Tabla de Contenidos

Prólogo 04

Referirse A Bitcoin Como Un Proyecto De La NSA/CIA Es Una Falta De Respeto A Los Cypherpunks **06**

Explicando El Lightning Network Para Que Hasta Un Niño De 10 Años Lo Pueda Entender 14

5 Razones Por Las Cuales Deberías Correr Tu Nodo De Bitcoin En Un Raspberry Pi 4 ..... **20**

Elon Musk No Comprende La Descentralización – Pero Tu Deberías 27

NFTs De Bitcoin En Counterparty (Y Como Obtener O Crear Tu Primero) **36**

Los Beneficios De Privacidad De Taproot 49

¿Puede Bitcoin Funcionar Como Papel Moneda? **54**

Billeteras Hardware DIY, Parte I: Construyendo Tu Propia Billetera Trezor One, Model T Y BitBox02 57

Billeteras Hardware DIY, Parte II: Construyendo Tu Propia Billetera PiTrezor, Specter DIY, SeedSigner Y Bowser **64**

No Puedes Retirar A Tu Billetera Propia? No Es Tu Bitcoin 72

Porque Bitcoin Incentiva La Sustentabilidad Y El Cuidado Del Medioambiente **74**

Cómo Casi Me Hago Rico Minando Bitcoin En Braiins Pool Durante Un Mes 78

Prólogo

Luego de haber vivido la mega crisis del año 2008, me fue muy claro que existe una diferencia abismal entre el ahorro y la inversión. En un sistema fiat inflacionario, y peor aún, con tasas de interés reales negativas, mantener el poder adquisitivo de la acumulación de energía puesta en mi trabajo, con el objetivo de proyectar a futuro y a largo plazo, se haría imposible. Comprar oro es demasiado engorroso y poco práctico, y almacenarlo es caro e inseguro. La única alternativa medianamente viable era invertir, es decir, tomar riesgo con el capital que tanto me había costado acumular. Me resultaba incomprensible que para hacer crecer mis ahorros, estos deberían temporariamente dejar de ser míos, y que debía dejarlos a disposición de otros que lo pondrían en riesgo. Claramente no era yo el único bajo este paradigma, sino que éramos billones de individuos alrededor del planeta.

Haber obtenido un título universitario en finanzas keynesianas, además de la prestigiosa designación profesional del CFA Institute exacerbaba mi frustración. Fue en ese momento que comencé a desarrollar un interés por la perspectiva de los no muy conocidos economistas de la escuela austriaca tales como Menger, von Mises y Hayek.

Pasaron los años, y las inversiones que había hecho a falta de una mejor alternativa, tuvieron rendimientos más que aceptables, pero nunca me senti comodo, y habiendo vivido desde adentro distintas crisis financieras y analizando las políticas expansionarias de los principales bancos centrales, percibia y sigo percibiendo que esta ruta de dinero fácil y emisión sin respaldo tarde o temprano terminaría mal. Esos elevados retornos generaron en mí una postura de complacencia, la cual dilato mi búsqueda de otra alternativa con la cual sintiera que mi capital fuese mío, sin intermediarios, y a disposición mía, y solo mía, sin importar el lugar y el tiempo.

Y pasaron los años, y a pesar de haber escuchado de Bitcoin, básicamente lo ignoré. Mi formación académica no ayudó, y ni mi curiosidad ni mi inclinación a aprender cosas nuevas me hizo reaccionar. Hasta que afortunadamente en 2016 me tope con un video de Andreas Antonopoulos y todo cambió. Finalmente parecía haber encontrado la alternativa ideal. Todo cambió. Desde mi forma de planear para el futuro hasta mi visión del mundo.

Gracias a haber tenido la fortuna de conocer el idioma inglés, pude aprovechar la infinidad de recursos gratuitos disponibles para profundizar mi conocimiento. Al mismo tiempo note que los mismos no existían es mi lengua natal, y desde entonces sentí que puedo hacer una pequeña diferencia y aportar mi grano de arena para que los 460 millones de personas de habla hispana puedan tener la oportunidad de embarcarse en este camino.

Mi primera idea para involucrarme en el mundo Bitcoin fue la de convertirme en un nexo entre los asesores en finanzas tradicionales y Bitcoin, pero no encontré entusiasmo por parte de estos actores, ni siquiera ofreciéndoles capacitación gratuita.

Para ese momento ya había encontrado una publicación en inglés que encajaba con mi forma de ver Bitcoin. Necesitaba que fuese exclusivamente de Bitcoin e ignorara los miles de otros tokens que en mi opinión no solucionan ningún problema. También era fundamental que no fuese patrocinada por compañías que condicionaran la calidad del material o contenido publicado. Aquí es donde entra Bitcoin Takeover, de Vlad Costea. Ofreciendo mi capacidad de traducción al español, pude no solo aprovechar y profundizar mi conocimiento, sino también satisfacer mi necesidad de acercar Bitcoin a todas las personas de habla hispana que pudieran beneficiarse de su contenido y así, comenzar su propio camino hacia la soberanía financiera, y poder mejorar su calidad de

vida presente y futura.

Debo mencionar que la ONG Bitcoin Argentina me permitió a través de sus charlas presenciales tener mayor facilidad de traducir los términos más técnicos que no dominaba.

El objetivo que me planteo es brindarle a la mayor cantidad de personas lo que me fue brindado a mi. Y así como yo lo obtuve sin costo alguno, considero que de la misma manera lo debo hacer yo. Pero también soy consciente de que hay un aspecto egoísta en todo esto o, cuanto menos, mutuamente beneficioso. Creo que Bitcoin es una herramienta extraordinaria pero el valor y la fortaleza del ecosistema está ligado a la cantidad de usuarios que lo utilicen. He ahí la importancia de ser embajador y difundir esta gran idea.

Para cerrar, les dejo una frase de Vlad que sintetiza lo que, en mi opinión, buscamos la mayoría de los Bitcoiners maximalistas, por llamarnos de alguna manera:

“Muchos Bitcoiners ya son ricos en términos de dinero fiat y han superado la fase especulativa de inversión. El objetivo no es enriquecerse más, es ser libre y ayudar al resto del mundo a lograr este objetivo. Están aquí por la revolución, y dedican más tiempo en educarse a ellos mismos y a otros en lugar de mirar gráficos de precio. Deben estar dispuestos a aprender a un nivel por encima de sus títulos académicos y fuera de su zona de confort, ya que las revoluciones no se dan si quienes las inician son torpes y poco educados - puedes sostener que sus ideas son ingenuas, pero nunca podrás cuestionar sus intelectos y preparación.”

–





Referirse A Bitcoin Como Un Proyecto De La NSA/CIA Es Una Falta De Respeto A Los Cypherpunks

Mientras que Satoshi Nakamoto pudo haber sido la NSA/CIA, Bitcoin definitivamente no lo es. Asimismo, los cypherpunks hicieron el 90% del trabajo de Satoshi.

Recientemente pregunté a mis seguidores de Twitter que compartieran su teoria conspirativa de Bitcoin favorita. Sorprendentemente, la mayoria mencionaron a la CIA, la NSA, u otra "agencia de tres letras" como potenciales creadores de la criptomoneda.

Deater Bob sugirio que Satoshi Nakamoto pudo haber filtrado el proyecto de Bitcoin de fuentes dentro del gobierno estadounidense. Gilroy menciono un plan maestro que eventualmente usaría las monedas de Satoshi como base para un nuevo departamento del tesoro estadounidense. Personas como Juan Galt y Jack también sugirieron que la NSA también pudo haber estado involucrada.



Y a pesar de algunas respuestas creativas (como la teoria de Wladimir Van Der Lean sobre que Bitcoin sea un hongo y la sugerencia de Bma Masari de que el internet mismo pudo haber obtenido conciencia para crear Bitcoin), no podia



dejar de pensar sobre las populares asociaciones de la creacion de Bitcoin con las agencias gubernamentales.

Debido a esto, explicare porque las asociacion es incorrecta – y aun si Satoshi Nakamoto es la CIA o la NSA, Bitcoin ya no pertenece a él, y no es tan innovador como la mayoria de la gente cree.

Bitcoin no surgio de la nada y utiliza multiples descubrimientos hechos por parte de los cypherpunks. Para darle crédito a Satoshi Nakamoto, el ha creado la mejor solucion al Problema del General Bizantino, y el/ellos son responsables de haber lanzado un tipo de dinero electronico descentralizado que se convirtió en un éxito. El ajuste de dificultad cada 2016 bloques también es un buen detalle, que ha sido crucial para la supervivencia de la red.

Sin embargo, existe una tradición de los cypherpunks que precede por más de 20 años al surgimiento de Satoshi. Este artículo presentara solo unas pocas invenciones que enseñaron a Satoshi a diseñar Bitcoin y que defectos evitar.

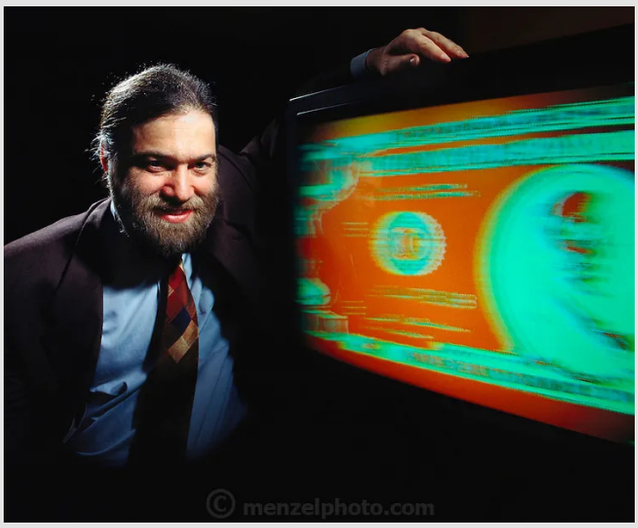
Satoshi Nakamoto Puede Ser La CIA/NSA, Pero Bitcoin Está Arraigado A La Tradición De Los Cypherpunks.

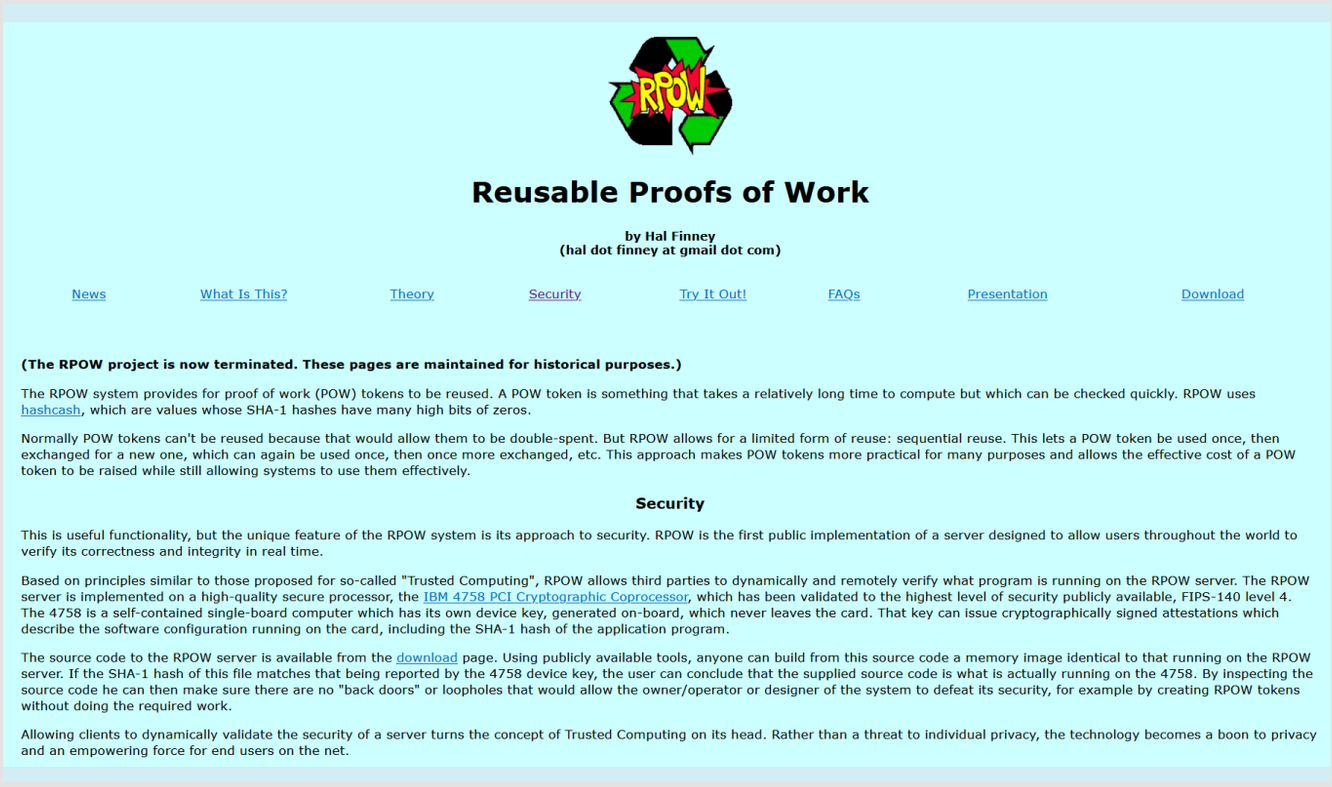
Mucha gente que no escucho, que duda, o que tienen poca informacion acerca de Bitcoin piensan que Satoshi Nakamoto inventó el blockchain y que merece reconocimiento por este sistema contable que generó una industria entera.

Tal como muchas otras invenciones criptograficas, el blockchain fue inicialmente conceptualizado por David Chaum durante su PhD en la Universidad de Berkeley. Su sistema Vault de 1979 hasta incluye controles y balances muy similares a los de Bitcoin: observadores (exploradores de bloque), hacedores (nodos), ejecutores (mineros), czars (desarrolladores).

Chaum también creó la primera forma de dinero digital (ecash) con la coorporacion DigiCash. Fue diseñado para arreglar cuestiones de confianza de los pagos por internet con tarjeta de crédito con un tipo de dinero lo suficientemente privado para ocultar la informacion personal que no fuese relevante para la transaccion. Sin embargo, su centralizacion, eventualmente provocó a fin de los 90 una caida decepcionante. Curiosamente, Satoshi no menciona a Chaum en el whitepaper de Bitcoin.

Volvamos al blockchain: la idea de una cadena de hashes usado para el marcado de hora enlazado también fue





Reusable Proofs of Work

by Hal Finney
(hal dot finney at gmail dot com)

News | What Is This? | Theory | Security | Try It Out! | FAQs | Presentation | Download

(The RPOW project is now terminated. These pages are maintained for historical purposes.)

The RPOW system provides for proof of work (POW) tokens to be reused. A POW token is something that takes a relatively long time to compute but which can be checked quickly. RPOW uses hashcash, which are values whose SHA-1 hashes have many high bits of zeros.

Normally POW tokens can't be reused because that would allow them to be double-spent. But RPOW allows for a limited form of reuse: sequential reuse. This lets a POW token be used once, then exchanged for a new one, which can again be used once, then once more exchanged, etc. This approach makes POW tokens more practical for many purposes and allows the effective cost of a POW token to be raised while still allowing systems to use them effectively.

Security

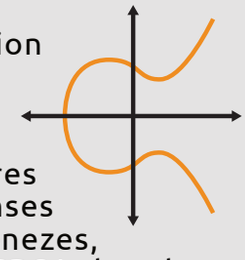
This is useful functionality, but the unique feature of the RPOW system is its approach to security. RPOW is the first public implementation of a server designed to allow users throughout the world to verify its correctness and integrity in real time.

Based on principles similar to those proposed for so-called "Trusted Computing", RPOW allows third parties to dynamically and remotely verify what program is running on the RPOW server. The RPOW server is implemented on a high-quality secure processor, the IBM 4758 PCI Cryptographic Coprocessor, which has been validated to the highest level of security publicly available, FIPS-140 level 4. The 4758 is a self-contained single-board computer which has its own device key, generated on-board, which never leaves the card. That key can issue cryptographically signed attestations which describe the software configuration running on the card, including the SHA-1 hash of the application program.

The source code to the RPOW server is available from the download page. Using publicly available tools, anyone can build from this source code a memory image identical to that running on the RPOW server. If the SHA-1 hash of this file matches that being reported by the 4758 device key, the user can conclude that the supplied source code is what is actually running on the 4758. By inspecting the source code he can then make sure there are no "back doors" or loopholes that would allow the owner/operator or designer of the system to defeat its security, for example by creating RPOW tokens without doing the required work.

Allowing clients to dynamically validate the security of a server turns the concept of Trusted Computing on its head. Rather than a threat to individual privacy, the technology becomes a boon to privacy and an empowering force for end users on the net.

presentado en 1991 en un paper de Stuart Haber y W. Scott Stornetta. A diferencia del trabajo de Chaum, Satoshi sí hace referencia a este descubrimiento en el whitepaper. También, el conocido bitcoiner Jameson Lopp ha mencionado esta investigación como precursor al blockchain de Bitcoin.



También está la eleccion de Elliptic Curve Digital Signature Algorithm (ECDSA), publicado en 1998 por los investigadores de informatica canadienses Don Johnson, Alfred Menezes, y Scott Vanstone. Con ECDSA, las claves públicas, las claves privadas, y las firmas son generadas con el fin de garantizar que los bitcoins solo puedan ser gastados por sus legitimos dueños.

Una teoria popular dice que Satoshi Nakamoto eligió firmas ECDSA por sobre firmas Schnorr por conveniencia, ya que habia disponibles un mayor número de bibliotecas que satisfacian mejor sus necesidades específicas a la hora de diseñar Bitcoin. Sin embargo hay muchas preocupaciones sobre privacidad (que incluyen la propension de la NSA de implantar backdoors) que eventualmente reemplazarán ECDSA por firmas Scnorr (gracias Pieter Wuille!).

La idea de que la criptografia utilice claves públicas tampoco es propiedad de Satoshi Nakamoto.: Ralph Merkle estaba investigando este tema en 1980 (mencionado por el creador de Bitcoin en el whitepaper), y PGP, la herramienta privacidad de correo electrónico de Phil Zimmermann (en la cual Hal Finney ha trabajado durante muchos años) ha estado disponible gratis en internet desde 1991.

Hablando de Hal Finney, también trató de descubrir Bitcoin con Reusable Proof of Work (RPOW). Sin embargo es Adam Back quien es mencionado en el whitepaper al ser el creador del sistema de hashcash en 1997 y perfeccionándolo para prevenir spam de correo electronico. Sin estos descubrimientos criptograficos, Bitcoin jamás hubiese obtenido el mismo nivel de seguridad – y los brillantes incentivos de minería muy probablemente no hubiesen existido.

Otro gran cypherpunk que tampoco

es mencionado en el whitepaper pero que ha descifrado el 90% de Bitcoin es Nick Szabo. Su sistema Bit gold combina exitosamente muchas piezas del rompecabeza de los más brillantes descubrimientos criptograficos, y tambien crea los principios del "oro digital" tan propios de la escuela Austriaca de economia (escasez, esquema fijo de emision para evitar los efectos de la hiperinflacion, facil verificacion).



Desafortunadamente, el diseño de Bit gold dependia de una mayoria de los usuarios de la red y facilmente podia ser blanco de un ataque de 51%. También, tenía un esquema de emision (inflacion) que decidia el mercado – lo cual significa que habría momentos en los cuales más bloques serian minados, y otros momentos en los cuales no habría ningun tipo de actividad y la seguridad del sistema muy probablemente sería menor. Lo que hizo Satoshi Nakamoto fue reemplazar la regla de los CPU con la regla del poder de hasheado, asi como tambien ingeniarselas para diseñar un sistema financiero desinflacionario (comenzar con un nivel de emision alta y reducirla a la mitad cada 4 años).

Estos cypherpunks valoraban por sobre todas las cosas la privacidad y la resistencia al NSA

El "punk" en "cypherpunk" marca claramente el movimiento el contra de la servidumbre al gobierno. Segun el opus de Tim May de 1994 "The Cyphernomicon", los cypherpunks estaban muy encontra de la vigilancia y buscaban mantener su

DOCID: 3839357 TOP SECRET

Approved for Release by NSA on 04-07-2008, FOIA Case # 10369

Vol III, No. 43 — Communicator, NSA's Employee Publication — 30 October 1995

THE FUTURE OF MONEY: PROTECTING DIGITAL "CASH" (U)

(U) Some of you may be aware that one of the big stumbling blocks in using the INTERNET for buying and selling goods and services is the lack of a secure and reliable system to pay for them. Several entrepreneurs have been attempting to develop reliable solutions to this problem. Mark Twain Bankshares of St. Louis recently announced that it would soon offer its customers electronic cash or "E-Cash" services developed by DIGICASH, an Amsterdam company run by cryptography-savvy David Chaum. Initially these services are intended to overcome many of the disadvantages of using credit cards for small dollar transactions, but these same technologies could offer new opportunities to those bent on counterfeiting, money laundering, or electronic theft.

privacidad en internet, al mismo tiempo desarrollando herramientas para ayudar a otros.

La obediencia de por sí era sinonimo de una capitulacion ideologica. David Chaum escribió “Firmas Ciegas para Pagos Irrastreables” en 1983, y “Seguridad Sin Identificación: Tarjetas para Computadoras para Convertir al Gran Hermano en Obsoleto” en 1985.



En un informe de la NSA en Octubre de 1985 (el cual fue desclasificado en 2008), fueron expresadas algunas preocupaciones con respecto a la manera en que DigiCash podia ser usado para actividades criminales. La existencia de este documento particular prueba que las intenciones de Chaum eran reales y que realmente estaba preocupado por la privacidad.



Es muy poco probable que cypherpunks como Finney, Szabo, Back, Haber, y Stornetta trabajasen para la NSA, la CIA o cualquier otra agencia gubernamental. De lo contrario su trabajo hubiese sido clasificado y restringido a solo ser usado por personal autorizado.

Y aun si asumimos que el trabajo open source fue publicado como tal con el proposito de obtener mejoras por parte de otros criptografos en internet, el hecho de que estas herramientas funcionan en contra de los intereses monopolicos de la NSA/CIA también hace lucir a los cypherpunks puros de corazón.

Si el NSA decide usar RPOW u otras idea detras de Bit gold para construir un sistema propio (lo cual muy probablemente ya haya sucedido en cierta medida), no significa que los inventores de estos sistemas hayan sido sus empleados.

Bitcoin fue inventado por Satoshi, pero nunca le perteneció a él

Como mucho, si retornara Satoshi Nakamoto podria mover sus monedas y gastarlas. No existe una clave backdoor,

no hay una posicion de desarrollador principal reservada, y no hay ningun desarrollador activo que esté esperando el regreso del creador.



Guste o no, Bitcoin no es la misma red que en el 2009. Ha pasado por numerosas mejoras y continuará dejando atras el legado a medida que más partes son reemplazadas.

En definitiva, el punto de Bitcoin no es permanecer sin cambios a traves del tiempo, sino mantener su politica monetaria, garantizar que Satoshi pueda regresar en cualquier momento y mover sus monedas, y preservar la descentralización.

Existen muchas cosas en las que Satoshi Nakamoto acertó, pero también mucho código que fue removido o reemplazado por desarrolladores. Hal Finney pasó mucho tiempo arreglando fallas de diseño en Bitcoin (hasta agregó ceros adicionales para definir la más baja unidad monetaria en 1/100.000.000 BTC) y sentó el precedente para que futuros desarrolladores busquen formas más elegantes y arreglos eficientes en un sistema que se veia rigido.



Bitcoin como sistema monetario está grabado en piedra con su esquema de emision fija, una tasa de inflacion predecible hasta 2140, recompensas de minería claras, y ajustes de dificultad convenientes cada 2016 bloques. Pero Bitcoin como red seguramente recibira muchas actualizaciones que lo haran mas rapido, mas privado, y más eficiente.

Propuestas de mejora tales como firmas Schorr, Taproot, y MAST están diseñados para traer mayor grado de privacidad y eficiencia del bloque (las transacciones se tornaran más chicas y más accesibles).

Hay muchas mejoras de privacidad que están siendo exploradas en redes de monedas alternativas y sidechains (es solo cuestión de tiempo para que Confidential Transaccions o MimbleWimble sean incorporadas en cierto grado a la capa base). En el futuro, es probable que la privacidad de las transacciones se torne más popular, y que sutiles trucos que garanticen la auditabilidad de la emision y la resistencia a la inflacion sean implementados.

Si Satoshi regresara, probablemente no reconoceria su propia invencion. Pero eso es para mejor, ya que la red está creciendo y convirtiéndose en mucho más eficiente para su proposito. Bitcoin es como un automovil potente al cual se le hacen muchas mejoras sin nunca cambiar su carrocería – siempre mantendrá sus atributos de diseño principales, pero con un mejor motor y ventanas a prueba de bala.

Si Satoshi Nakamoto fuese la NSA/CIA, igualmente Bitcoin no les pertenece

¿Fue Bitcoin diseñado por una agencia de tres letras? Es definitivamente posible. Podrian la CIA y la NSA utilizar Bitcoin para transacciones? Eso es aún más probable. Pero ninguna de estas dos posibilidades llevan a una conclusion que ponga a una agencia gubernamental en control.

Actualmente, Bitcoin posiblemente sea la red computacional más descentralizada del planeta. Ha funcionado desde Enero de 2009 con solo dos instancias de interrupcion (debido a un bug de inflacion en 2010 y debido a una pobre sincronizacion de red en 2013) y tiene unos 10000 nodos operando a traves del mundo (sin contar a los que están corriendo en Tor ni a los que no abrieron el puerto 8333).

Algunos argumentan que pueden existir backdoors: y el mayor daño que pueden causar es quebrar las firmas (lo cual permitiria el robo de fondos) o quebrar la criptografia detras de SHA256. En cualquiera de estos dos casos, es posible que la comunidad haga un hard fork hacia una nueva cadena, reemplazando ECDSA y SHA 256 con alternativas existentes que ya han sido desarrolladas, y restablecer la tenencia previa de monedas en bases a prueba criptografica. La solucion no luce popular en este momento, pero puede ser el último recurso en el caso de un fuerte ataque que Bitcoin nunca realmente afronto.

Pero aun si asumimos que Satoshi Nakamoto es el líder de todos los agentes de la CIA, el experimento ha escapado su control – y nunca más lo tendra, salvo que la red se torne más centralizada (como pasó con BCH y BSV).

Y aun si la mitad de la comunidad de Bitcoin estuviese paga por parte de la CIA, la otra mitad todavia podria resistir ataques pasando a otra cadena que retenga las reglas pero que cambie los mecanismos de seguridad. Es todo software open source y las formas de proteger la privacidad de uno deben hacerse cumplir.

A pesar de todo, gracias a los brillantes incentivos de la red, es mejor para todos (sean agentes de la CIA o no) mantenerse unidos y proteger la misma red. Mientras la codicia exista, Bitcoin seguira siendo seguro y adversario en terminos de quien se suma y por qué motivos lo hace.

El lema “no confies, verifica” se refiere principalmente a la validacion personal



de otras personas e implica que tengas tu propio nodo como manera de probar que los fondos existen y que son legítimamente tuyos. Por lo tanto, es una presuncion que todos los otros están para robarte, porque como bien sabes, todos son unos estafadores.



Muh Satoshi

El Satoshi Nakamoto que conocemos de los posteos en foros y de las listas de distribucion de correo electronico de los cypherpunks era bastante humilde y realista. Estaba dispuesto a ayudar a cualquiera a entender como funciona Bitcoin – con la excepcion de Daniel Larimer, quien fue rechazado de una forma impresionante.

Sin embargo, convertirlo en una especie de figura Mesianica que nos dio el poder de Espiritu Santo y que partio para regresar “algun día” es definitivamente equivoca. No podemos negar las contribuciones de Satoshi al mundo de la criptografia, pero tampoco podemos exagerar su trabajo.

Por supuesto, el cuento de un programador informatico desconocido que lanzó un innovador sistema de dinero digital de la nada suena romántico. Atrae a nuevas personas y mantiene a los medios ocupados con investigaciones falsas. Sin embargo, la genialidad de Satoshi Nakamoto está sobrevaluada y es muy poco lo que sumó a las impresionantes, pero menos populares, invenciones de sus colegas.

Es el clasico ejemplo de Isaac Newton y Gottfried Wilhelm Leibniz: todos conocen al primero y a su historia con la manzana, pero tienden a olvidar al segundo. Ambos descubrieron calculus matematico integral alrededor del mismo tiempo, pero la gloria parece estar del lado del erudito Inglés de una forma hasta cierto punto injusta.

La conclusion final es que no importa quien realmente fue Satoshi Nakamoto y es extremadamente irrelevante a esta altura en el desarrollo de Bitcoin. Al mismo tiempo, los relatos sobre la CIA/NSA son bastante desventurados dados los orígenes cypherpunk de Bitcoin. Mientras Satoshi pudo haber sido la NSA, entonces Bitcoin claramente no lo es.

–



Explicando El Lightning Network Para Que Hasta Un Niño De 10 Años Lo Pueda Entender

Como segunda capa de Bitcoin, el Lightning Network trae muchas mejoras. Cuenta con pagos instantaneos que la escala a una capacidad de rendimiento similar al de Visa, y lo más importante, es altamente privado. También puede hacer todo lo que las monedas alternativas como Ethereum ya hacen (NFTs, DeFi, creacion de tokens, contratos inteligentes avanzados), pero de una manera más elegante y más eficiente en terminos de costo.

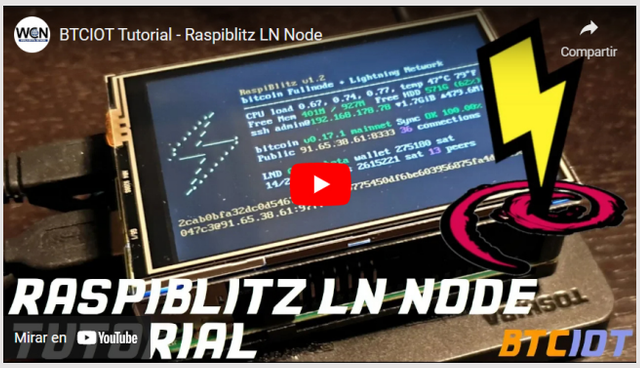
Pero a pesar de estas ventajas, mucha gente no se integra al Lightning Network simplemente porque no entienden lo que es, como funciona, ni cómo participar. Para facilitar la comprension de todos, voy a tratar de explicar la terminologia esencial usando ejemplos practicos y analogias. Y si tienes más de 10 años, lo vas a comprender.

Necesitas Tus Propios Nodos De Bitcoin Y De Lightning

Primero que nada, para poder correr el Lightning Network, tendras que correr tu propio nodo. Vivimos en un mundo descentralizado, haciendo lo mejor para desarrollar productos y servicios que no requieran confiar en una tercera parte. Idealmente, deberias comprar hardware especializado para tu nodo – y tienes soluciones ya fabricadas tales como:

- RaspiBlitz (unos $350, hay distribucion en Europa y Estados Unidos);
- MyNodeBTC (unos $339, puedes comprarlo en su tienda);
- Nodl ($529, puedes comprarlo en su tienda);
- Start9 Labs Embassy (unos $289, no incluye disco duro, puedes comprarlo en su tienda).

Si quieres reducir estos gastos y experimentar un lindo proyecto DIY de fin de semana, puedes comprarte un



BTCIOT Tutorial - Raspiblitz LN Node en World Crypto Network - youtube.com

RaspBerry Pi 4B con 4GB de RAM, un SSD de 1TB a tu eleccion (pero debe ser de una marca confiable), una tarjeta SD de 32GB, una cobertura de disparador térmico para mantener tu RaspBerry Pi frío durante los veranos y los procesos de recurso intensivo, y algunos cables. Mira este tutorial paso a paso de Ben Arc para entender mejor lo que necesitas hacer para correr un RaspiBlitz.

Si no quieres comprar un dispositivo especializado, hay por lo menos dos maneras populares de correr un nodo Lightning en tu computadora. El más avanzado usa la billetera Electrum (la guia completa puedes verla aqui), y la opcion mas basica y facil de usar te resultara Linux con Umbrel. Si estás para un desafío más grande, también puedes correr RaspBerry Pi OS en tu computadora Windows o Mac o usar máquinas virtuales.

Pero la recomendación de correr un dispositivo especializado es por cuestiones de eficiencia y seguridad: el RaspBerry Pi es muy eficiente energeticamente y ecologico (solo te costara un par de dólares tenerlo corriendo 24/7), y siendo un dispositivo que desempeña una sola tarea tiene una menor superficie de ataque que algo que se usa para abrir emails, instalar software de terceras partes, y acceder a sitios de internet dudosos.

Así que si puedes obtener un RaspBerry Pi para correr este nodo, deberias. No es muy accesible por ahora, pero esto solo mejorará con el tiempo a medida que avanza la tecnologia y se lanzan equipos más rapidos e innovadores.

Los Nodos Lightning Son Islas, Los Canales Son Rutas

Un malentendido comun sobre el Lightning Network es que correr un nodo es suficiente para conectarse con el resto de la red. Aunque el nodo sea un requisito esencial, el proximo paso en tu camino es abrir canales con gente.

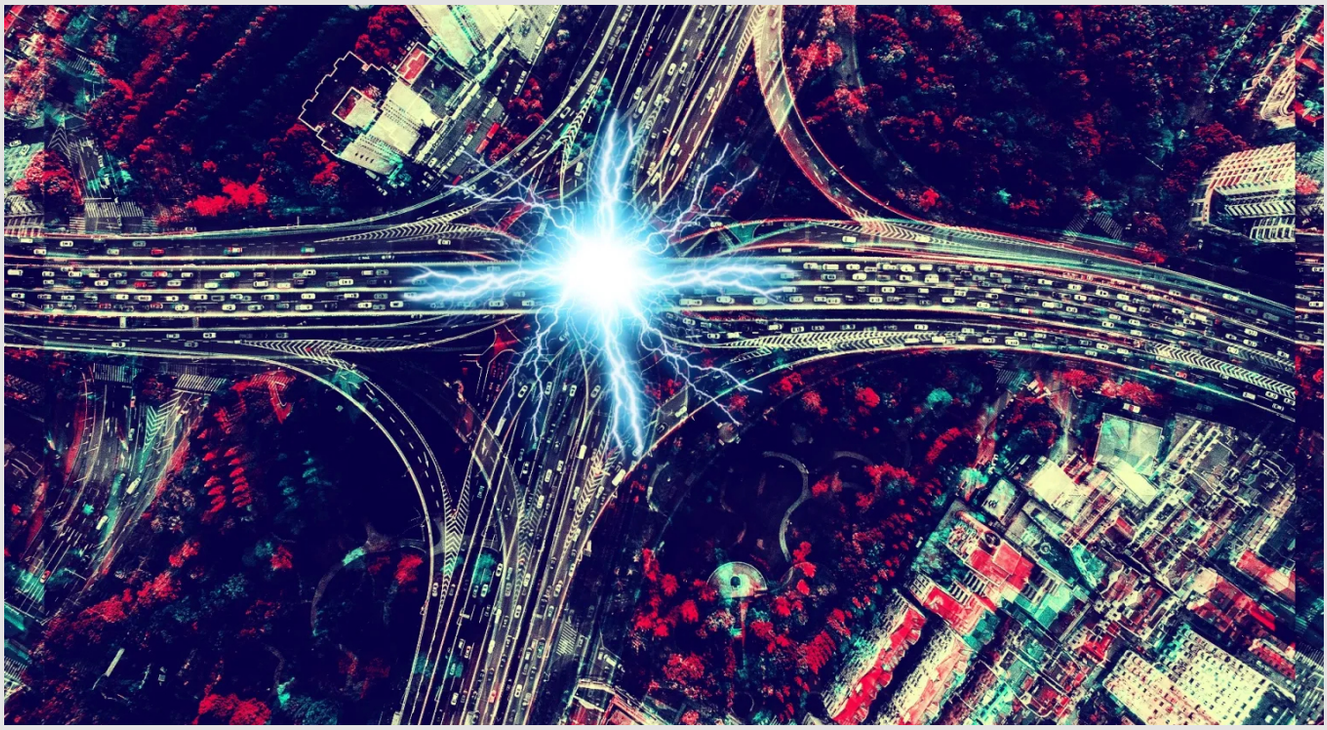
Para entender mejor el concepto, piensa en tu nodo como si fuera una isla que acaba de emerger en medio del océano. Tu objetivo es construir rutas con todos aquellos con los que estaras haciendo transacciones. Cuantas más rutas tengas más conexiones y mejores atajos tendras para llegar a ciertos destinos.

El tamaño de tus canales también es importante, ya que permite transacciones más grandes. Es como si tu puente a otra isla solo permitiera viajar vehiculos de hasta cierto peso – cuanto más resistente es el puente, mayor peso podrá aguantar durante un viaje.

Estas rutas van en ambos sentidos: puedes construirlas con otras islas (lo cual incrementa tu capacidad de enviar) u otras islas las pueden construir contigo (lo cual incrementa tu capacidad de recibir). Una isla bien conectada va a necesitar ambas.

Cuando envías dinero a una determinada isla en el mapa, vas a tomar una de las rutas existentes. Si tienes una ruta directa, todo es sencillo y puedes hacer una transaccion segun el tamaño de tu canal. Pero si están conectadas por la ruta de otro tendras que pagar una tasa de ruteo (basicamente un peaje).

Idealmente, deberias abrir canales con todos los otros nodos de la red para tener conexiones directas – pero eso no



es práctico e imposible de lograr en escala. Cuando millones de bitcoiners abran por lo menos un canal cada uno todos los dias, va a ser dificil tener los fondos, el tiempo, y la energia para seguirle el paso al crecimiento del Lightning Network. Pero rutear es altamente eficiente y también brinda algunos beneficios de privacidad: tal como es el caso con la red Tor, cada nodo relevador suma otra capa adicional de encriptación y anonimidad.

Si construyes rutas, también puedes cobrar comisiones a aquellos que usen tu infraestructura para llegar a su destino. Ser un intermediario de otras transacciones puede tener beneficios financieros, y la mayoria de los managers del Lightning Network te permiten escoger cuánto quieres cobrar a quienes usan tu ruta. Solo ten presente que usualmente es la ruta más corta, rapida y menos cara la que se elige. Entonces a menos que conectes una isla desconocida que otros ignoran, deberias pensarlo dos veces antes de cobrar una comision alta. A escala, estas pequeñas ganancias deberian subsidiar los costos de electricidad de correr tu nodo.

Los managers del Lightning Network tales como RTL (Run the Lightning) te permiten abrir canales privados. Esto significa que solo tu y el nodo con quien construiste el puente pueden ver el uso de esta infraestructura. A pesar de tener algunos beneficios de privacidad (nadie mas sabra de el), no rutea otras transacciones así que realmente no ayuda a la red y no te hará ganar comisiones de ruteo.

El tamaño de tus canales (o la resistencia al peso de tus rutas) no es permanente y puedes rebalancearlo para extender o reducir su capacidad. Vas a pagar comisiones por esta operacion, pero es un buen hábito monitorear las operaciones existentes y repriorizar segun lo que observas. Mayor popularidad y uso pueden beneficiarse de la mejor capacidad.

Por último, pero no menos importante, recuerda que los canales son más fáciles de remover que las rutas. Con el clic de un boton, puedes cerrar un canal y regresar los fondos a la capa base de Bitcoin. Cada vez que abres un canal pagas un fee de transaccion a los mineros de BTC, y lo mismo sucede cuando lo cierras. Para evitar pagar demasiado por estas transacciones, ve mi guia sobre como pagar menores fees de transaccion.



Los Clientes Lightning: LND, C-Lightning, Eclair, Y Nayuta

Así como las rutas pueden ser construidas de distintos materiales que vienen con sus ventajas y desventajas, el cliente de referencia de Lightning también tiene cuatro versiones con sus propias ventajas y desventajas. Historicamente, LND de Lightning Labs es la implementación más popular y también es la que es usada por los sistemas operativos de los nodos Raspberry Pi (con la excepcion de Embassy de Start9 Labs, que también viene con c-lightning). Gracias al gran espectro de aplicaciones y los efectos de red, es la más amigable para usuarios inexperimentados.

c-lightning de Blockstream es más refinado y mejor para desarrolladores, y está hecho en el lenguaje de programacion C (por eso el nombre). Sin embargo, tiene menos aplicaciones y es mayormente usado por exchanges y por servicios que necesitan mayor confiabilidad. También está diseñado para permitir atomic swaps entre activos del sidechain Liquid de Blockstream y BTC Lightning. Esto puede ser util si quieres realizar un peg-out sin usar servicios KYC de un exchange de la federacion Liquid. Si LND es como Windows, entonces c-lightning es una distribucion robusta de Linux no demasiado amigable con usuarios no tecnicos.

Eclair de ACINQ es también otra opcion popular, ya que está escrito en Scala y soporta plug-ins tanto de Java como de Java Virtual Machine. Como muchas aplicaciones de Android OS están escritas en Java, esta implementación es muy util para billeteras móviles. Phoenix y Eclair son dos de las billeteras móviles más populares, y definitivamente deberias probarlas.

Por último, pero no menos importante, tenemos a Nayuta – una compañía japonesa que comenzo a trabajar en un cliente de Lightning tan liviano que hasta un RaspBerry Pi Zero puede operarlo. Más recientemente, han lanzado una version alfa de Nayuta Core y también se enfocan en el desarrollo de billeteras móviles.



La Manera Mas Facil De Recorrer El Lightning

Idealmente, deberias correr tu propio nodo y hacer todo al pie de la letra. Pero si solo quieres probar lo que es Lightning y como funciona, puedes probar una billetera movil como Blue Wallet, Breez, o Eclair.

Blue Wallet se lleva el premio a la mejor experiencia de usuario de todas las billeteras de bitcoin. También es muy personalizable, permitiendote conectarte a tu propio nodo o bien depender de la infraestructura de la compañía. Y si quieres recibir un pago Lightning, instalas la aplicacion en tu telefono, generas un recibo por el monto que quieres recibir y te sorprenderás de la velocidad de la transaccion. Blue también tiene una version de escritorio, siendo así una de las maneras más convenientes para comenzar a usar el Lightning Network.

Breez Wallet es especial ya que abre un canal para ti. Luego de que depositas fondos y esperas por lo menos 3 confirmaciones, ya estás listo. El hecho de que esta simple experiencia de usuario ocurra de una manera sin custodia que aumenta tu soberanía es admirable. No puede compararse con tu experiencia con un nodo full, pero facilita las ventajas de Lightning con algunas contrapartidas elegantes.

Y luego tenemos Eclair Mobile de ACINQ, la cual corre una version liviana de un nodo Lightning directamente en tu telefono movil. También puedes conectarte con tu nodo full accediendo a la configuracion avanzada, pero aun por defecto es excelente para la soberanía financiera. Hubiese sido muy bueno si también estuviera disponible en iOS, pero esto puede deberse a limitaciones de Apple. Si tienes una tarjeta SD lo suficientemente grande, hasta puedes correr el nodo validador full en tu telefono.

Si buscas una forma de recibir tus primeros fondos en el Lightning Network de una manera fácil, registrate en servicios en redes sociales de propinas y pagos tales como Tippin.me y LNBits. Y si tienes algunos fondos del Lightning Network que necesitas convertir a bits en la red principal de Bitcoin y no tienes canales para cerrar porque estás completamente en custodia, prueba un servicio como ZigZag.

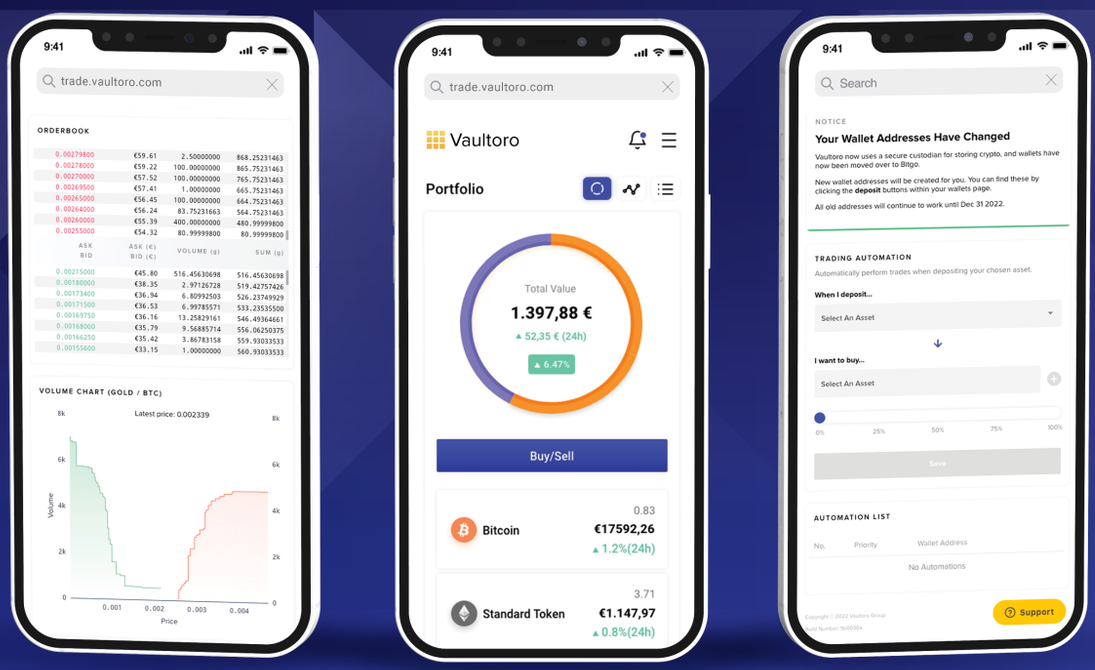
Abre Tu Primer Canal Con Bitcoin Takeover Y Haz Una Donacion

Si te gustaria comenzar tu camino de Lightning y abrir uno de tus primeros canales, por favor ten en cuenta el mio. Seras conectado a muchos grandes servicios, asi como tambien con miembros regulares de la comunidad que proveen rutas economicas.

–

Pubkey:
032ef154317acbb4077182eb1e74c75bdb81580fb51c3461c14c062491f9f6723d

Vaultoro



Tus ahorros en activos reales,
Haz crecer tu patrimonio

Compra y vende oro y plata con criptomonedas al mejor precio, asegurado profesionalmente en cámaras de seguridad en Suiza.

vaultoro.com



5 Razones Por Las Cuales Deberías Correr Tu Nodo De Bitcoin En Un Raspberry Pi 4

Los nodos de Bitcoin son los validadores de la red: mantienen honestos a los mineros y también permiten a los usuarios verificar sus propias transacciones y manejar su propia privacidad financiera. Son una herramienta de soberanía que funciona en prácticamente cualquier computadora fabricada desde 2010. Y aun así, por muchas razones, el Raspberry es una de las mejores opciones de equipo validador.

Este artículo no es pago o esponsorizado por la Fundación Raspberry y no es la idea convencerte de comprar un nuevo equipo. De hecho, la mejor computadora que puedes usar para correr un nodo full de Bitcoin es la que ya tienes. Sin embargo, existen algunas ventajas innegables que tienen estas pequeñas máquinas ARM.

Es cierto que las versiones anteriores eran lentas y no fidedignas. Cuando en febrero de 2019 testee un nodo Casa usando la Raspberry Pi 3, fue decepcionantemente lento. La mayor parte del tiempo no estaba seguro si estaba atascado o si debería esperar un poco más para que cargara. Pero más tarde ese año, lanzaron la Raspberry 4 con procesadores quad-core y 4 gigabytes de RAM – todo a un precio de $55.

Gracias a este avance en micro-procesamiento y a las economías de escala, convertirse en financieramente soberano nunca había sido tan fácil y accesible. Sin más, las siguientes son las razones por las cuales deberías correr tu nodo de Bitcoin en un Raspberry Pi 4.



1. El Raspberry Pi 4 Es Energéticamente Eficiente Y Sustentable



Dados todos los argumentos de "la minería de Bitcoin está hirviendo los océanos", es bueno que la parte de validación de Bitcoin sea operada utilizando equipos de bajo consumo. Mantener tu Raspberry Pi 4 en funcionamiento 24/7 consume lo mismo que dejar tu iPhone tamaño Max cargando todos los días. Y esto no es un dato menor – millones de personas pueden afrontar el costo de correr sus propios validadores de Bitcoin a costos de vmantenimiento y operación minimos.

En cualquier momento determinado, mi nodo de Bitcoin y Lightning Raspberry Pi 4 nunca usa más de un tercio de su poder de procesamiento. Esto significa que su consumo oscila alrededor del rango de 4 watts (aproximadamente un kilowatt cada 24 horas, o 365 kilowatts por año). Al costo de mi proveedor de electricidad de 8.5 centavos por kilowatt, me cuesta $31 por año tener mi nodo corriendo 24/7.

El hecho de que lo uso para correr tanto Bitcoin como Lightning es realmente asombroso. Y dada la gran cantidad de equipos Raspberry Pi que procesan transacciones Lightning, se podría decir que esta solución de segunda capa es la forma mas ecológica de mandar dinero que existe en el mundo.



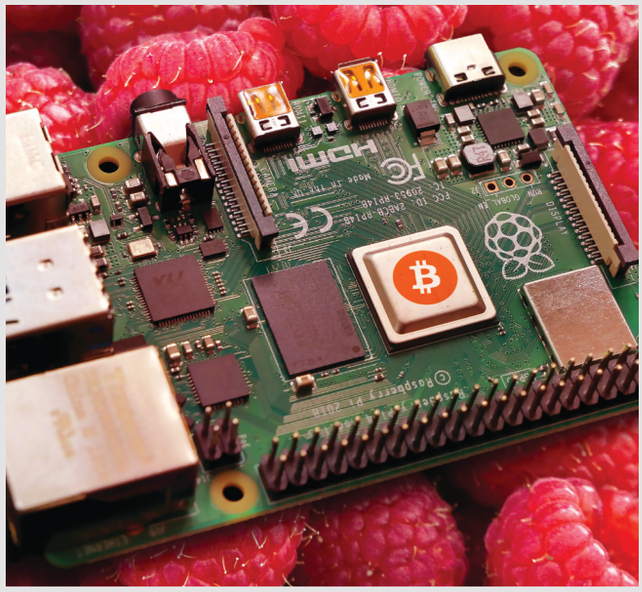
2. El Raspberry Pi 4 Es Económico, Multiuso Y Fácil De Distribuir Globalmente

Si los rigs de mineros pueden costar miles de dólares, comprar un Raspberry Pi 4 con un gran disco duro, una linda funda, pantalla táctil, y los cables, no debería costar más de $200. Para su instalación, lo que más cuesta es el disco duro de 1 TB (especíalmente si eliges el más rápido y silencioso, aunque su SSD sea el menos conveniente para volver a grabar).

Además, la popularidad del Raspberry Pi ha incrementado significativamente su disponibilidad y su variedad de usos. Asi que puedes ir a tu tienda de electrónica local (o ir a su sitio web) y comprar unos de estos pequeños equipos ARM con el mayor grado de negación plausible. Si tu gobierno autoritario pregunta, puedes simplemente decir que quieres armar una consola de videojuegos, o una simple computadora de escritorio con el mismo – ambos casos son populares y plausibles, de modo que nadie sospechara del mismo.

En el caso de los equipos de Bitcoin, es importante que no cumplan solo una

función específica o que sea conocida como tal. Si la potencial recompensa sean raras unidades de oro digital, entonces los actores malvados tendrán un mayor incentivo de tomar el riesgo de intervenir tu equipo durante su proceso de envío. Así y todo, sus usos de los equipos Raspberry Pi que no estén relacionados con Bitcoin son los menos comunes. Para tener mayor grado de negación plausible, puedes comprar un par de unidades y usar una para su uso más común y esperado. De esta manera, la probabilidad de ataque durante la cadena de suministro disminuye significativamente (aunque esto no quiere decir que no deberías hacer una verificación del chip tú mismo).



3. Existe Mucho Software De Bitcoin Que Funciona En El Raspberry Pi

El hardware es sólo tan bueno como el software que hace uso de sus capacidades. En el caso de Bitcoin existen muchas opciones open source robustas de nodos Raspberry Pi. Desde la creación del sistema operativo RaspiBolt por parte de Stadicus, hemos presenciado una gran ola de sistemas operativos de fácil uso que corren Bitcoin y Lightning en equipos accesibles.

Generalmente recomiendo a la gente usar RaspiBlitz, ya que ofrece un gran número de funciones y extensiones sobre una interfaz minimalista pero bien escrita. Sin embargo, hay otras muy buenas opciones disponibles tales como MyNode y Embassy OS de Start9 Labs. Otra opción popular es Umbrel – sin embargo su licencia no es específica para software open source gratuito (por lo menos no por ahora) y por eso no lo puedo recomendar.

Si fuese a encontrar sistemas operativos para computadoras de escritorio para estas soluciones, RaspiBolt sería Debian Linux, Raspblitz seria

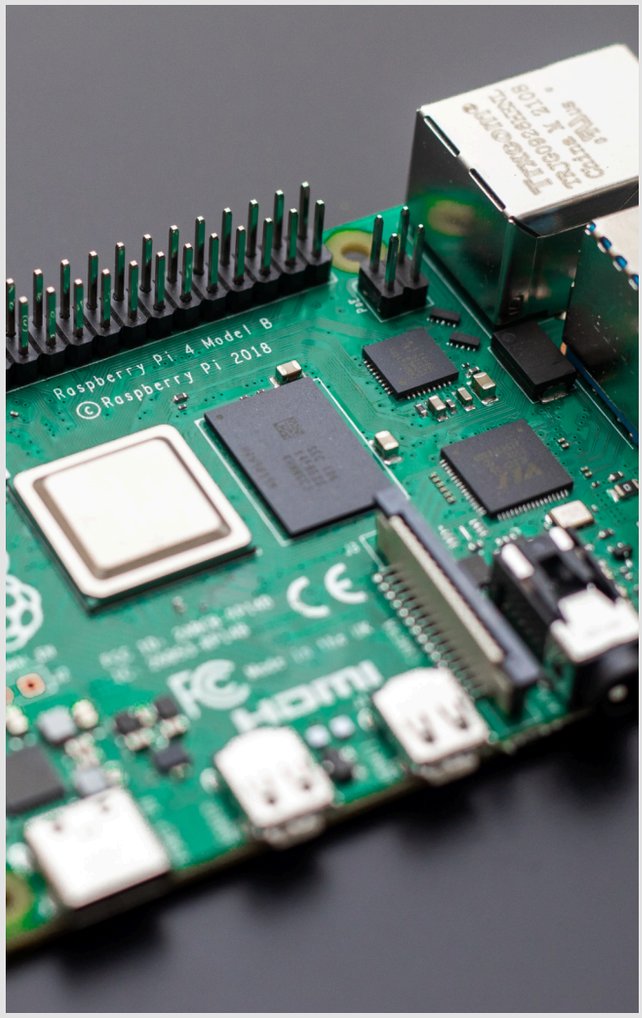


Ubuntu, MyNode sería Mint Linux, Embassy OS de Start9 sería Red Hat Linux, mientra que Umbrel sería Mac OS.

Independientemente de cual elijas, encontrarás algunos del mismo poderoso software. Esto incluye Electrum Server, Tor integration, LNBits, un servicio de mezcla como JoinMarket, y una aplicación descentralizada de chat como Sphinx (entre muchas otras).

Todas estas aplicaciones de software te ofrecen una manera segura y accesible para acceder a aplicaciones de Bitcoin y Lightning en un Raspberry Pi, conservando todas las ventajas de ser un ciudadano de primera clase de la red de Bitcoin. Validar tus propias transacciones, generar direcciones para recibir desde una xpub propia, abrir tus propios canales de Lightning y administrar tus claves privadas, son todas partes de esta experiencia técnica y gratificante.

Es medio increíble pensar que el Raspberry Pi ofrece una experiencia de Bitcoin más compacta y eficiente que una computadora personal corriendo Windows o MacOS.



4. El Raspberry Pi 4 Es Pequeño Y Silencioso

Hay mucho que decir sobre las ventajas de una computadora pequeña. Pero principalmente, y especialmente en el caso de que quieras tener un equipo siempre prendido, es muy bueno poder ponerlo en tu living sin tener que preocuparte por el ruido.

Si eliges una buena carcasa de aluminio la cual disipa el calor muy bien, ni siquiera tendrás que lidiar con ruidosas soluciones de enfriamiento activo. Y si corres tu nodo de Bitcoin y Lightning en un SSD, no habrá giros que produzcan ruidos. Obtienes la experiencia más silenciosa, más eficiente en términos de costo, y más ecológica.

El hecho de que venga en un formato pequeño del tamaño de una palma que puedes hacer caber detrás de muebles también suma a tu privacidad, negación plausible, y tranquilidad.

5. El Raspberry Pi Es Bastante Seguro Como Nodo De Bitcoin

La gente usa Raspberry Pi como computadoras para correr servidores, relevos, emuladores de videojuegos, máquinas de livestreaming, procesadores de pagos y la aplicación matadora suprema: validar transacciones Bitcoin y Lightning. Y no es que no podrían hacerlo en computadores más potentes que

corran todo en máquinas virtuales.

La cuestión en juego es la seguridad: si tienes un equipo que solo realiza una tarea específica y todo su hardware está optimizado para esta, entonces la superficie de ataque es menor. En cambio, la computadora de trabajo de múltiples usos que puede correr todo en máquinas virtuales es más vulnerable a ataques dada la mayor complejidad de su configuración.

Un nodo de Bitcoin Raspberry Pi te lleva a la época en la cual cada item en tu casa cumplía una única función básica: tenias bandejas para la música, una TV para entretenimiento de video, y una consola de juegos para los cartuchos. A pesar de que sea conveniente tenerlo todo en un teléfono inteligente o en una computadora, es al mismo tiempo fundamentalmente menos seguro. Este es el motivo por el cual tener hardware que solo ejecute una función es importante, especialmente cuando se trata de buen dinero.



Sin Embargo, El Raspberry Pi 4 NO Es Hardware Open Source

Recuerda el segundo párrafo de este artículo, en el cual mencione que la Fundación Raspberry Pi no me paga por esto y que esto es meramente una representación de mis pensamientos propios? Pues bien, lo decía seriamente. El Raspberry Pi es muy bueno para lo que hace, pero hay algunas razones por lo cual no es ideal para algo como Bitcoin.

Bitcoin es código open source gratuito que cualquiera puede leer, bajar, verificar, y potencialmente modificar. Funciona en base a una filosofía sin permiso en la cual no debes acudir a ninguna autoridad del mundo para poder acceder a la red. El software open source gratuito también necesita hardware open source gratuito. Sin embargo, no hay suficiente del mismo por el momento.

Entonces si quieres armar tu propio Raspberry Pi porque te encuentras en un país que no te permite importar uno, va a ser difícil. Y si necesitas reemplazar o mejorar parte de la plaqueta, también será poco probable encontrar su reemplazo (salvo que compres una nueva Raspberry Pi). Esto es parte del tradeoff que se da con la arquitectura ARM: obtienes sistemas en chips (SoCs) y sistemas en módulos (SoMs) que son difíciles de replicar usando partes de uso general disponibles en el mercado.

También hay un debate pendiente sobre los chips con backdoors NSA: siendo computadoras de calidad de uso general, los Raspberry Pi son probablemente vigilados y hackeables por parte de las agencias gubernamentales.

Si realmente quieres una verdadera experiencia de hardware open source,

fijate en las computadoras RISC-V. Al armar o comprar (y luego verificar) una de estas, sabrás que estás usando un estándar abierto que nadie puede comprometer sin dejar un rastro visible. Hay un precio a pagar por más privacidad sin embargo: una computadora que apenas puede navegar la web te costará alrededor de $4000 y no hay tanto software de Bitcoin que puedas usar en ella.

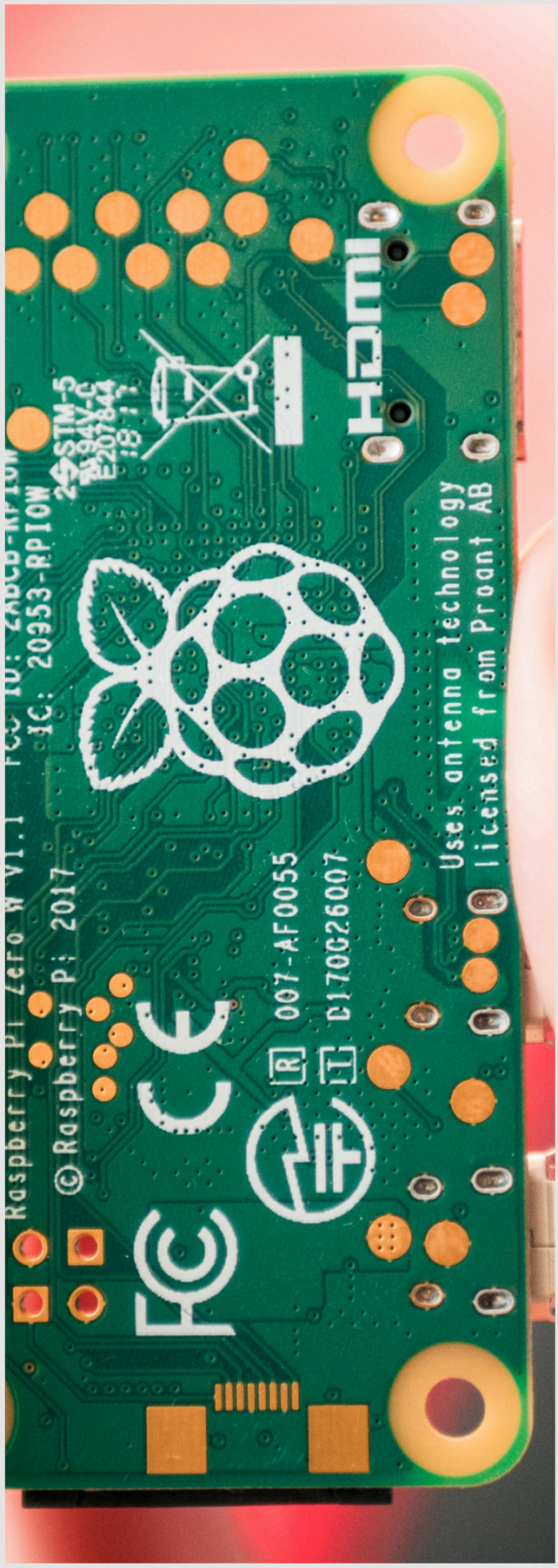
A pesar de que Bitcoin Core ha corrido en RISC-V desde el lanzamiento de la versión 0.18.0 en mayo de 2019, no pude encontrar ningún cliente de Lightning que funcione en estas CPU open source. Y si LND o c-lightning no funcionan no te beneficiaras de otras aplicaciones tampoco (RTL, LNBits, BTCPay, and Sphinx Relay).

Parte del motivo por el cual el estándar RISC-V no recibe mucho soporte es el costo del hardware – muy poca gente puede pagarlo, la cual es exactamente la razón opuesta por lo que el Raspberry Pi es tan popular. Pero dado el reciente resurgimiento de hardware open source gracias al Tropic Square de Trezor y al proyecto Precursor de bunnie, podemos esperanzarnos que en el futuro pondrán su atención en unidades de procesamiento, memoria RAM, y plaquetas madre que sean verificablemente open source y que no cuesten más que una PC de juego promedio.

Han solo pasado 12 años desde el lanzamiento de Bitcoin y 8 años desde que Edward Snowden reveló la magnitud de las operaciones de vigilancia de la NSA. Adicionalmente, no fue hasta el 2018-2019 que le RISC-V se hizo popular y los fabricantes de chips open source empezaron a buscar inversores.

Puede ser que por ahora, computadoras de bajo consumo como el Raspberry Pi y el Arduino sean los reyes del juego. Pero en el futuro, podríamos tener hardware completamente open source para correr todo el gran software gratuito y open source de Bitcoin.

–



FULMO

Building the Lightning Network



shop.fulmo.org



Elon Musk No Comprende La Descentralización – Pero Tu Deberías

La descentralización es difícil e Elon Musk claramente no la comprende. No solo tiene una mirada infantil sobre la escalabilidad de un blockchain y elige ignorar la investigación al respecto, sino que también es descaradamente ignorante en cuanto a la concentración de la riqueza (otra factor que hace que un proyecto se considere descentralizado) y no parece entender los incentivos en un sistema Prueba de Trabajo. En resumen, es el epítome del meme "recien oigo hablar de Bitcoin, estoy aquí para arreglarlo.



Tal vez no deberíamos pretender mucho de un CEO que sobresale a la hora de recibir subsidios estatales al mismo tiempo que los critica, y que también haya estado involucrado en la creación de PayPal – un sistema centralizado de pagos por internet que usa dinero estatal eternamente

inflacionario y que depende de un sistema de facturación que puede generar ganancias aun si dejara de cobrar fees por transacción (el hecho de que está manipulando tasas de conversión y que recolecta datos de usuarios ya es suficiente).

Pero el hecho de que el hombre más rico del mundo no entienda Bitcoin (ni su fork de memes favorito, Dogecoin) no significa que tú tampoco deberías. De hecho, yo me aseguraré de que para cuando termines de leer este artículo, entenderás de descentralización y de Bitcoin mucho más que Elon Musk.

La Descentralización Significa Que Cualquiera Debería Poder Participar En La Red

El 16 de mayo de 2016, Elon Musk tuiteó: "Idealmente, Doge acelera el tiempo de bloque 10X, agranda el tamaño de bloque 10X y disminuye fees 100X. De esta manera con seguridad se impone".



Antes de que comencemos a analizar las complejas implicaciones de este tweet, debo empezar por decir que Bitcoin y Dogecoin tienen una arquitectura bastante similar. En definitiva, Dogecoin es una copia más inflacionaria de Litecoin (que a su vez es un fork de Bitcoin modificado). Entonces por más que algunos parámetros como el tamaño de bloque, el tiempo de bloque difieren de una moneda a la otra, los principios subyacentes son exactamente los mismos – especialmente cuando





hablamos de descentralización.

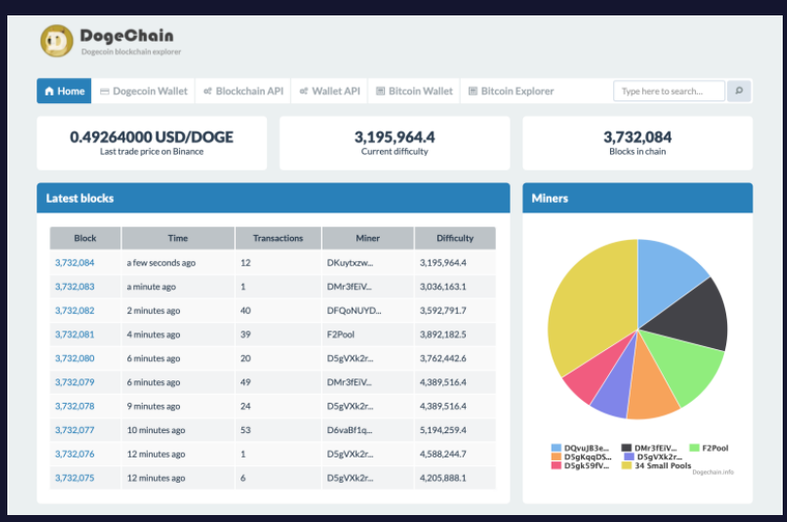
Ahora volvamos al tweet de Elon Musk, el cual menciona 3 parámetros de las criptomonedas: tiempo de bloque, tamaño de bloque, y fee de transacción. Los primeros dos son extremadamente importantes al definir descentralización, al tiempo que el tercer criterio es esencial para la seguridad y la sustentabilidad de largo plazo (y en consecuencia, también es indirectamente importante para la descentralización).

El tiempo de bloque es el factor que decide quién puede validar el blockchain en función a la velocidad de internet. Como es de público conocimiento, la red de Bitcoin mina un nuevo bloque cada aproximadamente 10 minutos.

Esto significa que los nodos alrededor del mundo pueden estar en sintonía si pueden bajar 1-2 megabytes cada 10 minutos. Y esto es especialmente muy bueno en casos en que los usuarios vengan de países autoritarios donde el acceso a internet es limitado o restringido. También es muy bueno para las personas que viven en áreas rurales en países de menor desarrollo, quienes pueden no tener acceso a conexiones de internet de alta velocidad. Cualquiera alrededor del mundo puede validar los bloques que se generan en la red de Bitcoin. Y, teoricamente, los mineros pueden instalar su operación en el medio de la nada accediendo a la señal de los satélites de Blockstream. He explicado esto en mayor detalle en mi artículo “Bitcoin No Es Lento – Es Sumamente Seguro”.

Dogecoin ya tiene un tiempo de bloque de 1 minuto – y este diseño favorece a los usuarios de internet con conexiones banda ancha y mayores velocidades de acceso. Billones de personas son privadas de la chance de sincronizar sus nodos, ya que solamente los habitantes de las ciudades pueden obtener toda la data en tiempo real. La situación también es mala para la transmisión interplanetaria (una de las ambiciones de Musk), ya que enviar una señal de radio puede demorar entre 4,2 y 21 minutos (dependiendo de la distancia momentánea). En la mayoría de los casos, Bitcoin sería más apropiado para este uso.

Y aun así el tiempo de bloque es bastante razonable dada la sorprendementemente baja demanda de espacio en el bloque. De hecho, este proyecto de $63 billones solo procesa un puñado de transacciones por bloque – lo cual es indicativo de la tenencia centralizada y del excesivo trading minorista en los balances de los exchanges. La cantidad de bloques vacíos de Dogecoin en medio de un mercado alcista (y claramente una burbuja) es asombrosa – ten en cuenta



que 1 transacción sola fue la recompensa de bloque que fue enviada al minero exitoso.

Esto nos lleva hacia la parte sobre incrementar el tiempo de bloque de Dogecoin 10 veces. Aunque parezca innecesario según los datos empíricos, asumamos que de alguna manera los usuarios empiezan a usar el blockchain. Si las transacciones de DOGE fuesen a llenar bloques de 10 megabytes cada 6 segundos, entonces el blockchain crecerá 100 megabytes por minuto, 6 gigabytes por hora, 144 gigabytes por día, y 4.32 terabytes por mes. Casi tan malo como Chia, la horrible y sobre apreciada Frankenstein de la Prueba de Trabajo.

Si, este escenario es improbable, ya que hasta en el caso de Bitcoin hay momentos en que los bloques no se llenan por completo. Pero aun si un promedio de un cuarto de bloque se llenara, entonces el blockchain de Dogecoin se expandiria en 252 gigabytes por semana. Para poner esto en perspectiva, le llevó 12 años al blockchain de Bitcoin llegar a un tamaño de 350 gigabytes.

Para la mayoría de la gente alrededor del mundo, un disco duro de 1TB es bastante caro. Pero si Dogecoin emitiera bloques de 10 megabytes por minuto, la capacidad del mismo se llenaría en una semana. En comparación, el blockchain de Bitcoin suma unos 51.32 gigabytes de data por año, por lo cual el disco duro de 1TB cubriria 19 años más corriendo un nodo full archivado.

Al diseñar un sistema descentralizado, debes asegurarte de no excluir a nadie por hacer un upgrade discriminatorio a la red. Si no puedes validar tus propias transacciones y chequear el estado completo de la red con tu propio nodo, pues entonces el sistema es centralizado.

El internet definitivamente no te pide que tengas una computadora de alta gama para acceder a sitios – y como sistema de dinero, Bitcoin apunta a ser tan inclusivo y abierto para la mayor cantidad posible de gente alrededor del mundo. Elon Musk claramente no entiende esto y busca centralizar un proyecto meme abandonado bajo su propia e impredecible dictadura, la cual busca convertir algo universal y abierto en un proyecto mascota.

En resumen: si no puedes unirte a la red como nodo validador, el proyecto no es descentralizado. Reducir el intervalo de tiempo entre bloques excluye a la gente con conexiones de internet lentas, mientras aumentar el tamaño de bloque incrementara el costo computacional y de almacenamiento de los participantes (y así eliminando a los que no se actualizan regularmente). Esto es porque existen segundas capas como el Lightning Network. Pero parece que Elon Musk quiere armar otro PayPal.



La Descentralización Requiere De Incentivos (Incluyendo Fees De Minería)

A pesar de que Dogecoin es extremadamente inflacionaria, su calendario de halvings debería reducir las recompensas de mineria significativamente durante los próximos años. Lo mismo ocurre con Bitcoin, el cual apuesta más en este juego desinflacionario de escasez cada 210.000

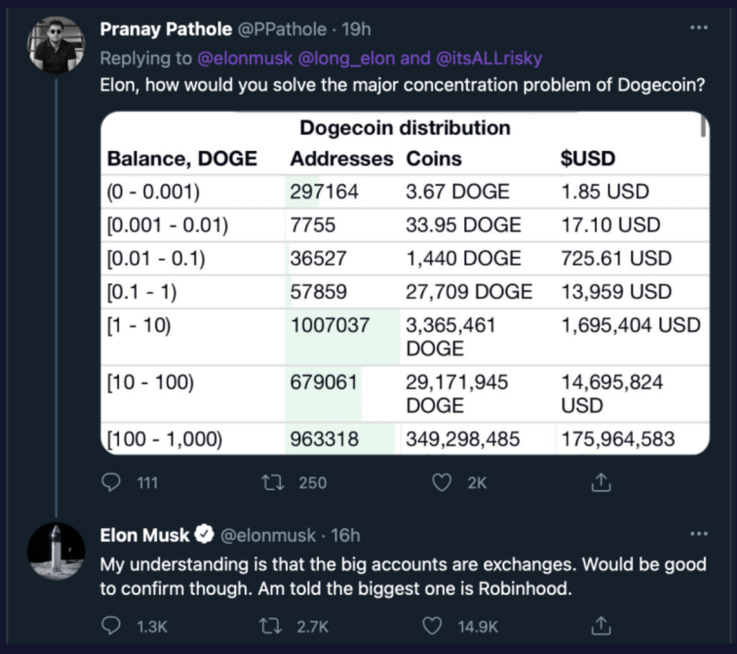
bloques (aproximadamente cada 4 años).

A medida que la recompensa de encontrar un bloque disminuye, los mineros deberían mantenerse incentivados en seguir proporcionando seguridad a la red. En la cuarta página de su whitepaper, Satoshi Nakamoto describe un sistema que eventualmente se convierte en libre de inflación y cuyos mineros son incentivados a seguir gracias a los fees de transacción.

Sin estos fees, los incentivos se quiebran y es probable que muchos mineros dejaran de dar soporte a la red. Pero la reducción de 100X en fees que describe Elon Musk podría ser ideal para que el tome control de la red y seguir minando bloques a pérdida mientras retiene el control.

Bajar los fees arbitrariamente llevará a reducir la cantidad de mineros. Y menos mineros significa menos descentralización y mayor posibilidad de controlar la red. Mientras esto puede ser lo que busca Elon Musk, es una idea horrible. No hay nada revolucionario ni disruptivo en un sistema en el cual el hombre mas rico del mundo puede censurar – despues de todo, es la dinámica geopolítica que convierte a Bitcoin y a Dogecoin mas fungible y resistente a la inclusión de transacciones en listas negras.

Pagar 100 veces menos fees suena muy bueno en la práctica, pero en largo plazo no solo erosionara al sistema y causara mas control/centralización o mas inflacion. Al mismo tiempo, los fees son muy buenos para prevenir transacciones de spam – si hay un costo involucrado, la gente estará menos dispuesta a atascar la red con muchas transacciones pequeñas puesto que deben pagar por cada una de ellas. La visión de Musk de Dogecoin es técnicamente defectuosa.



La Descentralización Y La Distribución De La Riqueza

En mayo de 2017 Elon Musk respondió a las preocupaciones de Pranay Pathole sobre la concentración de riqueza de Dogecoin. Según BitInfocharts, existen 107 direcciones de Dogecoin dueñas de más del 66.7% de la emision. También, hay una dirección dueña del 28.34% de la totalidad de la emisión – una cantidad desproporcionada, dada la supuesta ambición del proyecto. Elon Musk elige no analizar la situación dando la respuesta de que Robinhood es potencialmente la ballena más grande. Puede ser verdad, pero no está confirmado.

Pero comparemos esta situación con Bitcoin. Las primeras 3 direcciones están claramente identificadas como fondos almacenados offline de Huobi, Binance, y Bitfinex. Y cumulativamente, tienen el 2.68% de los fondos de los usuarios – así es, las entidades más grandes son en realidad custodios que almacenan los fondos de cientos de miles de clientes.

En Bitcoin, hay en la actualidad unas 16.000 direcciones dueñas del 62.95% del circulante. No es ideal, pero mejor que la situación de Dogecoin, donde 107 direcciones tienen más de un tercio de

Bitcoin distribution

Balance, BTC	Addresses	% Addresses (Total)	Coins	$USD	% Coins (Total)
(0 - 0.001)	19622119	51.64% (100%)	4,060 BTC	187,107,133 USD	0.02% (100%)
[0.001 - 0.01)	9421945	24.8% (48.36%)	35,992 BTC	1,658,595,444 USD	0.19% (99.98%)
[0.01 - 0.1)	5740398	15.11% (23.56%)	185,966 BTC	8,569,804,347 USD	0.99% (99.79%)
[0.1 - 1)	2400783	6.32% (8.46%)	752,247 BTC	34,665,493,898 USD	4.02% (98.79%)
[1 - 10)	665522	1.75% (2.14%)	1,697,758 BTC	78,237,101,339 USD	9.07% (94.77%)
[10 - 100)	130726	0.34% (0.39%)	4,255,733 BTC	196,115,278,881 USD	22.75% (85.7%)
[100 - 1,000)	13970	0.04% (0.04%)	3,947,599 BTC	181,915,645,208 USD	21.1% (62.95%)
[1,000 - 10,000)	2073	0.01% (0.01%)	5,092,326 BTC	234,667,670,041 USD	27.22% (41.85%)
[10,000 - 100,000)	84	0% (0%)	2,236,025 BTC	103,041,850,124 USD	11.95% (14.63%)
[100,000 - 1,000,000)	3	0% (0%)	501,390 BTC	23,105,341,964 USD	2.68% (2.68%)

Addresses richer than

1 USD	100 USD	1,000 USD	10,000 USD	100,000 USD	1,000,000 USD	10,000,000 USD
33,006,829	14,871,813	6,221,037	2,033,219	394,735	90,020	7,984

las monedas. Ethereum también luce peor, con grandes billeteras individuales teniendo demasiadas monedas (muy probablemente debido a su preminado de 70% y a los primeros inversores o cofundadores que no vendieron).

Entonces, por qué importa la distribución de la riqueza para la descentralización? También se trata de incentivos e inclusión. Nadie querría participar de un proyecto en el cual un pequeño grupo de élites controlan la mayoría del dinero. Los inversores no querían someterse a tal riesgo, los desarrolladores no querrían estar bajo el control de unos pocos actores, y los mineros también percibirán la desagradable centralización e insostenibilidad en el largo plazo.

Estos grandes tenedores son puntos únicos de falla lo cual manipula el juego para todos aquellos a su alrededor. Tener una posición más grande también implicaría tener mayor influencia en el desarrollo y algo de poder político en la red. Lo cual es definitivamente una amenaza para una red no mantenida como lo es Dogecoin.

No Le Digas A Elon: Dogecoin Es Una Cadena De Hashrate Minoritaria La Cual Es Minada Junto Con Litecoin

La continuidad de la existencia de Dogecoin como red es debido a la benevolencia por parte de algunos actores. El caso más importante, es que los mineros de Litecoin decidieron salvar a Dogecoin en 2014 al permitirle ser minada en coordinación. Entonces en vez de convertirse vulnerable a ataques malévolos, es protegida por los mismos mineros Script quienes protegen a la cadena de mayor hashrate.





La minería de Litecoin es casi tan energéticamente intensiva como la de Bitcoin, pero difiere en términos de especificaciones tecnicas (El SHA 256 de Bitcoin es de proceso intensivo, mientras que Scrypt de Litecoin y Dogecoin es intensivo en términos de memoria).

Pero si Elon Musk decide criticar a la minería de Bitcoin e ignorar la forma en que Dogecoin es producida, entonces es el típico hipócrita quien opina por apariencias utilizando información parcial para atraer a una banda enfadada (y alerta a injusticias) mientras opera con Dogecoin desde una posición de ignorancia.

Se puede decir que al menos, Elon Musk es intelectualmente deshonesto, inconsistente, y altamente influenciado. Si se la dejara sola, Dogecoin sería víctima de atacantes que puedan rentar algunos equipos de minería por un par de horas. Y si el proyecto es cooptado por parte de Tesla o SpaceX, pierde en términos de propuesta de valor.

Los Cambios Propuestos Por Elon Musk Requieren De Un Hard For Centralizante

Los hard forks son cambios en la red que requieren que todos los participantes se unan a un nuevo blockchain. Crean incompatibilidad entre el viejo blockchain y el nuevo, y así dependen del consenso de que todos migren.

Cuanto más fácil sea lograr hacer un hard fork, más centralizado es el proyecto. Idealmente, los operadores soberanos de nodos y los mineros deberían ser reacios a nuevos cambios, rechazar liderazgo, y optar por verificar cada línea de código individual y egoístamente. Pero cuando aparece el hombre más rico del mundo y dice que



quiere tomar un rol de liderazgo, esto ya es una mala señal y solo lleva a mas centralización. Y sí, también soy crítico del involucramiento de Michael Saylor.

Apoyarian los exchanges un hard fork solo porque Elon Musk está involucrado? Es cuestionable, ya que muchos de ellos tienen principios y realmente tratan de analizar los fundamentos de largo plazo (a diferencia de Binance, el cual parece apoyar cualquier cosa que genere volumen de trading).



Migrarán los usuarios al Dogecoin de la visión de Elon? Y, no hay tantos usuarios en comparación a Bitcoin (nodos soberanos). Así que queda en manos de los exchanges y de las entidades que tengan un incentivo de correr un nodo. Sin embargo hay demasiada centralización en juego.

A título de referencia, los desarrolladores de Bitcoin están haciendo lo más posible para evitar hard forks. La reciente prueba de taproot solo demuestra que la red es lo suficientemente madura como para decidir sobre un soft fork (un cambio que no cambia las reglas de consenso y es opcional para la totalidad de la red) de una manera descentralizada.

Hay Un Motivo Por El Cual El Desarrollo De Bitcoin Es Tan Conservador: La Descentralización Funciona

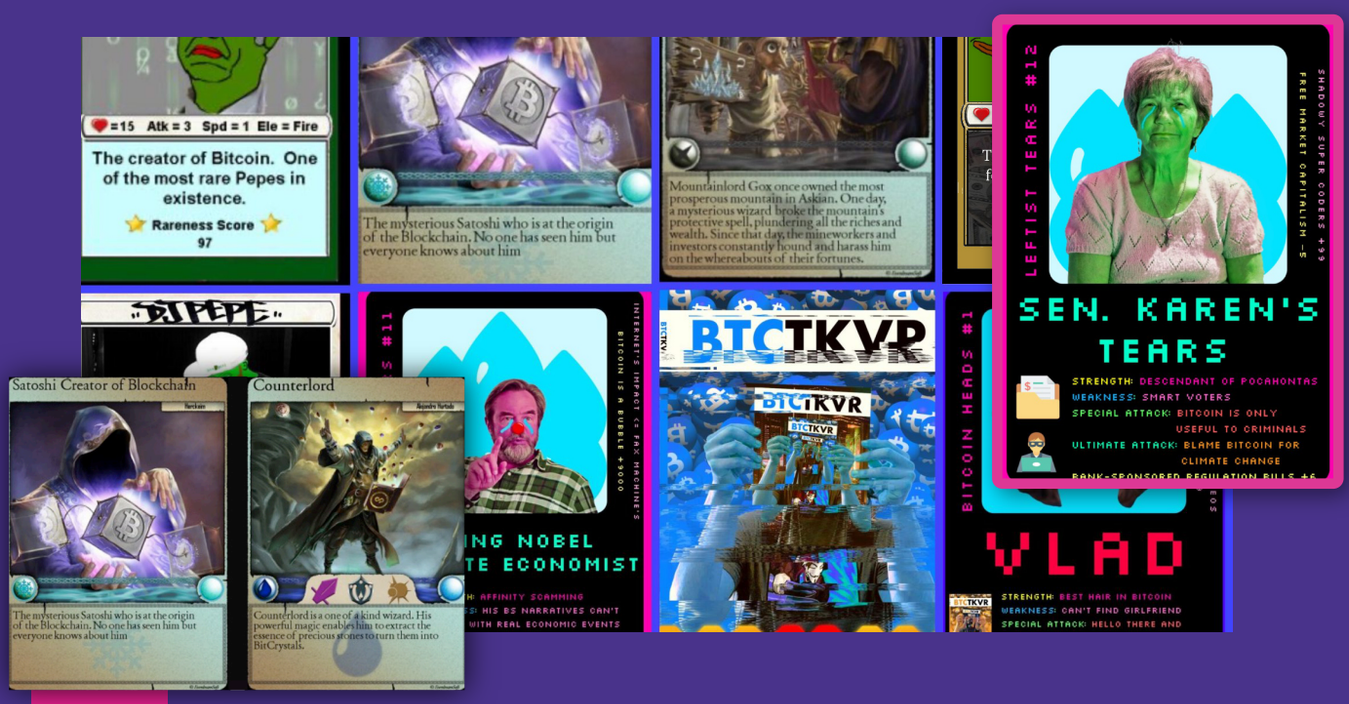
La descentralización es difícil. Y si eres nuevo en este espacio y estás acostumbrado a un mundo en el cual las actualizaciones de las aplicaciones del teléfono son hechas e instaladas en minutos, se te hará difícil comprender un sistema como Bitcoin, el cual depende de largas deliberaciones y tiende a ser osificado a través del tiempo.

Si mejorar blockchains fuese tan fácil, no tendría ya Bitcoin bloques más grandes, tiempos de bloque más rápidos, y fees más bajos? Es un tanto ingenuo asumir que estas propuestas son nuevas y que jamás nadie ha pensado en ponerlas en práctica. Y una mentalidad al estilo de Silicon Valley de “moverse rápido y romper cosas” definitivamente no ayuda a un sistema monetario cuyo propósito es darle seguridad a los ahorros de todos en lugar de ser rápido y fácil de hacer transferencias.

Nunca se suponía que Dogecoin iba a tener una valuacion tan alta y no fue creada con el propósito de incrementar la riqueza e influencia del hombre más rico del mundo. Pero aquí estamos hablando de este tema y tratando de definir cómo debería ser la descentralización – a diferencia de Elon Musk con sus reflexiones desinformadas.

La descentralización es difícil – y espero que este largo artículo te haya ayudado a entenderla mejor que Elon Musk. Si buscas una versión más corta, lee este hilo que publiqué en Twitter.

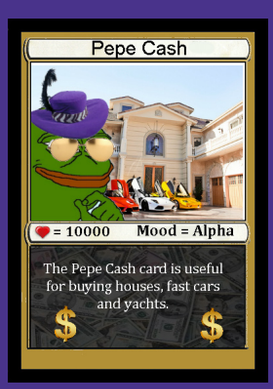
–



NFTs De Bitcoin En Counterparty (Y Como Obtener O Crear Tu Primero)

Omnipresentes en todos los canales de medios y aún mayormente malinterpretados, los NFTs son el tema de fascinacion y de (en su mayoría) especulación irracional. Dado el revuelo excesivo asociado con el movimiento "se ve extraño", algunos comentadores hasta han comparado a los NFTs con los ICOs de 2017 y 2018 – acertadamente, la euforia en relación a estos activos raros y escasos y la facilidad para "emitir" NFTs ha llevado a una situación donde todos parecen emitir y vender cualquier cosa que perciban como un coleccionable. Cuestiones del mundo fiat.

Pero a diferencia de los ICOs, con los NFTs lo que ves es lo que recibes. Nadie compra estos tokens con otra expectativa que la de recibir un activo digital único asociado a una pieza de arte. Mientras los ICOs se emiten con hojas de ruta y promesas acerca del futuro del proyecto, los NFTs son hashes criptográficos escritos en el blockchain. Básicamente figuritas deportivas de colección para nerds.



También vale la pena aclarar que no todos los NFTs son lo mismo: mientras que los más conocidos y comercializados son tokens ERC-721 sobre Ethereum, también existen tokens de la side chain Liquid que se tradean en Raretoshi. Sin embargo, los realmente especiales se emiten en el blockchain vía Counterparty, se benefician de la red más segura de todas, se almacenan en básicamente todos los nodos soberanos, y reciben nombres que actúan de la misma manera que los dominios de internet los cuales no pueden ser replicados. Si el token es el arte, será el más resistente y demostrablemente único el que más importe y más chances tendrá de sobrevivir el paso del tiempo.

La tarjeta Pepe Cash sirve para comprar casas, autos veloces y yates

Crypto trading cards.

- **To: CYPHERPUNKS <CYPHERPUNKS@TOAD.COM>**
- **Subject: Crypto trading cards.**
- **From: Hal <740761041@CompuServe.COM>**
- **Date: 17 Jan 93 13:48:02 EST**

Giving a little more thought to the idea of buying and selling digital cash, I thought of a way to present it. Were buying and selling "cryptographic trading cards". Fans of cryptography will love these fascinating examples of the cryptographic arts. Notice the fine way the bit patterns fit together - a mix of one-way functions and digital signatures, along with random blinding. What a perfect conversation piece to be treasured and shown to your friends and family.

Plus, your friends will undoubtedly love these cryptographic trading cards just as much. They'll be eager to trade for them. Collect a whole set! They come in all kinds of varieties, from the common l's, to the rarer 50's, all the way up to the seldom-seen 1000's. Hours of fun can be had for all.

Your friendly cryptographic trading card dealer wants to join the fun, too. He'll be as interested in buying your trading cards back as in selling them.

Try this fascinating and timely new hobby today!

Hal

Y si, también está el arte que está asociado. Presentado en formato jpeg, gif, link de YouTube, o hasta en archivo de audio, es básicamente la representación visual modificable del token. Pero el archivo de arte en sí no se almacena en el blockchain: la mayoría de ellos están en Imgur, IPFS, u otro sitio web centralizado especializado en permitir a sus usuarios subir y compartir imágenes. Esto significa que uno debería percibir el jpeg como no más que una linda envoltura que ofrece detalles visuales sobre el significado del token.

A pesar de que algunos usuarios inicien juicios y se ofendan cuando la misma imagen es usada para emitir otro NFT, deben recordar que efectivamente compraron un token único que demostrablemente no es posible que sea replicado. Es “no fungible” (no puedes reemplazar uno con otro, ya que no hay hash idéntico) y es esencialmente lo que Hal Finney describió en 1993 al sugerir que los cypherpunks pueden tener “horas de entretenimiento”.

“Criptocartas intercambiables

Dándole un poco más de reflexión a la idea de comprar y vender dinero digital, pensé en una manera de plantearlo. Estamos comprando y vendiendo “cartas criptográficas intercambiables”. A los adeptos a la criptografía les fascinaran estos ejemplos de arte criptográfico. Observen la manera en que encajan los patrones de bits – una mezcla de funciones de una vía y de firmas digitales, sumado al blinding aleatorio. Que tema de conversación perfecto para ser apreciado y enseñado a tus amigos y familiares.

Además, sus amigos sin duda también amarán de la misma manera estas tarjetas criptográficas intercambiables. Estarán dispuestos a intercambiar por ellas. ¡A coleccionar un juego entero! Vienen en todo tipo de variedades, de los 1s comunes a los más raros 50s, y así hasta los raramente vistos 1000s. Todos podrán disfrutar de horas de diversión.

Su comerciante favorito de tarjetas criptográficas intercambiables quiere también sumarse a la diversión. Estará tan interesado en recomprar tus tarjetas como en venderlas.

¡Este es hoy un oportuno y fascinante hobby!

Hal”

Tal como establecido previamente, las imágenes son meramente representación visuales que te ayudan a entender de qué se trata el token. Sin embargo, es el arte que es replicable y totalmente fungible lo que inicialmente te llama la atención y que te hace querer apoyar el trabajo de un determinado artista. Algunos de estos archivos (mayormente jpegs y gifs) son meritoriamente artísticos, otros cuentan con una oscuridad de principiante, pero la mayoría de ellos se ven flojos, sin inspiración, y seguramente solo existan para hacer un dinero rápido aprovechando el entusiasmo del momento.

Es por esto que tengo una opinión negativa sobre los NFTs de Ethereum y Solana, pero positiva de las creaciones en Counterparty de Bitcoin; no solo es que el arte es mejor, pero también lo suficientemente atemporales para aguantar el paso del tiempo y reaparecer aún cuando la burbuja de inversión

explote. Los Bitcoiners construyen protocolos y capas que perduran y encuentran un propósito años después de haber sido declarados muertos y abandonados. En Ethereum es solo encontrar nuevas fuentes de entusiasmo y de convenientemente enterrar fracasos pasados. En 2021, la capa Omni fue resucitada gracias al proyecto Synonym de John Carvalho, mientras que Counterparty regresó al protagonismo gracias a su rica historia de arte. No esperes leer noticias similares sobre Raiden o Plasma.



De Dónde Vienen Los NFTs?

Hay definitivamente más del jpeg de los que inicialmente parece. Y de la misma manera en que Ethereum se convirtió en un nido de ratas no escalable sin almar fundado por VCs, los NFTs fueron inicialmente hechos populares entre 2014 y 2016 a través del protocolo Counterparty de Bitcoin.

Ten en cuenta que fue Namecoin (previamente conocido como BitDNS, un hard fork de Bitcoin el cual Satoshi Nakamoto respaldo) quien recibe crédito por emitir el primer NFT de la historia: Quantum, Blockheads, Comicons y Cryptoeggs eran básicamente proyectos avatar que buscaban proveer a cada nuevo usuario una identidad digital única. No se suponía que se fuesen a convertir en coleccionables, pero la gente comenzó a intercambiarlos y adquirieron valor de mercado. Varios años después, Ethereum copió este enfoque con los CryptoPunks y otros avatares similares generados por computadoras los cuales puedes ver hoy en avatares de Twitter.

Pero luego del lanzamiento del protocolo Counterparty en Enero 2014, los bitcoiners comenzaron a crear su propio tipo de arte tokenizado. A partir de este momento existen dos corrientes de pensamiento: el lado innovador de la propiedad en videojuegos (siendo las tarjetas de “Spells of Genesis de Shaban Shaame y “SaruTobi Island” de Christian Moss do de los mejores ejemplos) y el lado meme (Rare Pepes, Fake Rares, Leftist Tears, Bitcoin Heads).

Por supuesto que no todos los NFTs surgieron en 2014. El directorio de Rare Pepe fue inicialmente creado en septiembre de 2016, las tarjetas de Spells of Genesis aparecieron inicialmente en Septiembre 2015, mientras que Fake Rares y Bitcoin Heads fueron emitidas durante la segunda mitad de 2021.



Pero el aspecto que las hace sobresalir es que son generadas por el usuario con software de diseño gráfico o hasta dibujadas a mano. Los Bitcoiners aman el proof of work – así que a diferencia de Namecoin y Ethereum, no emiten arte que una computadora haya generado automáticamente. Puedes encontrar un agradable elemento humano en todos estos NFTs de Bitcoin.



Para encontrar más información acerca de la historia de los NFTs, lee el excelente artículo de WhiteRabbit1111 “The origin assets of the digital antiquities market (NFTs)”. Es una mirada profunda a todo tipo de proyectos, algunos de los cuales son menos conocidos pero merecen elogio por ser precursores de lo que posteriormente se convertiría en un industria de mil bitcoin (particularmente, OLGA es realmente encantador).

¿Qué Es Counterparty?

Counterparty es un protocolo de Bitcoin el cual los libros de historia raramente mencionan. Hasta “Mastering Bitcoin”, que presumiblemente es la publicación sobre el tema más exhaustivo y extenso, solo describe a Counterparty en un párrafo, previo a continuar con monedas alternativas (las cuales reciben mayor cobertura).

Uno podría argumentar que Counterparty es una reliquia de una pasado lejano olvidado, un pueblo fantasma que sirve de recordatorio de las iniciales intenciones y aspiraciones de los bitcoiners. Esencialmente, es un protocolo que hace posible a cualquier persona emitir tokens sin necesidad de permiso y de establecer contratos que pagan dividendos a sus tenedores. Counterparty es un prototipo genuino que eventualmente se convertiría en el proyecto Ethereum – excepto que tuvo un lanzamiento justo, no tiene un blockchain propio, y todas sus transacciones (desde emisión a transferencias) se asientan en el blockchain de Bitcoin y pagan fees de transacción a los mineros de Bitcoin.

Los NFTs de Counterparty a menudo representan momentos de la historia de Bitcoin

En 2014, los bitcoiners soñaron con tokenizar a las acciones y commodities en su querida red. Tradear acciones de Apple, futuros de granos de cacao y tokens de oro sobre Bitcoin? Seguro, porque no! Construir compañías descentralizadas cuyos activos existen nativamente en la red de Bitcoin? Eso también es posible en Counterparty. Tokens que recaudan fondos y pagan dividendos a sus dueños? Si señor!

Esto fue antes del debate de escalabilidad y antes de decidir que los bloques deberían permanecer pequeños para preservar la descentralización y la resistencia a la censura. La mayoría de la gente detrás del proyecto luego migrarian a nuevo y reluciente Ethereum, el cual técnicamente podría hacer más y teóricamente escalar mejor para estos casos de uso.

Pues por un tiempo, las transacciones de Counterparty fueron injustamente consideradas “spam” lo cual no es beneficioso para el proyecto Bitcoin. Uno podría argumentar que el dinero de alguien no es confirmado más rápidamente debido al intercambio intensivo de tokens de Counterparty, ya que el primero paga fees más altos que el segundo. Adicionalmente, las transacciones OP_RETURN que usa Counterparty para insertar datos arbitrarios en los bloques de Bitcoin



consume más espacio de bloque que una transacción regular.

Pero de nuevo, esto significa que se paga un fee mayor. También, para mantener sustentables a los incentivos del proyecto Bitcoin, debemos construir un mercado de fees competitivo. También hay una pequeña pizca sobre Bitcoin siendo una red que no requiere permiso y permitir a los usuarios ser soberanos (es decir usar su dinero de cualquier forma que quieran). Entonces cómo puede ser spam si paga un justo fee a los mineros?

Counterparty ha estado en el lado equivocado de la historia de Bitcoin y muchos deciden nunca hablar de esto. Tiene un token nativo (XCP) que se usa para asignarle un nombre arbitrario a los activos: si pagas 0.5 XCP, puedes llamar "BTCTKVRMAG" a tu nuevo NFT en lugar de permitirle al protocolo que automáticamente lo nombre "A11137611919687294 90" (donde "A" significa "activo"). También puedes vender tus nuevos tokens y darle dividendos a los dueños usando el token XCP.



Pero existe un tema: Counterparty fue creado por bitcoiners quienes fueron testigos del ICO de Mastercoin (el cual luego se transformó en la capa OMNI) y lo odiaron. Los creadores del protocolo no querían captar fondos y ofrecer a los inversores un token. Eso no es lo suficientemente Bitcoin.

Así que alternativamente, les pidieron a los participantes que "quemaran" sus BTC y recibieron XCP a cambio. Lo que esto significa es que en Enero 2014, casi 2131 bitcoins fueron irreversiblemente enviados a la direccion 1CounterpartyXXXXXXXXXXXXXXXUWLpVr. Generaron a propósito una dirección que es difícil generar, y a la cual nadie tiene acceso. Entonces para que la totalidad de la emisión de 2,648,755 tokens XCP fue creada, se tuvieron que quemar BTC reales.

Según el artículo "Why Proof-of-Burn" del 23 de marzo de 2014, los bitcoiners que crearon Counterparty no querían que los desarrolladores tuvieran una ventaja injusta ni tampoco querían que grandes inversores tuvieran ningún control sobre la red. Todos tuvieron la misma posibilidad de quemar BTC y recibir XCP a cambio. También, nadie tuvo la ventaja de ser el primero para que no hubiese una entidad central que pudiera coordinar una trama "pump and dump". Todos están igualmente interesados en el éxito del proyecto y afrontan los mismos riesgos.

Sin embargo, esto no significa que el valor del token XCP esté ligado al precio de BTC, o que la capitalización de mercado debería a ser equivalente con los 2131 BTC. A Diciembre 28 de 2021, 2131 BTC tienen un valor de $105 millones mientras que el circulante entero de XCP es de solo $32.8 millones. La comparación ni era necesaria para demostrar que XCP no era un token de utilidad que compite con Bitcoin. No pretende ser una reserva de valor, solo lo compras para emitir tu activo con nombre usándolo para su propósito previsto. Atesorar XCP especulativamente seria tonto, ya que el token ni siquiera esta listado en los exchanges populares y la unica forma de adquirirlos es a traves de dispensadores.

Hablando de dispensadores, Counterparty es un exchange descentralizado genuino. Cualquiera puede vender activos sin permiso de nadie y transferir el BTC (o cualquier otro token de Counterparty) a una billetera personal luego de que cada transacción es asentada en el chain principal.

Si quieres comprar 0.5 XCP con tu BTC para ponerle nombre a tu nuevo NFT o para emitir dividendos a tus tenedores existentes de NFTs, vas a un dispensador y buscas al usuario con la oferta más conveniente. FreeWallet.io, posiblemente la mejor interfaz disponible en este momento, te permite navegar los exchanges (mercados abiertos para varios pares de tokens) y los dispensadores

(máquinas expendedoras donde compras/vendes tokens de Counterparty y NFTs por BTC).

El ingrediente de vanidad de emitir tokens con nombre es bastante exclusivo a Counterparty. Si miras a las NFTs en Raretoshi en Liquid, veras que son nombrados usando un hash criptografico aleatorio (por ejemplo, e9f53c1fd6f71eccbe2f3bf5523ef2091d9efbb9a155c7682808ffcd17299728). En Ethereum, llevan el nombre del contrato (por ejemplo, el spinoff de JScrilla de PEPEGOAT Rare Pepe Wallet ReDux se llama 0xb932a70A57673d89f4acfFBE830E8ed7f75Fb9e0). La principal diferencia es que en Counterparty compras activos adecuadamente nombrados y puedes usar el nombre del token para buscar cualquier tipo de información de la transacción en el explorador xchain.

Counterparty es básicamente una anterior versión de Ethereum construida sobre el blockchain de Bitcoin como un protocolo cuyas transacciones se liquidan con BTC pagando fees a los mineros de Bitcoin. Lo más probable es que haya sido abandonado porque escala pobremente. Pero a mediados de 2021, cuando la manía de los NFTs llegó a su punto más alto y Ethereum estaba lidiando con fees ridículamente altas, los bitcoiners se acordaron de Counterparty y aprovecharon la baja demanda de espacio en bloque de Bitcoin para resucitar algo del antiguo arte.



Mientras que algunos desalentaran el uso de Counterparty y recomendaran el uso de Raretoshi en Liquid o de RGB Spectrum en el Lightning Network, la realidad es que ninguno de estos son tan seguros y descentralizados que el blockchain de Bitcoin. Además, ninguno está garantizado sobrevivir tanto como la capa base. Y como existen muchas colecciones en Bitcoin, habrá coleccionistas que se interesaran en ellos. El objetivo no es claramente el de "escalar", sino el de proveer la más alta seguridad y longevidad a los activos.



Counterparty ha sido declarado "muerto" muchas veces ya, pero reapareció varias veces específicamente porque es desarrollado en Bitcoin y requiere de mínimo mantenimiento – los activos siempre existirán y son asegurados por una red global de mineros y nodos full, entonces son las interfaces de usuario (billeteras) las que necesitan mejoras de vez en cuando. Puede que tus NFTs sean más difíciles de crear y transferir (en comparación a plataformas centralizadas tales como Liquid y Ethereum), pero también son más seguras ya que cortar la red es virtualmente

imposible. Además, es realmente shitcoinear si lo construyes sobre Bitcoin y contribuyes a la seguridad de la red pagando fees con cada transacción?



Como Crear TU Primer NFT De Bitcoin En Counterparty Con Freeport

Dependiendo de cuánto te importe el nombre de tu activo, existen dos formas de emitir NFTs de Bitcoin en Counterparty y tienen distintos niveles de dificultad. Lejos, la manera más simple es obtener la billetera FreePort de Joe Looney (disponible como una extensión de navegador de Chrome o Firefox), transferir el equivalente de BTC de un par de transacciones, y luego seguir la simple interfaz para subir tu jpg/gif y emitir tu NFT.

Si usas FreePort, nunca tendrás que usar XCP o complicar tu existencia teniendo que comprar de dispensadores. Podrás acuñar, enviar, y admirar los NFTs en tu colección en una interfaz muy simple. Aquí van los pasos a seguir:

1. Ve a https://github.com/loon3.Freeport-extension
2. Si usas Chrome, cliquea en la URL que se encuentra debajo del subtítulo “Install from Web Store” y sigue las instrucciones en la pantalla. Cuando termines, verás el logo de Freeport en el extremo superior derecho de tu ventana de Chrome, pegada a la barra de dirección y a la izquierda del menú de opciones.
3. Si usas Firefox, debes usar la linea de commando web-ext para instalar el archivo disponible en https://github.com/loon3/Freeport-extension/raw/dev/packages/freeport-0.3.0-fx.xpi. Esta es la manera más complicada y deberás leer la sintaxis para instrucciones tales como “web-extrun”. Sin embargo, si lo que buscas es escapar del panóptico, valdrá la pena.
4. Establece una nueva billetera con Freeport. Por defecto, generará una semilla BIP39 de 12 palabras y también deberías establecer una frase de contraseña (recomiendo usar letras y números) para desbloquear tus activos. Esta es básicamente una billetera de Bitcoin, pues tratala como tal – cuida tu frase de contraseña, nunca se la enseñes a nadie ni la escribas en un papel ni en placas de metal.
5. Una vez que estés listo y logueado, verás el menú principal de Freeport el cual posee tres botones: Collect, Create, y Buy/Sell. En la esquina superior izquierda verás tu dirección de Bitcoin de Counterparty, y en la esquina superior derecha verás un botón naranja con el logo de Bitcoin – este te permite chequear tu saldo de BTC y enviar montos arbitrarios. Fíjate también que en el menú inferior tienes un botón “Settings”. Puedes usarlo para cambiar tu direccion para recibir/acuñar NFTs (una función que jamas encontraras en Ethereum porque por diseño no tiene UTXOs), ver tu frase de contraseña (nunca tomes capturas de pantalla), establecer manualmente fees de transacción, y resetear la aplicación para que cargue una billetera diferente.
6. Ve al menú “Create” y escoge “Create New Item. Aparecerá un menú pidiéndote que subas una imagen gif, jpg o png. Luego de subirla a Freeport, en realidad va a servidores de Imgur y se le asigna su propia URL.
7. Lo siguiente es nombrar tu activo (ten en cuenta que esta es la descripción del token, no el nombre del token), establece la emisión (por ejemplo, la colección de Leftist Tears tiene una emisión limitada de 21 tarjetas por edición) y decide si quieres que el activo sea divisible (cotizaras en unidades enteras y también en fracciones?). Luego de esto, debes elegir entre un fee prioritario o un fee económico – estas son estimaciones basadas en la observación del mempool de transacciones de Bitcoin de tu propia billetera. Para setear el fee manualmente

según tu propio análisis y preferencia de tiempo, vuelve al menú "Set transaction fees manually".

8. Una vez que finalices el seteo de los parámetros, presiona el botón "Create". Si tienes suficiente BTC en tu billetera para pagar el fee de transacción, la transacción OP_RETURN será transmitida a la red de Bitcoin y aguardara confirmación. Luego de tu primera confirmación de la red, tu NFT aparecerá en la sección de Freeport "Collect". Puedes enviarselo a amigos que compartan su dirección de Bitcoin contigo, pero la billetera Freeport no es lo suficientemente avanzada para permitirte establecer un dispensador para venderlo. También puedes recibir NFTs de amigos compartiendo alguna de tus direcciones con ellos. Pero si quieres aprovechar el potencial completo del protocolo Counterparty, tendrás que usar una billetera avanzada como FreeWallet.io en desktop.

Crea Y Administra Tus NFTs De Bitcoin Con FreeWallet.Io En Desktop (Mac, Windows, Y Linux)

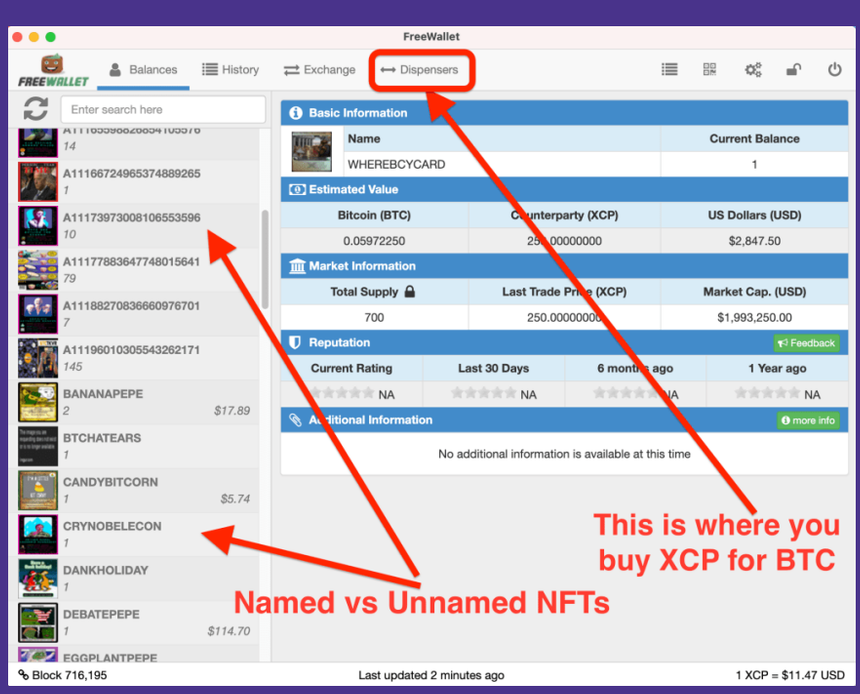
La segunda y más difícil forma de acuñar y administrar NFTs de Bitcoin involucra una billetera desktop como FreeWallet.io. Si quieres que tu nuevo activo lleve un nombre determinado, estás interesado en acceder a dispensers, y también quieres pagar dividendos a los tenedores de tus NFTs, entonces debes ir por esta mejor vía.

Antes de entrar en detalle, debes tener en cuenta que las versiones móviles del software de FreeWallet.io no han sido mantenidas durante años y definitivamente causará bugs no deseados. Estan bien para generar una billetera y recibir NFTs, pero para cualquier otra función deberías usar tu computadora desktop o laptop (o cualquier dispositivo que corra MacOS, Windows, o Linux)

Para asignarle nombre a tus activos, necesitarás 0.5 XCP (el token nativo de Counterparty). Y dado que los exchanges ya no lo listan, la única manera de adquirir XCP es de dispensadores.

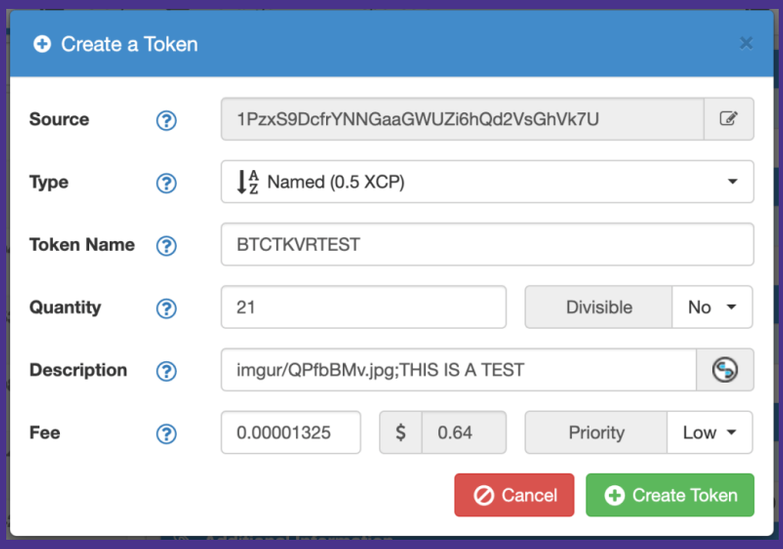
Un dispensador es básicamente una máquina expendedora: alguien bloquea un monto arbitrario de un activo y permite a cualquiera que envíe la cantidad de bitcoin correcta para obtener propiedad del activo. Ves lo que quieres comprar, escoges el trato que quieres, y luego procedes a realizar la compra.

Los dispensadores son un tipo básico de contrato inteligente. Pero su naturaleza automatizada también viene con un tradeoff: siempre existe el riesgo de que el dispensador sea vaciado antes de que tu transacción se confirme. Así que si seteas un fee de transacción bajo y esperas un par de días hasta la primera confirmación, te expones al riesgo de tratar con un dispensador cerrado o vacío. No hay forma de que una transacción de Bitcoin sea revertida y no existe un mecanismo para reembolsar tu dinero si la totalidad de los tokens de Counterparty se



venden todos antes de que puedas hacerte de este activo digital.

Este es el motivo por el cual deberías idealmente pagar un fee de transacción más alto, para asegurarte de estar entre los que consiguen un trato justo. También deberías tratar de solo comprar de dispensadores que hayan sido creados por direcciones que reconoces – si conoces al dueño y confías en su reputación, tendrás más chances de recuperar tus bitcoins si el intercambio no se lleva a cabo.



He perdido el equivalente a unos $40 de bitcoin tratando de comprar XCP para nombrar mis NFTs: la primera vez, el dispensador se cerró antes de recibir mi primera confirmación (clásica estafa de salida); la segunda vez, alguien compro todos los XCP del dispenser antes de antes de que recibiera mi primera confirmación. En ambos casos, no tenía idea con quien estaba tratando y no sabia como contactar al dueño. Esto es desafortunado, pero parte de un mercado digital descentralizado, no regulado y libre.

Luego de comprar tu primer XCP (recuerda, necesitas 0.5 XCP por NFT con nombre y deberías usarlo lo antes posible en vez de retenerlo con fines especulativos), ve al menu “Actions” en la esquina superior derecha de la ventana de FreeWallet y selecciona “Create a Token”.

Aquí, debes establecer una descripción. Y aquí es donde diriges tu archivo de imagen a FreeWallet. Deberás aprender a usar la sintaxis correcta, ya que la estructura es “imgur/imagename.jpg;DESCRIPTION OF YOUR TOKEN”. Nota que no ingrese el URL entero a tu activo Imgur o YouTube, sino que usas un formato acortado. Además, no hay espacio ni antes ni después del punto y coma. Esto es muy importante, ya que he cometido ese error y la imagen no fue presentada correctamente y tuve que enviar otra transacción que cambiara la descripción.

Existe un importante debate pendiente sobre Imgur y otros servicios centralizados, ya que pueden censurar o remover tu imagen. Sin embargo, puedes subirlo a algún otro lugar y cambiar la descripción de tu token con una transacción de BTC. Esto por esto que dicen que el token es el arte – porque mientras el activo de Counterparty es inimutable y no puede ser renombrado, la descripción puede ser cambiada en cualquier momento pagando el costo de una transacción on-chain.

Por último, debes setear un fee de transacción acorde a tu preferencia de tiempo. Idealmente, debes asegurarte de que confirme dentro de las dos semanas para evitar que la mayoría de los nodos la excluyan del mempool. Pero el fee de prioridad baja o media que recomienda mempool.space debería ser suficiente.

Nota que no seteas tu fee usando el clásico sistema sat/byte o bit/kb. En cambio, escoges el monto total que quieres pagar de fee. Recuerda que estas transacciones OP_RETURN son generalmente más grandes que la transferencia de dinero promedio (ocupan más espacio en el bloque) y toma nota de las recomendaciones de costo en dólares para tener una aproximación más precisa. Por default, FreeWallet no te permite pagar un fee inferior a 0.00001 BTC (10 bits, o 1000 sats) por transacción, pero puedes cambiarlo en el menú de Settings.

Una vez que seteas todos estos parámetros, cliquea el botón “Create Token” y estarás listo. Tu NFT estará

disponible luego de que su transacción OP_RETURN correspondiente reciba su primera confirmación en el blockchain de Bitcoin.

¿Ahora qué puedes hacer? Puedes enviarselo a amigos, puedes establecer un dispenser para venderlo, y hasta puedes quemar su circulante para hacerlo aún más raro. Si valoras a los tenedores de tus tokens, también puedes pagarles dividendos.

Con respecto al token en sí, puedes cambiar su descripción y su representación visual cuando te plazca. Pero el nombre quedará para siempre. Tal como en el caso de los nombres de dominios, el que está tomado no puede ser usado por otro – excepto que no es necesaria una renovación periódica. Una vez que lo emites, eres dueño del nombre del activo. Y en realidad, esto es lo que compra la gente.

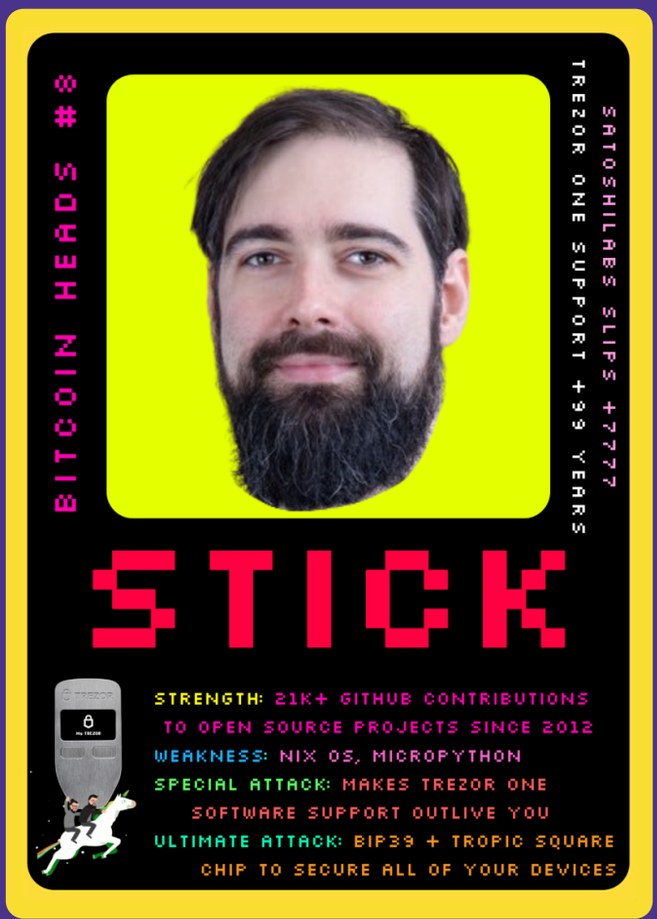
También puedes listar el token en exchanges a cambio de XCP – pero esta función está disponible en billeteras como Counterwallet (eds.counterwallet.io). La liquidez para nuevos NFTs es muy baja y probablemente te convendrá abrir dispensadores que te permitan vender tus tokens por BTC. Pero si quieres explorar este camino de financiarización y hacer más con tus XCP, eres libre de intentarlo.

Obten Tu Primer NFT De Counterparty

En los juegos de Pokemon, puedes elegir entre Charmander, Bulbasaur, y Squirtle. Inspirado por esta elección de principiante, estableci dispensadores que ofrecen NFTs de Counterparty accesibles para cualquiera que quiera entender como funciona esto.

Puedes obtener una de las primeras 3 tarjetas de la serie Bitcoin Heads por solo 23.45 bits (2345 sats, que al cambio de Diciembre 29 son poco más de $1). Y puedes elegir entre VLADHEAD, JOSHUAHEAD, y NOPARAHEAD.

¿Por qué no las reparti gratis? Pues porque técnicamente no puedo – a no ser



que me envíes tu dirección de Bitcoin de Counterparty en un mensaje privado, hago una lista, y luego loteo transacciones a los destinatarios. Además, el objetivo aquí es enseñarte sobre cómo funcionan los NFTs de una manera rápida y accesible. Todos los fondos que reciba serán utilizados para crear más activos de la serie Bitcoin Heads y distribuirlos sin cargo.

Entonces luego de cargar tu FreeWallet con al menos 0.00002354 BTC (el monto mínimo para comprar una tarjeta) y unos 0.00001000 BTC para el fee de transacción, puedes elegir una de las tres tarjetas para agregar a tu colección. Y si, puedes comprar las tres y ser codicioso y acumular cuantas más puedas con fines especulativos. Depende totalmente de ti.

Pero mientras estaba experimentando con los dispensadores, descubrí que algunas billeteras de Counterparty utilizan límites de polvo de BTC más antiguos de 54.6 bits o 5460 sats. Mientras tanto, los desarrolladores Core lo han seteado en 5.46 bits/546 sats. Pero puede



que algunas billeteras de Counterparty antiguas usen la política anterior.

Esto significa que cualquier transacción de menos de 0.00005460 BTC puede no ser transmitida a la red. Si esto ocurre, deberás comprar por lo menos 3 tarjetas en una transacción. Aunque pueda cerrar los dispensadores existentes y reabrirlos a un mayor precio por tarjeta para eliminar este inconveniente, creo que esta lección de cómo funciona Bitcoin será más útil para todos.

En fin, el propósito de estos NFTs es ayudar a la mayor cantidad de gente posible obtener su primero en Bitcoin para comprender cómo funciona. No fomento la especulación, pero lo que la gente haga con sus tarjetas luego de comprarlas va más allá de mi control y Bitcoin es una red que no requiere permiso que permite la existencia de mercados libres y abiertos.

También cree códigos QR que te llevan a la página del dispensador de cada uno de los tres NFTs. Si no puedes escanear QRs y quieres encontrar los activos en tu computadora, ve a xchain.io (el explorador de Counterparty más popular) y tipea VLADHEAD, JOSHUAHEAD, y/o NOPARAHEAD en la barra de búsqueda. Luego de cliquear en el nombre del token, encontrarás un solapa especial para los dispensadores.

En el futuro, encontrarás más de estas creaciones en btcheads.com y en nftears.com.

Cual Es El Punto De Los NFTs?

Los NFTs de Counterparty son una manera divertida de jugar con Bitcoin. Podrás explorar las características de un temprano protocolo que buscó introducir una completa gama de activos financieros a Bitcoin. También verás dónde se inició toda esta locura, te sumarás a canales de Telegram, y te harás amigo de los OGs que crearon Rare Pepes y Spells of Genesis (a quienes también puedes escuchar en la temporada 10 del podcast Bitcoin Takeover).

Pero para mi, es importante demostrar



que Bitcoin es mucho más que una herramienta financiera. Es también una red de computadoras distribuidas que permite la libre expresión. Mensajes que de otra manera serían censurados o suprimidos pueden encontrar su lugar en la red de Bitcoin – a cambio de un fee de transacción, por supuesto. Pero las intenciones no son siempre financieras y hay muchas maneras de expresarse a través de Bitcoin (siendo los NFTs de Counterparty una de ellas).

Tal como menciona el abogado del First Ammendment Estadounidense Justin Wales en el episodio 4 de la temporada 5 del podcast Bitcoin Takeover, Bitcoin es libertad de expresión y debería ser protegido bajo las disposiciones de la Constitución Estadounidense y del Bill of Rights. Entonces si realizamos usos no financieros de la red de Bitcoin más comúnmente, fortalecemos esta tesis y ganamos importantes batallas contra los reguladores que solo parecen escuchar las narrativas sobre simplificadas. Bitcoin no es un commodity, no es un activo bursátil, no es como nada que los sistemas jurídicos hayan jamás visto y puede ser usado para ejercer la libertad de expresión y divertirnos.

Por supuesto que estos casos de uso no son para todos. Si no es lo tuyo acumular y atesorar BTC, no comprenderás los NFTs. Y eso está completamente bien, no todos aspiran a coleccionar tarjetas de intercambio ni encuentran valor en tokens arbitrarios en la red de Bitcoin que también puedan tener un jpeg o gif asociado a ellos.

Los NFTs son una categoría de activo, no son “monedas”. Y no son totalmente como las tarjetas de baseball tampoco. Son coleccionables demostrablemente raros que cuentan una historia, significan algo para el coleccionista, o sino simplemente permiten a los bitcoiners más ricos apoyar el trabajo de jóvenes artistas. Y a pesar de que exista un mercado para la especulación con los NFTs, su propósito no es siempre especulativo – a veces solo se trata de divertirse de una forma nerd y costosa.

No todos los NFTs son creados de la misma manera y esa es la idea de algo “no fungible”. Son únicos de su propia manera, tienen algunas particularidades que a otros pueden resultarles atractivas al punto que están dispuestos a pagar dinero, y evocan un determinado sentimiento o recuerdo. Algunos son históricos, otros son divertidos, pero todos son recordatorios de que la comunidad de Bitcoin es realmente divertida y diversa.

Así que la próxima vez que alguien te mencione lo fantásticas que son la colecciones de Ethereum o Solana, recuerdales que Bitcoin lo hizo primero y lo hace mejor con Counterparty, Y si en algún momento quieres enviarme aguna de tus creaciones, mi direccion es 1PzxS9DcfrYNNGaaGWUZi6hQd2VsGhVk7U

–


Opere con NFT de Bitcoin como billetes
sato dime
By sato Chip
ELLIE WAS HERE
CALL ME XOXO
REKT
LYK
BITCOIN HEADS #1
ARTICLES, PODCASTS & VIDEOS ON BTCTKVR.COM +99999
VLAD
STRENGTH: BEST HAIR IN BITCOIN
WEAKNESS: CAN'T FIND GIRLFRIEND
SPECIAL ATTACK: HELLO THERE AND WELCOME TO THE BITCOIN TAKEOVER PODCAST
ULTIMATE ATTACK: BTCTKVR MAGAZINE CHANCE TO BUY BITCOIN MAGAZINE +10
BITCOIN HEADS #2
HARD, HONEST MONEY +99
BEATING INFLATION +69
JOSHUA
STRENGTH: SMARTER THAN PETER SCHIFF, WISER THAN BARRY SILBERT
WEAKNESS: TOO NICE FOR HIS OWN GOOD
SPECIAL ATTACK: BITCOIN AND GOLD ARE COMPLEMENTARY
ULTIMATE ATTACK: GOLD TOKENS ON BTC VAULTORO DOMINANCE +10
BITCOIN HEADS #3
FUN IN FUNGIBILITY +99
CHAINALYSIS HEADACHES +72
NOPARA
WASABI WALLET
STRENGTH: CODED MOST OF WASABI WALLET 1.0 BY HIMSELF
WEAKNESS: SPENDS TOO MUCH TIME FIGHTING RED NINJAS
SPECIAL ATTACK: WABISABI
ULTIMATE ATTACK: BUY MICROSOFT BITCOIN PRIVACY OVER 9000
BITCOIN HEADS #4
FAKE SOCRATES WHO USES MS PAINT +99
DEROSE
STRENGTH: WILL DESTROY YOUR BLOCKCHAIN THOUGHT LEADER IN DEBATE
WEAKNESS: SATOSHI ROUNDTABLE EVENTS, DERRIDA
SPECIAL ATTACK: HELLO, PARTY PEOPLE!
ULTIMATE ATTACK: DEROSE'S LAWS DECONSTRUCTS POSTMODERNISM +9000
BITCOIN HEADS #9
LIGHTNING NETWORK ADOPTION +69420
BEN ARC
STRENGTH: CRAFTY ENOUGH TO BUILD HIS OWN FOSS TOOLS
WEAKNESS: PROUDHON, CALLING HIMSELF BTC SOCIALIST
SPECIAL ATTACK: LNBITS IN EVERY NODE
ULTIMATE ATTACK: WILL ASSMILK ALL OF YOUR LIGHTNING FAUCETS
BITCOIN HEADS #1
ARTICLES, PODCASTS & VIDEOS ON BTCTKVR.COM +99999
POWERED BY
Satodime
By Satochip
BITCOIN HEADS #8
SATOSHILABS SLIPS +7777
TREZOR ONE SUPPORT +99 YEARS
STICK
STRENGTH: 21K+ GITHUB CONTRIBUTIONS TO OPEN SOURCE PROJECTS SINCE 2012
WEAKNESS: NIX OS, MICROPYTHON
SPECIAL ATTACK: MAKES TREZOR ONE SOFTWARE SUPPORT OUTLIVE YOU
ULTIMATE ATTACK: BIP39 + TROPIC SQUARE CHIP TO SECURE ALL OF YOUR DEVICES



Los Beneficios De Privacidad De Taproot

El soft fork de Taproot en Bitcoin es un paso esencial hacia la mejora de la privacidad on-chain de Bitcoin. Luego de que el upgrade fuera activado el 14 de noviembre de 2021 en el bloque 709632, a las companias de análisis de blockchain se les hará más dificultoso determinar lo que está ocurriendo en el registro público. Inconvenientemente para aquellos que buscan desanonimizar todas las transacciónes de bitcoin, Taproot hace que la mayoría de los contratos on-chain y las transferencias condicionales se vean identicas a una transaccion regular. Indirectamente, esto también beneficia a la escalabilidad (seteos multisig ya no ocupan mayor espacio en el bloque) y a los costos (los outputs de transacciones más pequeñas generan menores costos para el usuario).

Este artículo, sin embargo, se enfoca en el aspecto de privacidad del soft fork de Bitcoin. Busca explicar como Taproot incrementa la negacion plausible de cada usuario y potencialmente genera una amenaza para el negocio de análisis de blockchain. Para hacer que esta mejora sea fácil de comprender, los beneficios seran divididos segun sus casos de uso.

Cómo es que Taproot Incrementa la Privacidad del Lightning Network

El Lightning Network es la capa de Bitcoin para transacciones instantaneas, privadas y accesibles. A diferencia de un blockchain, es extremadamente escalable,

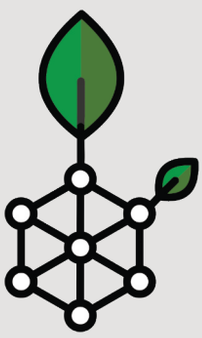
veloz y no requiere que la red entera almacene y valide cada operacion. Este diseño más elegante permite mayor privacidad: solamente las partes involucradas en una transferencia de dinero y los nodos de ruteo pueden obtener informacion sobre una transaccion en progreso. El resto queda totalmente a ciegas y no pueden saber nada sobre los participantes involucrados ni de la cantidad de bitcoin que movieron. Para una mejor comprension de como funciona Lightning, lea mi artículo "Explicando El Lightning Network Para Que Hasta Alguien de 10 Años de Edad Lo Pueda Entender".

Pero dado a que Taproot es una mejora en la capa base, realmente afecta a Lightning? Sin un upgrade compatible con Schnorr, el abrir y cerrar canales queda expuesto en el blockchain público exactamente como lo que son: multisigs 2 de 2 con contratos hasheados de tiempo fijo (HTLCs). Luego de la activacion de Taproot, cualquiera que abra o cierre un canal de Lightning en colaboracion se verá como que está realizando una transaccion normal la cual es indistinguible de otras.

Previamente, analistas de blockchain lograban identificar cuando algunas transacciones cerraban canales de Lightning. Pero luego de taproot, solo podran ver que las monedas se han movido. No saben cómo se movieron, sólo verán que la cantidad fue movida de una manera indistinguible.

Sin embargo, el nivel de privacidad aun no es perfecto. Tal como recalcó el creador de Wasabi Wallet Adam Ficsor, canales de Lightning no privados transmiten un punto en el canal que corresponde al output de apertura. Consecuentemente, esta pequeña informacion, que puede ser observada en el Lightning Network, revela informacion sobre el output que está detras de la apertura del canal. Taproot si permite que la apertura de canales de Lightning sea privada, pero solo si los canales también son privados. Del mismo modo, a pesar de que una transaccion CoinJoin antes y despues de abrir un canal Lightning puede ofuscar la previa y la futura, el chisme en Lightning aun revelara con precision el UTXO controlado por el operador del nodo. Existe investigación prometedora para mitigar el problema con pruebas ring-signature para proteccion DoS.

Cómo es que Taproot Incrementa la Privacidad de los Sidechains



De la misma manera que al abrir un canal Lightning, los peg-ins de un sidechain también dependen de un contrato multisig. En RSK (Rootstock, un sidechain de Bitcoin que busca portar contratos inteligentes de Ethereum), existe un peg de dos vias (2WP) que asegura que los BTC sean transferidos de una forma segura. Pero luego de Taproot, la transaccion será indistinguible de todas las otras y también ocupará menos espacio en el bloque.



Lo mismo ocurre con el sidechain Liquid de Blockstream, así como también con Drivechains. Las transacciones regulares, los peg-ins de Liquid, los canales Lightning y los multisig de usuarios se verán exactamente iguales.

Cómo es que Taproot Incrementa la Privacidad del Multisig

En años recientes, los armados mutisig se han convertido en extremadamente populares entre los bitcoiners. Dado que la experiencia del usuario ha mejorado con billeteras tales como Electrum, Sparrow y Specter, muchos miembros de la comunidad han decidido hacer de sus monedas más dificiles de robar, hackear o gastar. La idea detras es que no necesitas confiar en una sola billetera o entidad con la aleatoriedad y la seguridad de tu clave privada. Usas distintos dispositivos con distintas unidades de procesamiento, y luego puedes hasta distribuir tus backups de claves privadas en distintas partes del mundo.

Dependiendo de tu armado (la mayoria de los usuarios usan 2 de 3, pero pueden ser hasta 15 de 15 si prefieres complejidad), puedes obtener mucha seguridad adicional a costa de pérdida de accesibilidad – y si lo haces my dificil inclusive para ti recuperar las monedas, puedes perderlas.



Taproot posee dos beneficios esenciales para los armados multisig: los hace más accesibles (el costo de transaccion de firmar una transaccion 19 de 20 será el mismo que los de una unica firma) y al mismo tiempo suma una nueva capa de privacidad. Toda informacion innecesaria dejará de aparecer en el blockchain publico. Esto conserva la privacidad de todos los firmantes ya que solo muestra el input principal y su output correspondiente. Antes de Taproot, el análisis de blockchain podia determinar que claves del armado habian firmado la transaccion, Despues de Taproot, esta informacion será inaccesible al público.

Cómo es que Taproot Incrementa la Privacidad de los Contratos Inteligentes de Bitcoin

Desde el primer día, Bitcoin permite la funcionalidad de contratos inteligentes. Basicamente, los usuarios han podido transmitir transacciones condicionales las cuales instruirian al resto de la red cuando los fondos pasaban a estar disponibles para ser gastados. Los armados multisig, las aperturas de canales de Lightning y los peg-ins a sidechains son todas variaciones que hacen uso de distintos tipos de condiciones.

Pues consideremos un contrato basico en el cual Alice bloquea sus bitcoins hasta un cierto bloque en el cual cree que su

pequeño hijo Bob será un adulto, o sino permite a Bob desbloquear los montos apenas pueda tener la capacidad tecnica de firmar una transaccion multisig. Bajo la estructura actual, ambas condiciones son reveladas a la totalidad de la red y se convierten en parte del registro inmutable. Pero con Taproot, solo los que son ejecutados se haran publicos. Es una mejora en la eficiencia que ahorra espacio preciado en el bloque, y al mismo tiempo un gran truco de privacidad que permitira una gran cantidad de formas creativas para preservar riqueza a traves del tiempo.



Taproot Simplifica los Coins Swaps Invisibles

La billetera Mercury de Commerce-Block se ha hecho muy popular en meses recientes. Esto se debe a una prestacion especial que realiza un cambio de propiedad de un output en el Lightning Network y así efectivamente permite a los usuarios intercambiar la historia de transacciones de sus monedas de una forma elegante y escalable. Si los bitcoiners abren canales de Lightning e intercambian UTXOs entre sí, pueden ofuscar muchas de las actividades previas de su dinero y retornar al blockchain de BTC con otras monedas distintas. La billetera Mercury hace uso del concepto statechains de Ruben Somsen de bloquear fondos por una cantidad de tiempo predeterminada y hacer mezclas entre outputs equivalentes.



En cierta manera, los Coinswaps son CoinJoins que hacen uso de la escalabilidad y los bajos costos de Lightning. Gracias a Taproot, son demasiado indistinguibles de otras transacciones.

Sin embargo, con los Coinswaps, siempre existe el riesgo de que recibas un UTXO más problemático el cual podria tener una historia criminal. En lugar de combinar multiples historias de transacciones (como es el caso con CoinJoins), hace posible un mercado anonimo para intercambiar historias de transacciones. Tal como mencionó el creador de Wasabi Wallet Adam Ficsor en una reciente entrevista, las dos soluciones de privacidad pueden ser herramientas complementarias: “La combinacion parece ser más interesante sin embargo: CoinSwaps a y desde CoinJoins, lo cual podria permitir a sets de baja annonimidad de Coinjoin obtener tanta privacidad como la que obtendria un CoinSwapper.”





La Privacidad de Bitcoin Despues de Taproot

Con Taproot, Bitcoin atravesó una mejora deseada desde hace mucho tiempo hacia las más eficientes firmas Schnorr, y al mismo tiempo dar unos pasos hacia ganar la batalla de la vigilancia financiera. Sin embargo, esto no significa que el análisis de blockchain se vuelva obsoleto luego de este upgrade. Primero que nada, llevará tiempo que los usuarios actualicen sus nodos al más reciente cliente compatible con Taproot (así que los beneficios no seran aprovechados por todos). Segundo, los desarrolladores deben lanzar billeteras y aplicaciones que hagan uso de la totalidad del potencial de Taproot. Por ahora, mucho no ha cambiado desde el bloque 709632, cuando fue activado el soft fork. Pero los numerosos beneficios de Taproot generan la esperanza de una adopcion ligera.

Adicionalmente, el protocolo de Bitcoin puede optimizar aún más su escalabilidad y privacidad. Uno de ellos puede ser OP_CHECKTEMPLATEVERIFY (BIP 119, previamente conocido como OP_SECURETHEBAG) de Jeremy Rubin, el cual lotea transacciones para reducir la cantidad de inputs y recortar costos durante los momentos de alta demanda y congestion. Con el, los CoinJoins y CoinSwaps pueden obtener aun mas negacion plausible ya que la misma tecnica se hace un componente más natural de la rutina de transacciones de Bitcoin.

Otras soluciones incluyen Drivechains (Paul Sztorc a logrado crear una cadena estilo Zcash con el proposito de incrementar la fungibilidad de los bitcoins procesados), los bloques de extension Mimble Wimble (un experimento en proceso en Litecoin, el cual puede ser util si se demuestra que funciona), y esperar que los desarrolladores core encontrarán una manera de integrar zero-knowledge proofs o Confidential Transactions sin la necesidad de un hard fork. Sin embargo, Taproot potenciado por firmas Schnorr sigue siendo un gran punto de partida y la forma en la que fue activado nos da esperanza de que algun día los bitcoins obtendran fungibilidad casi absoluta.

_

WASABI.WALLET 2.0

Una Billetera de Bitcoin que provee privacidad por defecto



- Coinjoin cualquier monto
- Sin cargo de coordinación bajo 0.01 BTC
- Sin cargo de coordinación por remezclar directamente desde un coinjoin ni al estar a 1 transacción de una mezcla.

Wasabi es el estándar para la privacidad en Bitcoin.

wasabiwallet.io



¿Puede Bitcoin Funcionar Como Papel Moneda?

A pesar de que Bitcoin está al frente de las innovaciones financieras de estos tiempos, no es parte de la agenda de una sociedad sin efectivo. Consecuentemente, su proposito no es reemplazar al concepto de papel moneda o a la fisicalidad de los activos. Es el de cambiar su respaldo subyacente. En lugar de tener papel moneda respaldado por la deuda de un pais, en un futuro podriamos hacer compras cotidianas con papel que pueda ser redimido por BTC en la casa de cambio más cercana.

Transformar a bitcoin en un activo al portador es esencial para el uso de esta moneda como medio de intercambio y unidad contable. Gracias a innovaciones criptograficas y lecciones que hemos aprendido durante siglos de emision de billetes, podemos exitosamente hacer a los bitcoins más líquidos, más privados, y menos dependientes de una conexion de internet o de interacciones con la red.

El efectivo es la forma de dinero más privada y fungible que tenemos. Puede cambiar de dueño sin dejar ningun tipo de rastro y es el instrumento supremo para preservar los derechos económicos del individuo. Mientras que las transacciones en la capa base de Bitcoin dejan un registro permanente y enviar transacciones Lightning genera pruebas criptograficas que son verificadas por los participantes que rutean las transacciones, el efectivo no deja un rastro y no puede ser identificado.

Pero para que bitcoin funcione como papel moneda, debe cumplir con estos criterios:

- el billete debe tener elementos distintivos que lo hagan infalsificable, mientras que el dinero falsificado deberia ser detectado facilmente;
- el billete no deberia contener la clave



privada como es el caso con las billeteras de papel. En cambio, deberia tener una prueba criptografica distintiva (tal como un Open Time Stamp) para demostrar su emision por parte de una entidad determinada (exchange, gobierno, o cualquier otro emisor). Basado en este identificador unico, la entidad emisora debera permitir a los portadores redimir los bitcoins;

• el billete debera ser demostrablemente respaldado por una cantidad equivalente de bitcoin. Un billete equivale a un UTXO específico. Para garantizar que el monto correspondiente no haya sido redimido en un banco/exchange, una clave pública escaneable deberia ser impresa en el billete;

• en el caso de que el billete sea irreversiblemente extraviado o destruido, deberia ser facilmente reemplazado por el emisor. Esto puede ser estableciendo un esquema para reemplazar los billetes cada 5-10 años – todos deberia tener tiempo suficiente para cambiar sus billetes, y luego de un vencimiento arbitrario el viejo papel moneda deberia ser remplazado;

• la verificacion deberia incluir la totalidad de las reservas de bitcoin que respaldan a los billetes. Esto aseguraria que no haya impresion arbitraria por fuera de las reservas existentes.

Histórica y tradicionalmente, el papel moneda requiere de un emisor a quien pueda ser exigida la responsabilidad. A pesar de que bitcoin no requiere permiso y es una moneda descentralizada que puede ser tenida por una cantidad de tiempo ilimitada, la transicion al papel moneda no puede ser practica sin tener que romper alguna de estas reglas. Así como con los sidechains y las segundas capas, habra concesiones mutuas. En el caso del papel moneda, los usuarios apreciaran la privacidad irrastreable y la capacidad de hacer pagos en bitcoin sin usar internet.

Consecuentemente, el papel moneda de bitcoin puede ser emitido por exchanges, bancos, o gobiernos. El intercambio subsecuente deberia ser expeditivo, instantaneo y voluntario. Y tal como es el caso con los peg-outs de Liquid o las extracciones de Tether, la parte que redime los bitcoins debe someterse a un proceso de verificacion de identidad más riguroso (y los que redimen muy probablemente seran



empresas, organizaciones, y otras entidades legales que prefieran tener bitcoins reales).

Cuando los comerciantes reciben un pago de bitcoin en efectivo, haran uso de una aplicacion open source gratuita que verifica el UTXO, los fondos mayores que respaldan los billetes, y los elementos de diseño unicos que garantizan su autenticidad.

La verificacion no deberia tardar mas que un simple scan – y el mensaje en la pantalla deberia describir el estado de la verificacion. Ciertamente no es tan expeditivo como el efectivo y sigue requiriendo de una conexion de internet por parte del comerciante (para mayor grado de verificacion, el pagador también deberia correr el mismo software para evitar intentos de fraude). Pero sigue siendo una muy buena manera de poder usar bitcoin bajo el formato de papel moneda.

Propuestas Previas Para Papel Moneda De Bitcoin

Existen otras propuestas similares desde agosto de 2010, cuando el desarrollador de Bitcoin Gavin Andresen describio como "imprimir bitcoins" funcionaria (aunque describio la creacion de billeteras de papel).

En 2013, Sergio Damian Lerner (quien luego diseñó el sidechain RSK) describio un sistema mas avanzado y tecnico al cual llamo BitBanknotes. Y la propuesta de bitcoin en efectivo parece ser recurrente durante los mercados en alza, ya que Andreas Antonopoulos tuiteó una foto de un billete de $5 con un "tag de 5mBTC" cuando el precio de bitcoin toco los $5000 en octubre de 2017.

Más recientemente, Charlie Lee sugirio que El Salvador deberia imprimir papel moneda respaldado por la cantidad de bitcoin correspondiente. A pesar de que los nuevos bitcoiners actuaron por instinto y rotundamente rechazaron la idea, el experto en criptografia aplicada y desarrollador de Bitcoin Core Peter Todd confirmó que la idea es posible en virtud a pruebas criptograficas (habiendo trabajado en Open Timestamps y Proofmarshall, es una de las personas con mayor conocimiento de este tema).

–



Billeteras Hardware DIY, Parte I:

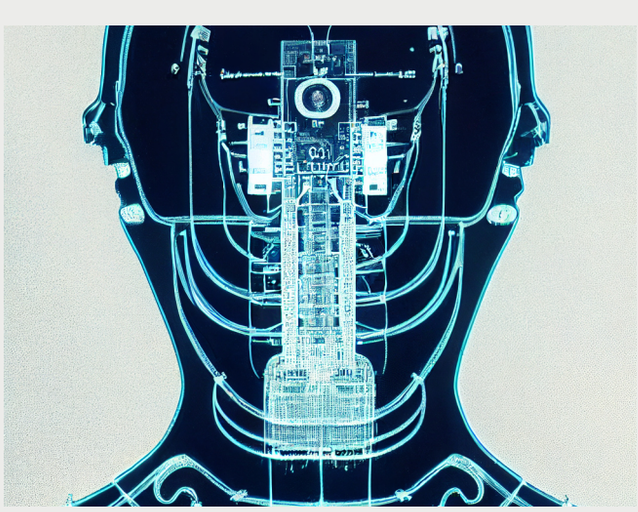
Construyendo Tu Propia Billetera Trezor One, Model T Y BitBox02

Estamos viviendo en la era dorada del hardware DIY. Gracias a los avances en el microprocesamiento y en la produccion/ distribucion, hoy podemos comprar computadoras pequeñas pero potentes a precios sorprendentemente bajos – y luego usarlas para tareas sorprendentemente complejas.

La comunidad de Bitcoin sin duda tomó nota de esto y convirtió algunos chips de uso general en máquinas de soberanía financiera. Desde los populares chips ARM Cortex STM32 al asombrosamente accesible Raspberry Pi Zero, existen muchas opciones que puedes usar para construir tu propia billetera hardware. Pero antes de hablar de las opciones que tienes para construir tu propia billetera hardware, es importante mencionar los motivos por los cuales deberias ir por esta vía.

¿Por Qué DIY Es Mejor?

Primero que nada, si vives en un pais donde no haya distribucion de Trezor, Ledger or BitBox02, construir tu propio equipo es ciertamente la manera mas economica. Segundo, si tu gobierno es hostil hacia Bitcoin y hacia todo lo que se relacione con él, es sumamente recomendable usar algunas de las mismas piezas que también sirven para armar un Tetris portatil, para proteger tu preciado oro digital.



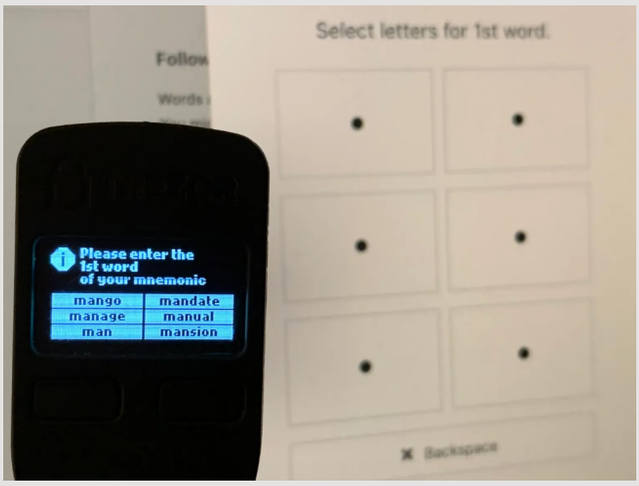


Inclusive si vives en un pais donde la distribucion de una billetera hardware comercial es posible, ir por la vía DIY sigue siendo una alternativa para considerar. Si estas preocupado por la privacidad (y deberias estarlo), no deberias darle tu nombre y direccion a un vendedor y a una compañía de entregas las cuales almacenarán tus datos por varios años – el caso del hackeo de la base de datos de Ledger es un muy buen ejemplo de porqué la privacidad y el hardware DIY son importantes.



Adicionalmente, los ataques a la cadena de suministro son reales: no sabes quien va a tocar tu billetera hardware desde el momento que sale de la fábrica hasta que finalmente te es entregada. Si alguien sabe lo que es un Trezor, puede comprometer su hardware o su empaquetado (un ataque muy popular consiste en insertar una frase seed BIP 39 previamente generada, a la espera de que un novato deposite sus monedas en direcciones controladas por el actor malevolo). Por supuesto, estas compañías hacen grandes esfuerzos para prevenir dichos ataques dividiendo su empaquetado e introduciendo trucos criptograficos para verificar la integridad del hardware y el software. Pero si sabes lo que haces, DIY es definitivamente más

seguro: usando hardware listo para su uso general, y software open source que puedes verificar tu mismo es definitivamente la manera de abordarlo para un usuario calificado.



Billeteras Hardware Que Puedes Construir Tu Mismo

Hablemos ahora de las billeteras hardware que puedes construir tú mismo. Basicamente, existen dos categorías: los dispositivos comerciales con circuitos y esquemas han sido hechos open source (Trezor, BitBox02) y los proyectos sin fines de lucro de comunidades que fueron creadas específicamente para trabajo DIY. Los Trezors y el BitBox02 vienen con la ventaja de un código y una arquitectura más testeados y examinados ya que son vendidos comercialmente. Los equipos detras de los proyectos pueden pagar premios y auditorías de seguridad, pero también es mayor el incentivo para los hackers de romperlos.

Por otro lado, proyectos DIY como SeedSigner, Specter DIY y Bowser ofrecen una capa adicional de conveniencia, ya que pueden ser construidos con partes muy comunes y casi no requieren soldaduras ni experiencia electronica. No son tan testeadas como las alternativas comerciales y no deberias esperar demasiado apoyo en el proceso. Aun así, tienen ventajas propias y proporcionan a cualquiera la oportunidad de ser financieramente soberano.

En este primer artículo, vamos a analizar qué se requiere para armar tu propio Trezor y/o BitBox02. Naturalmente, el seguimiento se enfocará en el SeedSigner, el Specter DIY, y la billetera Browser.

Construyendo Tu Propio Trezor One

Durante la campaña Kickstarter de 2014 que dio lugar a la primer billetera hardware de Bitcoin, los cofundadores de Trezor Marek “Slush” Palatinus y Pavol “Stick” Rusnak presentaron su intencion de crear un dispositivo que pudiese satisfacer las necesidades del creador de Bitcoin, Satoshi Nakamoto. Esto significa que el software y los circuitos son transparentes y 100% open source, para que cualquiera pueda ver que está haciendo el dispositivo en cualquier momento.

El repositorio de la compañía Checa en Github ofrece completamente la placa, el esquema, y el bill of materials (BOM). Segun estos documentos, necesitas 24 partes, siendo la más importante el monitor OLED, el microcontrolador STM32F10XRXT6, los botones, la carcasa, el interruptor tactil, y el puerto micro



USB. El costo de todo no deberia superar los $20, aunque también necesitas un soldador y la destreza para armarlo todo tú mismo.

Entonces a pesar de que el costo de construir una billetera hardware Trezor One es bajo, la parte del ensamblado puede ser dificil e intimidatoria para un nuevo usuario. Pero si necesitas construir tú mismo la billetera hardware más testeada del mundo, tendras que desarrollar algunas destrezas prácticas. Despues de todo, no es una sorpresa que el Trezor One sea el dispositivo más copiado del mundo y que hay cientos de compañías alrededor del mundo que la venden bajo distintas marcas. De hecho, dispositivos más nuevos como el BitBox02, el Coldcard y el Foundation Devices Passport usan partes significativas del código de Trezor y en cierta manera podrian llamarse “clones”.

Apenas terminas de armar tu Trezor One hecho a medida, puedes flashear el firmware segun las instrucciones del repositorio de Github. Cuando terminas, tu nueva billetera hardware DIY funcionara perfectamente con la billetera Wasabi – y elegir Wasabi en lugar de Trezor Suite te brindara algunos beneficios de privacidad con respecto a la conectividad a un nodo full y a la necesidad de no tener que confiar durante el proceso de induccion.

Para mayor informacion sobre el ethos open source y su compromiso, escucha esta entrevista al CEO Marek “Slush” Palatinus en el Bitcoin Takeover Podcast.

Construyendo Tu Propio Trezor Model T:

Lanzada en el otoño de 2017, la billetera hardware Trezor de segunda generacion presenta mejoras altamente utiles. Remplaza el esquema de dos botones con una pantalla tactil de color que es mas facil de usar, y tambien viene con un procesador mas rapido que permite backups mas complejos tales como Shamir Secret Sharing. El dispositivo también es más confiable para manejar setups de multisig más complejos, tal como demuestra la evaluacion comparativa de Jameson Lopp.

Sin embargo, el Model T de Trezor también viene con mayor complejidad electronica: el bill of materials lista 109 partes, al mismo tiempo que los esquemas son más elaborados y sofisticados. Esto significa que el Model T es un proyecto DIY más dificultoso y demandante que su antecesor. Para compensar esto, las instrucciones de armado también son más detalladas e incluyen graficos para guiarte paso a paso.

En terminos de seguridad, el Model T viene con la ventaja de permitirte tipear



tu frase de seguridad directamente desde el dispositivo – lo cual es un gran atributo para tener, especialmente cuando crees que el teclado de tu computadora podria estar comprometido o logged. Entonces por más que no te importe mucho la seguridad de multisig o los backups Shamir, sigue valiendo la pena considerar al Model T por su mejora en el input.

El chip que potencia al Trezor Model T es el microcontrolador STM32F427VIT6 – una unidad Cortex M4 que presenta 2 megabytes de memoria flash y está registrada a 168 Mhz. Puedes conseguirlo por unos $20, pero definitivamente encontrarás mejores ofertas si compras en

cantidad. La pantalla también cuesta unos $5, y las restantes piezas otros $20 (desde la carcasa hasta los puertos USB-C y SD, y hasta llegar a los varios conectores). Pero antes de juzgar a Trezor por vender el dispositivo a un precio que excede holgadamente los costos de produccion, no debemos olvidarnos que el dispositivo requiere para su armado una considerable destreza para soldar (mayor a la necesaria para el Trezor One), que la compañía está mayormente enfocada en mejorar los estándares de seguridad del software (así que pagas por la investigación y desarrollo de los SLIPs, y también existen los costos de ofrecer servicio al cliente.

Para un habilidoso aficionado de DIY, el Trezor Model T puede ser un proyecto de fin de semana divertido. El hecho de que las partes son de uso general y fáciles de encontrar en la web deberia proveer un alto grado de negacion plausible en estados autoritarios, y las prestaciones adicionales hacen que valga la pena el esfuerzo adicional (en comparación con el más simple Trezor One).

Igual que con el Trezor One, puedes usar tu recientemente armado Model T con la billetera Wasabi. Ten en cuenta, sin embargo, que Wasabi no funcionara con armados multisig ni con ShamirSecret Sharing. Solo los armados BIP39.

Construyendo Tu Propio BitBox02

Lanzado en el otoño de 2019, el BitBox02 es un spin del diseño original de Trezor que presenta algunas notables modificaciones del hardware y software. A pesar de que se inició del mismo código, es lo suficientemente diferente como para merecer atencion. Filosoficamente hablando, el dispositivo busca ofrecer un balance entre la auditabilidad open source y la seguridad fisica lo cual la hace el punto intermedio entre Trezor (100% open source) y Ledger (alrededor de 40% open source, con una seguridad de chip opaca).

La parte que hace que el BitBox02 sea menos open source que el Trezor pero más físicamente segura es la inclusion del chip de seguridad de uso general ATTEC608B. Esto significa que puedes proteger tu dispositivo del acceso fisico de un actor malevolo sin la necesidad de usar una frase de seguridad del software (lo cual puedes olvidar o perder si no eres lo suficientemente cuidadoso). Así que si quieres llevar tu seguridad fisica al proximo nivel, deberias considerar armarte un BitBox02.

Ademas de la seguridad del chip, la billetera hardware de segunda generacion de ShiftCrypto ofrece algunas opciones



interesantes: el dispositivo usa un conector USB-C macho el cual lo hace fácil de conectar a tu telefono movil (no se requiere cable siempre y cuando tengas el puerto correcto en tu computadora o telefono), y la pantalla tactil es reemplazada por sensores tactiles en la parte superior e inferior de la billetera hardware.

En terminos de software, el BitBox02 utiliza firmas Schnorr para verificar la integridad del software y prevenir ataques en la cadena de suministro. Este sistema se denomina anti-klepto y, a pesar de que no parezca muy relevante para quien arma sus propias billeteras hardware, sigue siendo una gran herramienta de autoverificacion la cual previene la intromision externa del código. Aprende más de este mecanismo de seguridad en esta entrevista con el desarrollador de software e investigador de ShiftCrypto Benma.

Para ayudarte a construir tu propio BitBox02, ShiftCrypto ha publicado un bill of materials (el cual deberia ser actualizado para incluir el chip ATECC608B el cual remplazo al 608A en 2021), una extensa datasheet, el esquema de placa de circuitos, y hasta la X-ray picture que deberia ayudarte a entender cómo conectar cada parte de la placa. La guía no es tan detallada como la de las billeteras hardware Trezor, pero cualquier aficionado experimentado deberia poder entenderla.

Ahora hablemos de los costos: en cantidades, el chip de seguridad ECC608B puede ser adquirido por $1. Pero debido a los problemas de suministro de la industria de microchips, parecen actualmente estar sin stock en algunos de los más populares sitios web minoristas (y muy probablemente se vendera con un recargo debido a su escasez). Al mismo tiempo, el chip microcontroladopr de 32 bits ARM Cortx M4F ATSAMD51J20A cuesta aproximadamente $6 y también parece dificil de encontrar. Los diodos de supresion PRTR5V0U2F y todas las otras partes pequeñas también suman otros $3 al costo de produccion. En total, comprar las partes requeridas para el armado de tu propio BitBox02 deberia costarte alrededor de $20 (incluyendo el puerto USB-C, el slot para la tarjeta micro-SD, los sensores tactiles y la pantalla OLED).

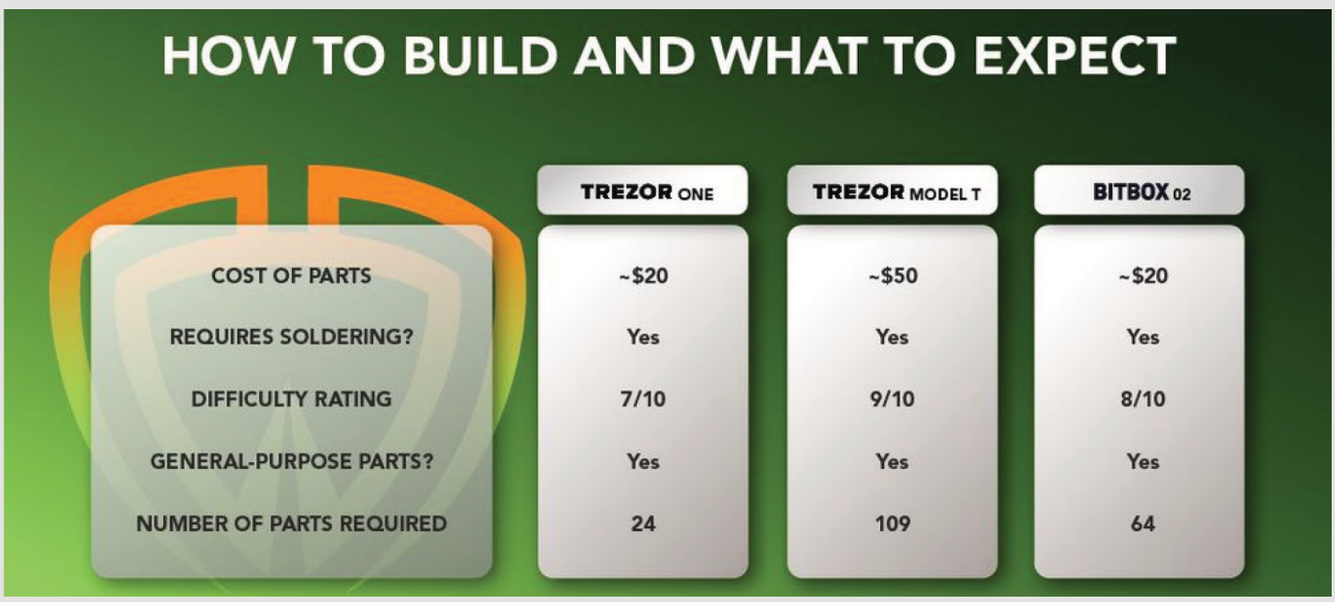
El BitBox02 tiene más partes que el Trezor One, pero menos que el Trezor model T. También posee partes más accesibles que el modelo de cabecera de Trezor y ofrece algo de seguridad fisica, Asi que si encuentras deseables estas caracteristicas, deberias tomar tu soldador y comenzar a ordenar las partes mientras todavia están en stock.

Y si, el BitBox02 funcionara con la billetera Wasabi. Pero al igual que los dispositivos de Trezor, deberas conectarte al software nativo (en este caso BitBoxApp) para actualizar el firmware.

Debe Ser Tan Dificil Construir Tu Propia Billetera Hardware?

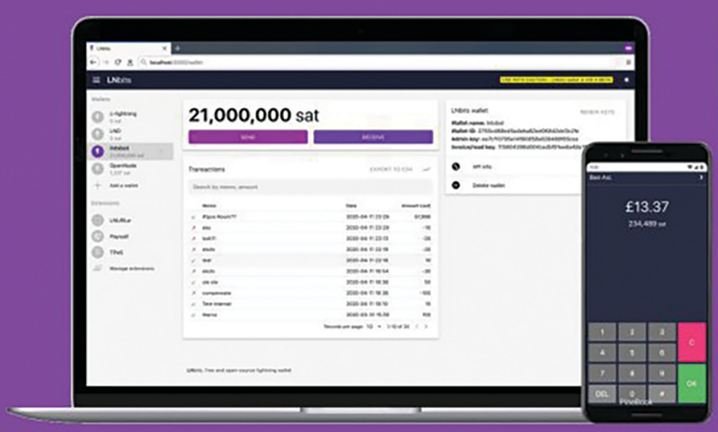
Pues no. En la actualidad tenemos los dispositivos SeedSigner, Specter DIY, y Bowser y son mucho más accesibles para los aficionados que no quieran soldar diodos a un PCB y estar consultando esquemas complejos. Sin embargo, no son tan testeados como los son los dispositivos comerciales, así que siempre hay concesiones. Encuentra mayor informacion de cómo construir estas billeteras hardware y los costos en el siguiente artículo!

–

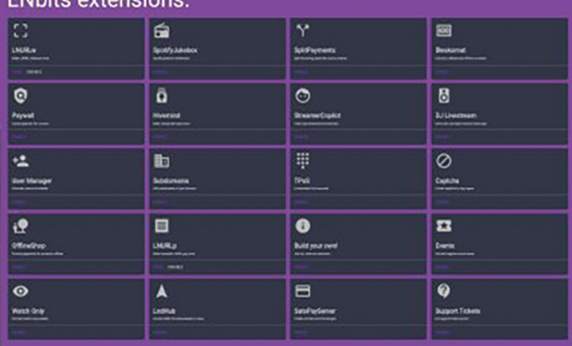


LNbits

Cuentas bitcoin open-source gratuitas y sistema de extensión.
Correlo para ti, amigos y familia o para el mundo entero!



LNbits extensions:



Sats gratuidos!
(Scan with a bitcoin lightning wallet)

Coinflip!
(Scan with a bitcoin lightning wallet)

LNbits puede ser usado como:

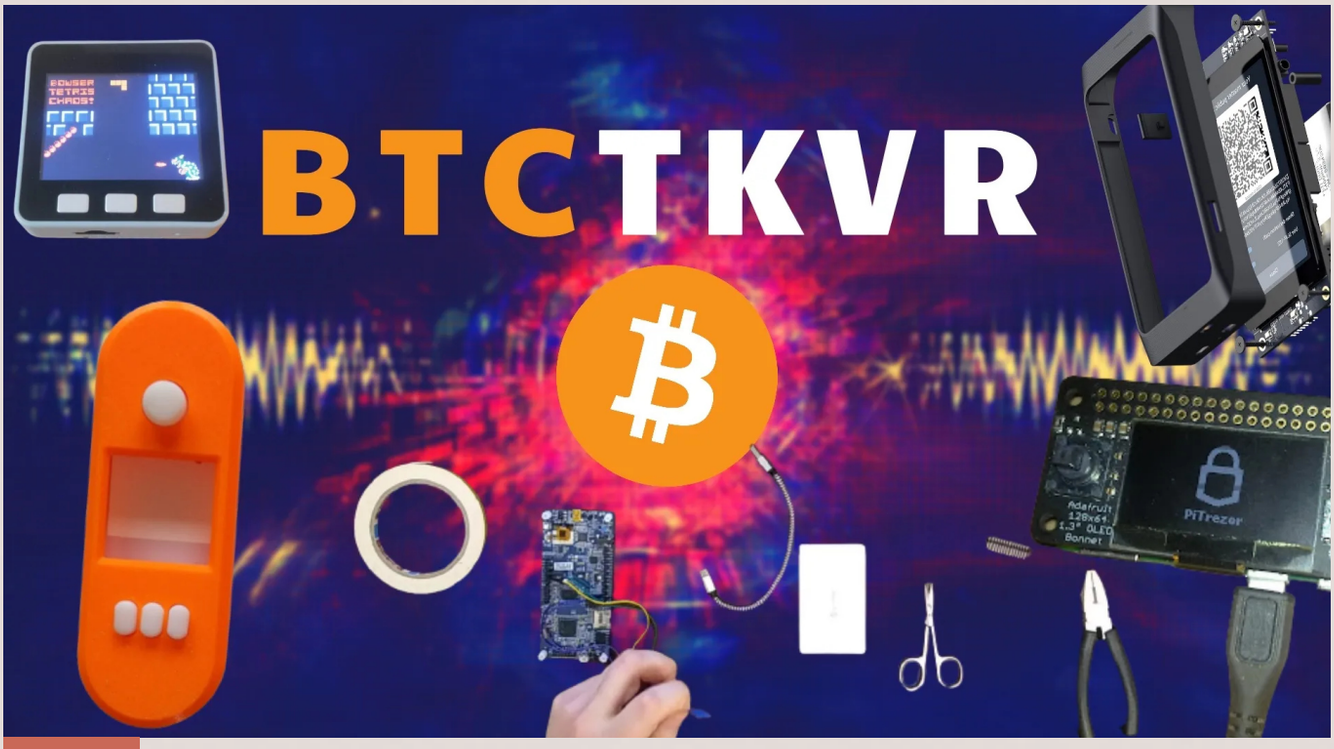
- Solución de banca/custodia comunitaria
- Sistema contable, cada billetera con sus propias claves API
- Plataforma extendible usando el esquema de extensión simple de LNbits
- Parte de un stack de desarrollo para un servicio de bitcoin
- Billetera lightning con tu marca propia
- Un sistema insta-wallet

LNbits puede correr en:

RASPI BLITZ Clightning LND
LNPay.co LNTXbot myNode
opennode spark Umbrel

Unete
a nosotros!

https://github.com/lnbits



Billeteras Hardware DIY, Parte II: Construyendo Tu Propia Billetera PiTrezor, Specter DIY, SeedSigner Y Bowser

Existen dos categorías importantes de billeteras hardware DIY que puedes construir con dispositivos electronicos de uso general: las que corren firmware portera (un grupo de desarrolladores hacen disponible un software bien testeado en un hardware más comun), y los que corren código original.

Ambas son razonablemente fáciles de construir y tienen muy pocas partes que debes ensamblar. Pero desde el comienzo, debes entender las concesiones mutuas: un proyecto como PiTrezor podria ser un puerto conveniente que te permite correr el software de billetera de hardware más testeado en un Raspberry Pi, pero no quiere decir que el puerto en sí está examinado por profesionales de seguridad o actualizado para tener las más recientes actualizaciones de Trezor. En cambio, un proyecto como SeedSigner o Specter DIY puede ser original y open source, pero esto tampoco quiere decir que muchos expertos han verificado el código.

Estos son los motivos por los cuales la recomendación de estos dispositivos que puedes construir tú mismo es chequear el código o pagarle a un profesional para que lo haga por ti. Si vas a usar billeteras hardware DIY para proteger grandes cantidades de bitcoin, entonces es mejor tomar la parte multisig. Si cada dispositivo no es más que una clave para tus monedas y no hay ningun punto unico de falla que pueda hacerte perder tus fondos, entonces es generalmente más seguro usar algo con un más alto perfil de riesgo.

En este momento, deberiamos hacer dos preguntas muy importantes: primero que nada, porque siquiera construir una billetera hardware DIY si la seguridad es cuestionable? Y, algunos de los dos mejores argumentos incluyen tu habilidad de sobrevivir autoritarismo

politico, y la evasion de los ataques de la cadena de suministro. Algo que construyes tú mismo con partes comunes te ayudará a mantener tu privacidad y negacion plausible en relacion a tu gobierno – y la compañía de entregas tampoco sabrá en qué andas.

La otra pregunta importante que deberiamos preguntar a esta altura es: ¿funcionará tu billetera hardware DIY con Wasabi? La respuesta depende del modelo de billetera hardware. Algo como el PiTrezor deberia funcionar ya que es esencialmente el firmware de Trezor en un sistema distinto más accesible. Specter DIY y Bowser también deberian funcionar ya que usan estándares incluidos en las especificaciones de HWI y PSBT. En el caso del SeedSigner, armados de firma unica todavia estan en camino a desarrollarse; por lo tanto, la compatibilidad con Wasabi debera esperar un poco.

Nuevamente, estas billeteras hardware DIY open source todavia están en una fase temprana de desarrollo y son mayormente recomendadas para armados multisig. No tomes riesgos peligrosos con tus bitcoins. Si eres un aficionado de las billeteras hardware o un individuo que está buscando soberanía financiera en un entorno autoritario, considera crear armados más elaborados que no dependan demasiado en un unico dispositivo – inclusive si esto significa que vas a hacer un backup Shamir o un armado multisig que no sea compatible con el software de Wasabi.

Luego de haber presentado las advertencias, echemos una mirada a las cuatro billeteras hardware DIYpara determinar los costos, la dificultad, y la complejidad de la tarea.

Construyendo Tu Propio PiTrezor

Una regla de oro en seguridad es seguir el rumbo más testeado. De esta manera, sabes más de la experiencia de otros y obtienes un mejor entendimiento de todas las concesiones mutuas que existen. Y dado que Trezor existe desde 2014 y el código ha estado bajo constante escrutinio desde su comienzo, es bastante seguro asumir que el firmware funciona bien y que ha sido constantemente robustecida con informacion detallada.

PiTrezor es un puerto del código original, lo cual hace que el firmware STM32F10XRXT6 optimizado corra en el más comun y popular Raspberry Pi Zero. Puedes comprar Pi para virtualmente cualquier cosa, desde emulacion de videojuegos hasta experimentacion IoT, robotica y relays de Tor. También, el Raspberry Pi Zero solo cuesta $5 y está entre las más accesibles micro-computadoras en terminos de precio y de la posibilidad de encontrar una en cada esquina del mundo. Comparado con el microcontrolador base de Trezor, el Pi Zero es mucho más popular y mucho más fácil de conseguir accesorios compatibles.

Adicionalmente, el puerto de PiTrezor también funciona con el raspberry Pi4 – el dispositivo más poderoso que es mayormente usado por operadores individuales de nodos de Bitcoin. Una ventaja importante de estos dispositivos es que vienen con puertos USB completos, lo cual te permite conectar tu teclado para usar de input. Esto significa que no debes preocuparte por encontrar botones que encajen en algun tipo de espacio limitado, ya que tienes la opcion de operar tu PiTrezor con un periferico que ya tienes.



Por lo tanto, el proceso es mucho más fácil y no requiere la soldadura de partes si corres tu PiTrezor en un Raspberry Pi 4. Sin embargo, los costos son unos $30 más altos. Para ver la guía completa dirigete al sitio web de PiTrezor.

Ahora hablemos de partes y costos. Existen dos versiones del Raspberry Pi Zero, y deberias comprar la más economica que no tiene bluetooth ni WiFi. No solo porque estos puertos son innecesarios, sino también porque pueden representar un vector de ataque adicional que podria quebrar al equipo o extraer informacion. A pesar de que el mantenedor de PiTrezor sugiere que el Zero W es igual de segura porque el firmware no tiene drivers cargados para los puertos de comunicacion, un hacker competente aun puede vulnerarlas si obtiene acceso fisico. En conclusion, por tu seguridad y por el ahorro de dinero, es mejor comprar el PiZero basico por $5.

Otras partes incluyen una tarjeta SD de más de 100 MB (basicamente cualquiera de las que consigues hoy en dia por un par de dólares), un cable micro-USB a USB (alrededor de $1), un cable mini HDMI que se conecta al monitor, TV o pantalla exclusiva (cuesta unos $3 asumiendo que ya tienes un monitor o TV), dos botones push que son compatibles con el Raspberry Pi (unos $2 y solo los necesitas para la configuracion del Pi Zero, ya que el Pi 4 puede usar tu teclado USB) y algunos cables para soldar los botones a la placa (alrededor de $1). Las partes opcionales incluyen una pantalla exclusiva que es util por razones de portabilidad, y una cobertura para proteger la placa y los circuitos del polvo, el daño fisico y otros factores.

Asumiendo que pagas $5 por el Raspberry Pi Zero y 9-10 dólares por las partes adicionales, concluimos que construir la más basica (pero electronicamente demandante) version del Pi Trezor te costara unos $15. Ten en cuenta que la pantalla, la cobertura, la soldadora, y el envío de todas estas partes no están siendo tenidas en cuenta y facilmente podrian duplicar los costos.

Si vas por la opcion del Raspberry Pi 4, solo necesitarás el dispositivo de $35 (escoge el modelo basico de 2 GB, no necesitaras mucha memoria para un Trezor), la tarjeta SD de 2 dólares y los cables micro-USB a USB y mini-HDMI a HDMI hembra. Estos deberian costar unos 6 dólares. Y mientras que el costo aproximado total de $41 puede parecer algo caro, por lo menos no tendras que soldar ningun cable y no requiere ningun equipo especial para dicha tarea. Flasheas el firmware en la tarjeta SD, enchufas el Raspberry Pi a la pared, conectas el puerto de video externo a tu monitor o pantalla de TV compatible con HDMI (cualquiera de no más de 10 años la tiene), y usas tu teclado USB de input. Es bastante geek, pero alguien viviendo en un lugar donde la billeteras hardware Trezor no tengan distribucion oficial va a realmente disfrutar el poder de la soberanía DIY.

Antes de continuar a la proxima seccion, aqui va otro recordatorio de que mientras que el código del PiTrezor es open source y basicamente un puerto del lanzamiento oficial de Trezor, deberias ser cauteloso y no poner demasiadas monedas en este dispositivo sin antes cuidadosamente verificar el código. La manera más segura de usar un PiTrezor es hacer de él uno de tus dispositivos multisig, para



que no haya un punto unico de falla. Pero siempre debes ser cauteloso como dijo el CEO de Trezor Marek “Slush” Palatinus en el episodio 8 de la temporada 4 del podcast Bitcoin Takeover, existen unos 40 clones de Trezor en el mundo y su código modificado no siempre atraviesa el escrutinio que deberia.

Construyendo Tu Propio Specter DIY

El creador de Specter Stepan Snigirev ha generado una total revolucion DIY en el espacio de las billeteras hardware. Gracias a sus proyectos micro-bitcoin y micro-arduino, dispositivos de baja potencia son ahora capaces de correr una version de poco peso del cliente de Bitcoin. Lo más notable es que ha creado una billetera hardware que puede ser construida usando partes comunes que corre código no de Trezor. Mientras cada dispositivo electronico comercial para el manejo seguro de claves, desde KeepKey a Coldcard y Foundation Devices Passport hacen uso del firmware open source de Trezor en algun grado, el Specter DIY se atreve a ser diferente.

Para construir tu propio Specter DIY, solo necesitas una placa de desarrollador STM32F469I-DISCO que puedes comprar por unos $62, Asi como tambien un cable mini USB de $1 y uno micro USB de $1 (que probablemente ya los tengas de algun telefono o de otra wallet hardware). El dispositivo en sí tiene todo lo que necesitas, desde la pantalla tactil hasta la memoria flash que usas para instalar el firmware de Specter. Así que es una solucion todo en uno, que como máximo, solo recesitaras una carcasa para protegerlo del polvo.

Hoy por hoy, muchos potentes usuarios de Bitcooin construyen su propia billetera hardware DIY Specter para prevenir ataques en la cadena de sumisistro. Pero como el código no fue tan testeado como el de Trezor y podria tener vulnerabilidades que no han sido desbubiertas dada la falta de incentivos (el Specter DIY todavia es un producto de nicho dificil de encontrar y la recompensa por romper el código no se asemeja a la de Trezor), lo mejor es usar este dispositivo para multisig. Esto es exactamente lo que los desarrolladores de Specter recomiendan: ven su proyecto DIY como un complemento a otras billeteras hardware. Puedes usarlo como un dispositivo de firma unica, pero el caso de uso en el que brilla es multisig.

Una recomendación para el Specter DIY es que también compres un modulo adicional de lectura de código de barra el cual cuesta $40. Hará que tu dispositivo sea más utilizable de una manera en la cual nunca la conectas a internet, ya que puedes escanear codigos QR y confirmar transacciones sin conectar tu dispositivo a una computadora. Adicionalmente, puedes darle autonomia al Specter DIY con una batería. Las instrucciones de armado completas están disponibles en el repositorio de GitHub del proyecto. También puedes encontrar un video instructivo en YouTube.



En total, armar el Specter DIY deberia costar entre 64 y 120 dólares. Y si también quieres una carcasa, puedes o imprimirla en 3D segun las especificaciones o comprarsela a un profesional como Richard de la República Checa (no es un endoso directo, pero yo le compre las mias a el). Esto hace parecer que el Specter es un dispositivo caro, pero si lo compras ya armado te costará 350 euros (414 dólares) el armado completo con todos sus atributos, y 60 euros (71 dólares) para también obtener adjunta la placa STM32F-469I-DISCO.

Por eso es definitivamente mejor pagar 150 dólares por un dispositivo con todos los atributos que construyes tú mismo con partes que compras de distintos lugares que gastar $485 por un Specter Shield.



Para entender mejor el alcance y el proposito del proyecto Specter DIY, escucha a Stepan Snigirev dar todas las explicaciones en el episodio 11 de la temporada 8 del podcast Bitcoin Takeover.

Construyendo Tu Propio SeedSigner

El SeedSigner es una bifurcacion simplificada del Specter DIY, el cual reemplaza la experiencia de la placa de la pantalla tactil con la poderosa accesibilidad del Raspberry Pi Zero. Su objetivo principal es ofrecer un dispositivo poderoso que cualquiera pueda construir por aproximadamente $50.

A diferencia del Specter DIY, el SeedSigner está actualmente solo optimizado para la generacion de xpub multisig y hace uso de una presentacion más tradicional con botones fisicos. La principal desventaja de este diseño es que se requiere algo de soldadura para armar el dispositivo. Pero cómo se apoya en la arquitectura del popular Raspberry Pi, uno puede facilmente comprar encabezados de martillo GPIO (que cuestan $7) para evitar esta molestia.

Para armar el SeedSigner, necesitas una computadora Raspberry Pi Zero (de nuevo, se recomienda la version basica de $5 sin WiFi ni bluetooth), una pantalla LCD cuadrada de 1.3 pulgadas con resolucion de 240X240 pixels (que cuesta alrededor de $14) y una cámara compatible con el sistema PiZero (el modelo recomendado es el AuviPal 5MP 1080p, el cual actualmente esta sin stock pero deberia costar unos $20).

El desarrollador principal de SeedSigner ha tambien hecho open source las especificaciones de la carcasa, así que cualquiera con una impresora 3D puede crear la suya. Esto es mala noticia para aquellos que no tengan acceso a una impresora 3D, especialmente dado que el input requiere botones fisicos que vienen





con la carcasa. Sin embargo, hay comerciantes y aficionados (de nuevo, como Richard de la República Checa) quienes imprimen carcasas por unos $20.

Así que mientras la piezas electronicas para construir el SeedSigner cuestan alrededor de $39 (por debajo del objetivo de $50), deberas gastar un poco más para tener la experiencia completa. Así y todo,

Construyendo Tu Propia Billetera Bowser

Creada por Ben Arc, la billetera Bowser es una bifurcacion del Specter DIY aún más simplificada. Todo lo que tienes que hacer para construir esta billetera hardware es comprar un M5Stack ESP32 Basic Core de $40 e instalar el firmware con una tarjeta micro-SD.

Esto significa que la billetera Bowser es lejos la billetera hardware DIY más accesible y fácil de configurar. Hasta recibes una guía paso a paso en YouTube la cual te ayuda en el proceso. Sin embargo, hay un par de peculiaridades

armar el SeedSigner es más económico que el Specter DIY del cual toma prestado su código.

Hablando del código, una vez que armes el hardware necesitarás una tarjeta SD y también deberias tipear algunos comandos en un teclado externo. La guia completa lo hace simple de seguir, así que si no entiendes lo que estás haciendo podras setear tu SeedSigner exitosamente.

También debes tener presente que el SeedSigner es un dispositivo sin conexion a internet optimizado para trabajar con billeteras aptas para multisig tales como Specter Desktop, Sparrow, y BlueWallet. Así que no podras acceder a ella desde la billetera Wasabi hasta que se agregue el soporte de firma unica para los seteos PSBT. Por el momento, todavia es un proyecto DIY geek que usuarios casuales no encontrarán muy simpatico y accesible. Pero gracias a las contribuciones de la comunidad, está mejorando rapidamente.

Para entender mejor la filosofia detrás de SeedSigner, escucha el episodio 10 de la temporada 8 del podcast Bitcoin Takeover. Si durante la tarea necesitas ayuda, puedes usar esta guía de armado completa en YouTube.



de geek que debes considerar: primero que nada, la billetera hardware también funciona como sistema de videojuegos que corre una version estilizada de Tetris, Esto es bueno para la negacion plausible, ya que nadie sospechara que este dispositivo de apariencia genérica que tienes en tus manos también es un dispositivo de Bitcoin – lo cual es muy util para aquellos que buscan maximizar

BOWSER WALLET

su privacidad en lugares que pueden ser hostiles a la idea de la soberanía financiera.

Segundo, la billetera Bowser hace uso del código Morse como input. Esta es lejos la caracteristica más geek de todas las billeteras hardware, ya que tienes que, o llevar una hoja de papel que te indique como tipear cada letra del alfabeto, o memorizar el código. De nuevo, como la mayoria de la gente no tiene idea de como funciona el código Morse (y hasta lo pueden confundir con Braille) esto es excelente para la privacidad. Pero este atributo en efecto hace que el dispositivo sea más dificil de usar hasta para los dueños de la billetera hardware, así que de acuerdo a tu modelo de amenaza deberias evaluar hasta qué punto necesitas esta complejidad adicional.

La billetera hardware Bowser es un dispositivo bastante cypherpunk ya que combina la privacidad de los videojuegos con la conveniencia de usar una computadora compacta de uso general. Puedes deshacerte de la unidad en cualquier momento y obtener una nueva – solo asegúrate de tener tu backup en un lugar seguro.

Actualmente, Bowser está diseñada para trabajar con la billetera Electrum y hace uso del estandar PSBT para firmar transacciones. Esto significa que también deberia funcionar con la billetera Wasabi, siempre y cuando uses las opciones asociadas con la billetera Coldcard.



Para mayor informacion y para tener un mejor entendimiento de la billetera Bowser, escucha a Ben Arc en el episodio 9 de la temporada 8 del podcast Bitcoin Takeover.

–

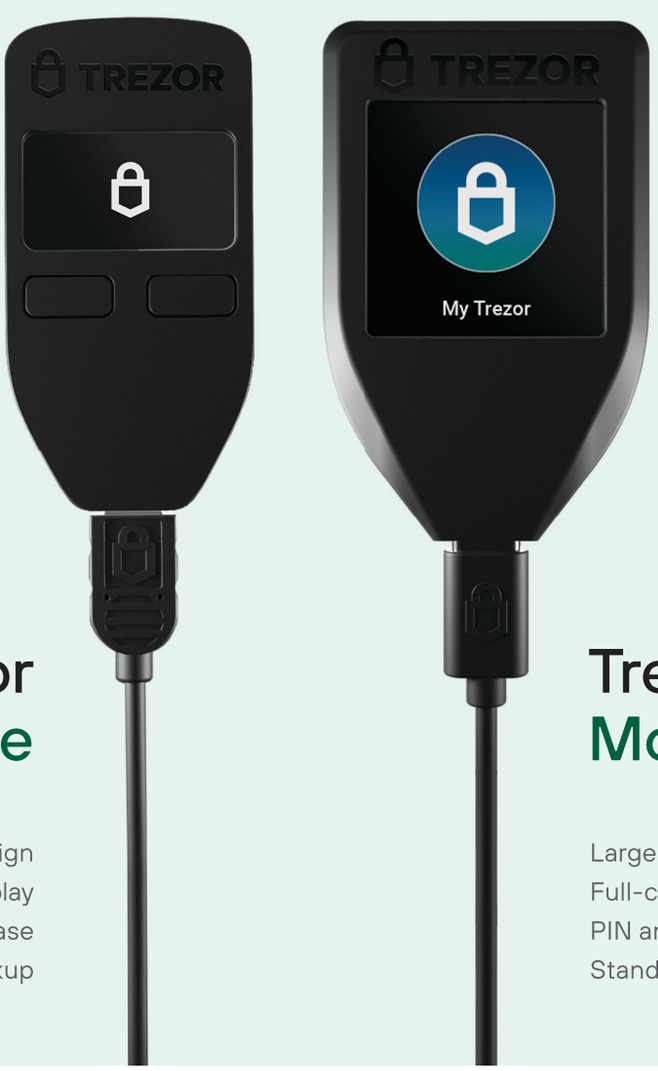
HOW TO BUILD AND WHAT TO EXPECT

	PI TREZOR	SPECTER	SEED SIGNER	BOWSER
COST OF PARTS	$15-$30 RPi Zero / $41-$60 RPi 4	$65-$150	~$60	~$40
REQUIRES SOLDERING?	Yes RPi ZERO / No RPi 4	No	Depends on setup	No
DIFFICULTY RATING	5/10 for RPi Zero 3/10 for RPi 4	2/10	4/10	1/10
GENERAL-PURPOSE PARTS?	Yes	Yes	Yes	Yes
NUMBER OF PARTS REQUIRED	6-8 for RPi Zero 4 for RPi 4	For the most basic build, but you can add a battery, QR scanner, smart card reader and a case.	4	1 (plus SD card)

TREZOR

Putting control in your hands.

Take control of your Bitcoin with a Trezor hardware wallet.
Boost your privacy and manage coins securely, with the integrity and independence of open-source design.



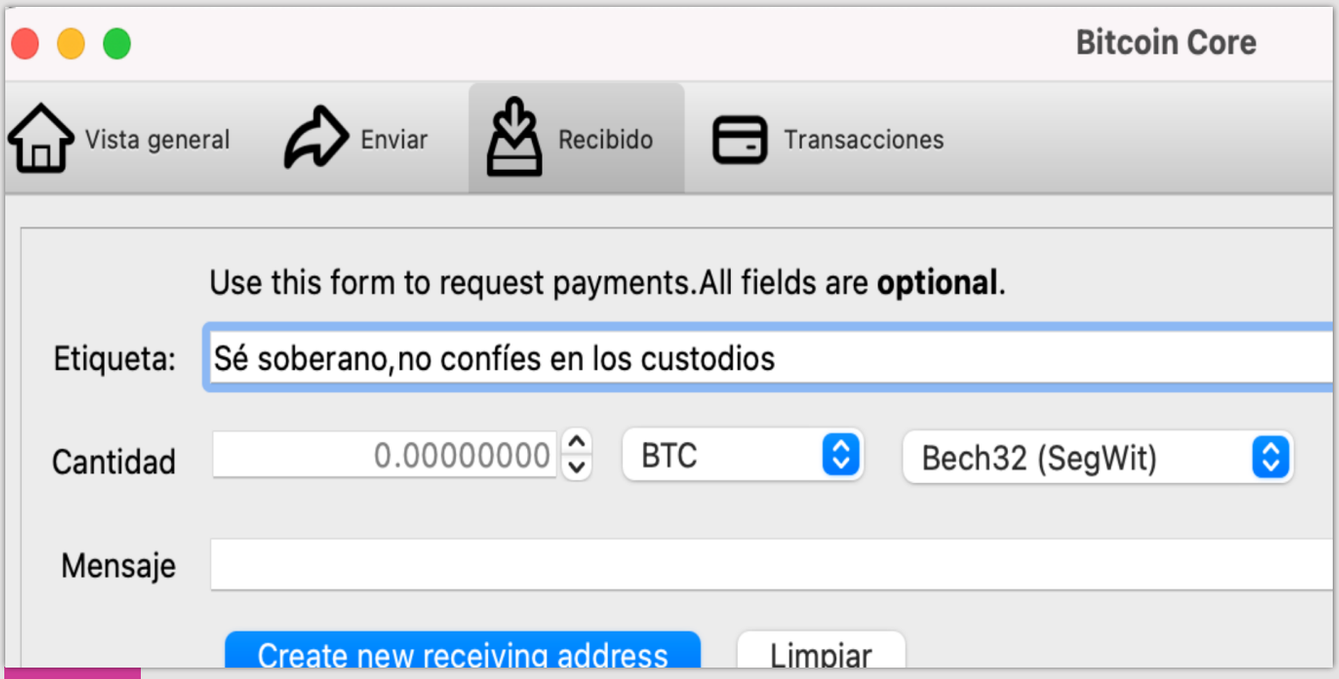
Trezor Model One

Simple durable design
Monochrome trusted display
PIN and Passphrase
Standard backup

Trezor Model T

Large comfortable touchscreen
Full-color trusted display
PIN and Passphrase
Standard or Shamir backup

Find out more at **trezor.io**



¿No Puedes Retirar A Tu Billetera Propia? No Es Tu Bitcoin

Hoy en día, bitcoin se ha convertido en un activo de moda al cual las instituciones financieras tradicionales dan acceso a sus clientes. A julio 22 de 2022, bloque 746060, tenemos compañías como Robinhood, PayPal, Revolut, y hasta bancos que permiten a sus clientes comprar bitcoins. Y segun noticias recientes "cientos de bancos estadounidenses" están proximos a agregar servicios de custodia de bitcoin.

Muchos podrian argumentar que esto es muy bueno para la adopcion de BTC, ya que servicios financieros que la gente ha venido usando durante años permiten ahora la compra y venta de dinero sólido. Pero el argumento que voy a presentar en este artículo, más alla del mantra "no son tus claves, no son tus bitcoins", es que no hay forma de probar que la institucion financiera realmente sea dueña de los bitcoins que compras.

En el caso de fiat, siempre puedes retirar el dinero de tu cuenta. Vas a un cajero automatico, introduces tu tarjeta y digitas tu código, y luego seleccionas el monto que quieras extraer. Pero incluso en este escenario en el que puedes retirar tu dinero, no significa que el resto pueda. Todos los bancos actuales usan reservas fraccionarias – así que en cualquier momento determinado, existe solo suficiente dinero para afrontar los retiros de un cierto número de clientes. Si depositas mucho dinero, es probable que la extraccion sea lenta y engorrosa.

Pero independientemente de tu situación financiera, estás legalmente habilitado a retirar tu dinero y usarlo para cualquier proposito que consideres necesario.

Teoricamente, Bitcoin deberia resolver todas estas cuestiones al ofrecer un sistema más transparente. Sabes que el dinero es tuyo porque lo verificas con un nodo full. Y cuando quieres gastar tus UTXOs, no necesitas permiso de nadie para hacerlo. Eres tu propio banco y el objetivo es que sea una parte integral de tu soberanía financiera.

Desafortunadamente, se torna feo cuando se involucran terceras partes del sistema de finanzas tradicional. No solo están acostumbrados a la banca de reservas fraccionarias, pero no existe autoridad para imponerles que tengan reservas de bitcoin para todas las unidades que están vendiendo. Podria llevar a la paradoja de la inflacion artificial que previamente describi en mi artículo sobre los ETFs: la gente compra y vende bitcoins que no pueden ser verificados en el registro público, y para los cuales ni siquiera existe prueba de que existan. ¿Que previene que estas compañías efectivamente inflen el circulante de bitcoin a traves de una venta legal e institucional de activos sin respaldo?

Es poco probable que jamás exista una auditoría de las reservas de bitcoin y una verificacion de las cuentas de los usuarios. Y aunque la haya, estas compañías pueden operar sin efectivamente comprar una cantidad correspondiente de BTC cuando un cliente convierte moneda fiat a bitcoin en su plataforma.

Así que si tienes bitcoins en PayPal, Revolut, Robinhood, o cualquier otro servicio financiero que no te permita retirar, por el bien de tu soberanía financiera, deberias vender tus monedas por fiat y transferir el dinero a un exchange que te permita retirar tu verificablemente verdadero BTC. Siempre y cuando pagues el mismo precio que el resto, no querras ser un usuario de segunda clase.

¿Cuál exchange deberias usar? Personalmente recomendaria los P2P como Bisq y HodlHodl. Pero si quieres ir por la vía centralizada, Kraken y Bitfinex son unos de los más antiguos y amigables con bitcoin del mercado (no me pagan por recomendar a ninguno ni tengo links de referidos).

Luego de que hagas la compra de BTC verificablemente reales y escasos, toma nota de los fees de la red, determina tu preferencia de tiempo, y retira las monedas a tu billetera propia. Para mayor privacidad, puedes hacer CoinJoin con Wasabi y romper el lazo entre el exchange y tu nueva billetera. Y si buscas mejores maneras de asegurar tus monedas, obtén una billetera hardware open source como Trezor, BitBox02, o Coldcard.

Deja de arriesgar dinero en compañías que ni siquiera demuestran que tus bitcoins fueron minados y que existen en una de sus billeteras. Es anti BTC y va en contra de los principios de soberanía financiera individual.

–





Porque Bitcoin Incentiva La Sustentabilidad Y El Cuidado Del Medioambiente

Cuando primero compras bitcoin y aprendes el arte de holdear, tu preferencia de tiempo sufre un golpe y tu tentacion de gastar disminuye gradualmente. Y cuando tu paciencia genera frutos, solamente quieres gastar tu dinero duro en algo que consideras valioso y de alta calidad. Estas son las dos fases que irreversiblemente cambian la vida de los bitcoiners e indirectamente benefician al medioambiente.

Hoy en día, los banqueros y los gobiernos hacen grandes esfuerzos para convencer a todos de que Bitcoin es un desastre ambiental que no produce nada de valor. Al mismo tiempo, perpetuan un entorno económico en el cual el dinero pierde valor y debe ser gastado rapidamente – lo cual incentiva el desarrollo de productos baratos de produccion masiva y baja calidad.

En este articulo, me gustaria argumentar que Bitcoin nos ayuda a volver a una serie de valores que nos hacen consumir menos y enfocarnos en la calidad por sobre la cantidad. Y esto es algo que jamás va a ser fomentado por parte de los bancos, especialmente en una era en que los las tasas de interes son una broma y que el ahorro es activamente desalentado. De hecho, dado que un gran número de personas tendran para gastar pequeñas cantidades de dinero que se deprecia, buscarán artículos baratos que puedan comprar cada vez que cobran.

La Nueva Vestimenta Sustentable De Bitcoin

El consumismo es insostenible y mucho peor para el medioambiente que la minería de Bitcoin. Por ejemplo la vestimenta: las prendas de alta calidad son tan caras como siempre y pueden

costar un alto porcentaje de tu ingreso mensual; pero si compras algo hecho de poliéster en vez de algodon o lana, puedes ir a H&M, New Yorker y Zara y puedes llenar tu ropero a un muy bajo costo.



¿Es buena esta ropa? En general se empieza a ver y sentir horrible luego de un par de lavados. Así que en efecto estas comprando futura basura diseñada para solo durar una temporada. Si compraras algo de mejor calidad, podrias vestirlo y lavarlo durante años.

Pero debido a los incentivos que existen en la economia fiat, estás comprando ítems de menor calidad más frecuentemente para que tu presupuesto monetario no sufra un golpe. Aún debes pagar la renta, comprar comida, y poder pagar el resto de tus cuentas – así que en vez de ahorrar durante varios meses, el sistema financiero te empuja a endeudarte (lo cual es bastante irracional en la mayoria de los casos), o comprar lo que te alcance en un determinado momento.

También habra que debatir sobre los items de baja calidad producidos en masa y la huella de carbono que esta produccion deja. El algodon y la seda son más caros, pero tienen un menor impacto en el medioambiente. El poliéster y la disolucion de elastano reducen los costos de produccion y de venta, pero significativamente incrementan el daño inicial y de largo plazo al medioambiente.

Y estoy seguro de que el ejemplo también aplica a muchos rubros, incluyendo la alimentacion (la comida organica es mas cara, pero más natural y menos dependiente de envases de plastico), los electrodomesticos (una refrigeradora que tenga más plastico probablemente se rompa antes y es menos eficiente, la electronica (una imitacion barata del Nintendo se rompera antes y recibe menos apoyo de software), los automóviles (el vehículo de $10000 hace mas daño ambiental durante su vida util y aun despues tambien que los hibridos que son más caros), y todo el resto de las cosas de precios bajos que compramos por conveniencia.

Bitcoin = Preferencia De Largo Plazo = Sustentabilidad Y Cuidado Del Medioambiente

Si compras y mantienes bitcoins, vas a estar expuesto a un activo cuya emision es fija y predecible. Esto significa que si la demanda también aumenta a traves del tiempo, tu poder adquisitivo también aumenta en relacion a activos inflacionarios tales como las monedas fiat. Pero en el corto plazo, también podrias perder algo de poder adquisitivo – así que serás incentivado a planear en consecuencia y esperar más tiempo.

A medida que ejercitas paciencia y austeridad, descubriras cuantas de las cosas que comprabas no son esenciales. Y hasta en el caso de los ítems esenciales, tendras expectativas más altas. Bitcoin te convierte en un consumidor consciente aun sin que te des cuenta.

En lugar de decir “me comprare un telefono nuevo este año”, querras esperar hasta que salga algo significativamente mejor que potencialmente mejore tu calidad de vida. En vez de cambiar tu vestimenta cada





temporada, compraras algo de mayor costo, pero menor costo por uso. Y en lugar de cambiar tu vehículo para obtener alguna particularidad no esencial (como un mejor equipo de audio o asientos de cuero), ahorras para un cambio significativo.

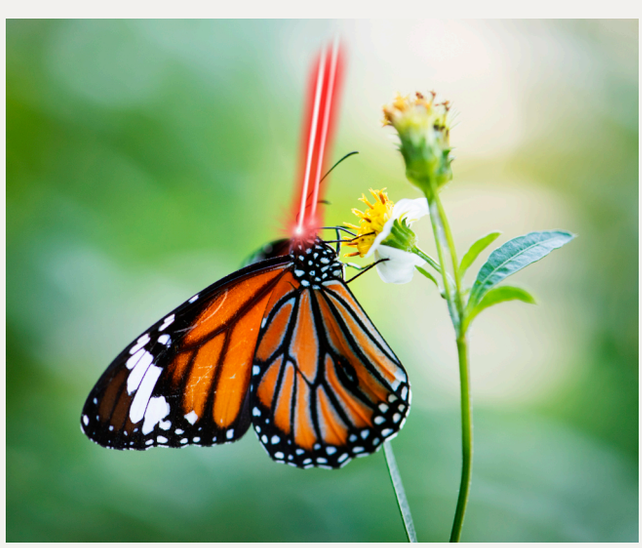
Los productos de alta calidad son usualmente más sustentables y más ecologicos. Y Bitcoin hace que los queramos y que tengamos paciencia hasta poder obtenerlos. En el proceso, nos deshacemos de nuestros instintos consumistas y aprendemos a apreciar la calidad por sobre la cantidad. Rompemos el ciclo, mejoramos nuestras vidas, y también vivimos más sustentablemente y con mayor cuidado hacia el medioambiente.

Es un poco ironico, no? Bitcoin, la moneda de internet que los medios de consumo masivo pintan como derrochadora y de uso dudoso, nos puede ayudar a ser más considerados con el medioambiente. Gracias a su politica monetaria desinflacionaria, queremos gastar menos frecuentemente, esperar más, tomar decisiones más informadas, y obtener el mejor redito por nuestro dinero.

Esto no es algo que la Reserva Federal o el Banco Central Europeo pudan decir sobre las monedas que manejan. Aun así es muy similar al tipo de forma de nuestros abuelos de pensar del ahorro cuando usaban al oro como unidad de cuenta preferida.

Así que la proxima vez que un comentador de red social de baja preferencia de tiempo sugiera que Bitcoin está hirviendo los oceanos, dile que su estilo de vida es mucho peor. Y por cada onza de dioxido de carbono que genera la minería de Bitcoin, ayudas a reducir otros tipos de polucion aun mas dañinos para el medioambiente.

–




SLUSH POOL
IS NOW
BRAIINS POOL
MINING BITCOIN
SINCE 2010
LEARN MORE AT BRAIINS.COM/POOL



Cómo Casi Me Hago Rico Minando Bitcoin En Braiins Pool Durante Un Mes

Cuando mi amigo AdventureDr me ofreció usar un Antminer S9 durante un mes y dejarme quedar con la recompensa a cambio de darle la revista BTCKVR, no pude decir que no a su generosa oferta. En preparación para esta ocasión especial, establecí una cuenta en Slush Pool y le envié a AdventureDr la información requerida para linkear la S9 a mi billetera de Bitcoin.

Durante los siguientes 30 días mi usuario contribuyó a encontrar 200 bloques de Bitcoin. Durante el actual periodo de recompensa, cada nuevo bloque ofrecía una recompensa de 6,25 BTC. lo cual significa que en un mes, el Antminer S9 ayudó exitosamente a agregar 1250 bitcoins al circulante total.

Entonces debería ser rico, no? Pues no. Es que haberme sumado a Braiins Pool significa que opte por minar en colaboración con otros usuarios alrededor del mundo. En vez de tratar de obtener la totalidad de la recompensa para mi con muy bajas probabilidades, opte por recompensas más frecuentes pero menores.

Con una hashrate de aproximadamente 13 terahashes por segundo (13.000 billones h/s), el Antminer S9 ha sido uno de los aproximadamente 143.000 trabajadores de Braiins Pool, los cuales generan un rendimiento de 7272 exa hashes (7272 millones de billones de h/s). Consecuentemente, el equipo que AdventureDr operó por mi solo produjo el 0,0000179% del total del trabajo del pool.

Al momento de la escritura de este artículo, la red de Bitcoin es protegida por un hashrate de 161,9 Eh/s. Esto significa que Braiins Pool solo produce el 4.9% de la Prueba de Trabajo, y mi Antminer S9 prestado provee el 0,000008% de la



seguridad de Bitcoin. Este porcentaje aparentemente insignificante también está reflejado en las recompensas que recibí.



Durante mi mes de minero remoto, gane un total de 0.00237392 BTC (2373,92 bits, o 237.392 satoshis), que al precio actual de $61.258 están valuados en $145,82. Obtuve con mi Antminer S9 aproximadamente el 0,00019% de los 1250 bitcoins que obtuvo Slush Pool.

Estas Ganancias De Minería No Incluyen Equipo, Electricidad, Ni Costos De Mantenimiento.

En promedio, un Antminer S9 usado cuesta unos $600 en eBay. Y el consumo eléctrico de este minero ASIC es de 1800 watts por hora, que equivale a 1296 kilowatts por mes. Donde yo vivo un kilowatt cuesta 15 centavos. Entonces utilizar el S9 durante 30 días me cuesta no menos de $194. Esto significa que si vendiese los BTC minados para cubrir mis costos de electricidad, perdería $48,18 por mes.

Afortunadamente para mí, puedo quedarme con todo los BTC y mi factura de electricidad permanecerá igual que todos los meses – AdventureDr aprecio mucho la revista BTCTKVR y operó el minero ASIC para mi en su ubicación dedicada a la minería. Pero si yo fuese a comprar un Antminer S9, pagaria $600 y subsecuentemente cubriria un costo mensual de electricidad de $194 para operarlo.

Definitivamente no tendría perdida y recuperaria mi inversión inicial si pudiese



holdear mientras el precio de BTC sube durante los próximos años. Pero desde una perspectiva económica, tendría mucho más sentido si usara los $600 y los $194 mensuales de energía para comprar bitcoins. Durante el mismo periodo de tiempo tendría un rendimiento de inversión significativamente mayor y nunca tendría que lidiar con la ansiedad de operar una operación de minería a pérdida.

Naturalmente, uno puede expresar dos argumentos:

1. que debería hacerme de una maquina mas eficiente (mas Th/s con el mismo consumos de energía) para obtener una ganancia mensual y eventualmente recuperar mi inversión;

2. que debería llevar el Antminer S9 a un lugar donde los costos de electricidad permitan que la minería sea rentable (como es el caso con AdventureDr).

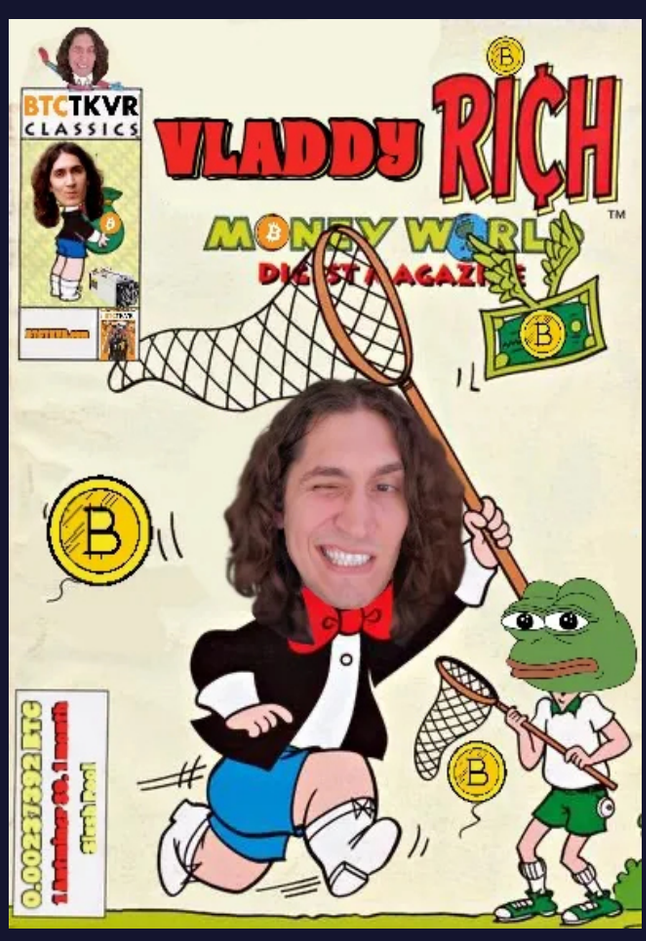
Entonces Si Es Más Rentable Comprar Bitcoin Que Minarlo, Para Que Molestarse?

Hay dos razones muy significativas. Primero y principal, es importante contribuir con la seguridad de la red de Bitcoin. No deberíamos dejarlo centralizarse en grandes centros de datos los cuales obtienen las más bajas tarifas de energía y aprovechan las economías de escala para obtener ganancias enormes. Desde ya que proveen fiabilidad porque les conviene financieramente mantener la operación en marcha 24/7. Pero también son fáciles de regular y de ser clausurados por los gobiernos.

Durante el breve periodo en el que Satoshi fue desarrollador, educador, y asesor técnico, visualizaba a la minería de Bitcoin como algo que todos los nodos podrían hacer con sus CPUs. La competencia por descubrir nuevos bloques era un proceso en el cual todos los participantes encaraban por su cuenta. En el whitepaper, Nakamoto inclusive definió Prueba de Trabajo como “basicamente un-CPU-un-voto”.

Este tipo de descentralización garantiza la resistencia a la censura de la red y reduce las chances de que exista un participante importante que ataque a la red – más allá de los incentivos, es técnica y computacionalmente más difícil que haya un único CPU malévolo cuyo hashpower exceda el esfuerzo total de todos los otros mineros honestos.

Pero en noviembre del 2010, Satoshi supo del enfoque colaborativo de Slush Pool – un descubrimiento que cambiaría la economía y la teoría del juego de la minería de Bitcoin para siempre. El cypherpunk Checo Marek “Slush” Palatinus basicamente se pregunto a si mismo “Que seria si los mineros, en lugar de competir entre ellos para obtener la recompensa de bloque entera, trabajasen juntos para descubrir bloques más rápido y luego compartieran los bitcoins obtenidos según su contribución?”



Desde entonces, hemos visto un incremento en el número de pools de minería y hemos observado las distintas dinámicas existentes que ocurren al haber un oligopolio de hash power. Los mineros que busquen obtener recompensas frecuentes buscarian un pool que les de la parte más grande del subsidio de bloque al ritmo más consistente. En lugar de hacer minería solo y tener las mismas probabilidades de ganar la lotería, combinarian su poder de hashing para cobrar más seguido y para poder financiar sus operaciones con mayor previsibilidad.

En teoría, ningún pool debería convertirse en demasiado grande y potencialmente comprometer la inmutabilidad del blockchain de Bitcoin. Pero en la práctica, en el 2018 Bitmain llegó a controlar más del 40% del hashrate, y en aquel entonces había preocupación sobre las implicancias de tal concentración de minería. Un debate similar se dio en el 2014, cuando GHASH.io controlaba alrededor del 40% del hashrate, mientras que BTC Guild aproximadamente un 25%.

Es cierto, los pools de minería no son compañías que controlan cada equipo que trabaja para ellos. Muchos participantes son independientes y cambian al pool que mejor les paga por su trabajo. Pero hipoteticamente hablando, si un grupo de pools importantes se juntan para reorganizar bloques y revertir transacciones, podrían hacerlo. Y este es un escenario que debemos prevenir.

La minería independiente desde el hogar es esencial para la red de Bitcoin: contribuye a la descentralización del hashrate e incrementa la resistencia a la censura de las transacciones. Porque si, los mineros pueden optar por no seleccionar transacciones originadas de direcciones en lista negra (asumiendo el costo de no cobrar los fees que se pagaron). Consecuentemente, minar altruistamente contribuye a eliminar la discriminacion y así incrementa la fungibilidad de bitcoin como moneda. Aunque no sea rentable en términos de dinero fiat, provee de un gran servicio.

Ahora hablemos del la segunda razon para minar Bitcoin, la cual es más egoista y tiene más que ver con el estado de las politicas humanas y las leyes; los BTC que acaban de minarse están libres de KYC. Esto significa que recibes monedas que no están manchadas por un custodio regulado lo cual desanonimiza las transacciones. La minería es mucho mas privada que comprar en un exchange, y hasta existen individuos y empresas que optan por comprar sus bitcoins directamente de los mineros para evitar cualquier tipo de trazabilidad documentada.

En países donde Bitcoin está prohibido o es excesivamente vigilado, la minería permite a la gente escapar del Gran Hermano. Aquellos que viven bajo un régimen totalitario podrían minar BTC para ganar el tipo de dinero que los libera y les da soberanía. Y casi siempre, necesitan Bitcoin para sobornar oficiales corruptos para poder empezar una nueva vida en algún otro lugar.



Por Que Minar Bitcoin Desde Casa

Para lograr nuestros objetivos de descentralización, necesitamos ASICs SHA-256 que sean diseñados para su uso doméstico No solo equipos de minería de escala industrial, sino equipos que cualquiera pueda utilizar en el living de su casa y poder obtener una pequeña rentabilidad. Un notable producto que



atrajo mi atención es el Futurebit Apollo BTC. Tiene una producción de 3 Th/s a un consumo de electricidad de 200 Watts, con la adicion del modo Eco con el cual solamente consume 125 Watts funcionando más silenciosamente.

Hice los calculos y, si usara el Apollo en vez del Antminer, tendria una ganancia actual de $1 (tomando el precio actual de BTC). Lo cual significa que necesitaría unos 800 meses para recuperar mi inversion, asumiendo tener ese costo de electricidad, precio de bitcoin, y manteniendo constante la dificultad de minar.

Pero al mismo tiempo, el punto de adquirir uno de estos no es enriquecerse, sino darle soporte a la red. A 150 Watts/hour consume 10 veces menos que usar constantemente un equipo económico de aire acondicionado. Y durante el invierno, puedo usar modo Turbo para generar más calor y mantener mi cuarto a temperatura cálida (de hecho, esto sería interesante para cortar mi dependencia al gas natural).

Esto no es, de ninguna manera, una recomendación del minero Futurebit Apollo BTC. El equipo es caro por lo que hace y está siendo producido en cantidades tan bajas que se agota antes de que pueda tener la oportunidad de comprarlo (me pasó 3 veces este año). Se que resultados similares pueden ser alcanzados con el uso de una equipo ASIC de escala industrial modificado, más viejo y más barato, pero su fiabilidad es siempre cuestionable.

Alternativamente, desearia que más compañías estuviesen ideológicamente alineadas con este movimiento de descentralizar la minería de Bitcoin con usuarios individuales. Deberíamos tener un minero chico, energéticamente eficiente y silencioso para tener junto a nuestro router de internet. Así como usamos nodos Raspberry Pi, deberíamos tener equipos de minería similares y pools que los soporten. En el verdadero espíritu de “no confies, verifica”, debemos disminuir nuestra dependencia en granjas de minería importantes, que siguen regulaciones y son políticamente frágiles.

Si, nuestros nodos full pueden rechazar bloques creados por mineros deshonestos. Pero al mismo tiempo, los mineros pueden comportarse acorde a las reglas de consenso y nunca incluir transacciones que tú hayas transmitido. No hay nada que los nodos puedan hacer para obligar a los mineros a incluir cierto tipo de transacciones en un bloque de Bitcoin. Y esta resistencia a la censura no nos es proporcionada por Satoshi, ni por el whitepaper, ni por alguna concepción ideológica de la red de Bitcoin – necesitamos tomarla a través del uso de nuestro propio equipamiento y operación.

Al final, no me hice rico minando Bitcoin. Pero aprendí una importante lección sobre rentabilidad, economías de escala, las limitaciones y la obsolescencia técnica de los ASICs, y como las naciones pueden desincentivarnos de minar añadiendo impuestos adicionales a la electricidad. Pero lo más importante, descubrimos el significado de la descentralización voluntaria. No debemos esperar que otros protejan la red de Bitcoin honestamente – ellos tienen las granjas, pero nosotros tenemos los números.

Un Curso Rapido De Minería De Bitcoin



La minería de Bitcoin es un proceso energeticamente intensivo el cual brinda seguridad a la red de Bitcoin. Aproximadamente cada 10 minutos, un nuevo bloque es descubierto – y el primer minero que resuelva un complejo problema matematico es premiado con la recompensa del bloque y con los fees de transacciones que los usuarios pagaron para priorizar sus transacciones.

A cambio de proveer seguridad a la red, los mineros de Bitcoin también se convierten en participantes de esta carrera en la cual el que gana se lleva todo. Existen costos energeticos ligados a la produccion de cada unidad de BTC, y siempre es más caro atacar al sistema que participar en él honestamente. Basicamente, la seguridad de la red de Bitcoin depende de la avaricia competitiva y el propio interes financiero de los mineros.

El sistema está basado en Prueba de Trabajo, del Dr Adam Back, el cual fue inicialmente incluido en hashcash en 1997. En su primera version, la "minería" era una forma de prevenir el spam del correo electronico. Para asegurarse de que quienes envían dejaran de llenar las casillas de correo de un número ilimitado de receptores, sin costo alguno, los enviadores de correos electronicos deberian o usar la capacidad de procesamiento de sus computadoras para minar hashcash o de lo contrario pagar por cada email. De esta manera, enviar spam conllevaria costos coputacionales o financieros.

Satoshi Nakamoto tomó los principios de hashcash y los usó para resolver el Problema del General Bizantino (también conocido como Tolerancia Bizantina a la Falla). Esencialmente, el asunto de "cómo nos aseguramos de que los participantes descentralizados que no se comunican entre sí se coordinen para ir tras el mismo objetivo de una manera honesta?" fue resuelto con Prueba de Trabajo e incentivos. Esto es parte de lo que a veces llamamos el "Consenso Nakamoto".

El blockchain de Bitcoin es gobernado por las leyes de la fisica – y más precisamente entropia como consecuencia de la primera regla de termodinamica. Cada evento se hace posible a traves del consumo de energia, y así se torna demostrable e irreversible. Esto es de máxima importancia para la seguridad de las transacciones, ya que deben ser resistentes a politicas humanas.

Es de consenso general que luego de que seis nuevos bloques hayan sido minados, el costo de lanzar un ataque de reorganizacion del blockchain es realmente demasiado alto como para revertir una transaccion pasada. El matematico Español Ricardo Perez-Marco y el investigador matematico Frances Cyril Grunspan han inclusive publicado un paper academico en el cual argumentan que 2 confirmaciones de la red son más que suficientes para determinar la resolucion final de una transaccion, específicamente debido al costo de multiples millones de dólares para realizar un ataque contra la misma.

Los mineros de Bitcoin compiten por una recompensa de bloque que disminuye en un 50% cada 210.000 bloques (aproximadamente 4 años). Al comienzo, la recompensa era de 50 bitcoins por bloque. En noviembre de 2012, el bloque de Bitcoin 210.000 fue minado y la nueva recompensa bajó a 25 BTC. Desde el bloque 420.000 (julio 2016) y hasta el bloque 630.000 (mayo



2020), resolver exitosamente el complejo problema matematico y asi darle seguridad a la red es compensado con 6,25 BTC, y será reducido a la mitad nuevamente luego del bloque 840.000 (en algun momento de 2024).

Así es como el circulante total de 21 millones de bitcoins se emite. Tomará hasta el año 2140 (el corte a la mitad número 34) para que se complete la totalidad de la emision. Pero esto no significa que la minería concluye. El diseño de Satoshi Nakamoto es de tener los fees de las transacciones como un segundo incentivo. Y dentro de un par de decadas, la suma de los fees seran mayores que la recompensa de descubrir un bloque.

Cada transaccion de Bitcoin es data que ocupa espacio de un bloque de Bitcoin. Entonces para tener una transaccion incluida en un bloque, debes pagar una cierta cantidad de unidades de BTC por cada byte de data que vas a ocupar. A medida que sube la demanda, un juego de prioridad comienza a favor del mayor postor -los usuarios de Bitcoin que más pagan por sus transacciones son los que primero recibirán las confirmaciones.

El dinero pagado en fees de transacciones va para el minero (o pool de mineros) que descubre el bloque. Esto significa que la recompensa total de bloque al minero consiste del subsidio correspondiente a la epoca (la cual es constante durante 210.000 bloques), más los fees de las transacciones. Por ejemplo, un minero en 2021 recibe 6,25 BTC de recompensa de bloque, así como también unos 0,05 BTC adicionales de fees de transacciones (a una media de 4 sat/byte).

Pero a medida que más mineros se unen, la dificultad de encontrar nuevos bloques aumenta exponencialmente, correcto? Esto significa que a traves del tiempo, más energia debera ser consumida para producir más bitcoins. En realidad no es tan así. Satoshi Nakamoto diseñó un sistema de reajuste de dificultad.

Cada 2016 bloques, la dificultad se reajusta segun la actividad del momento: si se agregó más poder de hashing durante el ciclo previo de 2016 bloques, entonces la dificultad se incrementa. Pero si los mineros comienzan a rendirse producto de su interes personal (el costo de la electricidad sube más que la recompensa), entonces la dificultad de encontrar un nuevo bloque disminuira.

Este proceso dinamico crea oportunidades unicas para buscar el momento perfecto para empezar a minar, y también incentiva una busqueda permanente de costos de electricidad más bajos. Cuando un minero se baja y disminuye la dificultad, siempre habra otro en alguna parte del mundo que aprovechara la oportunidad de obtener más bitcoins con un esfuerzo menor.

Coincidentemente, el tipo de energia mas accesible es la que es generada con recursos renovables. La minería Prueba de Trabajo de Bitcoin ha dado lugar a una busqueda global de energia economica: en China los mineros utilizan ruedas de agua (energia hidroelectrica): en Estados Unidos, los mineros usan gas natural que normalmente se desperdicia durante la extraccion de petroleo: en El Salvador, se utiliza la energia geotermica de los volcanes para abastecer a los mineros ASIC.

Y alrededor de todo el mundo, el superavit de energia que las plantas y redes eléctricas no pueden transportar a los consumidores se utiliza para darle seguridad a la red de Bitcoin y se genera una utilidad adicional. Lo que algunos describen como un proceso de desperdicio en realidad incentiva la expansion y el desarrollo de energia renovable.

La minería de Bitcoin es una de las industrias más dinamicas del mundo. Desde enero 2009, ha logrado transicionar del diseño original de “un CPU un voto” a la minería GPU, y posteriormente dar inicio al rentable negocio de los equipos ASIC (Circuitos Integrados de Aplicacion Específica, o computadoras especializadas que solo pueden realizar una tarea, de una forma muy eficiente).

La minería desde casa ha rapidamente migrado hacia granjas industriales, y durante un tiempo la mayoria de la actividad tenía lugar en China. Pero desde el segundo semestre de 2021, debido a las politicas autoritarias de China, el nuevo líder de la minería de Bitcoin es Estados Unidos de America. Sin embargo, mi esperanza es que las compañías de equipos encontrarán formas creativas para que la minería retorne a las casas de la gente.

Gente astuta alrededor del mundo ya han encontrado maneras de usar el calor generado por los mineros de Bitcoin para aclimatar sus hogares, o para hervir agua para sus baños. Al final de cuentas, el ingenio humano es infinito y vamos a ver muchos acontecimientos tan brillantes que nuestras mentes hoy no pueden concebir. Y siempre y cuando la red de Bitcoin se torna más descentralizada y logra su objetivo de separar al dinero de la politica humana, estoy totalmente comprometido.



_

Vaultoro

WASABI WALLET

MAACHI

BTCTKVR



APPLE PODCASTS

Spotify