitcoin anarchy

Escenario I:

Este primer escenario significa volver al clásico Gold Standard, un gobierno decide emitir una cantidad de CBDCs que va a fijar a una reserva de oro para que la población lo pueda usar como método de pago. Entiendo que los economistas lo definen con la palabra respaldar. El hecho de tener indexada la moneda a un activo con una oferta monetaria prácticamente fija, imposibilita la creación de nueva moneda, acabando así con los problemas de inflación estructural del actual modelo FIAT.

Sin el poder de aumentar la masa monetaria en el dinero sobre el que llevamos nuestra contabilidad, podemos ver los efectos del "Austrian Economics" al que se expone una economía sin rescates ni subvenciones financiados con nuevo dinero. A su vez vemos como vuelven a haber

incentivos para los ahorradores al desaparecer la inflación estructural. Por lo que tener una moneda en circulación indexada a Oro o a Bitcoin es muy prometedor para la economía en el medio-largo plazo. En el diseño donde la moneda se respalde en oro tenemos dos puntos donde puede existir la violencia contra el capital del individuo: la confiscación del oro y la confiscación de la moneda intercambiable por oro.

El oro físico por ser confiscable jugó un papel muy importante en el diseño del feudalismo, creando incentivos que justifican movimientos Imperialistas, Colonialistas y Estatistas. Actualmente el oro ya está repartido, los poseedores de este ya crearon sus activos respaldados en oro y los usan como dinero o deuda para seguir financiando sus economías. Es importante entender que la violencia sobre la propiedad es lo que permite la financiación de la seguridad y es esta la que garantiza la propiedad privada como la entendemos en occidente. Sin propiedad privada, desaparecen los privilegios de los vencedores del modelo FIAT, por ese motivo los fascistas buscan conservar la confiscabilidad a toda costa en los futuros diseños.

Un diseño donde no se puede imprimir pero se puede confiscar podría no ser tan diferente a un sistema FIAT solo que no gozaríamos de los equilibrios artificiosos por la impresión de dinero. Si el estado puede seguir intimidando al ciudadano y tomando su propiedad puede seguir financiándose y por lo tanto existiendo. Entrar en un modelo así ya sea respaldado por Oro o por Bitcoin yo lo entiendo como volver a mediados del s.XX donde el dólar (moneda de reserva mundial) estaba sujeto al Gold Standard. También es importante destacar que hoy en día se puede confiscar el dinero del ciudadano con un click, no hace falta movilizar soldados a su puerta para confiscar las monedas de oro que haya podido acumular.

Un modelo donde se puede confiscar el dinero al ciudadano, es un modelo donde existe la posibilidad de desindexarse al activo de respaldo. Eso es muy peligroso para la economía y para los individuos que interactúan a través de esa contabilidad haciéndolos susceptibles a la estafa de la impresión monetaria una vez más.

## Escenario II

Ya aceptamos que intentar crear un diseño que no esté basado en Oro o Bitcoin en el largo plazo está condenado al fracaso por sus problemas estructurales sobre la oferta monetaria del activo. En este escenario quería describir como imaginé que sería el rol de Bitcoin en los diseños venideros por entender que la red On-chain de Bitcoin es muy lenta para soportar la red financiera de la economía mundial. Aquellos que no han indagado en la Lightning Network pero han entendido que Bitcoin por sus propiedades se impone como moneda de reserva mundial, creo que imaginan un escenario futuro como el que describiré a continuación:

Necesitas una red rápida y con bajas comisiones para que cuadre con el estilo de consumo que llevan los territorios desarrollados. He abandonado la palabra país porque dejan de tener sentido sin los estados, disculpen. Como Bitcoin On-Chain no te da lo que necesitas, creas una moneda que sí cumpla las necesidades como pagar un café y no tener que esperar unos 8 minutos a ver tu transacción en el nuevo bloque de la mempool. Eliges la oferta total de la nueva moneda y la indexas a una cantidad de Bitcoin, esto te permite manipular la nueva moneda y poder convertirla en todo momento a Bitcoin otra vez. Este planteamiento tiene varios adeptos de naturalezas muy

distintas, a mi me gusta centrarme en el diseño, no en las explicaciones que condujeron a este.

A continuación voy a poner algunos ejemplos, todos gozan de una oferta monetaria fija pero algunos abordan la confiscabilidad por diferentes frentes. Como vemos, esto es un tema de custodia del verdadero Bitcoin y del grado de confianza que queramos en nuestro sistema.

Nayib Bukele, presidente de El Salvador con su Wallet Chivo:

El Chivo Wallet es un wallet custodial que está conectado a la Lightning Network pero no corre completamente sobre la Lightning Network. Se entiende que el político pionero no decida abandonar la cultura del KYC al haber abrazado Bitcoin y podríamos decir que se está haciendo con "buenas intenciones". Pero en realidad, puede que lo que se está moviendo dentro de Chivo no sea Bitcoin sino una moneda que usan como moneda-lateral. Esto podría hacerse para evitar fondos perdidos en los wallets de los ciudadanos que interactúan por primera vez con sus aplicaciones. Siempre hay que buscar paternalismos para justificar como se escusan los políticos. El hecho es que el día de mañana Chivo puede caer y los fondos de los Salvadoreños desaparecer.

Citadel que desea su propio dinero local

En algunos escenarios sobre citadels hemos imaginado un poblado que en total cuentan con 0.001 bitcoin (100.000 sats) y tienen miedo de manipularlo para pagos diarios porque su economía es básicamente interna y se puede perder o gastar en comisiones más de lo deseado. Deciden crear una moneda física o digital, con una oferta mayor o menor a 100.000, para usar en el día a día y deciden que el 0.001 bitcoin se moverá únicamente para comerciar con otras citadels. En este ejemplo es importante la custodia y la confianza entre los integrantes de la citadel en su sistema. Por supuesto si la moneda lateral es digital debemos buscar garantizar que nunca nadie podrá alterar el código pudiendo aumentar la oferta. En caso de querer una moneda lateral cash habrá que conseguir un buen diseño para evitar falsificaciones que aumenten la oferta.

Eurodigital indexado a Bitcoin

Viendo el colapso del Euro, es de esperar que nos presenten el Euro Digital como el sistema de contabilidad donde los precios se estabilizarán. Bien si el Euro Digital lo respaldasen con una reserva de Bitcoin, sufriríamos problemas inflacionarios por los problemas en las cadenas de suministro y los ajustes que hay después de la recesión y destrucción de oferta de los años venideros, pero dejamos de tener inflación estructural. Siempre que vuelvan a emitir volverán a perder esa contabilidad. Desde luego solo conseguirán engañar a los que siguen sin entender que el valor reside en la escasez, y una vez se entiende no se puede olvidar por lo que la tendencia es clara. En este caso el estado puede seguir usando la violencia contra la propiedad del individuo confiscando sus Euros digitales. Volvemos una vez más a la custodia, si no lo puedes defender no es tuyo.

Bitcoin trae la Anarquía mientras que todas estas propuestas buscan el Orden apoyándose en el perfecto diseño de Bitcoin. Habrá citadels libres de todo tipo y si buscáis dictaduras también las habrá, solo debéis entender el diseño del dinero que estáis validando. Hemos visto también como en los tres ejemplos anteriores la custodia es un tema crucial, de ahí sale el Escenario III que tiene que ver con la custodia en Smart Contracts no solo en Wallets.

## Escenario III

Bitcoin imponiéndose como moneda de reserva mundial desmaterializa la propiedad privada, la constitución pasa a ser un papel que expresa como nos gustaría que fuera la realidad más que una pauta a seguir. Sin una seguridad organizada, el registro de la propiedad deja de ser respetado por las clases que no han podido acceder a estos recursos y no hay forma de hacer cumplir las obligaciones de pago. Es ante este caos donde muchos constructores deciden unirse a la creación del Orden que hasta ahora ha venido en forma de "Smart Contract", entendiendo que es una herramienta, no tiene moral.

En mis inicios intentando entender la propuesta de las criptomonedas, entendí que los Smart Contracts podían ejecutar un contrato de compraventa sin necesidad de un validador intermediario. Lo que el sector inmobiliario entendió como que podían ahorrar en costes burocráticos y además los dejaba como pioneros por experimentar con estas nuevas tecnologías. Eso sin entender que el registro de la propiedad, ya estuviera en papel o en ethereum, deja de tener sentido sin una seguridad organizada que garantice las promesas hechas en los contratos.

De igual forma, imaginando una ciudad que consiga abastecerse con su producción y comercio, puede decidir que quiere organizarse de una forma similar a como entendemos actualmente la propiedad privada, asignando una propiedad a la tierra y siendo garantizada por una seguridad privada financiada por los propios individuos de la ciudad. Para una infraestructura así necesitaríamos smart-contracts sobre una blockchain, voy a poner un par de ejemplos. Con un modelo de smart contracts sobre Ethereum donde a través de NFTs se distribuya la propiedad inmobiliaria necesitas que los habitantes de estas propiedades inmobiliarias respeten lo escrito sobre la red Ethereum, sino no tienen ningún incentivo a seguir en un modelo que los perjudica. En este ejemplo la ciudad podría usar bitcoin en el día a día pero organizar el urbanismo a través de Smart Contracts sobre Ethereum, para esto ser posible es necesario que todos los habitantes de la ciudad estén de acuerdo en usar la red de Ethereum a parte de Bitcoin. Sin algo que perder por parte del habitante, podría decidir romper las promesas del contrato. Una vez más vemos que todo depende de quien tenga acceso a mover los fondos, en mejores palabras, la "Custodia" del dinero.

Para los buscadores del orden que no confían en Ethereum por su mal diseño o únicamente porque no es indestructible, aparecen propuestas como Smart Contracts sobre Sidechains de Bitcoin, por como tengo entendido, RSK es una de ellas. Una infraestructura que permita lo mismo que Ethereum promete sobre Bitcoin, claramente tiene más números para imponerse. Pero en el momento en que nuestro Bitcoin es capturado por el Smart Contract perdemos la custodia sobre él y puede que el día de mañana deseemos acabar con ese contrato perdiendo así esa cantidad "avalada". El riesgo aquí es el ejemplo de una ciudad donde decidan organizar la tierra con un modelo similar a la propiedad privada sobre Smart contracts sobre Bitcoin y cambien la legislación o las condiciones que permiten acceder o confiscar esos fondos. Para evitar cualquier estafa o cambio de condiciones lo mejor es tener el Bitcoin bajo custodia propia, por eso hay que tener cuidado con los modelos que se diseñan sobre estas herramientas que prometen orden.

Estos dos ejemplos proponen limitar la inconfiscabilidad a nivel práctico para organizar una sociedad. Será elección de cada individuo elegir en qué tipo de ciudad quiere vivir adaptándose a sus preferencias y necesidades. Es importante entender que esta herramienta permitirá la tiranía,

pero es imposible luchar contra el avance tecnológico, solo debemos procurar que no todo el territorio esté bajo el dominio de tiranos. Hay individuos que por miedo al caos renunciarán a su libertad por la promesa de la protección, estas comunidades faltas de líderes buscarán modelos sobre los que construir estos sistemas que los protejan, solo hay que entender la naturaleza de la confianza y de la custodia.

#### Escenario IV

Aquellos que no prestaron tanta atención al ruido ni se perdieron por madrigueras técnicas, vieron nacer la Lightning Network, que dotaba a Bitcoin de lo necesario para soportar la red financiera mundial. Trasladando la seguridad de la transacción del sistema de minería al Nodo Lightning al que está conectado el Wallet Lightning. Si eso permite la propia custodia me parece una solución acorde con el Ethos de Bitcoin donde el individuo se responsabiliza de la custodia de su propiedad.

Si en una citadel no se busca crear mecanismos para recuperar terreno en la confiscabilidad de la propiedad del individuo, significa que ambos aceptan la falta de herramientas suficientes como para articular un contrato social basado en violencia. Este es el único escenario donde considero que la comunidad ha abrazado la anarquía y se ha expuesto a ver los resultados de la libertad. La mera existencia de ciudades libres ya sumerge a la economía mundial en la anarquía, ya que el orden necesita ser completo mientras que el caos solo hace falta encontrarlo. Consideramos como ciudad libre aquella en que los individuos si deciden usar el dinero eligen Bitcoin por ser la única forma de dinero honesto.

Usamos la palabra honesto porque detrás de Bitcoin hay una democracia total, lo que la mayoría entienda que es Bitcoin, será Bitcoin. Pero Bitcoin, como el espejo de Harry, muestra a todos algo diferente, nos desvela diferentes secretos según nuestro background y profundidad. Muchos han visto en Bitcoin un excel, otros una timechain, a mi gusto lo realmente valioso que creó Satoshi y los maximalistas se han encargado de conservar, es su diseño. Cualquier propuesta de modificación del diseño de Bitcoin que cambie su entendimiento como activo monetario debe ser interpretado como un ataque a aquellos que posean Bitcoin por entenderlo como reserva de valor. Pero aquellas herramientas que cuadren con el Ethos y Lenguaje de Bitcoin deben ser entendidas como variaciones que produce la libertad aunque la naturaleza de su creación vayan contra la libertad misma.

También es necesario comentar que la Lightning Network no es necesaria, si bien nos hace la vida más cómoda, puede que el ritmo que estamos buscando sea innecesario en un mundo con nuevos incentivos y equilibrios. Es fácil de imaginar el modelo de citadel que decide funcionar con trueque entre los habitantes y usar el bitcoin únicamente para comerciar con sus vecinos que le pidan bitcoin On-Chain.

Una sociedad que abraza la anarquía abandona varios pilares de nuestros filósofos más influyentes en las corrientes liberales bajo las que se han aguantado los estados occidentales. Satoshi creando esta tecnología nos sumergió en un experimento del que no se puede escapar, un límite que ya sabemos a qué valor tiende. Impuso el estado natural creando la verdadera propiedad que es resistente a la violencia, que únicamente encontramos en el cuarto escenario del artículo. En los otros tres vemos que el tema es la custodia, se proponen modelos donde encontramos la

Dialéctica del Amo y el Esclavo de Hegel.

También hemos visto en estos escenarios que todas las políticas macroeconómicas que entendíamos como herramientas para procurar el bien, estaban basadas en la violencia. Algunos decidirán que eso no es carga suya y se entregarán a las tiranías que prometen comodidades, los individuos que acepten el estado natural serán expuestos a la libertad por primera vez en estas condiciones. La propiedad y el sector inmobiliario son algunos de los temas en cuestión más importantes ya que condicionan el día a día de los habitantes de dicho territorio.

En mi humilde opinión, todos los modelos que hemos comentado en estos artículos los podremos ver en diferentes citadels una vez haya acabado la transición del modelo Fiat al Bitcoin Standard. Debemos entender la importancia del diseño y debemos estudiar cómo cambian los diferentes sectores que nos rodean.

# Cypherpunks | El origen y la filosofía detrás de Bitcoin

"Privacy is necessary for an open society in the electronic age. **Privacy is not secrecy.** A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. **Privacy is the power to selectively reveal oneself to the world.**"

— Eric Hughes, *A Cypherpunk's Manifesto* (1993)

[Bebop](#)

Publicado: 17/10/2022

Tags: Historia, Cypherpunk

Para entender el presente hay que mirar al pasado. En este clip de audio, os preparo una ruta hacia las entrañas de la corriente filosófica Cypherpunk. A lo largo de la ruta nos detendremos en 3 grandes paradas que marcaron la historia, el origen, el por qué y el cómo de la aparición de Bitcoin como lo conocemos hoy en día. Espero que lo disfruteis.

Link (MEGA) del podcast: <https://mega.nz/file/lH0HkCjI#8Q9LjAD-DXdGCT9GiVQcYcPcc2JRxLTtO4ngPBjaqJ0>

Especial agradecimiento a:

[@lunaticoin](#) [@alfremancera](#) [@satoshinakamotoinstitute](#) [@bitcoinmagazine](#)

California de los '70. Universidad de Berkeley, sociedad abierta. Contexto social liberal. Caldo de cultivo perfecto...

- UNIX: primer SO
- '76: la AECA otorga a la criptografía la categoría de arma. Al mismo tiempo y a modo reivindicativo Diffie-Helman-Merkel => Sistemas de clave asimétrica (dos claves, pública y privada)
- '81: empiezan las primeras conferencias cryptologia<sup>1</sup> en sta barbara, caifornia. David chau, crean correos electrónicos digitales intraqueables y firmas ciegas para pagos no traceables. Seguridad sin identificación: sistemas de transacción para hacer obsoleto al Big brother. Electronic cash intraceable (firmado por David Chaum. Moni Naor y Amos Fiat)
- '83: GNU

Por aquel entonces los procesadores de Intel padecían un problema inducido por partículas Alpha. El joven ingeniero Timothy C. May que trabajaba para Intel fue el encargado de descubrir y solucionar la falla. Gracias a su trabajo se pudo retirar a los 34, lo que hoy conoceríamos como libertad financiera. El resto de su vida la dedicó en cuerpo y alma al movimiento que despertó gracias al:

# Manifiesto crypto-anarquísta

*Un espectro está surgiendo en el mundo moderno, el espectro de la cripto anarquía.*

*La informática está al borde de proporcionar a grupos e individuos, la capacidad de comunicarse e interactuar entre ellos de forma totalmente anónima. Dos personas podrán intercambiar mensajes, hacer negocios y negociar contratos electrónicos, sin saber nunca el nombre real o identidad legal de la otra parte. Las interacciones sobre las redes serán intrazables, gracias al uso extendido de re- enrutado de paquetes encriptados en máquinas a prueba de manipulación que implementen protocolos criptográficos con garantías casi perfectas contra cualquier intento de alteración. Las reputaciones tendrán una importancia crucial, mucho más importante en los acuerdos que las calificaciones crediticias de hoy en día. Estos progresos alterarán completamente la naturaleza de la regulación del gobierno, la capacidad de gravar, de controlar las interacciones económicas, la capacidad de mantener la información secreta e incluso alterarán la naturaleza de la confianza y*

de la reputación.

*La tecnología para esta revolución (que de bien seguro será social y económica) ha existido teóricamente durante la última década. Los métodos están basados en el cifrado de clave pública, sistemas interactivos de prueba de cero-conocimiento, y varios protocolos de software para la interacción, autenticación y verificación. El foco hasta ahora ha estado en conferencias académicas de Europa y EE.UU., conferencias monitorizadas de cerca por la Agencia de Seguridad Nacional. Pero solo recientemente las redes de ordenadores y computadoras personales han alcanzado la velocidad suficiente para hacer las ideas realizables en la práctica. Y los próximos 10 años traerán suficiente velocidad adicional para hacer estas ideas factibles económicamente y, en esencia, imparables. Redes de alta velocidad, ISDN, tarjetas inteligentes, satélites, transmisores Ku-Band, ordenadores personales multi-MIPS, y chips de cifrado, ahora en desarrollo, serán algunas de las tecnologías que lo permitirán.*

*El Estado intentará, por supuesto, retardar o detener la expansión de esta tecnología, citando preocupaciones de seguridad nacional, el uso de esta tecnología por parte de traficantes de droga y evasores fiscales,,, y miedos de desintegración social. Muchas de estas preocupaciones serán válidas; la criptoanarquía permitirá la comercialización libre de secretos nacionales y la comercialización de materiales ilícitos y robados. Un mercado computarizado anónimo permitirá incluso el establecimiento de horribles mercados de asesinato y extorsión. Varios elementos criminales y extranjeros serán usuarios activos de la CryptoNet. Pero esto no detendrá la expansión de la cripto anarquía.*

*Al igual que la tecnología de impresión alteró y redujo el poder de los gremios medievales y la estructura del poder social, también los métodos criptológicos alterarán la naturaleza de las corporaciones y la interferencia del gobierno en las transacciones económicas.*

*La cripto anarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes. Y de la misma manera que una invención aparentemente menor como el alambre de espino hizo posible el cercado de grandes ranchos y granjas, alterando así para siempre los conceptos de tierra y los derechos de propiedad en las fronteras de Occidente, así también el descubrimiento aparentemente menor de una rama arcana de las matemáticas se convertirá en el alicate que desmantele el alambre de espino alrededor de la propiedad intelectual.*

*¡Levántate, no tienes nada que perder excepto tus propias cercos de alambre de espino!*

*La cripto anarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes. Y de la misma manera que una invención aparentemente menor como el alambre de espino hizo posible el cercado de grandes ranchos y granjas, alterando así para siempre los conceptos de tierra y los derechos de propiedad en las fronteras de Occidente, así también el descubrimiento aparentemente menor de una rama arcana de las matemáticas se convertirá en el alicate que desmantele el alambre de espino alrededor de la propiedad intelectual.*

*¡Levántate, no tienes nada que perder excepto tus propias cercos de alambre de espino!*

**Timothy C. May, 1998 [tcmay@netcom.com]**

**W.A.S.T.E.: Aptos, CA**

Tim May reparte panfletos del discurso por una conferencia hacker y al recibir un feedback tan bueno se anima a mantener el contacto via mail con la gente interesada.

- '90: Empresa digicash por David chaum Equipo formado por Nick sabo, Eric huge, sistema de dinero electrónico basado en cryptogafia para implementarlo en sistemas bancarios.
- '91: phil Zimmerman:PGP 1.0 (pretty Good privacy) modesto el hombre. Sistema de cifrado de cryptografia fuerte el cual fue publicado a internet por el mismo Phil. Por ese motivo tubo problemas con las autoridades estadounidense. Quedó absuelto luego de múltiples investigaciones
- '91: unión de GNU/Linux
- '92: Mientras tanto Tim May , Eric Hughes y Johon Gilmour abrumados por el potencial del movimiento criptoanarquico, se reúnen i invitan a otros criptologos para idear formas de potenciar el movimiento. Se reúnen en la casa de Gilmour en Oclan. A la reunión se unen dos personajes más: Hal finey y Jude milhon asisten a la reunion
- A todo esto; jude milhon, activista y apasionada del género cyberpunk (género de ciencia ficción donde se plantea un futuro distòpico de tecnología avanzada con una gran desigualdad entre clases) suelta la broma de: vosotros sois cypherpunks (haciendo la analogía entre cypher: cifrage y punk como a parte reivindicativa y en contra del orden estableció)
- Eric Hughes 9 de Marzo 1993:

# Manifiesto Cypherpunk

*La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es confidencialidad. Un asunto privado es algo que uno no quiere que todo el mundo sepa, pero un asunto secreto es algo que uno no quiere que nadie sepa. La privacidad es el poder de revelarse uno mismo al mundo de forma selectiva.*

*Si dos personas tienen algún tipo de trato, entonces cada una tiene un recuerdo de su interacción. Cada parte puede hablar de su propio recuerdo sobre el tema; ¿Cómo podría prevenirse esto? Se podrían aprobar leyes en su contra, pero la libertad de expresión, es aún más fundamental, para una sociedad abierta, que la privacidad. Nuestra intención no es restringir ningún discurso. Si muchas partes hablan entre ellas en un mismo foro, cada una puede hablar con todas las demás y agregar conocimientos sobre individuos y otras partes. El poder de las comunicaciones electrónicas ha permitido tal comunicación grupal, y esto, no desaparecerá simplemente porque nosotros queramos.*

*Dado que deseamos privacidad, debemos asegurarnos de que cada parte de una transacción tenga conocimiento solo de lo que es estrictamente necesario para tal transacción. Dado que cualquier información puede ser reproducida, debemos asegurarnos de revelar lo menos posible. En la mayoría de los casos, la identidad personal no es relevante. Cuando compro una revista en el quiosco y le doy dinero en efectivo al empleado, no hay necesidad de saber quién soy. Cuando le pido a mi proveedor de correo electrónico que envíe y reciba mensajes, mi proveedor no necesita saber con quién estoy hablando o qué estoy diciendo o lo que otros me están diciendo; mi proveedor solo necesita saber cómo hacer llegar el mensaje y cuál es mi tarifa por su servicio. Cuando mi identidad es revelada por el mecanismo subyacente de la transacción, no tengo privacidad. Aquí, no puedo revelarme selectivamente; aquí debo revelarme siempre.*

*Por esta razón, la privacidad en una sociedad abierta requiere sistemas de transacciones anónimos. Hasta ahora, el efectivo ha sido el principal sistema de este tipo.*

*Un sistema de transacciones anónimo, no es un sistema de transacciones secretas. Un sistema anónimo permite a las personas revelar su identidad cuando lo deseen y solo cuando lo deseen; esta es la esencia de la privacidad.*

*La privacidad en una sociedad abierta requiere criptografía. Si digo algo, quiero que sea escuchado solo por aquellos a quienes me propongo. Si el contenido de mi discurso es accesible para el mundo, no tengo privacidad. Encriptar es indicar el deseo de privacidad, y encriptar con criptografía débil es indicar no tener demasiado deseo de privacidad. Además, revelar la propia identidad con certeza cuando el anonimato es la norma, requerirá de firma criptográfica.*

*No podemos esperar que los gobiernos, las corporaciones u otras grandes organizaciones nos otorguen privacidad por pura caridad. Es beneficioso para ellos hablar de nosotros, y debemos esperar que lo hagan. Intentar impedir su discurso es luchar contra la realidad de la información. La información no solo quiere ser libre, anhela ser libre. La información se expande hasta llenar el espacio de almacenamiento disponible. La información es la prima más joven y fuerte del rumor. La información es más veloz, tiene más ojos, sabe más, pero comprende menos que el rumor.*

*Debemos defender nuestra propia privacidad si esperamos tener alguna. Debemos unirnos y crear sistemas que permitan que se realicen transacciones anónimas. La gente ha estado defendiendo su propia privacidad durante siglos con susurros, ocultación, sobres, puertas cerradas, apretones de manos secretos y mensajeros. Las tecnologías del pasado no permitían una privacidad fuerte, pero las tecnologías electrónicas sí lo hacen.*

*Nosotros, los Cypherpunks nos dedicamos a construir sistemas anónimos. Defendemos nuestra privacidad con criptografía, con sistemas de reenvío de correo anónimo, con firmas digitales y con dinero electrónico.*

*Los Cypherpunks escriben código. Sabemos que alguien tiene que escribir software para defender la privacidad, y como no podemos obtener privacidad a menos que todos lo hagamos, lo vamos a escribir nosotros mismos. Publicamos nuestro código para que nuestros compañeros Cypherpunks puedan practicar y jugar con él. Nuestro código es libre para todo el mundo que quiera usarlo. No nos importa mucho si no aprueba el software que escribimos. Sabemos que el software no puede*

*ser destruido y que un sistema ampliamente disperso no se puede destruir.*

*Los Cypherpunks deploran las regulaciones sobre criptografía, ya que el encriptado es fundamentalmente un acto privado. El acto de encriptar, de hecho, elimina información del ámbito público. Incluso las leyes contra la criptografía solo se extienden hasta la frontera de una nación, hasta donde alcanza el brazo de su violencia. La criptografía se extenderá ineludiblemente por todo el mundo, y con ella los sistemas de transacciones anónimas que habilita.*

*Para que la criptografía sea generalizada, debe ser parte de un contrato social. La gente debe unirse y desplegar estos sistemas para el bien común. La privacidad solo llega tan lejos como la cooperación entre miembros de cada sociedad. Nosotros los Cypherpunks buscamos tus preguntas e inquietudes y esperamos que te involucres para que no nos engañemos a nosotros mismos. Sea como sea, no nos desviemos de nuestro rumbo porque algunos puedan estar en desacuerdo con nuestras metas.*

*Los Cypherpunks estamos comprometidos en hacer de las redes un lugar más seguro para la privacidad. Procedamos juntos, a toda prisa, adelante.*

**Eric Hughes, 9 de Marzo 1993**

El movimiento salió en la portada de la revista WIRED con el título:

Rebeldes con una causa. El discurso se propagó a las masas.

Se crea una lista de correo con remailers anónimos (anteriormente creado por hal finei y huge). Acordaban reuniones una vez al mes en la empresa de John Gilmore. Se crean debates y el cyphernomicon (FAQ's) por Tim May

'94: Clipper Chip, back door por la NSA. eCASH David Chaum con digicash y hace una demostración de transacción anónima

'96: John Perry Barlow íntimo amigo de John Gilmore y crean la EFF (fundación sin ánimo de lucro para defender los derechos civiles en el medio digital)

El 8 de febrero de 1996 se firmó en Estados Unidos la Ley de Telecomunicaciones, la cual proponía transformar el mercado de las telecomunicaciones eliminando imposiciones que en el pasado habían limitado los alcances de las empresas. Entre otras cosas, la ley contenía el Decency Act, una cláusula que pretendía volver ilegal ciertos contenidos sensibles en internet. La Ley de Telecomunicaciones -precedente claro de leyes que se intentarían aprobar después, como CISA (Cybersecurity Information Sharing Act) - detonó la indignación de los usuarios de la Red, quienes por primera vez tuvieron que defender la autonomía cibernética ante los poderes de los Estados. John Perry Barlow, poeta, ensayista y ciberactivista, publicó esta declaración desde Davos, Suiza, el mismo día que la ley fue aprobada. A poco más de un año de su muerte - 7 de febrero del año pasado -, Tierra Adentro reproduce la declaración, en traducción de Luis Ham, para recordar (hoy como todos los días) la importancia de la libertad en el ciberespacio.

8 de febrero de 1996, en la ciudad de Davos, Suiza:

# Declaración de independencia del Ciberespacio

*Gobiernos del Mundo Industrial, vosotros, fatigados gigantes de carne y acero: vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro os pido en el pasado, que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin más autoridad que aquélla con la que la libertad siempre habla:*

*Los gobiernos obtienen su poder del consentimiento de los gobernados. No habéis pedido ni recibido el nuestro. No os hemos invitado. No nos conocéis, ni conocéis nuestro mundo. El Ciberespacio no se halla dentro de vuestras fronteras. No penséis que podéis construirlo, como si fuera un proyecto público de construcción. No podéis. Es un acto natural que crece por medio de nuestras acciones colectivas.*

*No os habéis unido a nuestra gran conversación colectiva, ni creasteis la riqueza de nuestros mercados. No conocéis nuestra cultura, nuestra ética, o los códigos no escritos que ya proporcionan a nuestra sociedad más orden que el que podría obtenerse por cualquiera de vuestras imposiciones.*

*Proclamáis que hay problemas entre nosotros que necesitáis resolver. Usáis esto como una excusa para invadir nuestros límites. Muchos de estos problemas no existen. Donde haya verdaderos conflictos, donde haya errores, los identificaremos y resolveremos por nuestros propios medios. Estamos creando nuestro propio Contrato Social. Esta forma de gobierno se creará según las condiciones de nuestro mundo, no del vuestro. Nuestro mundo es diferente.*

*El Ciberespacio está formado por transacciones, relaciones, y pensamientos en sí mismo, que se extienden como una onda estacionaria en la telaraña de nuestras comunicaciones. El nuestro es un mundo que está a la vez en todas partes y en ninguna, pero no está donde viven los cuerpos físicos.*

*Estamos creando un mundo en el que todos pueden entrar, sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento.*

*Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado mediante el silencio o el conformismo.*

*Vuestros conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Se basan en la materia, y aquí no hay materia.*

*Nuestras identidades no tienen cuerpo, así que, a diferencia de vosotros, no podemos obtener orden por coacción física. Creemos que nuestra autoridad emanará de la moral, de un progresista interés propio, y del bien común. Nuestras identidades pueden distribuirse a través de muchas de vuestras jurisdicciones. La única ley que todas nuestras culturas reconocerían es la Regla Dorada. Esperamos ser capaces de construir nuestras soluciones particulares sobre esa base. Pero no podemos aceptar las soluciones que estáis tratando de imponer.*

*En Estados Unidos hoy habéis creado una ley, el Acta de Reforma de las Telecomunicaciones, que repudia vuestra propia Constitución e insulta los sueños de Jefferson, Washington, Mill, Madison, De Tocqueville y Brandeis. Estos sueños deben renacer ahora en nosotros.*

*Os atemorizan vuestros propios hijos, ya que ellos son nativos en un mundo donde vosotros siempre seréis inmigrantes. Como les teméis, encomendáis a vuestras burocracias las responsabilidades paternas a las que sois demasiado cobardes para enfrentaros por vosotros mismos.*

*En nuestro mundo, todos los sentimientos y expresiones de humanidad, desde las más viles a las más angelicales, son parte de un todo único, la conversación global de bits. No podemos separar el aire que asfixia del aire sobre el que se baten las alas.*

*En China, Alemania, Francia, Rusia, Singapur, Italia y los Estados Unidos estáis intentando rechazar el virus de la libertad erigiendo puestos de guardia en las fronteras del Ciberespacio. Éstos puede que impidan el contagio durante un corto lapso de tiempo, pero no funcionarán en un mundo que pronto estará cubierto por los medios de transmisión de bits.*

*Vuestras cada vez más obsoletas industrias de la información se perpetuarían a sí mismas proponiendo leyes, en América y en cualquier parte del mundo, reclamando la posesión de la palabra. Estas leyes declararían que las ideas son otro producto industrial, no más noble que el hierro oxidado. En nuestro mundo, sea lo que sea lo que la mente humana pueda crear, puede ser reproducido y distribuido infinitamente sin coste alguno. El trasvase global de pensamiento ya no necesita de vuestras fábricas para ser realizado.*

*Estas medidas, cada vez más hostiles y colonialistas, nos colocan en la misma situación en la que estuvieron aquellos amantes de la libertad y la autodeterminación que tuvieron que luchar contra la autoridad de un poder lejano e ignorante. Debemos declarar nuestros «yos» virtuales inmunes a vuestra soberanía, aunque continuemos consintiendo vuestro poder sobre nuestros cuerpos. Nos extenderemos a través del planeta para que nadie pueda encarcelar nuestros pensamientos.*

*Vamos a crear una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado hasta ahora.*

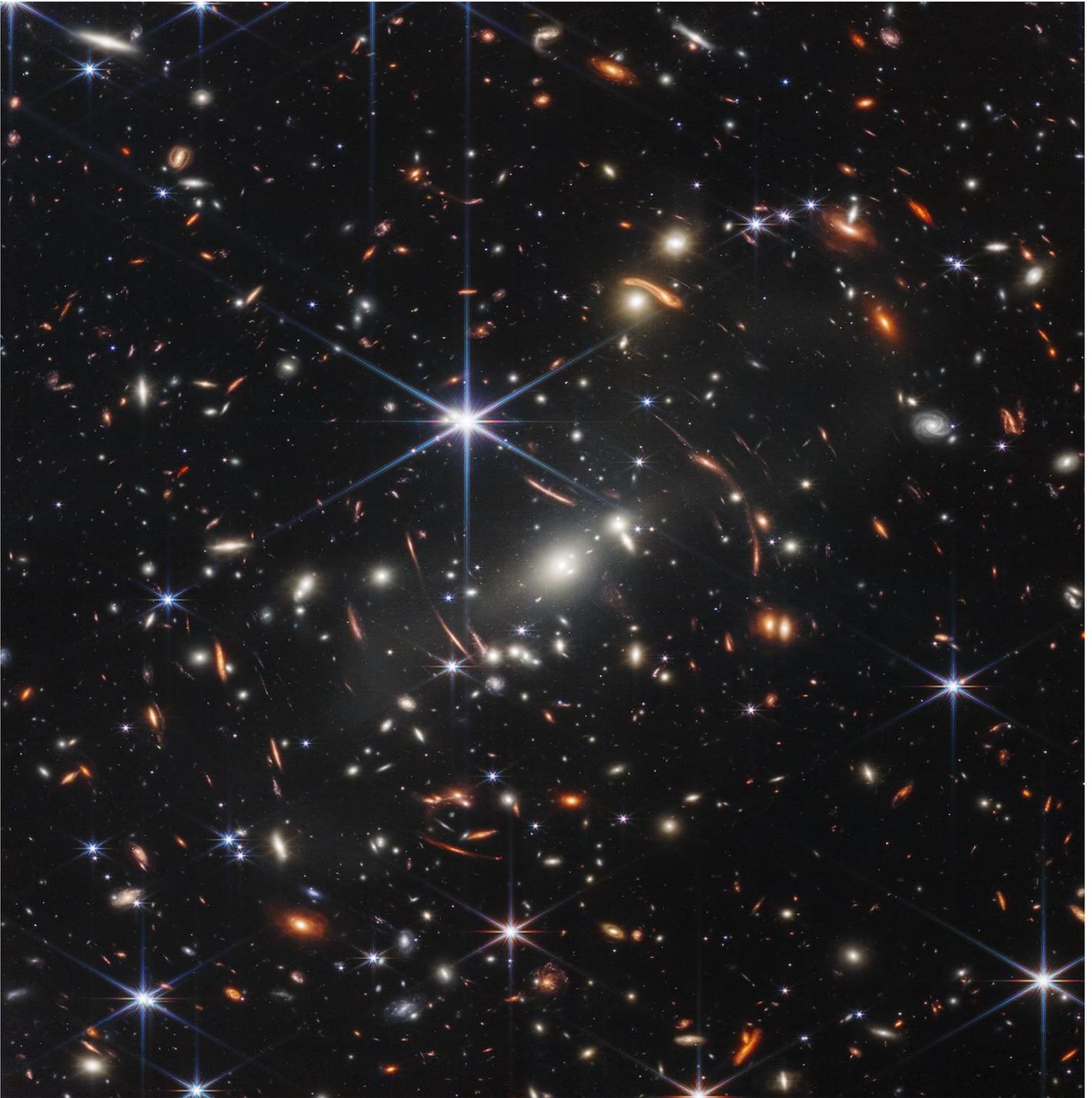
**John Perry Barlow, 8 de Febrero 1996**

*Cyberpunks en la actualidad:*

- *Adam Back*
- *Nick Szabo*
- *Mad Blaze*
- *Jamison Loop*
- *Pavel Durov*

## 1 Cryptografía y cryptoanálisis

# Bitcoin ya existe



Nancy Quirós Aguilar y Eugenio Corea Zúñiga

Publicado: 13/11/2022

Tags:

# Resumen

Bitcoin es dinero en efectivo de forma digital que además cuenta con las propiedades de dinero duro y está emergiendo del mercado. Es un activo real digital por lo tanto no está basado en deuda y parte de su innovación es que representa la escasez digital.

Bitcoin se compone de la unidad de valor llamada bitcoin y de la red peer-to-peer (nodos, mineros y blockchain). La Prueba de Trabajo es el elemento que permite que la red llegue a un consenso sin la presencia de intermediarios y que las transacciones en su blockchain sean inmutables ya que enlaza Bitcoin con el mundo tangible.

Bitcoin es la tecnología en sí por lo tanto es único e irrepetible y cada proyecto que intente replicar sus propiedades se convierte en un intento fracasado. Además, Bitcoin redefine el concepto de propiedad privada lo cual tiene consecuencias profundas. Sin embargo, en estas fases tempranas de adopción, la humanidad todavía no ha logrado asimilar los alcances de esta innovación.

Este ensayo tiene como objetivo aclarar los mitos más comunes con respecto a Bitcoin, mostrar su lugar en el mundo y que sirva como una guía de referencias para el principiante en Bitcoin.

Puedes leer este documento aquí: <upload bitcoin-ya-existe.pdf desde <https://bitcoinbarcelona.xyz/barcelona-bitcoin/Bitcoin-ya-existe-81590bd7357d4393b4dcb5922662dba6>>

# Rutas de distribución e incentivos



[Begleri \(@begleristirner\)](#)

Publicado: 30/01/2023

Tags: Económica

Esto es únicamente un in-put que quisiera dar al lector, no estoy buscando postular mi verdad sino solo poner en duda varias cuestiones. Para estudiar estas ideas debemos dejar claras las premisas:

El comercio con drogas está considerada una actividad ilegal (no le gusta al estado)

Por muy ilegal que sea siempre existirá una demanda de estos productos

Bitcoin sustituirá al dólar como moneda de reserva y de intercambio global

Aquellos territorios donde se produce la cocaína o hachís por ejemplo, tienen incentivos para enviar su mercadería (recursos naturales) a otros territorios a cambio de dinero FIAT (Dólar, Euro...). Ya que con ese dinero podrán conseguir los bienes que demandan en los demás

mercados. En cada caso, el producto debe llegar al consumidor y es donde entran en juego los factores de distribución. Esto condicionará el precio que pagarán los consumidores, ya sea por costes de transporte, riesgo, cantidad de competidores...

En el caso Latinoamericano, vemos como colombianos están enviando cocaína a Estados Unidos que es donde se puede sacar más beneficio con la venta de este producto. Esto ha condicionado a todo Centroamérica y sobre todo a México por su frontera terrestre con Estados Unidos. En la serie de Netflix Narcos y Narcos México explican la importancia de las rutas de distribución en este mercado. México tiene la forma que tiene porque hay incentivos para que así sea, ser el vecino del más rico del barrio puede traer muchos problemas. Se crean incentivos a nivel micro y a nivel macro, ahí les van un par de ejemplos:

**Micro:** Pasar una bolsa de mercadería al otro lado de la frontera para vender a precios Americanos parece una negocio atractivo a un joven sin acceso a un trabajo del primer mundo. Esto trae asesinatos, sobornos, rechazo de parte de la población americana a una migración que puede traer conflictos.

**Macro:** El gobierno Mexicano debe aceptar que la mercadería colombiana va a estar entrando a Estados Unidos. Puede poner un recargo por permitir que pase por su territorio, puede encargarse él mismo de la distribución, puede declarar la guerra contra el narcotráfico para convertirlo en una discusión política a su favor...

Hasta ahora nada nuevo, en el caso Europeo al haber más control estatal, el perfil del narcotráfico es más bajo. Pero de igual manera media Europa está consumiendo hachís de Marruecos que entra por Portugal y España para distribuirse por el resto del continente. No podemos decir que sea un sector a la baja ya que los beneficios del sector se considera que han estado aumentando en términos nominales las últimas décadas, si bien es cierto que han entrado otros productos competidores, queremos fijarnos en los canales de distribución de aquellas drogas de origen natural ya que aquí la distribución juega un papel mucho más clave que en el caso de algunas drogas químicas.

Una vez hecha la pincelada sobre como es este mercado, debemos añadirle el shock que estamos viviendo: transición del modelo económico mundial. Es cuestión de tiempo que las monedas Fiat desaparezcan y que el mundo entero funcione bajo un Bitcoin Standard. Mientras exista un precio de Bitcoin expresado en Dólares significa que la puerta aún está abierta, estamos en la parte pacífica de la transición. No sabemos cómo será el camino pero sabemos el final, si Bitcoin mantiene su diseño, que lo mantiene limitado, se posicionará como el dinero preferido para el comercio internacional. Por lo que en todos los mercados los agentes deben cambiar la forma de dinero que están aceptando si quieren sobrevivir. Todos aquellos mercados que sean sobre productos de consumo tienen ventaja sobre aquellos productos o servicios que son promesas. A este mercado en concreto, el anonimato que se puede conseguir en Bitcoin facilita mucho el comercio minimizando riesgos y facilitando la logística.

Aceptar esta premisa trae implícitas varias más, aquí las que veo más relevantes:

Desaparición del privilegio monetario de la Reserva Federal Americana así como de los Bancos Centrales de las demás monedas FIAT.

Descubrimiento de precios al entrar en una economía con una base monetaria fija, lo que se conoce como Austrian Economics en el ecosistema Bitcoin.

Imposibilidad de rastrear y confiscar el bitcoin de las empresas no permite la localización del dinero.

Sin posibilidad de financiar sus déficits de forma infinita, la economía americana pasará por una brusca transición. Ante un shock así, está por ver cuánto tiempo puede tardar la economía americana en recuperarse. Para saber si las rutas de distribución seguirán siendo las mismas debemos estudiar si la demanda será igual. Los consumidores de cocaína en Estados Unidos van a seguir demandándola pero no sabemos si van a ser los más competitivos para pagarla a los precios que exija la oferta. Es en ese momento donde puede que a los colombianos les sea más rentable vender a otros países que también la demanden y sí que tengan Bitcoin para pagarla. Pero esto nos lleva a preguntarnos como saber dónde estará el Bitcoin en el futuro, debido a su diseño, no podemos saber cuánto dinero puede ser gastado en un territorio. La libre circulación de capitales junto a la imposibilidad de confiscarlo nos lleva a un escenario donde el libre-mercado es inevitable a largo plazo.

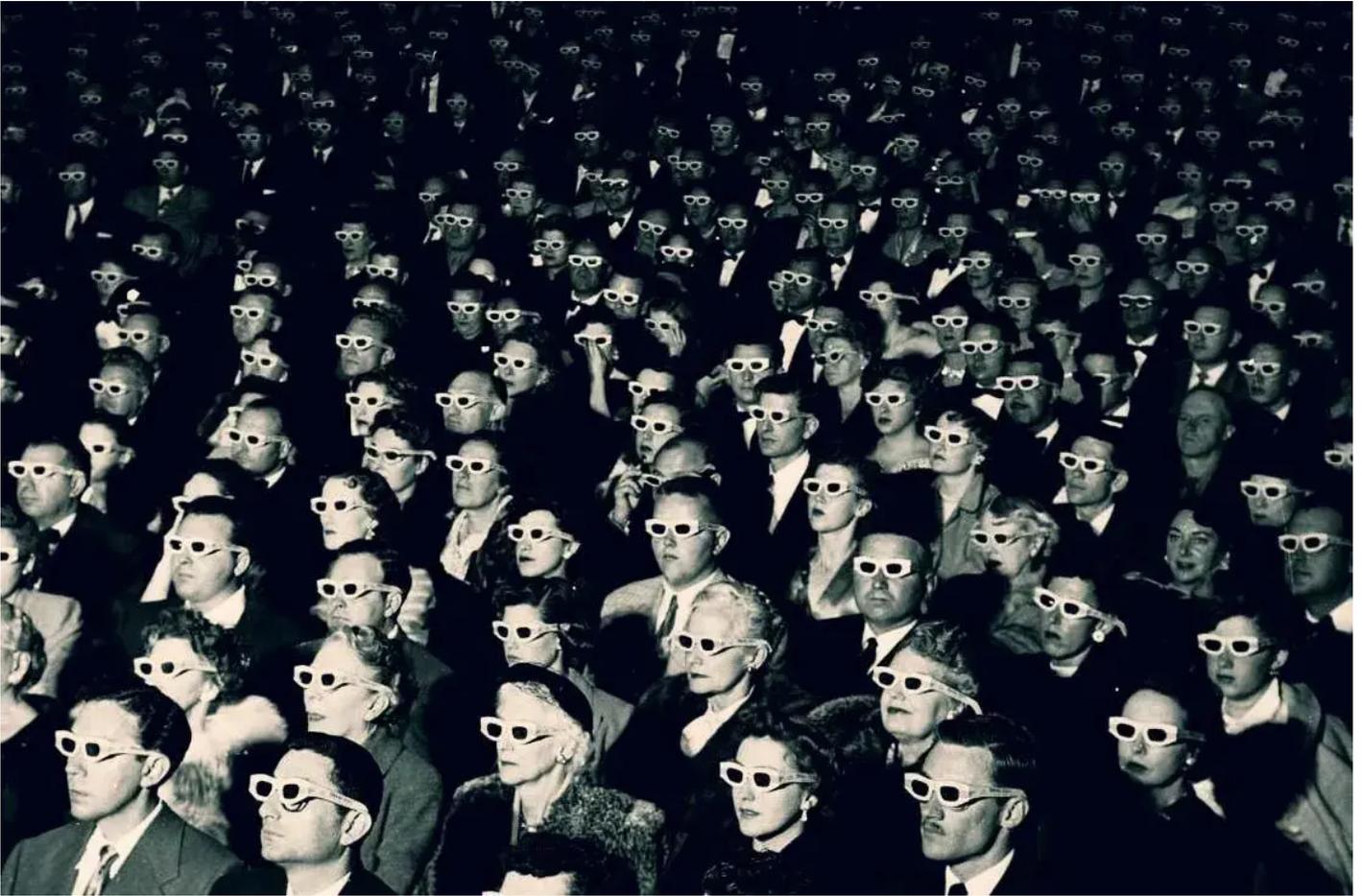
Si la cocaína colombiana empieza a ser vendida a otros territorios que hayan conseguido organizarse mejor, México deja de jugar un papel tan importante en la distribución de este mercado. Esto podría desincentivar tanta violencia en el territorio, lo que es bueno para los civiles mexicanos a nivel convivencia. Por supuesto nada se dará de la noche a la mañana, solo estoy intentando describir una tendencia que veo. No dudo que el gigante americano se recupere, solamente dudo que lo haga con la suficiente rapidez como para que los productores no busquen colocar su producto en mercados que estén más capacitados para demandarlo a corto plazo. En Europa auguro lo mismo, si los países que demandan el hachís marroquí no tienen Bitcoin ni saben cómo generarlo con rapidez, puede que veamos como el producto se distribuye a otros territorios.

Este punto tiene que ver con la cantidad de Bitcoin que haya en los países que demandan droga, pero si hablamos de la pérdida del privilegio monetario del que ha dispuesto occidente, puede que cambien otros mercados como podría llegar a ser el energético en Europa. Si empezamos a jugar sobre unas reglas y un tablero claro, puede que los países nórdicos no dominen sobre los del Sud con tanta facilidad. También juega un papel esencial la forma en que en cada territorio rediseñen el concepto de propiedad.

Me gustaría cerrar este breve artículo con algunos in-puts que buscan hacer pensar al lector. Lo primero es decir lo gracioso que me parece que el Narco a día de hoy siga enterrando grandes cantidades de efectivo. Los problemas que tienen con los cuerpos antidrogas por usar el sistema bancario tradicional. Cuando descubran como usar debidamente Bitcoin, las reglas de ese juego cambiarán. También quisiera decir que en un escenario Bitcoin Standard donde el estado desaparece por sus problemas de financiación, el control de fronteras, prisiones y tribunales se dificulta mucho. Esto podría generar una verdadera crisis nacional ya que sin recursos para financiar esta parte de la seguridad, es mucho más complicado intentar detener algunos negocios.

Ahora mismo la distribución es relativamente barata porque los estados y funcionarios ya están acostumbrados a la corrupción, pero una vez paren los flujos hacia estos agentes no sabemos si será más arriesgado comerciar este tipo de productos. Para mi esta es una de las cosas más bonitas de Bitcoin, por mucho que cambie el dinero y toda la estructura, puede que convirtamos este mundo en un lugar más inseguro y eso puede llegar a dificultar el comercio. No es que esto sea malo, sino que significará un descubrimiento de precios que nos demuestra la realidad de la economía. No puede haber libre comercio si no existe un consenso, ningún bitcoiner estará a salvo si el mundo no alcanza la paz.

# Situacionismo



[Begleri \(@begleristirner\)](#)

Publicado: 07/02/2023

Tags: Filosofía

Tomé la orangepill en junio de 2021 y pasé hasta julio transmitiendo aquello que había entendido a familia y amigos. Sentí que debía compartir lo que me impulsaba a cambiar de estrategia de forma rápida, ya que sentía que el mercado podía desestabilizarse en cualquier momento, el precio de Bitcoin empezar a dispararse y las quiebras y posibles guerras empezar a disparar los precios de los productos que llegaban a los consumidores.

En la primera semana se lo conté a un amigo arquitecto al que tengo un gran aprecio. Él ya había hecho su búsqueda en el mundo de las criptomonedas y contaba con un portfolio con menos volumen del que ya había tomado ganancias para costear viajes de surf. Me compartió el Manifiesto Situacionista, escrito por Guy Debord en el año 1960, algo que quedaba bastante lejos de mis áreas de búsqueda. En caso de que el lector no haya leído el manifiesto, le recomiendo mirárselo antes de seguir con este artículo, es mejor recibir los in-puts por primera vez sin una

referencia desde la que enfocarlo. En mi caso, alinee al momento la crisis que se describe con la transición a la que creo que Bitcoin nos aboca. Quisiera ordenar mi explicación en cinco puntos: Propiedad, Tiempo, Artistas, Cultura, Teoría del Valor.

## **1. Propiedad**

Bitcoin sustituye al dólar como moneda de reserva y comercio. El estado queda fuera de juego por no poder confiscar, sin financiación para los instrumentos que garantizan la seguridad y la propiedad no podemos esperar que los ciudadanos se opriman a sí mismos y respeten las antiguas convenciones sociales. Desde luego en algún momento hay un vencedor o un territorio decide organizarse pacíficamente, pero si ahora este grupo que se hace llamar gobierno consigue financiarse será de forma privada. La palabra pública como se entiende en Economía desaparece en el momento en que no hay ningún agente que pueda confiscar. De igual forma si alguien decide contribuir o aportar a una organización de forma monetaria, no puede ser llamado impuesto, ya que ya no existe la forma de imponer la confiscación. En un modelo donde esta forma de ?? violencia blanda?? como la confiscación no existe, está por ver si las nuevas leyes creadas por el nuevo gobierno van a respetar la propiedad privada como es entendida en la actualidad.

En aquellas ciudades donde un grupo terrateniente tome el poder e imponga sus leyes, seguirá habiendo un modelo como el actual donde algunos individuos deberán estar dedicando parte de su día a generar unos recursos que deberán entregar a ese grupo. Pero en aquellas ciudades donde el grupo que tome el poder no imponga la propiedad sobre la tierra, experimentará un cambio en el comportamiento de todos los ciudadanos por haber cambiado los incentivos. Consideramos que todo lo que gasta el individuo se puede clasificar entre Refugio, Alimento y Ocio. Entendiendo el ocio como todas aquellas voluntades que no tienen que ver con la supervivencia del individuo. Si el individuo ya no tiene que generar recursos para tener un refugio, puede disponer de más tiempo y decidir donde emplearlo. Para generar el suficiente alimento que necesita un individuo en un mes puede que no se requieran 40 horas semanales contando con una economía en funcionamiento aunque sea a nivel local. Sin propiedad, las preferencias e incentivos cambian, llevando a la economía a nuevos equilibrios.

## **2. Tiempo**

El individuo tiene unas necesidades fisiológicas que debe saciar para su supervivencia. También tiene unas amenazas en el mundo real que condicionan su comportamiento y por lo general lo llevan a buscar la sensación de protección. Una vez ha saciado estas necesidades ya no está pensando en sobrevivir, está pensando en vivir. De aquí salen los tres bloques referentes a gastos del individuo del apartado anterior.

El tiempo es el único recurso del que realmente dispone el individuo y es un recurso limitado. De ahí que nos veamos obligados a dedicar parte del tiempo a la supervivencia y el resto a buscar maximizar el bienestar o el placer. Un esclavo es entendido como un individuo no-libre ya que es propiedad de otro individuo. La propiedad se origina en un contrato social, puede que únicamente entre esos dos individuos si uno consigue que el otro acepte esa idea y la interiorice. Pero ser un esclavo de facto significa que un individuo no dispone de tiempo que pueda emplear en maximizar su bienestar o su placer. Más allá del entendimiento que tenga el individuo de su vida, lo que

realmente importa es lo que hace con el tiempo del que dispone. Es por este motivo que la emisión monetaria es una estafa a los individuos que sufren las consecuencias en forma de inflación, están desvalorizando su tiempo haciendo que deban dedicar más recursos a la supervivencia que a la vivencia.

El objetivo de una sociedad debería ser procurar el mayor tiempo libre posible a los habitantes. Cada individuo tiene voluntades y preferencias diferentes y debe dedicar su tiempo a saciar aquellas que más prefiera. Sin un modelo basado en propiedad, el individuo no debe estar generando recursos para entregarlos a los terratenientes y puede disponer de ese tiempo para otras actividades. Aquellos individuos que centran su tiempo, recursos y energías en la búsqueda de la virtud son los que considero artistas. Si vemos un cambio en los equilibrios económicos, los artistas tendrán más tiempo para Ocio y deberán destinar menos tiempo a la supervivencia.

### **3. Artistas**

Los situacionistas al igual que más movimientos avant-gardistas van contra la idea de que el arte la encontramos en un expositor. De igual forma, el artista no es una persona especial sino que todos los individuos pueden ser artistas. Es esta aceptación de que el arte está en todo lo que provoca la propia desvalorización del arte como es entendida previamente. Siendo artista cualquier individuo que cree buscando la virtud, su arte se puede considerar puro cuando el artista crea aquello que quiere expresar. Muy diferente es cuando el artista debe conseguir sobrevivir y ofrece sus servicios al mercado a cambio de una remuneración. En este caso con su talento crea algo que el mercado quiere que sea expresado, pero no son propias del artista estas ideas. Si los artistas dejan de tener tantas obligaciones de pago, podrán dedicar más tiempo a producir su arte en vez de lo que el mercado demanda de ellos. Esto nos aboca a un escenario donde habrá más producciones, más artistas y por lo tanto una explosión de creatividad que puede ayudar a otros campos como puede ser el tecnológico.

### **4. Cultura**

Este punto puede que sea el más emblemático de la propuesta del manifiesto, atacar la conservación de arte, conectándola directamente con la necesidad de dejar huella. Los autores asocian los dos conceptos desde la oferta, por la participación total de los individuos se tendería a una producción colectiva y anónima. Me parece muy interesante como presentan que la Novedad desaparece, aún no me atrevo a dar mis puntos sobre esas percepciones del tiempo.

Esa participación total se da cuando termina el ocio pasivo, entendido el ocio pasivo como la relación entre artista como productor y espectador como consumidor. Al caer los instrumentos que garantizan la propiedad privada a base de violencia, las nuevas sociedades libres de propiedad podrán dedicar su tiempo a la creación de una nueva cultura y pueden decidir en qué medida respetarán la cultura del modelo anterior. No estoy manteniendo que se deba destruir la cultura pasada, solo pongo en duda que esa sea más valiosa que la nueva cultura que se está generando. No se puede esperar que las generaciones presenten destruyan la cultura pasada y esperen que las generaciones futuras respeten sus creaciones.

Atacar la conservación del arte me parece un argumento socrático, quién atacó que se repitiera la misma obra teatral por difundir ideología sobre los individuos de la polis. Me parece interesante como se relacionan la conservación del arte y la política, ya que es a través de la cultura como se expanden las ideas en política que son las que acaban determinando quién controla el territorio y los recursos. Por ese motivo la creación de un arte sin buscar su conservación me parece un arte puro, sin incentivos de mercado ni sociales, ya que no busca convencer de ninguna ideología. Es esta la arquetípica relación entre Ulises y Aquiles sobre la gloria y el concepto de ??Dejar huella??. En cada ciudad se tendrá una opinión colectiva diferente al respecto y se respetará más o menos la cultura anterior y se producirá diferente la cultura contemporánea.

## 5. Teoría del Valor

Bitcoin a mi parecer me demuestra que los austríacos habían acertado en la forma en la que entendían el valor. Una teoría del valor marginal que resuelve la paradoja del agua y del diamante me demuestra que el valor es una proporción y está en constante cambio. Sucede de la misma forma en el mundo del arte donde no se puede llegar a determinar el valor de una obra. Es un grave error pensar que el valor y el precio van por separado, ese es el argumento de aquellos que entienden que el valor se genera desde la oferta y el mercado lleva su valor a una apreciación con la que no están de acuerdo. En el arte al igual que en cualquier mercado, el producto vale siempre que la demanda vea alguna utilidad en él. Si ahora los productores dejan de producir para los consumidores porque ya no buscan vender sus obras, puede que haya un gran desajuste en los precios como se han entendido hasta ahora en el sector.

Recordemos que los productores ya no piensan en vender, ya que no necesitan ingresar para pagar al grupo en el poder que domina la propiedad sobre la tierra. Ahora producirán por el placer de producir, sin importar la venta puede que algunos artistas le pierdan la razón a la conservación.

Me parece muy interesante la forma en la que tratan el arte los situacionistas, yo he querido entender que describen al artista como el individuo que crea pensando en la virtud. En el mundo crypto han basado el valor de los NFTs en la certificación alardeando de que la Blockchain permite la conservación de esa verificación. Entendiendo que la certificación, que es un concepto importante en un modelo sustentado en la propiedad privada, seguiría siendo valiosa en los modelos futuros. Personalmente en el momento que empecé a entender que Bitcoin desmonetizaría a todos sus competidores, entendí que sería la única Blockchain donde tiene sentido registrar una obra como puede ser un texto, un jpeg etc Pensar que esa certificación le dará un valor en el futuro es demostrar no haber entendido que el Valor es una proporción, tiene una naturaleza dinámica, no estática.

En este inicio de 2023 la creación de NFTs sobre Bitcoin gracias a Ordinals pone varios debates sobre la mesa. Desde la parte artística opino que se debería debatir si tiene un sentido la certificación de contenido que no tiene nada que ver con Bitcoin. Desde luego si se hace buscando la permanencia de ese registro sí que lo tiene, ya que todos los nodos que se comuniquen en el mismo lenguaje que el que crea el NFT tendrán una copia de esa información. Si se hace con la idea de empezar a registrar arte para construir un mercado sobre ese registro, creo que los in-puts que nos dejan los situacionistas pueden ayudar a aquellos individuos que no tienen clara su opinión sobre el debate Aquiles / Ulises.

En mi formación al igual que en la de muchos plebs, el libro Bitcoin Standard de Saifdean ha tenido una gran influencia. Ayuda a entender la utilidad de Bitcoin comparándola con el oro, por lo que se fija en una discusión monetaria más que en los aspectos técnicos de la red. Sin embargo el autor da una opinión personal sobre el arte contemporáneo comparándola con el arte renacentista. Su punto es que los productores actuales buscan vender su producto al mercado y por lo tanto buscan ser eficientes en la producción. Emplear poco tiempo, pocos recursos y buscar agradar a la demanda para obtener más ventas. Lo compara con como los artistas renacentistas producían de forma más elaborada buscando un producto de mejor calidad. Lo acompaña con la idea de que a esos artistas los financiaban grandes familias que pudieron permitirse invertir esos recursos en los artistas gracias al oro. Yo no pongo en duda nada de este razonamiento, únicamente quiero criticar la osadía del autor de afirmar que las obras renacentistas eran más valiosas por ser producidas buscando la virtud.

La virtud en el mundo del deporte puede llegar a ser objetiva, un corredor es más rápido que otro si consigue recorrer una distancia determinada en menos tiempo. Pero en las disciplinas donde hay jueces se suelen tener en cuenta factores como la creatividad o belleza que están llenos de discusiones subjetivas. Lo mismo sucede con el arte ya venga en formato gráfico, musical o escenográfico, por mucho que la producción sea buscando la virtud o buscando la venta, no existe forma de diferenciar el valor de lo inútil más allá de la apreciación colectiva. Viene a ser la discusión entre los amantes de Rock que critican el Techno o el Reggaetón, atreverse a decir que una música es mejor que otra es querer estandarizar gustos lo cual es imposible.

Por este motivo creo que el ecosistema bitcoiner debería plantear las discusiones sobre arte de la misma forma que las planteamos sobre la teoría del valor, aceptar que no existen unos parámetros universales. Lo que sí es objetivo es afirmar que en un modelo basado en el consenso como es Bitcoin, no se pueden imponer incentivos que ocupen el tiempo de los artistas, por lo que es de esperar un incremento de la producción de arte. No podemos afirmar que será un incremento de la cultura, ya que no sabemos si los artistas contemporáneos tendrán esta fijación en la conservación de las obras y tampoco sabemos la posición de cada sociedad respecto a la conservación de la cultura pasada.