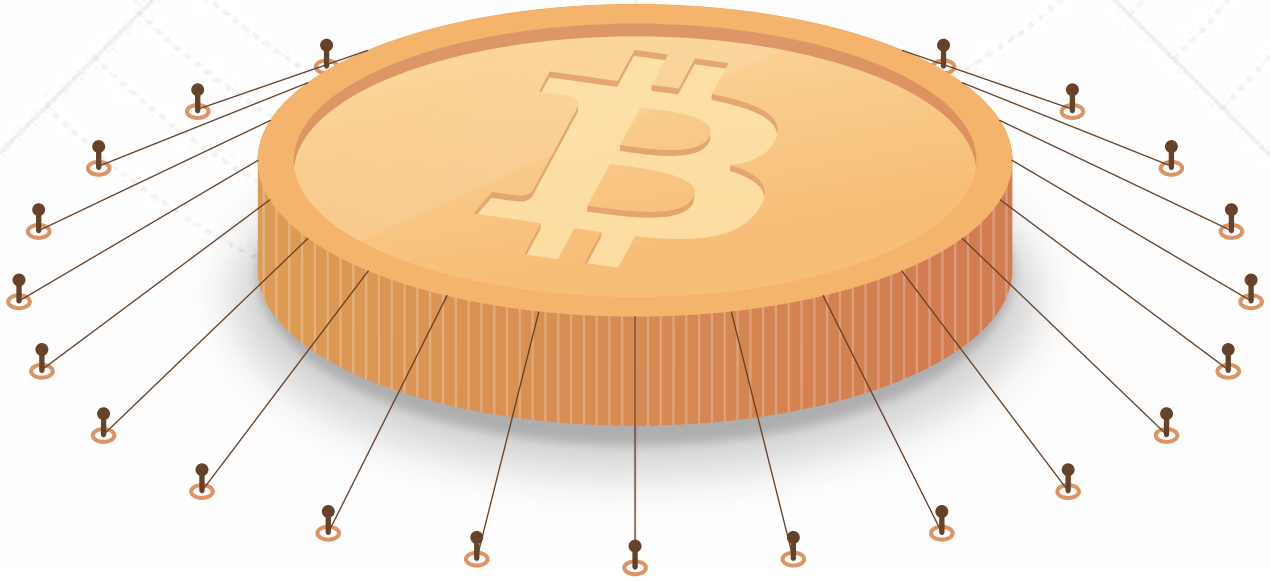
Del bestseller en inglés

The Book of Satoshi

PHIL CHAMPAGNE

El Libro de Satoshi



ALIANZA BLOCKCHAIN IBEROAMÉRICA

BITCOIN IBEROAMÉRICA

BLOCKCHAIN ESPAÑA

blockchainespana.com

EL LIBRO DE
SATOSHI

EL LIBRO DE

SATOSHI

<<<< >>>>

La Colección de Escritos del Creador de Bitcoin

Satoshi Nakamoto

PHIL CHAMPAGNE

BLOCKCHAIN ESPAÑA
BlockchainEspana.com

Publicado en inglés en Estados Unidos por e53 Publishing LLC

Publicado en español por Blockchain España con una licencia Creative Commons by Sharealike (CC BY SA) por cesión de Phil Champagne. Consultar con libroblockchain@gmail.com para la reproducción del texto español.

Se debe citar:
Champagne, Phil. El Libro de Satoshi (Edición BlockchainEspana.com):
Descargable desde: http://www.libroblockchain.com/satoshi/

ISBN 978-0-9960613-0-8 Tapa dura inglés
ISBN 978-0-9960613-1-5 Tapa blanda inglés

e53 Publishing LLC
e53publishing.com

Ilustración de portada original edición en inglés de Lisa Weichel

Edición inglés de Mary Graybeal

Edición en español de Iñigo Molero Manglano y Arturo Monzón Seminario

Diseño y composición de portada y texto en inglés por John Reinhardt Book Design
Diseño y composición de portada y texto en español por Vita Valka

Este libro también está disponible en formato de libro electrónico.
Para obtener una copia gratuita, vaya a: BookOfSatoshi.com en inglés
o LibroBlockchain.com/satoshi/ en español.

Contenidos

Agradecimientos

ME GUSTARÍA EXTENDER mi profundo agradecimiento a las siguientes personas por su contribución a este trabajo:

Dustin Trammell (dustintrammell.com) por compartir los correos electrónicos intercambiados con Satoshi Nakamoto, Gavin Andresen, desarrollador principal del proyecto Bitcoin, por su contribución a Bitcoin y también por compartir sus correos electrónicos con Satoshi Nakamoto.

Por su apoyo, experiencia, aportes y contribuciones, me gustaría dar las gracias a mi hijo, Samuel, mi hija Vivianne y mi esposa, Marie Gagnon. Y, por último, me gustaría agradecer a todas las personas que me ayudaron a componer este libro, en particular a Mary Graybeal, nuestra editora que realizó un gran trabajo, y a John Reinhardt, a quien se le ocurrió este gran diseño para el libro.

Y, por último, un sincero agradecimiento a Satoshi Nakamoto. Sin él, ¿cuánto tiempo habríamos tenido que esperar antes de que se descubriera y compartiera un concepto tan revolucionario como el de Bitcoin?

Phil Champagne

A Quién Está Dirigido Este Libro

ESTE LIBRO CONTIENE la mayoría de los escritos de Satoshi Nakamoto, creador de Bitcoin, publicados en correos electrónicos y foros durante el lapso de poco más de dos años durante el cual se lanzó Bitcoin y se consolidó. Cualquier persona interesada en aprender sobre Bitcoin y, más específicamente, sobre los procesos de pensamiento de su creador, apreciará este libro. Su contenido será de lectura fácil para cualquiera que tenga experiencia en software. Sin embargo, los economistas e inversores sin experiencia en tecnología de la información también pueden estar interesados en los escritos de Satoshi, algunos de los cuales se refieren a conceptos económicos. Dependiendo de la experiencia y el interés, ciertos lectores pueden estar interesados sólo en algunos capítulos.

Para que los lectores obtengan el máximo beneficio de los escritos de Satoshi, hemos incluido un capítulo titulado "Cómo y por qué funciona Bitcoin" que proporciona una introducción a los conceptos clave de Bitcoin y los principios fundamentales en los que se basa. Esto debería ayudar al lector a comprender lo suficiente como para comprender la mayoría de los capítulos que siguen. Los capítulos se presentan en orden cronológico, desde la primera publicación en la que Satoshi presenta la idea germinal de Bitcoin hasta la más reciente, que marca su retirada de la vida pública.

Parte del contenido de este libro proviene de varios foros de Internet: *p2pfoundation.org*, *bitcointalk.org* y el archivo de correo criptográfico. Puede visitar el sitio web *TheBookOfSatoshi.com* para su edición en inglés y LibroBlockchain.com/satoshi/ para obtener referencias sencillas a los enlaces URL web a los que se hace referencia en el libro. Se enumeran por capítulo.

Prólogo a la Versión en Español

Hasta principios de 2017 Bitcoin y la tecnología Blockchain erán temas de poco dominio público, y a raíz del boom especulativo de las criptomonedas y de las ICOs (Initial Coin Offering, Oferta inicial de monedas), que, sumado al interés corporativo por esta tecnología, impulsaron su interés a nivel global. Una de las razones por las que escribimos a finales de 2016 el libro "Blockchain: la revolución industrial de internet" fue para intentar crear una herramienta de acceso a la tecnología Blockchain para la población de habla hispana, y, que el idioma no fuera una barrera de entrada al conocimiento de esta tecnología. Queríamos que nuestros países pudieran participar en el cambio global que se avecina, y no ser meros espectadores de lo que hacían otros.

Blockchain, la base de datos transaccional descentralizada inmutable, es uno de los elementos que tiene cualquier Blockchain pública. La primera de todas es Bitcoin que se compone de un protocolo (Bitcoin con B mayúscula), una unidad de cuenta o token (bitcoin con b minúscula) y una Blockchain (la base de datos transaccional). La mayoría de las blockchain públicas suelen tener esos tres componentes para operar como un sistema descentralizado. Ethereum es otro ejemplo de Blockchain pública importante junto a las muchas otras con las que se experimenta.

El talento desarrollador y los nuevos modelos de negocio de las blockchains públicas viene en muchos casos de personas que piensan que el sistema centralizado ha fracasado a muchos niveles, tanto a nivel social como global. Cualquier persona que quizás trabaje de día en una multinacional como desarrollador pero con una baja satisfacción en algunos casos colabora fuera de su horario laboral con proyectos de código abierto (que pueden ser de Blockchain o cualquier otra tecnología) para aprender, dar propósito a su vida o simplemente porque siente que estas colaboraciones están más alineadas con su

visión del mundo. El dinero que ha alimentado las blockchain públicas es dinero especulativo principalmente, pero también de personas que creen que es la tecnología del futuro. Y el objetivo de la misma es la disrupción del estatus quo de todos los modelos de negocio actuales para crear el futuro Facebook, Uber o Banco descentralizado a modo de ejemplo.

Por eso Blockchain no sólo es una tecnología. Es mucho más que eso. Por lo menos así fue para las personas que iniciaron las Blockchain públicas. Satoshi Nakamoto quería crear Bitcoin como un dinero de las personas que funcionara entre pares (P2P o Peer to Peer). Satoshi se inspiró en soluciones propuestas por diferentes Cypherpunks, un movimiento anarcocapitalista tecnológico que quiere dar herramientas a las personas para proteger su privacidad. El origen de este movimiento lo encontramos en los años 90 y venía a su vez inspirado en otros movimientos similares de décadas anteriores, dentro del ámbito académico y científico en muchos casos.

Algunas de las personas en las que se inspiró Satoshi fueron Hal Finney, destinatario de la primera transacción de bitcoins realizada por Satoshi y que en 2004 creó un sistema llamado Real Proof of Work para crear un tipo de dinero digital descentralizado. Nick Szabo, al que se le atribuye ser el inspirador del concepto de contrato inteligente (Smart Contract) – tan omnipresente en las conversaciones actuales - y promotor de un prototipo de moneda llamado Bitgold. Wei Dai que diseñó un sistema llamado B-money o Adam Back, que conceptualizó un sistema antispamming para los emails, llamado HashCash, y que sirvió de inspiración para crear el modelo de consenso de Prueba de Trabajo (Proof of Work). Back sigue activo en el ecosistema y es cofundador de la conocida startup Blockstream donde desarrollan las posibilidades de Bitcoin. Todos ellos se identifican como Cypherpunks, al igual que lo hace Vitalik Buterin, co creador de Ethereum. Todas estas personas citadas no participaron en estos proyectos para lucrarse sino para crear herramientas que ayudarán a la humanidad a progresar, poniendo a nuestra disposición desarrollos y nuevos de sistemas de organización social que quizás pudieran ayudar a superar las limitaciones de nuestros sistemas de organización, muy centralizados desde los últimos 200 años.

Por todas estas razones Blockchain es mucho más que una tecnología, es un instrumento de cambio social.

Aquellas personas que se interesaron antes de 2013 o 2014 por la tecnología y que siguieron involucrados con el transcurrir del tiempo han podido conocer directamente la comunidad Bitcoin en sus orígenes, pero para los más recientes el mundo de las criptomonedas podría parecerles un gigantesco casino. La generación anterior a pesar de las bajadas drásticas de precio, tenía como motivación principal, en muchos casos, la posibilidad que brindaba la descentralización como instrumento de cambio social, aunque obviamente también existían muchos especuladores. En 2017 la descentralización ha pasado a segundo plano y el foco ha sido la especulación.

Ambos objetivos son legítimos, pero ha habido un secuestro del discurso de la descentralización, el bien social y el progreso a través de la colaboración y compartir experiencias y conocimientos, para llevarlo a un nivel de egoísmo cortoplacista que, en muchos casos, se convierte en casi sólo ruido, con poca substancia. Esto es un fenómeno global, pero divide a la comunidad y va en contra de lo que a algunas personas nos habría gustado ver, un entorno colaborativo sustentado en el respeto y la causa del progreso en común.

En su origen más purista "Comunidad Blockchain" representaba para muchos un interés por una tecnología que podría permitir recrear modelos sociales más justos y descentralizados pero la subida de los precios de los cripto activos ha diluido este concepto original de comunidad. Quizás tengamos que esperar, tras una larga y pronunciada bajada de los precios, para volver a hablar de comunidad como lo hayamos podido vivir en el pasado.

España, y muchos otros países de habla hispana, tienen una magnífica oportunidad para desarrollar y utilizar la tecnología Blockchain y posicionarse en este incipiente mercado global, además de poder fomentar otras tecnologías exponenciales. Tenemos el talento, las infraestructuras y el capital para lograrlo. Pero nos falta coordinarnos y tener una predisposición por invertir, experimentar e innovar con Blockchain. Para eso, sólo se necesita un marco regulatorio favorable y proactivo que permita que muchos de estos proyectos puedan nacer y desarrollarse en España y latinoamérica porque, de lo contrario, lamentablemente tendrán que emigrar.

Como siempre sucede, cada vez que asistimos a una revolución tecnológica, los países más avanzados del mundo ya se están posicionando. Así que, de nosotros depende si queremos formar parte del siglo XXI o ser parte de

un imperio en declive (el de la UE) que nos impida ser protagonistas del progreso global.

Para entender a dónde nos dirigimos en el futuro necesitamos entender de dónde vinimos. Phil Champagne en esta magnífica obra nos abre una ventana estructurada al pensamiento de Satoshi Nakamoto. El genio (mujer, hombre o grupo), que lanzó Bitcoin cambiando nuestra forma de entender las relaciones humanas y la importancia de ver el mundo como un todo de relaciones entre pares.

Todo esto no habría sido posible sin la incansable labor de coordinación de Arturo Monzón Seminario, la valiosísima labor de edición de Iñigo Molero Manglano, compañero incansable de batalla del ecosistema español de blockchain y la magnífica labor de traducción de los capítulos de Jose Antonio Bravo, Beatriz Lizarraga Mariezcurrena, Adrián Bernabéu Escudero, Alex Viñas Salles, Enrique Palacios Rojo, Jose Manuel Arenillas, Roberto Fernández Hergueta, Iván Durán Fabeiro y Jose Luis Abia Elvira. Muchas gracias a todos por su contribución desinteresada en favor del ecosistema Bitcoin.

Alex Preukschat,

Nodo Coordinador Blockchain España
Junio 2017

1

Introducción

Traducción por **Iván Durán Fabeiro**

HEMOS VISTOS MUCHAS revoluciones tecnológicas asombrosas a lo largo de la historia de la humanidad. La imprenta de Guttenberg ayudó a llevar los libros a las masas. El telégrafo habilitó una comunicación rudimentaria pero eficaz a través de grandes distancias. Más recientemente, los ordenadores personales han aumentado enormemente la productividad humana y de ahí, la creación de Internet, las comunicaciones digitales y el advenimiento del periodismo ciudadano. Fotos de los principales eventos se suben casi instantáneamente a Twitter y otras redes sociales a través de teléfonos inteligentes, que podemos decir que son ordenadores pequeños por derecho propio. Sin embargo, si nos fijamos en el sistema monetario, hasta hace muy poco tiempo, no se había visto afectado por un gran avance.

Bitcoin es ejecutado por un software (código fuente) que está disponible gratuitamente para que cualquiera pueda verlo e incluso adaptarlo para su propio uso. Actualmente se ejecuta en múltiples ordenadores conectados a Internet a través de un protocolo de red común definido por este mismo software.

Existe dentro de este software y existe debido a que es una moneda digital conocida como *bitcoin*, escrito con una minúscula b y abreviado BTC.

Bitcoin, tanto una moneda virtual como un sistema de pago, representa un concepto revolucionario cuyo significado rápidamente se hace evidente con una primera transacción. Un sujeto que realiza una compra en BTCs sólo tiene que proporcionar al comerciante información personal relevante para la

compra, por ejemplo, la dirección de envío o correo electrónico y así poder pagar. Compare esta situación con una compra realizada con tarjeta de crédito, que requiere que el comprador tenga que proporcionar suficiente información personal que facilita la labor de los hackers o empleados deshonestos para hacer compras fraudulentas con la tarjeta.

Sin embargo, el significado de Bitcoin no se limita a la simplicidad del sistema de pago. El suministro de moneda Bitcoin se define por el software y su protocolo subyacente. Sólo 21 millones de bitcoins llegarán a existir, con 17 millones creados hasta ahora. Se espera que el último bitcoin sea creado alrededor del año 2140. Esta oferta de dinero muy específica y limitada ha provocado muchas controversias. Algunas derivadas con la falta de comprensión del protocolo informático o con la economía, más que con el software en sí mismo. Aunque 21 millones de BTC podrían parecer insuficientes con una población mundial de 7.000 millones de personas, la moneda bitcoin es altamente divisible. La denominación más pequeña permitida por el software actual es 0.00000001 BTC (10^{-8} BTC), que ha sido definido como 1 *satoshi*, en honor al supuesto creador del software, Satoshi Nakamoto. Hay por lo tanto 100 millones de satoshis en un solo bitcoin, y por lo tanto el suministro máximo de 21 millones de BTC será equivalente a 2,1 cuatrillones de satoshis o, si usted lo prefiere 2.100 trillones de satoshis.

Bitcoin fue creado por una persona anónima (o grupo de personas) conocida como Satoshi Nakamoto. En el momento en que Nakamoto hizo su primer anuncio público, compartiendo su artículo sobre Bitcoin, él era sólo otro usuario anónimo como millones de otros tantos que publican en foros de Internet. Su nuevo software estaba entonces todavía en la fase inicial de desarrollo, y Bitcoin fue sólo un experimento en sus primeras etapas. La interacción de Satoshi se limitó a los intercambios de correo electrónico y por un breve periodo de poco más de 2 años. Desde entonces, no hemos sabido nada más de él. En el momento de su último post, el valor de Bitcoin se estaba disparando, y los medios de comunicación comenzaron a interesarse por el tema. Justo cuando Bitcoin parecía listo para despegar y empezaba a atraer un gran interés, Satoshi Nakamoto se retiró del foco público.

Pocos años después, Satoshi se ha convertido en una especie de figura icónica, y su retiro sólo ha servido para ampliar el misterio que le rodea. Su identidad es irrelevante para el buen comportamiento de Bitcoin, ya que el

código es de software abierto y, de hecho, se está actualizando y mejorando constantemente mientras lee estas líneas. Sin embargo, adquirir una comprensión de la mentalidad de la persona misteriosa (o grupo de personas) detrás de esta maravillosa nueva tecnología es ciertamente interesante.

Los dos años de "vida pública" de Satoshi se superpone al desarrollo de Bitcoin y el lanzamiento de la publicación de su artículo "Bitcoin: Un Sistema de Dinero Electrónico Peer-to-Peer", publicado el 1ª de noviembre de 2008, en la Lista de Correo de Criptografía. En ese momento, este white paper podía descargarse en el dominio *bitcoin.org*, que había sido registrado unos meses antes, el 18 de agosto de 2008, a través de *anonymousspeech.com*. El 9 de noviembre de 2008, el proyecto Bitcoin fue registrado en *SourceForge.net* y, a principios de 2009 se creó el bloque génesis. Para entender el bloque génesis, imagine un libro de contabilidad que agrega nuevas páginas (bloques) diariamente y que contiene un registro de todas las transacciones de bitcoin que se hayan realizado. La primera página de este libro se llama el bloque génesis y se explicará con más detalle en el siguiente capítulo. Satoshi incorporó esta interesante cita en el bloque génesis en referencia a los rescates bancarios ocurridos en ese momento:

The Times 03/Enero/2009

El ministro de hacienda al borde del segundo rescate bancario

Los rescates bancarios fueron y siguen siendo acontecimientos extremadamente desagradables, especialmente para los libertarios, que caricaturizaron nuestro entorno político y económico con esta cita: "Privatizar las ganancias y socializar las pérdidas".

Seis días después, el 9 de enero de 2009, Nakamoto publicó el código fuente de Bitcoin versión 0.01 en *SourceForge.net*. A partir de la publicación de este libro en idioma español (junio 2018), Bitcoin v.0.16.0 es la última versión operativa.

La última entrada de Satoshi fue publicada en el foro *bitcointalk.org* el 12 de diciembre de 2010. Su última comunicación conocida es un correo electrónico privado enviado unos meses después a Gavin Andresen, actual desarrollador principal líder del proyecto Bitcoin[1].

A continuación, se muestra un gráfico con la información de negociación pública dada por *bitcoinmarket.com*, la primera web de intercambio de Bitcoin que ya no opera. Como se puede ver, el valor de un bitcoin pasó de 10 centavos a un dólar en muy poco tiempo. En el momento de la última entrada de Satoshi en el foro, se estaba negociando alrededor de 25 centavos y se acercaba a 30 centavos por bitcoin.

Historial de precios inicial de Bitcoin

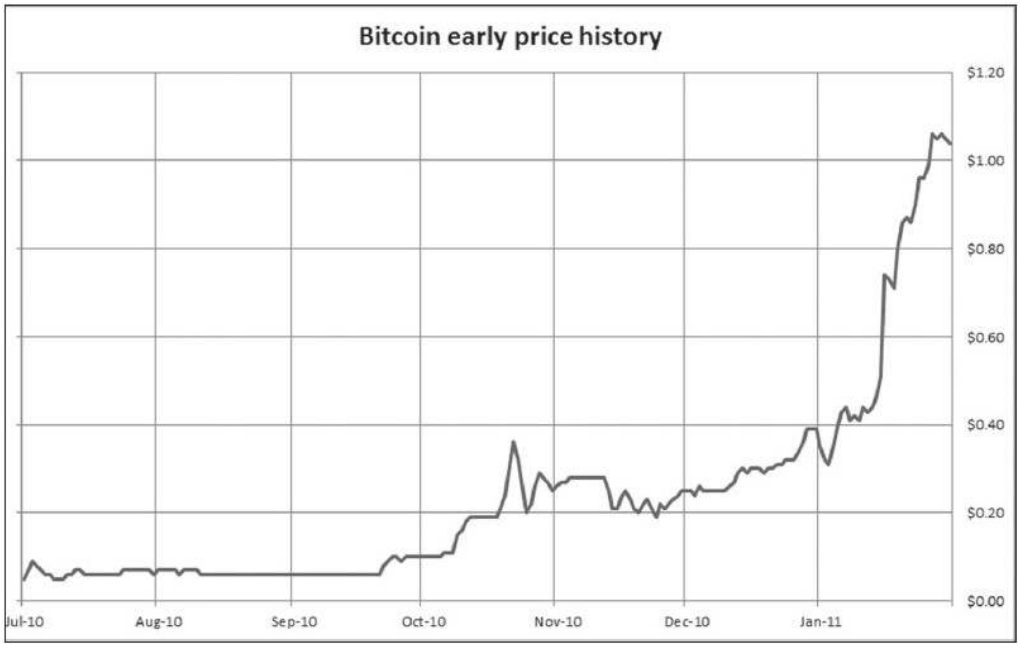


FIGURA 1 – GRÁFICO INICIAL DE PRECIOS DE BITCOIN EN USD

Este libro es una colección de los textos y escritos publicados bajo el nombre de Satoshi en varios foros e incluimos los intercambios de correos

[1] En 2014 Andresen dejó la función de desarrollador líder de bitcoin, dejando a cargo a Wladimir van der Laan.

electrónicos. He optado por excluir los comunicados de carácter técnico, como los relacionados con la codificación, la compilación de software y el funcionamiento técnico detallado del software de Bitcoin. El lector notará que se discuten algunos temas interesantes; uno en particular que involucra el Problema de los Generales Bizantinos, considerado hasta ahora como irresoluble, que describe el desafío de una comunicación segura en un ambiente de desconfianza. Algunos de los comentarios de Satoshi se relacionan con la cobertura informativa que se desarrolló cuando Bitcoin empezó a atraer la atención de los medios de comunicación. Uno de estos eventos tuvo lugar cuando PayPal dejó de procesar pagos para WikiLeaks, una organización periodística sin ánimo de lucro dedicada a publicar información secreta y clasificada proporcionada por fuentes anónimas. Un artículo posterior publicado en la revista *PC World* especula cómo WikiLeaks podría beneficiarse de Bitcoin.

El texto de Satoshi parece indicar que no se sentía cómodo con que Bitcoin recibiera este tipo de atención y que no estaba preparado para tal relación, al menos no todavía:

> HABRÍA SIDO BUENO HABER CAPTADO LA ATENCIÓN EN CUALQUIER OTRO CONTEXTO. WIKILEAKS HA PATEADO EL PANAL Y EL ENJAMBRE DE ABEJAS SE DIRIGE HACIA NOSOTROS.

No se sabe hasta qué punto este acontecimiento influyó en su decisión de "retirarse" del desarrollo de Bitcoin, pero el momento era interesante, por decirlo suavemente. Este post fue escrito sólo diecinueve horas antes de su último post en el foro, el anuncio del lanzamiento de la versión 0.3.19 de Bitcoin.

Muchos periodistas e investigadores han intentado identificar quién podría ser la persona detrás de Satoshi Nakamoto. Hasta ahora se han hecho al menos tres intentos de identificación. Las opciones típicas han sido científicos conocidos en el campo de la criptografía, ninguno de cuyos nombres reales son

Satoshi Nakamoto. Todos han sido probados como falsos y todos negaron ser Satoshi Nakamoto también. Sin embargo, muy recientemente, un periódico afirmó haber identificado a un californiano, un ingeniero con el nombre actual de Dorian Satoshi Nakamoto, como el Satoshi Nakamoto de Bitcoin. Dorian Nakamoto lo ha negado y yo me inclino a creerle. Por un lado, Dorian Nakamoto no demuestra el dominio del inglés que el Satoshi Nakamoto de Bitcoin ha demostrado a través de sus escritos. Lo más relevante para este libro concerniente a este episodio es que, aparentemente provocó que el Satoshi Nakamoto de Bitcoin rompiera su silencio y publicará este mensaje en el foro de *p2pfoundation* el viernes 7 de marzo de 2014:

NO SOY DORIAN NAKAMOTO

Como verán en el libro, las respuestas de Satoshi se refirieron a muchas de las preguntas y críticas más frecuentes con respecto a Bitcoin, que hoy siguen siendo pertinentes. Sospecho que, si todavía estuviera involucrado en el desarrollo de Bitcoin y fuera entrevistado, los escritos contenidos en este libro reflejarán el tipo de respuestas que daría Satoshi. Sea lo que sea que le ocurra eventualmente a Bitcoin en sí mismo, es indiscutible que el software ha abierto la mente del mundo a un nuevo concepto. Como código abierto, ha permitido la entrada en escena de una multitud de otras monedas digitales distribuidas. Mientras que la mayoría de ellas no representan ninguna innovación significativa -sólo han cambiado el número de monedas, la velocidad de confirmación de la transacción (en Bitcoin denominada *creación de bloques*) o el algoritmo de encriptación computarizada-, unas pocas nuevas incorporan nuevas características significativas o nuevos conceptos que están siendo desarrollados. Uno de ellos es "Truthcoin", descrito como mercado de predicción de bitcoin escalable, sin confianza, descentralizado, a prueba de censura, compatible con incentivos. Ethereum (ver *ethereum.org*) es otra moneda digital que, según su creador, permitirá a los usuarios codificar avanzados tipos de transacciones, contratos inteligentes y aplicaciones descentralizadas en la cadena de bloques (el gran registro público de bitcoin que crece en tamaño diariamente).

Los que piensan en la innovación intentan utilizar algunos de los conceptos introducidos por Bitcoin en un verdadero sistema de votación abierto, en el que los votantes pueden confirmar que sus votos han sido adecuadamente contados y pueden, en cualquier momento, ver un completo conteo de votos, garantizando así la transparencia. Por lo tanto, Bitcoin ha desencadenado claramente una nueva revolución tecnológica que capitaliza Internet, otra innovación que cambió el mundo.

Estoy abierto a recibir sugerencias y correcciones con respecto a este libro y su contenido. Además, si usted tiene intercambios de correo electrónico privados con Satoshi que, crea que pueden hacerse públicos, estaré encantado de considerarlos para una posible inclusión. Por favor, no dude en contactar conmigo en BookOfSatoshi@gmail.com

2

Cómo y Por Qué Funciona Bitcoin

Traducción por **Iván Durán Fabeiro**

BITCOIN HA SIDO DESCRITO como libertario por naturaleza, pero ni todos los libertarios, ni los que están a favor de una moneda respaldada por oro, lo aprecian y alguno de estos, además, lo desprecian activamente. En nuestra experiencia, algunos conceptos fundamentales relacionados con Bitcoin no son bien entendidos por ellos. Para un total entendimiento de Bitcoin, o saber cómo funciona y, lo que es igual de importante, conocer la filosofía por la que funciona, es esencial. ¿Cómo puede un sistema distribuido, compuesto por varios grupos diferentes y manejado por distintos individuos al mismo tiempo, mantener su integridad y evitar la llamada "tragedia de los comunes" apuntada por Garret Hardin? En esta situación económica, individuos, actuando independiente y racionalmente de acuerdo con sus intereses, se comportan de manera contraria al mejor interés de todo el grupo a largo plazo, agotando los recursos comunes. Un ejemplo típico es cuando un grupo de granjeros comparten los campos comunes para el pastoreo de su ganado. La sobreexplotación y el agotamiento del recurso común, los pastizales, puede darse debido a que no es del interés individual de ningún granjero conservar ni limitar el consumo de su propio ganado.

Empecemos con una discusión de cómo funciona Bitcoin. Para apreciar y entender la mayor parte de este libro, es necesario un básico entendimiento de los conceptos clave de Bitcoin. Este capítulo proporcionará esto y concluirá con una perspectiva sobre por qué Bitcoin, como un sistema de pago, ha

demostrado, hasta ahora ser una solución viable. Para completar nuestra exposición, revisaremos las implicaciones económicas que tiene Bitcoin.

En su esencia, Bitcoin incorpora los siguientes conceptos:

- Un libro público mayor (llamado *cadena de bloques* de Bitcoin). Esencialmente, considere este punto como un libro públicamente disponible y que contiene los registros contables de todas las transacciones realizadas en el sistema Bitcoin, al que constantemente se le añaden nuevas páginas.
- Un algoritmo criptográfico, llamado cifrado asimétrico, utilizado para autorizar transacciones.
- Una red distribuida de *nodos* computarizados (también comúnmente conocidos como *mineros*) que verifican y validan las transacciones de Bitcoin y de actualizan el libro de contabilidad pública.

Exploremos estos conceptos con mayor detalle.

Cadena de bloques de Bitcoin: contabilidad pública

Todos los miembros de la red Bitcoin comparten su libro mayor público, la *cadena de bloques*. Imagine un libro de contabilidad gigante con páginas que enumeran una serie de transacciones. Una nueva página que contiene las últimas transacciones de Bitcoin enviadas por pagadores de todo el mundo se agrega aproximadamente cada 10 minutos. Este libro gigante está constantemente disponible en Internet para quién ejecute el software Bitcoin. Tenga en cuenta que los programas de software llamados Bitcoin *wallets* (monederos) pueden ejecutarse en *smartphones* u ordenadores personales y permiten al usuario realizar pagos a través de la red Bitcoin.

En el contexto de Bitcoin, las páginas que forman el libro mayor se llaman *bloques* porque representan "bloques" de datos. La cadena de bloques, compuesta por muchos bloques individuales, crece constantemente en longitud

y abarca todas las transacciones realizadas en Bitcoin desde su lanzamiento en enero de 2009.

Una solicitud de transacción Bitcoin contiene lo siguiente:

1. La dirección Bitcoin del pagador, que contiene la fuente de fondos para el pago,
2. La dirección de Bitcoin del receptor (receptor del pago) y
3. La cantidad de bitcoins que han sido transferidos.

Dado que la cadena de bloques contiene todo el historial de pagos salientes y entrantes asociados con la dirección Bitcoin del pagador, los mineros, que también gestionan la red Bitcoin, pueden validar que el pagador tiene fondos suficientes para cubrir el pago. En cualquier momento, cualquiera puede ver la cantidad de bitcoins vinculados a (o, de forma abstracta, mantenidos en) en una específica dirección de Bitcoin. Compruébelo usted mismo. Vaya a *blockchain.info* e introduzca la siguiente dirección:

1GaMmGRxKCNuyymancjmAcu3mvUnVjTVmh

En "Buscar", se devolverá el número de bitcoins asociados a esta dirección.

Aunque la identidad del propietario no puede ser conocida desde su dirección de Bitcoin sin que él haya proporcionado esta información, cualquier transferencia dentro y fuera de su cuenta, así como su saldo actual, están a disposición del público para su visualización.

Encriptación asimétrica: Quien puede gastar esos bitcoins

Las claves de encriptación están asociadas a una transacción como la descrita anteriormente. Bitcoin emplea un sistema de cifrado asimétrico (también conocido como criptografía de clave pública), denominado así porque el algoritmo cifrado requiere un par de claves, cada una de las cuales consta de una larga serie de dígitos. Una es pública y controla la operación de

descifrado, mientras que la otra, la clave privada, gobierna la operación de cifrado, o viceversa.

Es fácil para el algoritmo crear una clave privada y derivar su correspondiente clave pública. Sin embargo, determinar una clave privada a partir de la clave pública correspondiente es inviable desde el punto de vista computacional, lo que permite que la clave pública, como su nombre lo indica, se haga pública. Con la clave pública, el beneficiario puede recuperar la información de la transacción, permitiendo la transferencia de bitcoins a procesar. La siguiente figura 2 ilustra conceptualmente el sistema de doble llave de Bitcoin, que proporciona parte de la base para el funcionamiento de Bitcoin.

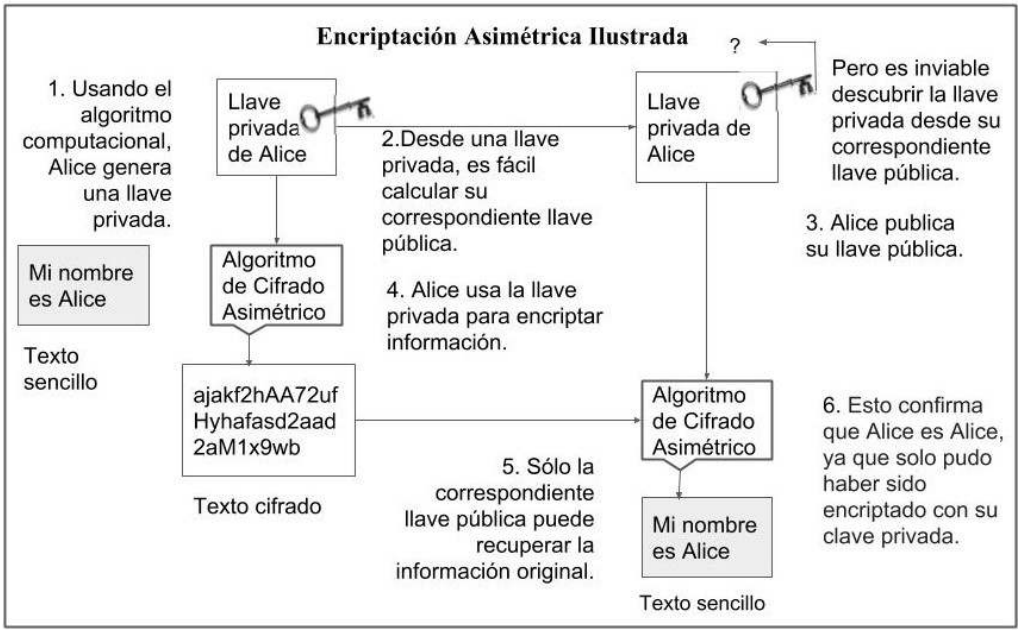


FIGURA 2: ENCRIPTACIÓN ASIMÉTRICA ILUSTRADA

El algoritmo del software Bitcoin sólo permite al propietario de la clave privada "gastar" bitcoins asociados a esa dirección Bitcoin. El receptor, o beneficiario, comparte su dirección de Bitcoin con el pagador. Puesto que sólo el destinatario conoce la clave privada vinculada a su dirección, sólo él podrá acceder, gastar o transferir esos bitcoins más tarde.

Dentro de Bitcoin, un remitente firma digitalmente una transacción de Bitcoin con su clave privada. Las transacciones de Bitcoin contienen realmente la clave pública (suponga que ésta es la dirección de Bitcoin por ahora). Utilizando esta clave pública, el sistema verifica que la firma digital es válida y, por lo tanto, confirma que el remitente es el propietario de la clave privada. Este sistema permite al propietario "gastar" los bitcoins asociados a su dirección Bitcoin en el libro público mayor, y el libro público mayor (es decir, la cadena de bloques) se actualizará con una nueva página (es decir, bloque) conteniendo esta transacción. La incorporación de esta nueva transacción a la cadena de bloques le indica a la red de Bitcoin que debe abonar esos bitcoins a la dirección del destinatario y restarse de la dirección de Bitcoin del remitente. Las claves privadas se componen de una larga serie de dígitos almacenados y administrados por *monederos* Bitcoin protegidos con contraseña (es decir, software en el ordenador del usuario, dispositivo móvil u otra aplicación web).

UNA RED DE MINEROS QUE ACTÚA COMO ACUÑADORES, CONTABLES Y REGULADORES DEL SISTEMA

Hasta ahora, hemos hablado de cómo se ven las transacciones y cómo son validadas. Si Bitcoin fuera un sistema operado centralmente, la historia podría terminar aquí: una sola entidad sería responsable de esta tarea. Sin embargo, Bitcoin es un sistema descentralizado y, como tal, esta tarea se comparte entre un conjunto de nodos (mineros) que participan voluntariamente distribuidos por todo el mundo. Entender cómo un sistema que incluye la contabilidad y la autorización de transferencia de pagos puede ser operado por diferentes entidades, de tal manera que se apoye en sus propios intereses personales, es esencial. Esta característica del sistema es una de esas claves que hay que comprender y a la que aludí antes como una que a menudo se les escapa a los críticos de Bitcoin.

Los mineros, los nodos responsables de operar la red Bitcoin, verifican que las transacciones son válidas y actualizan la cadena de bloques con nuevos bloques que consisten en las últimas transacciones de forma regular. El

software de Bitcoin que los mineros ejecutan en sus ordenadores personales incorpora el protocolo Bitcoin con su conjunto de reglas y acuerdos.

En general, la red Bitcoin requiere que la cadena de bloques (libro público mayor) se actualice continuamente con la incorporación de nuevos bloques (páginas en el libro de contabilidad). Aproximadamente cada 10 minutos, se añade un nuevo bloque con la lista de las últimas transacciones. Aunque todos los mineros están trabajando en el siguiente bloque, sólo se seleccionará uno para añadir su versión específica del bloque a la cadena de bloques. De hecho, cada minero está operando en su propio interés cuando crea su propia versión de este siguiente bloque y, por lo tanto, recauda personalmente las comisiones de transacción, así es como acumula las recompensas asociadas a ese bloque de transacciones. Aunque los parámetros básicos de las transacciones de Bitcoin son inalterables (pagador, beneficiario, importe), la mayoría de ellos incluyen comisiones de transacción, desembolsadas por el pagador y que deben abonarse en la cuenta del minero cuyo bloque se selecciona para incorporarlo a la cadena de bloques. Por lo tanto, este minero actualizará cada una de estas transacciones y reclamará los honorarios asociados a esas transacciones para recibirlos en su propia dirección de Bitcoin.

Además de los honorarios de transacción, los mineros cuyos bloques se agregan a la cadena de bloques también ganan pagos adicionales de los nuevos bitcoins acuñados. Crean una transacción extra que se añade a sus propias cuentas de bitcoin. Esto se llama recompensa de bloque. Actualmente, el protocolo de Bitcoin permite a los mineros asignarse 12.5 nuevos bitcoins por bloque creado (25 bitcoins en la fecha de edición en Inglés de este libro). Esto se suma a las comisiones de transacción. Inicialmente, en el lanzamiento de Bitcoin, 50 bitcoins (BTC) fueron asignados como la recompensa de bloque por cada bloque, que se reduce a la mitad aproximadamente cada cuatro años.

Con los nuevos bitcoins acreditados en su dirección, el minero cuya versión del bloque es seleccionada para su inclusión en la cadena de bloques se beneficia claramente de encontrar una solución antes que sus compañeros mineros. En breve se explicará cómo funciona este proceso de selección. Por el momento, sin embargo, lo ven como la solución de un problema matemático ejecutando una tarea de computación muy costosa. La solución es difícil de encontrar, pero, una vez encontrada, su exactitud es fácil de verificar. El primer

minero que encuentre la solución a su bloque puede publicar esta versión en toda la red de mineros.

Estos mineros reciben el bloque y su solución, y luego trabajan para autenticarlo y validarlo, es decir, certificar que la solución encontrada por el primer minero del bloque es correcta. El protocolo Bitcoin establece la dificultad del problema de tal forma que se requiere un promedio de unos 10 minutos para encontrar la solución.

Si el minero que resuelve el bloque trata de adjudicarse a sí mismo más de los 12.5 nuevos bitcoins permitidos actualmente, los otros mineros rechazarían el bloque del minero y seguirían trabajando en la búsqueda de la solución para sus propias versiones de bloque. Cada bloque es ligeramente diferente, y, por lo tanto, cada uno tiene una solución diferente.

Aunque no parece muy intuitivo, cuando un minero resuelve la tarea de computación y resuelve un bloque, todos los demás mineros aceptan la derrota e incluyen ese bloque como el siguiente en la cadena de bloques, siempre que pueda ser validado, y comienzan a trabajar en el bloque siguiente. Este trabajo implica que, cada minero agregue en un nuevo bloque todas las transacciones más recientes que han llegado desde la creación del bloque anterior, las cuales a su vez serán resueltas y añadidas a la cadena sucesiva de bloques.

La forma en que opera Bitcoin explica por qué el minero que fue el primero en llegar a una solución, se acreditará a sí mismo la cantidad de recompensa por bloque permitido por el protocolo Bitcoin. Así, se asegura la aceptación de su bloque por parte de los otros mineros y la recepción de sus recompensas asociadas (por ejemplo, las comisiones de transacción). De la misma forma, los otros mineros no consiguen ninguna ganancia rechazando el bloque, aunque sea válido. El sistema de pago de Bitcoin mantendrá su valor sólo cuando funcione correctamente. Si los mineros rechazaran todos los bloques, excepto los propios, no se alcanzaría un consenso, el valor del sistema en general se destruiría y, ninguno de los mineros se beneficiaría. En tal caso, cualquier cantidad de bitcoins que los mineros posean perdería su valor. Por lo tanto, todos los mineros se benefician si todos respetan el protocolo Bitcoin establecido en el software compartido de Bitcoin. Así, Bitcoin encarna lo inverso de la tragedia de los comunes descrita anteriormente.

Ahora vamos a profundizar en los detalles antes descritos, como la costosa tarea informática que es necesaria para resolver el problema matemático de un bloque. Para que un minero tenga su bloque seleccionado, tiene que haber resuelto un problema asociado con el bloque. Este proceso de selección se llama "prueba de trabajo", ya que implica que el minero tuvo que trabajar para ello. Para comprender plenamente el mecanismo involucrado, primero necesitamos entender un concepto criptográfico conocido como *función hash*. Entonces, podemos explicar cómo este concepto es usado en el contexto de la prueba de trabajo de un minero.

FUNCIÓN CRIPTOGRÁFICA HASH – "UNA HUELLA DIGITAL"

El hash criptográfico es un algoritmo complejo que realiza una tarea muy básica: transformar un texto de longitud arbitraria (un libro entero, un documento, una oración o incluso, una sola palabra) en una cadena de números de longitud fija que parece aleatoria. La figura 3 siguiente muestra algunos ejemplos. La salida de una función hash, o simplemente hash, es llamada, por lo general, el mensaje resumen y puede ser considerada la "huella dactilar" del documento.

En la figura siguiente, tenga en cuenta que la entrada "Hay 2 perros en el patio trasero" conduce a un resultado completamente diferente que "Hay 3 perros en el patio trasero". El simple cambio de un carácter conduce a un resultado con todos los dígitos completamente diferentes. Los resultados de salida de esta figura se expresan en números hexadecimales. A diferencia del sistema decimal que usamos comúnmente, el sistema hexadecimal tiene una base de 16. Emplea dieciséis símbolos para representar los dieciséis números en el sistema. Los símbolos del "0" al "9" representan los números del "0" al "9", y las letras de la "A" a la "F" representan los números del "10" al "15". Así, el hexadecimal "F" representa el número "15". Por lo tanto, el número hexadecimal 5A36 equivale por lo tanto a $(5 \times 16^3) + (10 \times 16^2) + (3 \times 16^1) + (6 \times 16^0)$, lo que equivale, en el sistema de numeración decimal, a 23.094. Experimenta cambiando de Hex a Dec en la calculadora de tu propio ordenador para ver cómo funciona.

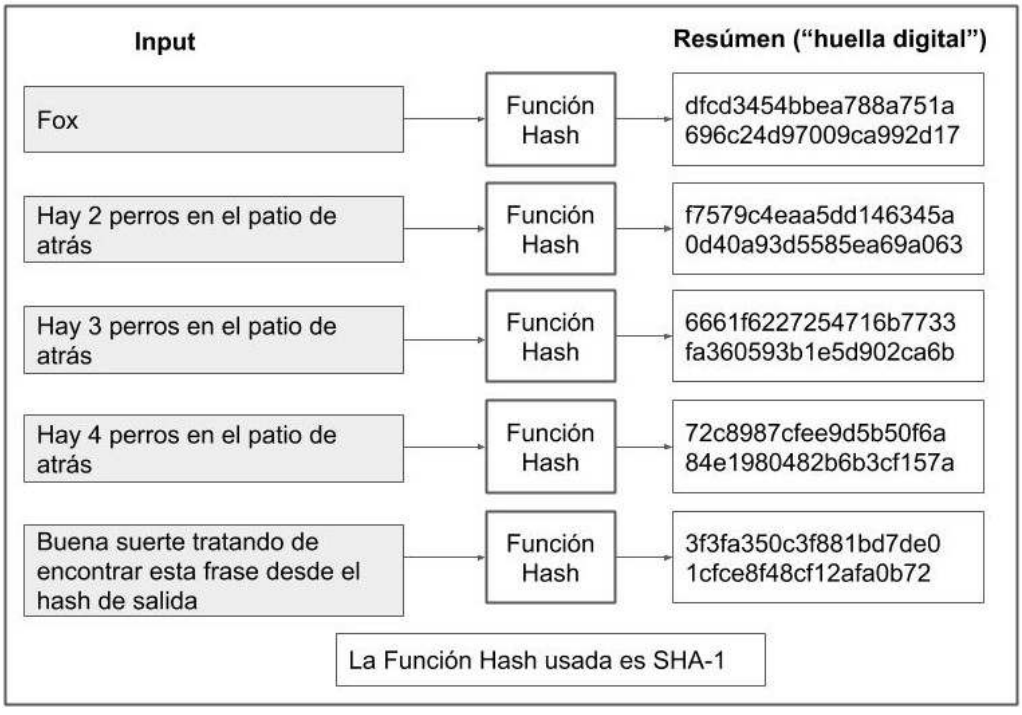


FIGURA 3: EL ALGORITMO HASH EN ACCIÓN

Un usuario de Bitcoin no tiene control sobre el resultado que tendrá la salida (el resumen de la Figura 3). Además, teniendo en cuenta esto, es casi imposible encontrar una entrada que la genere. Por lo tanto, es fácil generar un resumen, pero es imposible averiguar el texto original a partir del resumen. Utilizando la analogía de la huella dactilar humana, dada una sola huella dactilar, nos resultaría imposible identificar a la persona que la dejó, a menos que se le hubieran tomado las huellas dactilares de antemano.

Antes mencionamos que todos los mineros pueden verificar fácilmente que una solución es correcta una vez que se ha encontrado, pero que encontrarla es la parte difícil. Por eso el hash criptográfico es ideal para el propósito de Bitcoin. Los mineros, en sus intentos por resolver un bloque, tienen que reproducir un patrón específico mostrado por el contenido del resumen. Dado que es imposible reproducir una salida específica dentro del resumen, deben incrementar un dígito en el texto y recalcular el hash una y otra vez, hasta que encuentren el patrón específico en el resumen que requiere el

protocolo Bitcoin. Este proceso es análogo a la variación del número de perros ("2 perros","3 perros","4 perros") en el ejemplo de la Figura 3 para crear resúmenes diferentes. Por ejemplo, digamos que el protocolo Bitcoin actual especificó que el contenido del resumen muestra un patrón que comienza con "00". Variando el número de perros en el ejemplo, el número hexadecimal correspondiente en el resumen eventualmente va a satisfacer este requisito, indicando una solución al bloque.

Los mineros que buscan la solución por lo general deben calcular el hash millones de veces para encontrar el patrón correcto, pero sólo se necesita un único cálculo de hash por parte de otros mineros para validarlo una vez que se encuentra.

El algoritmo hash de Bitcoin, que crea el contenido del resumen a partir del texto de entrada, hace posible el sistema descrito anteriormente. Por lo tanto, una función ideal criptográfica de hash tiene cuatro propiedades principales[1]:

- *El cálculo del valor de hash correspondiente a un mensaje dado es sencillo.*
- *Generar un mensaje que tenga un determinado hash es imposible.*
- *Modificar un mensaje sin cambiar el hash es imposible.*
- *Encontrar dos mensajes diferentes que tengan el mismo hash es imposible.*

El siguiente ejemplo, tomado de Wikipedia, ilustra la función hash en uso.

Alice le plantea un problema matemático difícil a Bob y dice que lo ha resuelto. A Bob le gustaría intentarlo él mismo, pero también le gustaría asegurarse de que Alice no lo está engañando. Por lo tanto, Alice anota su solución, calcula su hash y le dice a Bob el valor del hash (mientras mantiene en secreto la solución). Entonces, cuando Bob llega con la solución unos días

[1] http://en.wikipedia.org/wiki/Cryptographic_hash_function

después, Alice puede probar que ella tenía la solución más temprano revelándola y, teniendo Bob el hash del resultado, puede comprobar que coincide con el valor de hash que se le dio antes. (Este es un ejemplo de un simple esquema de transacción; en la práctica, Alice y Bob serán programas de computadora, y el secreto sería algo menos fácil de falsificar que una supuesta solución de rompecabezas).

Las funciones hash forman parte del proceso que permite a los usuarios firmar digitalmente un documento o texto en Bitcoin. En el contexto del trabajo de prueba de Bitcoin, que se discutirá a continuación, las dos características más útiles de las funciones hash son las siguientes:

- La imposibilidad de generar un mensaje desde un determinado hash.
- Se genera un hash completamente nuevo cambiando sólo un carácter en el mensaje

Se han creado varios tipos de algoritmos hash y Bitcoin utiliza dos de ellos: SHA-256 para la prueba de trabajo y RIPEMD-160 para la dirección de Bitcoin. La función hash es el corazón de la prueba de trabajo, que discutiremos a continuación.

PRUEBA DE TRABAJO DEL MINERO

En cualquier momento dado, cada minero participa activamente en la creación del siguiente bloque que se agrega a la cadena de bloques resolviendo un problema difícil, llamado prueba de trabajo. El primer minero que resuelve la prueba de trabajo es recompensado con bitcoins recién acuñados (12.5 bitcoins a la publicación de la versión digital en español de este libro) y las comisiones acumuladas en las transacciones realizadas en el bloque que está siendo creado. Las comisiones de transacción, normalmente un importe nominal, son añadidas por los pagadores cuando envían sus transacciones. Alrededor del año 2140, todos los bitcoins habrán sido minados y los mineros serán recompensados únicamente con las comisiones de transacción.

La prueba de trabajo puede pensarse, por tanto, como una carrera entre mineros bitcoin para descubrir el hash SHA-256 del bloque que intentan crear y que tendrá una cierta característica. Como vimos anteriormente, la producción del hash es simplemente un número muy grande expresado en hexadecimal. El objetivo del minero, el problema que debe ser resuelto, es generar una producción de hash inferior a un valor determinado. El primer minero que calcule un valor con esta característica gana, y su versión del bloque, una vez validado por los otros mineros, será agregado a la cadena de bloques discutida anteriormente en este capítulo.

Para simplificar, imagine que el hash de salida es, en realidad, un número entre 0 y 1.000.000, y que el primer minero en obtener un hash de salida inferior a 10.000 gana. Los 10.000 actúan como el umbral, y cada bloque dentro de Bitcoin contiene un número cuyo único propósito es obtener ese umbral.

El número dentro del bloque Bitcoin que se prueba contra el valor límite se conoce como "nonce". Cada minero incrementa su nonce en una cierta cantidad hasta que el hash de salida para su bloque está por debajo del umbral establecido. Como dijimos anteriormente, cada bloque del minero tiene información diferente y por lo tanto un hash de salida diferente para el mismo "nonce". Este proceso se ilustra en la Figura 4.

El protocolo Bitcoin, operado por el software que se ejecuta en el ordenador de cada minero, ajusta el nivel de dificultad del problema para que tarde unos 10 minutos en ser resuelto por el primer minero. El propósito es tener la cadena de bloques actualizada regularmente con un nuevo bloque que contenga las últimas transacciones enviadas durante los 10 minutos anteriores. Este valor es un tanto arbitrario y, como se verá en capítulos posteriores, Satoshi dedicó algunas de sus discusiones a este tema.

La discusión anterior comparó el nonce con un umbral. Debido a que los números del hash, llamados prueba de trabajo, están en un sistema de numeración hexadecimal, o base 16, esto se traduce en que el primer número X de bytes es el dígito 0, donde X se ajusta periódicamente para mantener el nivel de dificultad de la prueba de trabajo bastante constante.

Por ejemplo, suponga que el bloque #282.435 de la cadena de bloques tiene la siguiente salida SHA-256:

0000000000000000000c6647dad26b01b28f534343450d75d3b6b6b2882855039b673

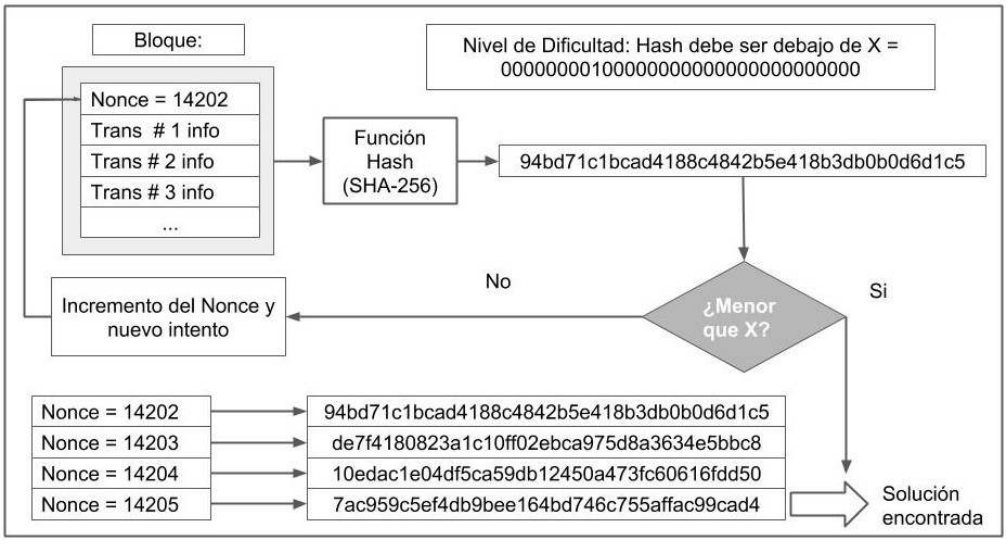


FIGURA 4: PRUEBA DE TRABAJO ILUSTRADA

Recuerde que en el sistema numérico de base 16, hay símbolos que representan los dieciséis números del 0 al 15; los símbolos que representan del 0 al 9 en este sistema son del 0 al 9 como en el sistema decimal, o base 10, y los números del 10 al 15 del sistema hexadecimal están representados por la A a la F. El número hexadecimal anterior está compuesto de 64 dígitos. Dado que los términos a la izquierda en un número hexadecimal representan potencias superiores de 16 y, por lo tanto, números mayores, para que el hash de salida sea menor, los dígitos principales dentro del hash de salida deben ser 0. Esta es la razón por la que el indicar que el hash de salida requiere estar por debajo de cierto umbral se traduce en que cierto número de dígitos a la izquierda son 0. Visto de cualquier manera, la prueba de trabajo es encontrar un valor para el nonce que genera un hash de salida por debajo del umbral establecido por el protocolo Bitcoin en ese momento.

En el ejemplo ilustrado en la Figura 4 -Prueba de trabajo ilustrada-, sólo

con los primeros dieciséis dígitos de la salida que igualan a 0, el hash de salida podría caer por debajo del umbral establecido por el protocolo de Bitcoin. Por lo tanto, el minero que obtuvo este número primero -y así "ganó" ese bloque- tuvo que seguir cambiando el número "nonce" hasta que se generó un número hexadecimal que tenía al menos el número deseado de 0s delante. Al igual que en una lotería, los mineros que compran la mayoría de los "tickets" (es decir, que generan la mayoría de los números de salida del SHA-256) tienen más posibilidades de encontrar un número con el número correcto de 0s. Este requerimiento del sistema Bitcoin ha llevado a una carrera para crear hardware capaz de generar más hashes por segundo. El afortunado minero que primero descubrió el hash del bloque #282.435 de la cadena de bloques incrementó el nonce a 505.482.605 indicado en decimal, lo que significa que este minero tuvo que generar más de 500 millones de hashes antes de encontrar uno con el número correcto de ceros anteriores.

Como se mencionó anteriormente, el objetivo del protocolo Bitcoin es tener un bloque de transacciones creado aproximadamente cada 10 minutos. Para un nivel de dificultad dado, si más mineros se unen -o, mejor dicho-, cuantos como más hashes son calculados por segundo, las posibilidades de descubrir el resumen requerido (hash de salida) en menos de 10 minutos aumentan. Después de un cierto número de bloques, el protocolo Bitcoin evalúa lo rápido se están generando los bloques; si en promedio son menos de 10 minutos, el nivel de dificultad se incrementa (es decir, el número de ceros a la izquierda aumenta, disminuyendo la probabilidad de que un solo minero obtenga un resumen que tenga esa característica); si toma un tiempo mayor, la dificultad disminuye (es decir, el número de ceros a la izquierda disminuye aumentando la probabilidad de obtenerlo).

Una vez que un minero descubre un nonce con el correcto hash de salida, el bloque es transmitido y otros mineros lo verifican, lo aceptan, y comienzan a trabajar en el siguiente bloque. Por lo tanto, Bitcoin funciona como un juego de lotería en curso que se reinicia cada 10 minutos. ¿Quién será el afortunado minero que encontrará un nonce con las características correctas?

La figura 5 ilustra el concepto detrás de la prueba de trabajo. Nótese que hay más información en los bloques que la que se muestra; se ha reducido por simplicidad.

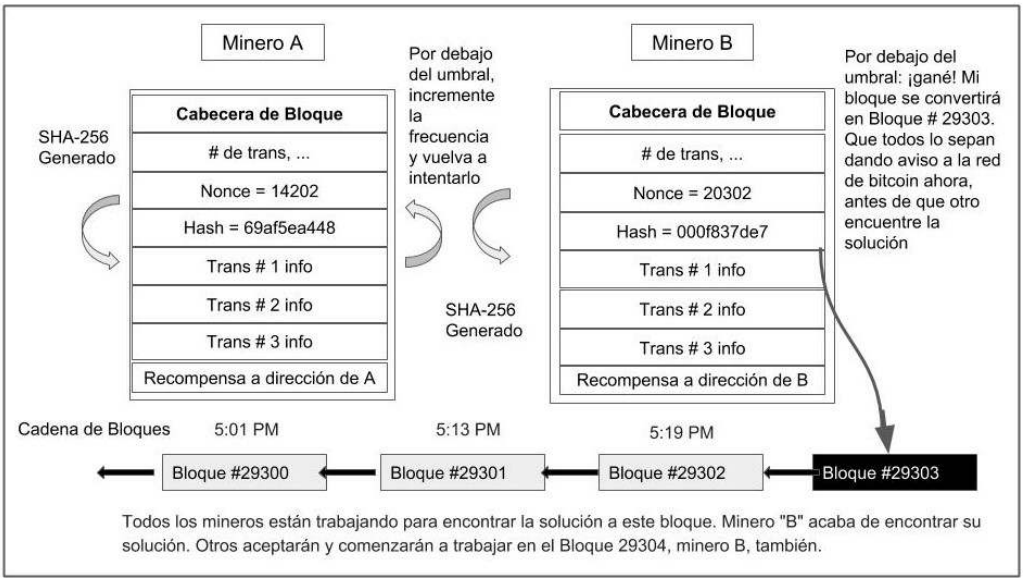


FIGURA 5: GANADOR DE LA PRUEBA DE TRABAJO

Consenso de mineros y bloques huérfanos

Como se ha dicho anteriormente, Bitcoin se apoya en gran medida en el consenso para funcionar. Este concepto, que se discutirá más adelante en el capítulo 9, entra en juego cuando dos mineros resuelven sus bloques más o menos al mismo tiempo. Cuando esto ocurre, los dos mineros emiten sus bloques incluyendo sus soluciones a través del sistema Bitcoin. Todos los demás mineros reciben y retienen ambos, pero su trabajo para generar el siguiente bloque se basará en cuál de estos dos bloques recibieron primero. Digamos que el 50% de los mineros reciben primero el bloque del Minero A y los demás reciben primero el bloque de Minero B. Esta situación se ilustra para el bloque #29302 en la Figura 6 abajo.

Esta situación es análoga a una carrera en el tiempo suplementario. Cuál de los dos bloques llega a ser parte de la verdadera cadena de bloques dependerá de cuán rápido se resuelva el siguiente bloque y por quién, si por un minero que recibió el bloque de A o por uno que recibió el bloque de B. En este punto, existen dos versiones de la cadena de bloques, con la mitad de los

mineros dando por buena la versión del bloque #29302 del minero A y la otra mitad, la versión del minero B. Cuál de estas dos versiones sobrevivirá

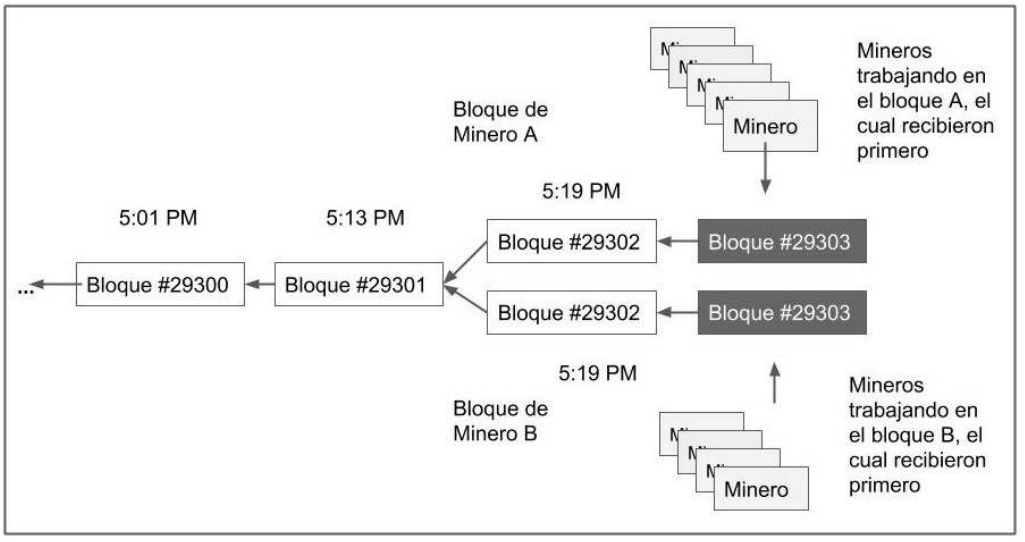


FIGURA 6: UNA DIVISIÓN DE BLOQUES

depende de la versión elegida por el minero que resuelve el siguiente bloque, #29303 en la Figura 6, en su computadora. Cuando se resuelve el bloque #29303, esta versión de la cadena de bloques se convierte en la más larga de las dos y por lo tanto la oficial. Todos los mineros dejan la otra versión de la cadena de bloques, y entonces se convierte en lo que se conoce como un bloque huérfano. Este proceso se ilustra en la Figura 7.

¿Por qué funciona el Bitcoin?

Hasta ahora hemos cubierto cómo funciona Bitcoin, pero no por qué. Para entender esto, es necesario conocer algunos conceptos adicionales, por ejemplo, qué es un programa informático de código abierto. Estos conceptos los citamos y explicamos a continuación:

- Bitcoin es un *software de código abierto.*

- El software de Bitcoin establece *las directrices operativas* que deben seguir los mineros y clientes de los monederos.
- El software de Bitcoin también define y opera un *protocolo de comunicación.*
- *Compartir archivos distribuidos* de la cadena de bloques permite la contabilidad abierta.

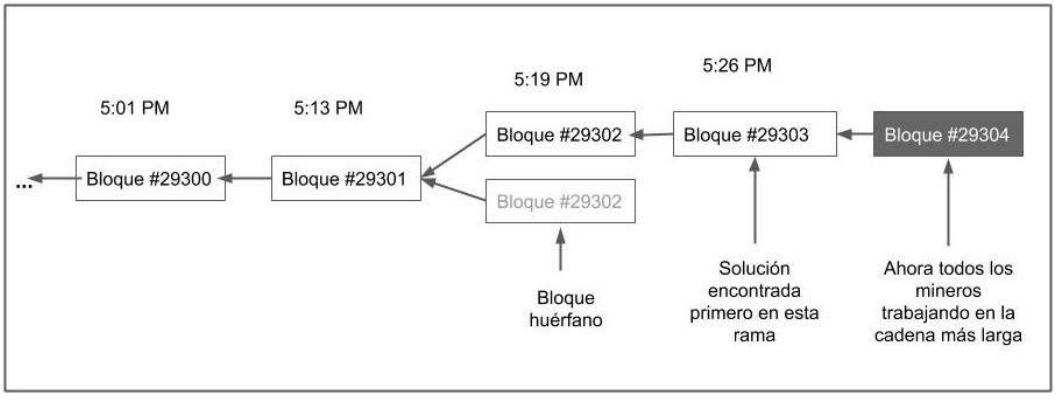


FIGURA 7: LA CADENA MÁS LARGA GANA

El software de código abierto es un software informático cuyo código fuente está disponible para que cualquiera lo pueda ver. Además, opera bajo una licencia especial que permite a cualquiera modificarlo y usarlo. Con el código fuente, un programador puede recrear el programa (el archivo binario que se ejecuta en las computadoras) y modificarlo a voluntad. De este modo, han surgido muchos imitadores de Bitcoin como otras monedas virtuales que se diferencian de él sólo cosméticamente y, en su mayor parte, no incorporan innovaciones significativas, con la excepción de muy pocos como Namecoin. La mayoría de estas monedas virtuales alternativas se basan en el cambio de velocidad en la que se crean los bloques, el número total de monedas en circulación y el algoritmo criptográfico de hash utilizado.

El código de un software que es de código abierto permite a un experto analizarlo y validar su integridad, es decir, confirmar que hace lo que pretende hacer. Un ejemplo prominente de software de código abierto es Linux, que ha desplazado a Microsoft Windows en cuota de mercado en la industria de

servidores. Debido a que es de código abierto, los problemas son encontrados y corregidos mucho más rápidamente que de tratarse de una marca registrada, ya que la multitud de programadores están continuamente examinando y mejorando el código. Linux ha demostrado hasta ahora que el bien mayor y el interés propio puede funcionar de forma combinada, al menos con respecto a la gestión del programa informático de código abierto. Esta franqueza asegura un alto nivel de integridad no alcanzable en software privado, donde sólo la reputación de la empresa responsable del programa informático garantiza que hace lo que debe hacer.

Bitcoin también opera a través de Internet utilizando un protocolo definido de operaciones que los mineros y clientes de carteras deben seguir. Las carteras cliente -programas de software que son aplicaciones en smartphones o programas en ordenadores personales- son las que se utilizan cuando alguien está enviando una transacción de pago, que los mineros validan antes de ser incorporados a la cadena de bloques. Un solo minero que se desviara del protocolo vería su operación rechazada por el resto de los mineros y no se le permitiría contribuir a la operación de la red.

Un argumento típico planteado en contra Bitcoin es sobre el límite del número máximo de bitcoins que serán creados, que Satoshi Nakamoto fijó en 21 millones. Una vez alcanzado, ¿qué puede impedir que alguien aumente este límite? Nada en realidad, pero necesitaría la cooperación de la mayoría de los mineros para que este cambio fuera aceptado. Incluso si la mayoría de los mineros aceptaran levantar esta restricción, los que no estuvieran de acuerdo, producirían una ruptura en la cadena de bloques. Los que estén a favor de levantar la restricción usarían una versión de la cadena de bloques, mientras que los que no usarían una versión diferente. En efecto, podríamos tener dos monedas virtuales en lugar de una, el "Bitcoin original" y un "*Quantitative Easing Bitcoin*" (expansión cuantitativa de Bitcoin). A largo plazo, uno mantendría su valor mejor y durante más tiempo y, por lo tanto, se convertiría en la versión preferida, mientras que el otro perdería valor. ¿Cuál sería el que mantendría su valor por más tiempo y retendría el interés de los usuarios de Bitcoin? Personalmente, tengo una buena idea de cuál sería.

La comunidad de desarrollo de Bitcoin es muy conservadora con respecto a los cambios y, al menos hasta ahora, el medio preferido para introducir cambios importantes ha sido la creación de nuevas monedas virtuales, algunas

de las cuales no tienen límites en cuanto a la generación del número de monedas.

Una característica final que sostiene a Bitcoin es que, no sólo es software de código abierto, sino que también lo es su contabilidad. Algunos han llamado a la cadena de bloques "contabilidad de triple entrada" porque revoluciona la contabilidad. Cualquiera puede inspeccionar la cadena de bloques y verificar que la contabilidad sigue los requisitos y especificaciones actuales del protocolo Bitcoin. El uso compartido de archivos distribuido de la cadena de bloques significa que cualquier persona que ejecute el software Bitcoin está conectada a la red de Bitcoin y tiene acceso a la cadena de bloques.

Para obtener una mayor comprensión del brillante concepto de la base conceptual de Bitcoin, recomiendo encarecidamente leer el *white paper* de Satoshi Nakamoto. La información que proveo en este espacio debería hacer el documento más accesible. Al final de este libro se incluye una reproducción del documento de Nakamoto.

http://bitcoin.org/bitcoin.pdf

Esperamos que este capítulo le haya ayudado a entender los principales conceptos. Ahora debería ser capaz de leer el documento de Bitcoin y el resto de este libro con mayor facilidad.

IMPLICACIONES DEL BITCOIN

El impacto de Bitcoin como sistema monetario es tremendo. Una ventaja es la capacidad que le da a la gente para "transferir" dinero a través de todo el planeta de manera tan simple como es enviar un correo electrónico. Esto es particularmente ventajoso para los trabajadores inmigrantes que desean enviar dinero a sus familiares en sus países de origen. En contraste, las compañías que envían dinero en remesas internacionales cobran altas comisiones por hacerlo. Hay cargos asociados con la conversión de monedas nacionales a BTC y

viceversa, pero estos cargos de conversión son pequeños en comparación con los costos de estos giros.

Otro beneficio se refiere a las compras y donaciones por internet. Confío en que el sistema actual de pago con tarjeta de crédito cambiará completamente en el futuro. Los pagos con tarjeta de crédito requieren dar amplia información sobre el pagador, incluyendo la dirección de facturación y el código de 3 dígitos en la parte posterior de las tarjetas de crédito. En esencia, este es el equivalente de Bitcoin en dar sus claves de encriptación privadas al comerciante. El alto número de fraudes resultantes de esta debilidad de seguridad se ha manifestado por sí mismo en forma de altas tarifas y contra cargos con los que los comerciantes tienen que lidiar a diario. Las compañías de tarjetas de crédito destinan una gran cantidad de dinero cada año para hacer frente a estos fraudes. Estos costos se transfieren a los comerciantes, quienes, a su vez, los transfieren a los consumidores y se materializan en precios más altos por los bienes y servicios.

Otro impacto importante de Bitcoin es en el sistema monetario, por ser capaz de crear un nuevo sistema de ser dinero y no limitarse a ser sólo una moneda. Una moneda tiene las siguientes propiedades:

- Es un medio de intercambio (utilizado como intermediario en el comercio)
- Es una unidad de cuenta (se puede contar, es cuantificable)
- Es perdurable (duración larga)
- Es divisible (para tener unidades más pequeñas)
- Es portátil (para ser fácilmente transportable)
- Es fungible (mutuamente intercambiable, 1 unidad de un valor específico puede reemplazar a otra unidad idéntica)

El dinero tiene todas las propiedades listadas arriba y, además, una más:

- La capacidad de preservar su valor a largo plazo.

A diferencia del dinero, una moneda está sujeta a la inflación. A principios de los 1900s, la inflación se definía simplemente como la acción de inflar algo, como en el caso de una moneda, imprimiendo más unidades de ella. El diccionario actual lo define como un aumento general de los precios. Sin

embargo, el aumento de los precios es un síntoma de la devaluación de la moneda, que se produce cuando hay más unidades en circulación que antes. Es interesante, pero no sorprendente, que este cambio en la definición corresponda a un tiempo en el que las monedas de papel se han ido desligando cada vez más de patrones como el oro y la plata, y que nos ha llevado a un encarecimiento de los precios. Nuestros antepasados vieron, por ejemplo, que los precios de los alimentos permanecieron prácticamente inalterados a lo largo de sus vidas. Sin embargo, la población actual ha estado condicionada a ver el aumento de los precios como un hecho inmutable a lo largo de su vida, de la misma forma que actúa la ley de la gravedad. Es como si, en un lugar donde llueve todo el tiempo, nadie hubiera hecho la conexión entre las nubes y la lluvia. Pero ¿quién podría culparlos si nunca han visto un cielo azul? De la misma manera, la mayoría de la gente hoy en día no percibe que el aumento de los precios de los alimentos sea causado por la inflación monetaria porque, a veces, transcurren varios años para que el aumento de los precios se manifieste. Este ha sido el caso de la inflación monetaria de los años sesenta, que sólo se manifestó en la década siguiente, la de los setenta.

Para mantener su poder adquisitivo a largo plazo (es decir, no estar sujeto a la inflación), la oferta monetaria debe ser limitada. El oro y la plata han sido utilizados como dinero durante miles de años. Su suministro en este planeta es limitado y requiere que cualquiera que tenga la intención de adquirir estos metales tenga que emplear tiempo y energía para destinarlos a la minería. Se podría decir que el esfuerzo invertido en la minería de un metal precioso es análogo a la prueba de trabajo en el sistema Bitcoin. Compare este trabajo real con lo sencillo que es imprimir billetes de dólar. El papel moneda se adoptó inicialmente para actuar sólo como un sustituto conveniente (derivado) de los metales preciosos, facilitando así las transacciones. Las monedas de papel, al ser fácilmente reproducibles, siempre han estado sujetas a la inflación, ya que los orfebres -y más tarde los banqueros- utilizaban la reserva fraccionada para prestar más (es decir, imprimir más papel moneda), de lo que en realidad tenían respaldado por oro almacenado. Esto ha conducido a las frecuentes crisis y "corralitos bancarios" que ensucian los libros de historia.

Antes de la llegada de los ordenadores y las conexiones en redes, las transacciones se limitaban a metales preciosos y papel moneda. Desde entonces, las comunicaciones electrónicas han introducido una nueva forma de

realizar transacciones con las que el oro y la plata nunca han podido competir directamente. Hasta ahora, sólo existían monedas controladas por un ente central y transmisibles electrónicamente, lo que permitía a los controladores decidir libremente el tamaño de la oferta de la moneda subyacente. El Presidente Nixon lo demostró claramente cuando eliminó la convertibilidad del dólar en oro en los mercados de divisas. La guerra de Vietnam y la "gran sociedad" de Lyndon Johnson se financiaron diluyendo el dólar estadounidense en una imprenta electrónica. Tomó tiempo para manifestarse vía la subida de precios de los *commodities*, pero una vez que lo hizo, el precio del oro en dólares ha sido efectivamente más alto que el establecido de $ 35 por onza de oro que prevalecía antes de que el dólar dejara de estar asociado al patrón oro. Luego se convirtió en una moneda que libre flotación, de constante inflación, como cualquier otra moneda nacional existente en la actualidad.

Como se discute en el Capítulo 7, las monedas de papel (dinero FIAT) permiten a los gobernantes financiar el gasto deficitario robando el valor de la moneda en circulación. Los pobres y, en cierta medida, la clase media son los más afectados por la inflación monetaria, mientras que los ricos utilizan la deuda y diversos derivados financieros para adquirir empresas y bienes raíces comerciales que generan cuantiosos ingresos. Saben que la deuda se devaluará junto con la moneda, proporcionando una ganancia adicional obtenida artificialmente. La primera manera de abordar la "guerra contra la pobreza" es librarse de la inflación monetaria y volver a una forma de dinero cuyo valor se mantenga a largo plazo. Pero no espere que el gobierno proponga o incluso acepte una propuesta que apueste por esta medida.

Actualmente, muchos artículos de revistas y periódicos prescriben la naturaleza "deflacionaria" de Bitcoin como su principal aspecto negativo. Por deflación, significan que los precios medidos en BTC disminuirán. En realidad, ese es el beneficio principal de Bitcoin. El argumento esgrimido es que la gente va a "atesorar" bitcoins en lugar de gastarlos en la economía. En primer lugar, imagínese que mañana bitcoin fuera la moneda preferida de su país. Como ser humano, todavía tendría que comer y tener un lugar donde vivir; por lo tanto, tendrías que hacer estos dos gastos. Lo que los comentarios en estos artículos demuestran es un concepto erróneo sobre lo que es el dinero. Ahorrando en lugar de gastar, - "atesorar" es simplemente un término peyorativo para

“ahorrar”- la gente sólo retrasa el consumo a un momento posterior. Hemos visto este tipo de comportamiento exhibido recientemente por algunos de los llamados "millonarios bitcoin", quienes, en algún momento, se sienten lo suficientemente cómodos como para gastar algunos de sus bitcoins en artículos de lujo. En un sistema económico basado en dinero -moneda que mantiene su valor a largo plazo- los ahorradores no compiten por los recursos con fabricantes, constructores, fábricas y aquellos que extraen productos básicos (es decir, artículos comercializables) mediante el aplazamiento del gasto. Por recursos nos referimos a cualquier forma de energía, mercancías, tiempo y mano de obra, particularmente mano de obra especializada. Imagínese el caso de una persona que decide ahorrar quedándose en casa en lugar de enganchar su remolque y viajar a través del país de vacaciones. Al no viajar, permite que la gasolina que hubiera gastado en viajes sea utilizada por un fabricante para, por ejemplo, utilizar esos recursos para transportar materiales para la construcción de una nueva planta. Imprimir dólares no crea más barriles de petróleo, más gigavatios de electricidad o más horas en un día. He ilustrado este concepto con ejemplos bastante sencillos, pero espero que puedan ver que una moneda como Bitcoin, con la capacidad de mantener su valor, gracias a su limitada oferta, tiene importantes implicaciones.

En este capítulo, hemos cubierto la tecnología subyacente a Bitcoin, el software que lo hace posible y, hemos tocado una visión alternativa de la economía a la que el propio Satoshi Nakamoto probablemente estaba adherido. Ahora que usted tiene una buena comprensión de todo lo que es Bitcoin y cómo funciona, pase la página y conozca al creador de Bitcoin, ¡Satoshi Nakamoto!

3

El Primer Mensaje en la Lista de Correo de Criptografía

Traducción por **Iván Durán Fabeiro**

ESTE ES EL ANUNCIO DE SATOSHI NAKAMOTO sobre Bitcoin, el cual fue publicado en la lista de Correo de Criptografía, un foro para aquellos interesados en todo lo relacionado con la criptografía.

Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, sábado 01 de noviembre 2008, 16:16:33 -0700

He estado trabajando en un nuevo sistema electrónico de efectivo que es totalmente de peer-to-peer, sin terceros confiables.

El documento está disponible en:

http://www.bitcoin.org/bitcoin.pdf

Las principales propiedades:

- El doble gasto se previene con una red peer-to-peer.
- Sin Banco Central u otras partes de confianza.
- Los participantes pueden ser anónimos.
- Las nuevas monedas se crean de la prueba de trabajo estilo Hashcash.

- La prueba de trabajo para la nueva generación de monedas también impulsa a la red para evitar el doble gasto.

Bitcoin: Un Sistema de Dinero Electrónico Peer-to-Peer

Resumen. Una versión puramente peer-to-peer de dinero electrónico que permitiría que los pagos en línea se envíen directamente de una parte a otra sin tener que pasar por una institución financiera. Las firmas digitales proporcionan parte de la solución, pero los principales beneficios se pierden si un tercero de confianza es aún requerido para evitar el doble gasto. Proponemos una solución al problema de doble gasto utilizando una red peer-to-peer. La red marca el tiempo de las transacciones al tiempo que las va hasheando (hacer un resumen criptográfico), que va dentro de una cadena continua de prueba de trabajo basados en hashes, formando un registro que no puede modificarse sin rehacer la prueba de trabajo. La cadena más larga no solo sirve como prueba de la secuencia de eventos ocurridos, sino, como prueba de que proviene del mayor conjunto de potencia de CPU. Siempre que la mayor potencia de CPU esté controlada por nodos que no están cooperando para atacar la red, generarán la cadena más larga y superarán a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes se transmiten según el mejor esfuerzo, y los nodos pueden salir y unirse a la red a voluntad, aceptando la cadena de prueba de trabajo más larga como prueba de lo sucedido mientras ellos no estaban.

Documento completo en: http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

La Lista de Correo de Criptografía

4

Problemas de Escalabilidad

Traducción por **Iván Durán Fabeiro**

AQUÍ, SATOSHI RESPONDE a un comentario sobre la escalabilidad. Para realizar un pago, la billetera de un cliente debe tener la cadena de bloque completa, y con una cadena de bloques en constante crecimiento, se añadiría una carga de memoria en esa pequeña billetera del cliente. Este problema fue abordado por Satoshi en una versión posterior. Hoy en día, una aplicación de monedero en un smartphone puede realizar fácilmente las transacciones conectándose a un servidor de confianza que tenga la cadena de bloques completa.

Re: Artículo dinero electrónico Bitcoin P2P

Satoshi Nakamoto, domingo 02 de noviembre 2008, 17:56:27 -0800

James A Donald escribió:

Satoshi Nakamoto escribió:

He estado trabajando en un nuevo sistema electrónico de efectivo que es totalmente peer-to-peer entre personas, sin tercera parte

de confianza.

El documento está disponible en:
http://www.bitcoin.org/bitcoin.pdf

Necesitamos en gran medida tal sistema, pero por la forma en que entiendo su propuesta, no parece escalar al tamaño requerido.

Para que la transferencia de prueba de trabajo de los tokens tenga valor, deben tener valor monetario. Para tener valor monetario, deben de ser transferidos dentro de una red muy grande - por ejemplo, una red de intercambio de archivos similar a bittorrent.

Para detectar y rechazar un evento de doble gasto de manera oportuna, se debe tener la mayoría de las transacciones anteriores de monedas en la transacción, que, ingenuamente implementadas, requiere que cada punto tenga la mayoría de las transacciones pasadas, o la mayoría de las transacciones anteriores que ocurrieron recientemente. Si cientos de millones de personas están haciendo transacciones, eso es mucho ancho de banda, cada uno debe saberlo todo, o una parte sustancial del mismo.

Mucho antes de que la red llegue a ser tan grande como eso, sería seguro para los usuarios usar la Verificación Simplificada de Pago (sección 8) para verificar el doble gasto, que sólo requiere tener la cadena de los encabezados de bloque, o aproximadamente 12KB por día. Solo las personas que intentan crear nuevas monedas necesitarán ejecutar nodos de red. Al principio, la mayoría de los usuarios ejecutaría la red de nodos, pero a medida que la red crezca más allá de cierto punto, se dejaría cada vez más a especialistas con granjas de servidores de hardware especializado. Una granja de servidores solo necesitaría tener un nodo en la red y el resto de la LAN conectada con ese nodo.

El ancho de banda puede no ser tan prohibitivo como crees. Una transacción típica sería de unos 400 bytes (ECC es muy compacto). Cada transacción debe transmitirse dos veces, por lo que digamos 1KB por transacción. Visa procesó 37 mil millones de transacciones en el año fiscal 2008, o un promedio de 100 millones de transacciones por día. Esas muchas transacciones requieren 100GB de ancho de banda, o el tamaño de 12 DVD o 2 películas de calidad HD, o aproximadamente $ 18 en ancho

de banda a precios actuales.

Si la red llegará a ser tan grande, tomaría varios años, y para entonces, enviar 2 películas HD a través de Internet probablemente no parecería un gran problema.

Satoshi Nakamoto

La Lista de Correo de Criptografía

5

El Ataque del 51%

Traducción por **Jose Manuel Arenillas**

EN ESTE CORREO, Satoshi aborda un argumento sobre el llamado ataque del 51%. En esta situación, un minero o grupo de mineros podrían acaparar la mayoría del poder de cómputo (prueba de trabajo) para anular transacciones y realizar un doble gasto, para evitar que algunas transacciones se confirmen o evitar que uno o el resto de los mineros minen bloques válidos.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto lunes, 03 de noviembre 2008, 11:45:58 -0800

John Levine escribió:

> Satoshi Nakamoto escribió:
>
> Mientras que nodos honestos controlen la mayoría de potencia de CPU de la red, pueden generar la cadena más larga y superar a cualquier atacante.
>
> ---

Pero y si no lo hacen. Nodos deshonestos que regularmente controlan granjas de 100.000 máquinas infectadas o más. Gente que conozco administran listas negras de máquinas infectadas que envían spam y a menudo ven un millón de nuevas infecciones al día.

> Esta es la misma razón por la que hashcash no puede funcionar en el Internet de hoy en día. Los buenos tienen considerablemente menos poder de cómputo que los malos.

Gracias por referirte a este punto.

No hice esa afirmación con la firmeza que requería. El requisito es que los buenos, colectivamente, tengan mayor potencia de CPU que cualquier atacante único.

Podría haber muchas granjas pequeñas de máquinas infectadas que no son lo suficientemente grandes como para superar en poder de cómputo a la red, y todavía podrían hacer dinero generando bitcoins. Entonces, las granjas más pequeñas son los "nodos honestos". (Necesito un mejor término que "honestos"). Cuantas más granjas pequeñas participen en generar bitcoins más alta es la potencia necesaria para superar a la de la red. Montando granjas mayores, también serían demasiado pequeñas como para superar la potencia de la red, para que también generen bitcoins. De acuerdo con la teoría de "la cola larga", las pequeñas, medianas y grandes granjas unidas sumarán más potencia que la mayor granja de equipos infectados.

Incluso si un malintencionado superará la potencia de la red, no es que se vaya a hacer rico instantáneamente. Todo lo que puede conseguir es recuperar el dinero que él mismo ha gastado, como rebotar un cheque. Para aprovecharlo, debería comprar algo a un comercio, esperar al envío, y en ese momento utilizar su potencia e intentar recuperar su dinero. No creo que pudiera hacer tanto dinero con esa táctica como lo haría generando bitcoins. Con una granja tan grande de máquinas infectadas, podría generar más bitcoins que todo el resto de los mineros combinados.

La red Bitcoin podría reducir el spam mediante el desvío de las granjas zombies a la generación de bitcoins en su lugar.

Satoshi Nakamoto

La Lista de Correo de Criptografía

6

Sobre Redes Centralmente Controladas Versus Redes Peer-to-Peer

Traducción por **Jose Manuel Arenillas**

SATOSHI HACE REFERENCIA a la capacidad de los gobiernos de cerrar cualquier sistema centralizado como una web para compartir música, Napster o la divisa de oro digital E-gold. Los sistemas peer-to-peer han demostrado ser más resistentes.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, viernes 07 de noviembre 2008, 09:30:36 -0800

> [Extensa exposición de la vulnerabilidad de un sistema al uso de la fuerza por parte de los monopolios eludidos]
>
> No vas a encontrar la solución a problemas políticos en la criptografía.

Si, pero podemos ganar una gran batalla en la carrera y conquistar un nuevo territorio de libertad para varios años.

Los gobiernos son buenos cortando cabezas de redes centralizadas como Napster, pero las redes P2P puras como Gnutella y Tor parece que aguantan por sí mismas.

Satoshi

La Lista de Correo de Criptografía

7

Satoshi Sobre la Tasa de Inflación Inicial del 35%

Traducción por **Jose Manuel Arenillas**

INICIALMENTE, con 50 bitcoins creados cada 10 minutos durante los primeros años, se crearían 2,6 millones de bitcoins anualmente. Tras el inicio de Bitcoin con un balance de 0 bitcoins en enero de 2009, el ritmo inflación de la divisa bitcoin fue inicialmente impactante. Sin embargo, el crecimiento de la demanda de la moneda dada su muy limitada oferta inicial explica su alta tasa de inflación. Por el contrario, monedas nacionales establecidas como el Bolívar venezolano, el Peso argentino o el Dólar de Zimbabwe comenzaron con suministros suficientes y relativamente estables. Sin embargo, el ritmo de impresión de estas monedas se incrementó luego como un método para que el gobierno del país financiara su gasto deficitario.

Hay tres formas por las que un gobierno puede financiar un gasto deficitario: inflación de moneda (impresión de nueva moneda), préstamos públicos, e impuestos. Los gobiernos tienden a favorecer la creación de moneda por decreto (es decir, crear nueva moneda), lo que permite culpar de los inevitables aumentos de precios a los especuladores más que a su verdadero culpable, la inflación monetaria. Esta fue la excusa utilizada por el gobierno de Venezuela en 2013 y nuevamente en 2014. Si los gobiernos se vieran obligados a usar oro, plata o bitcoins para financiar su gasto deficitario, tendrían que financiarlo con subidas de impuestos, un recurso nada popular entre el público, o con préstamos en los mercados de crédito. Esta última acción conduce a tipos de interés más altos, a medida que aumenta la demanda para pedir dinero

prestado, y, si los gobiernos no abordan su gasto deficitario con recortes en el gasto, se ven obligados a aumentar los impuestos.

Re: artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, sábado 08 de noviembre 2008 13:38:26 -0800

> Ray Dillinger:
>
> la “moneda” es inflacionaria alrededor de un 35%, ya que es como los ordenadores más rápidos lo obtienen anualmente … la tasa de inflación del 35% está casi asegurada por la tecnología.

Gestionando el aumento de velocidad del hardware: "Para compensar el aumento de velocidad del hardware y el interés variable de ejecutar nodos a lo largo del tiempo, la dificultad de la prueba de trabajo está determinada por una media móvil que apunta a una cantidad promedio de bloques por hora. Si se generan muy rápido, la dificultad aumenta".

A medida que los ordenadores se vuelven más rápidos y aumenta la potencia total para generar bitcoins, la dificultad aumenta proporcionalmente para mantener constante la nueva producción total. Por lo tanto, se sabe de antemano cuántos nuevos bitcoins se crearán cada año en el futuro.

El hecho de que se produzcan nuevas monedas significa que la oferta monetaria aumenta en una cantidad planificada, pero esto no se da necesariamente como resultado la inflación. Si el suministro de dinero se incrementa a la misma velocidad que aumenta el número de personas que lo usan, los precios se mantienen estables. Si no aumenta tan rápido como la demanda, habrá deflación y los primeros tenedores de dinero verán que su valor aumenta.

Las monedas tienen que distribuirse inicialmente de alguna manera, y a una tasa constante parece ser la mejor fórmula.

Satoshi Nakamoto

La Lista de Correo de Criptografía

8

Sobre Transacciones

Traducción por **Jose Manuel Arenillas**

VARIAS PREGUNTAS y respuestas fueron abordadas en este correo. Hal Finney, el primer destinatario de una transacción bitcoin, generó las preguntas.

En la primera parte, Satoshi explica cómo los mineros retienen las transacciones hasta incluirlas en un bloque.

En la segunda, explica cómo no puede suceder un doble gasto en una cadena de bloques específica y cómo sólo una cadena de bloques prevalecerá en caso de que dos mineros resolvieran un bloque simultáneamente. También aborda el hecho de cómo los destinatarios deben mantener las transacciones durante una hora hasta estar formalmente confirmadas en la cadena de bloques. Satoshi menciona seis bloques (10 minutos por bloque, seis bloques hacen una hora), como un periodo de tiempo apropiado para que una transacción esté confirmada y forme parte de la cadena de bloques para siempre.

Sobre la tercera pregunta, describe lo que un atacante debería de hacer para "reescribir la historia", es decir, reconstruir y cambiar la cadena de bloques. Para agregar o eliminar transacciones en bloques previos requeriría escribirlos más rápido que todos los mineros que están trabajando en la cadena de bloques existente. Recordemos de la conversación sobre bloques huérfanos que la cadena más larga es la que utiliza la red. Satoshi dice: *La potencia de la prueba de trabajo del CPU debe ser la última palabra. La única manera de*

que todo el mundo esté en la misma página es creer que la cadena más larga es siempre la válida, pase lo que pase.

La cuarta pregunta aborda la verificación de un pago por parte del destinatario.

La quinta pregunta aborda el rol de los nodos (mineros) en el sistema. Cuando un minero descubre la prueba de trabajo (el hash que comienza con el número de ceros apropiado), publicará el bloque que acaba de "minar", el cual contiene varias transacciones. Cada minero en la red que recibe este bloque tiene que validarlo confirmando cada transacción contenida en el bloque.

Finalmente, Satoshi menciona que escribió el código antes de escribir el *white paper* anunciando Bitcoin para probarse a sí mismo que todas las incidencias estaban resueltas.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, domingo 09 de noviembre 2008, 11:13:34 -0800

> Hal Finney escribió:
>
> Se ha mencionado que, si una transacción emitida no llega a todos los nodos, está bien, ya que se incluirá en la cadena de bloques en poco tiempo. ¿Cómo sucede esto - qué pasa si el nodo que crea el "siguiente" bloque (el primer nodo que encuentra la colisión hashcash) no tiene constancia de la transacción y se añaden algunos bloques más de nodos que tampoco tienen constancia de ella? ¿Todos los nodos que han recibido la transacción tienen que guardarla con la esperanza de agregarla en un bloque cuando hayan tenido la suerte suficiente como para ser quien encuentre la siguiente colisión?
>
> ---

Correcto, los nodos mantienen las transacciones en su set de trabajo hasta que la incluyen en un bloque. Si una transacción llega al 90% de los nodos, cada vez que se encuentra un bloque, tiene un 90% de posibilidades de estar en él.

> O, por ejemplo, ¿qué ocurre si un nodo mantiene dos o más cadenas esperando a ver cuál crece más rápido, y aparece un bloque para la cadena A que incluye un doble gasto de una moneda que está en la cadena B? ¿Esto se verifica o no? (Podría suceder si alguien hizo un doble gasto y dos conjuntos diferentes de nodos recibieron las diferentes transacciones con la misma moneda).

No hace falta comprobar eso. La transacción incluida en la rama más larga se convierte en la válida, la otra no es. Si alguien intenta realizar un doble gasto de esa manera, uno y solo un gasto será válido siempre, el otro no lo será.

Los receptores de las transacciones normalmente necesitarán esperar por una hora o quizás más para dar tiempo a resolver este tipo de posibilidad.

Ellos aún pueden volver a gastar las monedas inmediatamente, pero deberían esperar antes de tomar una acción como el envío de bienes.

> Tampoco entiendo exactamente como el doble gasto, o la cancelación de transacciones, es consumado por un atacante superior que debería reunir mayor poder de cómputo que todos los nodos honestos participantes. Entiendo que puede crear nuevos bloques y añadirlos para generar la cadena más larga, pero ¿cómo puede borrar o añadir transacciones antiguas a la cadena? A medida que el atacante envía sus nuevos bloques, ¿no hay verificaciones de consistencia que puedan realizar los nodos honestos para asegurarse de que nada sea eliminado? Más explicaciones sobre este ataque serían de ayuda para juzgar las ganancias de un atacante a partir de aquí, versus simplemente usar su poder de cómputo para minar nuevas monedas honestamente.

El atacante no está añadiendo bloques al final. Tiene que volver atrás y rehacer el bloque en el que está su transacción y todos los bloques tras este, así como todos los nuevos bloques que la red sigue añadiendo a la cadena mientras está realizando el ataque. Está reescribiendo la historia. Una vez que su rama es más larga se convierte en la válida.

Esto toca un punto clave porque, aunque todos los presentes pueden ver las jugarretas, no hay forma de aprovecharse de ese hecho.

Es estrictamente necesario que la cadena más larga siempre se considere como válida. Los nodos presentes pueden recordar qué cadena estaba primero y cómo fue reemplazada por otra, pero no habría forma de convencer a los nodos que no estaban presentes durante el hecho. No podemos tener sub-acciones de nodos que se adhieren a una rama que creen que es la primera, otros que vieron otra rama como la primera, y otros que se unen más tarde y nunca han visto lo que ha sucedido. El voto de la prueba de trabajo del CPU debe tener la última palabra. La única manera de que todos permanezcan en la misma página es creer que la cadena más larga siempre es la válida, pase lo que pase.

En cuanto a las transacciones de gastos, ¿qué comprobaciones tiene que realizar el destinatario de una moneda? ¿Tiene que ir hacia atrás de todo el histórico de transferencias de esa moneda, y asegurarse de que todas las transacciones de la lista están asociadas a la "marca de tiempo" de la cadena de bloques? ¿O solo puede comprobar la última?

El destinatario solo necesita validar hacia atrás hasta una profundidad suficiente en la cadena de bloques, lo que requerirá normalmente una profundidad de 2 transacciones. Todas las transacciones antes de esa pueden descartarse.

¿Los nodos de marca de tiempo verifican las transacciones, asegurándose de que la anterior transacción de una moneda está en la cadena y, por lo tanto, asegurando la regla de que todas las transacciones en la cadena representan monedas válidas?

Correcto, exactamente. Cuando un nodo recibe un bloque, verifica las firmas de todas las transacciones que contiene contra las transacciones previas en los bloques. Los bloques sólo pueden contener transacciones que dependan de transacciones válidas en bloques anteriores o en el mismo. La transacción C puede depender de la transacción B que está en el mismo bloque y B depender de la transacción A que está en un bloque anterior.

Perdona por tantas preguntas, pero como he dicho parece una idea muy original y prometedora y tengo ganas de ver cómo se desarrolla el

> proyecto. Sería de ayuda ver una descripción de la idea más orientada al proceso, con detalles concretos de la estructura de datos de varios objetos (monedas, bloques, transacciones), los datos que se incluyen en mensajes y descripciones algorítmicas de los procedimientos para manejar los diversos eventos que podrían ocurrir en este sistema. Mencionaste que estás trabajando en una implementación, pero creo que una descripción más formal del sistema sería un próximo paso útil.

Aprecio tus preguntas. De hecho, hice esto al revés. Tuve que escribir todo el código antes de poder convencerme a mí mismo de que podría resolver todos los problemas, después escribí el documento técnico. Creo que podré publicar el código más pronto de lo que podría escribir una especificación detallada. Estás en lo cierto en la mayoría de tus suposiciones con las que has rellenado los espacios en blanco.

Satoshi Nakamoto

La Lista de Correo de Criptografía

9

Sobre los Bloques Huérfanos

Traducción por **Jose Antonio Bravo**

UN "BLOQUE HUÉRFANO" se produce cuando dos mineros realizan la prueba de trabajo aproximadamente al mismo tiempo. Los dos bloques creados por los dos mineros son diferentes dado que puede ser que no contengan las mismas transacciones de bitcoins, en cuyo caso las transacciones en las que los dos mineros "ganadores" transfieren las comisiones de transacción del bloque a sus cuentas también son diferentes. Pero solamente uno de estos dos bloques será finalmente añadido a la cadena de bloques, mientras que el otro se convertirá en un "bloque huérfano". Cualquier transacción presente en el bloque huérfano que no esté incluida en el bloque aceptado será incluida en el siguiente bloque por el que compiten los mineros. Para mayor detalle, véase la explicación de los bloques huérfanos en el Capítulo 2.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, domingo 9 de noviembre 2008, 11:17:24 -0800

James A. Donald escribió:

De acuerdo, supongamos que un nodo incorpora un grupo de transacciones en su prueba de trabajo, todos ellos gastos únicos,

> legítimos y honestos, y otro nodo incorpora un grupo diferente de transacciones en su prueba de trabajo, todos ellos igualmente gastos únicos, legítimos y honestos, y ambas pruebas se generan al mismo tiempo.

¿Qué ocurre entonces?

Ambos transmiten sus bloques. Todos los nodos los reciben y mantienen ambos bloques, pero solamente trabajan con el primero que recibieron. Supondremos que exactamente la mitad de ellos recibió el primero y la otra mitad recibió el otro.

En un tiempo corto, todas las transacciones terminarán propagándose de forma que todo el mundo tenga el conjunto completo. Los nodos que estén trabajando en cada grupo estarán intentando añadir las transacciones que faltan en su grupo. Cuando se halle la siguiente prueba de trabajo, sea cual sea el bloque previo con el que ese nodo esté trabajando, esta rama se convertirá en más larga y el vínculo se rompe. En cualquiera de los dos equipos, el nuevo bloque contendrá la otra mitad de las transacciones, por lo que, en cualquier caso, la rama contendrá todas las transacciones. Incluso en el improbable caso que hubiese una escisión dos veces seguidas, ambos equipos provenientes de la segunda escisión contendrían de todas formas el conjunto completo de transacciones.

No hay problema si las transacciones han de esperar uno o algunos ciclos extra para meterse en un bloque.

Satoshi Nakamoto

La Lista de Correo de Criptografía

10

Sobre la Sincronización de Transacciones

Traducción por **Jose Antonio Bravo**

EN ESTE CORREO, Satoshi explica lo que ocurre cuando un minero recibe dos transacciones contradictorias. La primera transacción recibida es la única que el minero incorpora en la siguiente prueba de trabajo. Si se necesita información adicional, véase la explicación en el Capítulo 2.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, domingo 9 de noviembre 2008, 11:14:17 -0800

James A. Donald escribió:

El concepto central es que muchos entes mantienen información completa y coherente de quién posee determinados bitcoins.

Pero mantener la coherencia es complicado. No tengo claro lo que sucede cuando alguien informa de una transacción a un mantenedor, y otra persona más transporta otra transacción a otro mantenedor. No es posible saber si la transacción es válida hasta que se haya incorporado a una vista globalmente compartida de todas las transacciones anteriores, y nadie puede saber si una vista globalmente compartida de todas las transacciones pasadas se comparte globalmente hasta que haya pasado, y después de que muchas transacciones nuevas hayan

llegado.

¿Explicaste cómo hacer esto, y es difícil de entender para mí, o confiabas en que podía hacerse, y de ahí que los detalles son un poco vagos?

La cadena de prueba de trabajo es la solución al problema de la sincronización, y para conocer cuál es la visión globalmente compartida sin necesidad de confiar en nadie.

Una transacción se propagará rápidamente a través de la red, por lo que, si se transmitieran dos versiones de la misma transacción casi al mismo tiempo, la que salga en cabeza tendría una gran ventaja para alcanzar muchos nodos en primer lugar. Los nodos solo aceptarán la primera que vean, rechazando la que llegase en segundo lugar, de modo que la transacción más antigua tendría muchos más nodos trabajando para incorporarla en la siguiente prueba de trabajo. En efecto, cada nodo vota su punto de vista de la transacción que vio primero al incluirlo en su esfuerzo de prueba de trabajo.

Si las transacciones llegaran exactamente al mismo tiempo y hubiera una bifurcación, hay una decisión entre ambas basadas en cuál de las dos alcanza antes una prueba de trabajo, y este hecho decide cuál de las dos es válida.

Cuando un nodo encuentra una prueba de trabajo, el nuevo bloque se propaga por la red y todos lo añaden a la cadena y comienza a funcionar en el siguiente bloque. Los nodos que tuviesen la otra transacción dejarán de intentar incluirla en un bloque, desde que no es válida de acuerdo con la cadena aceptada.

La cadena de prueba de trabajo es por sí misma una prueba autoevidente de que vino desde la visión globalmente compartida. Solo la mayoría de la red junta tiene suficiente potencia de CPU para generar una cadena tan difícil de prueba de trabajo. Cualquier usuario, tras recibir la cadena de prueba de trabajo, puede ver lo que ha aprobado la mayoría de la red. Una vez que una transacción está en un hash dentro de un enlace que está unos pocos enlaces por detrás en la cadena, está firmemente grabada en la historia global.

Satoshi Nakamoto

La Lista de Correo de Criptografía.

11

Satoshi Discute las Comisiones de Transacción

Traducción por **Jose Antonio Bravo**

ESTE CORREO DISCUTE EL USO de las comisiones por transacción como opuesto al *señoreaje* y como forma de pagar a los mineros por su trabajo de mantenimiento de la red Bitcoin. El *señoreaje* es un término económico usado para describir la creación de unidades adicionales de una moneda. Cuando todos los bitcoins hayan sido minados y el máximo de 21 millones de BTCs hayan sido creados, los incentivos para que los mineros mantengan la red Bitcoin vendrán únicamente de las comisiones por transacción recolectadas en el curso del mantenimiento de Bitcoin. Sin embargo, antes de que se dé este hecho, la tasa anual de inflación de bitcoin será tan baja que será efectivamente la misma que después de que todos los bitcoins hayan sido minados.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, lunes 10 de noviembre de 2008, 11:09:26 -0800

James A. Donald escribió:

Por otra parte, no se puede poner a funcionar, ya que en el sistema propuesto la tarea de seguir quién posee ciertas monedas es pagada por *señoreaje*, lo cual requiere de inflación.

Si tienes problemas con el asunto de la inflación, es sencillo cambiarla en este caso por comisiones por transacción. Es así de simple: dejemos que el valor de salida de cada transacción sea de 1 céntimo menos que el valor de entrada. De esa forma el software cliente escribe las transacciones automáticamente por 1 céntimo más que el valor de pago previsto, o podría salir del lado del beneficiario. El valor del incentivo cuando un nodo resuelve una prueba de trabajo para un bloque podría ser el total de comisiones del bloque.

Satoshi Nakamoto

La Lista de Correo de Criptografía

12

Sobre Confirmación y Tiempo de Bloque

Traducción por **Jose Antonio Bravo**

EN LA PRIMERA RESPUESTA, Satoshi habla del *doble gasto* y la *confirmación*.

En la segunda respuesta, trata de cómo la dificultad en la prueba de trabajo se ajusta con base en el tiempo efectivo entre cada bloque de forma que la red intenta mantener 10 minutos por bloque. La discusión en el capítulo 2 sobre la prueba de trabajo la comparaba a una lotería. Un número máximo, en hexadecimal o en base 16, es seleccionada, y la prueba de trabajo de los mineros consiste en generar un número que es menor que ese número. Este número se genera a través del sistema Bitcoin y es aleatorio. El primer minero que obtiene una salida hash menor que la máxima "gana" el derecho a procesar ese bloque y es recompensado con sus comisiones por transacción y los 25 BTC de recompensa por bloque. El valor elegido como máximo determina el nivel de dificultad de la prueba de trabajo; cuanto mayor sea el valor, más probable es que la salida hash generada por el sistema del minero caiga por debajo del máximo, y cuanto más pequeño sea el número, menos probable es que el número del minero caiga por debajo del máximo.

La última pregunta que se realiza es respecto a que la velocidad de la transacción no sea una característica. Señala que los cheques devueltos y las devoluciones de tarjetas de crédito pueden tardar varios días e incluso semanas en ser procesados, a diferencia de los más o menos 60 minutos que tarda

Bitcoin en validar una transacción de bitcoins completamente irreversible con un alto nivel de confianza.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, martes 11 de noviembre 2008, 06:30:22 -0800

> James A. Donald escribió:
>
> Entonces, ¿qué ocurre con la moneda que perdió la carrera?
>
> ---

… es un poco duro si el tipo llegó segundo porque es probable que pierda su moneda.

Cuando hay múltiples versiones de doble gasto de la misma transacción, una y solamente una se convertirá en válida.

El receptor de un pago debe esperar una hora aproximadamente antes de creer que es válida. La red resolverá cualquier posible carrera de doble gasto para entonces.

El tipo que recibió el doble gasto que se convirtió en no válido nunca pensó que lo tendría en primer lugar. Su software hubiera mostrado cómo la transacción pasaba de “no confirmada” a “no válida”. Si fuese necesario, la interfaz de usuario puede hacerse de forma que oculte transacciones hasta que las mismas sean lo suficientemente profundas en la cadena de bloques.

> Además, su descripción de eventos implica restricciones en el tiempo y generación de monedas - toda la red genera monedas lentamente en comparación con el tiempo que se requiere para que las noticias de una nueva moneda inunden la red.
>
> ---

Siento no haberlo aclarado. El tiempo objetivo entre bloques será probablemente de 10 minutos.

Cada bloque incluye su tiempo de creación. Si el tiempo está desactivado por más de 36 horas, otros nodos no funcionarán con él. Si el intervalo de tiempo en los últimos 6*24*30 bloques es inferior a 15 días, los bloques se están generando demasiado rápido y la dificultad de la prueba de trabajo se duplica. Todos hacen el mismo cálculo con los mismos datos de cadena, de forma que todos obtienen el mismo resultado en el mismo enlace de la cadena.

> Queremos que los que gastan dinero tengan la certeza de que su transacción es válida en el momento en que se necesita que un gasto inunde la red, no en el momento que toma para una carrera de rama ser resuelta.

El no repudio instantáneo no es una característica, pero es mucho más rápido que los sistemas existentes. Los cheques en papel pueden ser devueltos hasta una semana o dos más tarde. Las transacciones con tarjeta de crédito pueden disputarse entre 60 y 180 días después. Las transacciones con bitcoins pueden ser lo suficientemente irreversibles en una hora o dos.

> Si un nodo ignora todas las transacciones que no le importan, no sufre consecuencias adversas.

Con el sistema de incentivos basado en comisiones de transacción que he publicado recientemente, los nodos tendrían un incentivo para incluir todas las transacciones de pago que reciben.

Satoshi Nakamoto

La Lista de Correo de Criptografía

13

El Problema del General Bizantino

Traducción por **Beatriz Lizarraga**

EN LA QUE ES POSIBLEMENTE la publicación más interesante hecha por Satoshi, explica cómo la cadena de bloques resuelve un problema informático conocido como la "tolerancia de fallas Bizantina", una versión más generalizada del "Problema de los Dos Generales". En este problema, dos (o más) personas deben compartir información en un entorno de comunicación poco confiable, donde los mensajes enviados pueden perderse o alterarse. La declaración del problema apareció por primera vez en la década de 1970 en la literatura de computación en red, en ese momento el problema se consideró irresoluble. En esta publicación, Satoshi afirma que Bitcoin lo resuelve.

Para ilustrar el problema, imagine que dos generales son requeridos para atacar una ciudad al mismo tiempo. Si uno ataca y el otro no, las fuerzas del general atacante serán aniquiladas por las defensas de la ciudad. La comunicación entre los generales no es confiable; el mensajero que lleva el mensaje sobre cuándo atacar debe atravesar la ciudad y, por lo tanto, podría ser interceptado. El primer general puede, antes de las 9 a.m., enviar al mensajero con el mensaje que comunica que el ataque comenzará ese mismo día. Sin embargo, una vez enviado, el primer general no sabrá si el mensajero consiguió pasar o no. Esta incertidumbre puede llevar al primer general a dudar en atacar, ya que podría estar atacando solo si es que el segundo general no recibió su mensaje.

Consciente de esto, el segundo general puede enviar una confirmación al primero para indicar que recibió el mensaje de atacar. Pero ese mensaje,

también podría ser interceptado, lo que llevaría al segundo general a vacilar también. El primer general podría estar enviando una confirmación de la confirmación, pero ésta también podría haber sido interceptada. Por lo tanto, nuevamente, el primer general podría dudar a menos que obtenga una confirmación de esta confirmación de la primera confirmación. Este proceso podría ocurrir infinitas veces, sin que ninguno de los dos pudiera saber si los mensajes fueron enviados o si fueron interceptados por el enemigo.

Para obtener más información, lea la sección "Ilustrando el problema" en el siguiente artículo de Wikipedia:

http://en.wikipedia.org/wiki/Two_Generals%27_Problem

Ver también este artículo sobre la tolerancia de fallas Bizantina:

http://en.wikipedia.org/wiki/Byzantine_fault_tolerance

Re: Papel del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, jueves 13 de noviembre 2008, 19:34:25 -0800

> James A. Donald escribió:
>
> No es suficiente que todos sepan X. También necesitamos que todos sepan que todos conocen X, y que todos saben que todos saben que todos conocen X - lo que, como en el problema de los generales bizantinos, es el clásico y difícil problema del procesamiento distribuido de datos.

La cadena de prueba de trabajo es una solución al Problema de los Generales Bizantinos. Trataré de re-expresarlo en ese contexto.

Varios generales bizantinos tienen cada uno un ordenador y quieren atacar por fuerza bruta la contraseña del wi-fi del Rey, que han descubierto que tiene una cierta cantidad de caracteres. Una vez que animan a la red a generar un ataque, deben descifrar la contraseña dentro de un tiempo limitado para entrar y borrar los registros, de lo

contrario serán descubiertos y tendrán problemas. Solo tendrán suficiente poder de CPU para descifrarlo lo suficientemente rápido si la mayoría de ellos atacan al mismo tiempo.

No les importa especialmente cuándo será el ataque, solo que todos estén de acuerdo. Se ha decidido que cualquiera que lo desee puede anunciar un momento concreto, y que cualquier momento que se escuche primero será el momento oficial de ataque. El problema es que la red no es instantánea, y si dos generales anuncian diferentes momentos de ataque casi al mismo tiempo, algunos pueden escuchar a uno primero y otros escuchar al otro primero.

Usan una cadena de prueba de trabajo para resolver el problema. Una vez que cada general recibe la hora de ataque que escuchan primero, configuran su ordenador para resolver un problema de prueba de trabajo extremadamente difícil que incluye el momento de ataque en su hash. La prueba de trabajo es tan difícil que se espera que tarden 10 minutos en trabajar todos a la vez antes que uno de ellos encuentre una solución. Una vez que uno de los generales encuentra una prueba de trabajo, lo transmite a la red, y todos cambian su cómputo actual de prueba de trabajo para incluir esa prueba de trabajo en el hash en el que están trabajando. Si alguien estaba trabajando con un momento de ataque diferente, cambia a este, porque su cadena de prueba de trabajo ahora es más larga.

Después de dos horas, el momento de ataque debe ser *hasheado* por una cadena de 12 pruebas de trabajo. Cada general, verificando la dificultad de la cadena de prueba de trabajo, puede estimar cuánta potencia de CPU paralela fue gastada por hora, y ver lo que debe de haber requerido la mayoría de los ordenadores para producir tanta prueba de trabajo en el momento asignado. Todos debieron haberlo visto porque la prueba de trabajo es prueba de que trabajaron en ello. Si la potencia de CPU exhibida por la cadena de prueba de trabajo es suficiente para descifrar la contraseña, ellos pueden atacar con seguridad a la hora acordada.

La cadena de prueba de trabajo es lo que resuelve todos los problemas de sincronización, de base de datos distribuida y de visión global que pedías.

La Lista de Correo de Criptografía

14

Tiempo de Bloque, una Prueba Automatizada y el Punto de Vista Libertario

Traducción por **Beatriz Lizarraga**

EN ESTE CORREO, Satoshi explica por qué se requiere un único pool de transacciones pendiente y cómo se mantienen estas transacciones dada la existencia de ramas paralelas de bloques. Hace referencia a algunas funciones dentro del código. Recuerde la discusión sobre la prueba de trabajo en el Capítulo 2. No todos los mineros tienen por qué haber reunido las mismas transacciones, algunas podrían haber llegado demasiado tarde para ser incluidas en el bloque en el que están trabajando. A medida que les van llegando nuevas transacciones mientras trabajan en el hash de su bloque existente, almacenarán estas transacciones en un pool de transacciones.

Después, vuelve a tocar la propagación de la transacción y los 10 minutos asignados por creación de un bloque, discutiendo el tema de que si eso podría ser un período de tiempo muy corto.

Por último, hace una referencia a cómo Bitcoin podría ser atractivo para los libertarios, personas que abogan por las libertades individuales.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, viernes 14 de noviembre 2008, 14:29:22 -0800

> Hal Finney escribió:
>
> Creo que es necesario que los nodos mantengan una lista separada de transacciones pendientes asociada a cada cadena candidata.
>
> . . . Uno podría preguntar también. . . ¿Cuántas cadenas candidatas debe mantener un nodo al mismo tiempo, en promedio?

Afortunadamente, solo es necesario mantener un pool de transacciones pendientes para la mejor rama de ese momento. Cuando llega un nuevo bloque a la mejor rama, ConnectBlock elimina las transacciones pendientes en el pool. Si una rama diferente se vuelve más larga, llama a DisconnectBlock en la rama principal hasta la bifurcación, devolviendo al bloque las transacciones como pendientes en el pool, y llama a ConnectBlock en la nueva rama, realizando copias de seguridad de todas las transacciones que se encontraban en ambas ramas. Se espera que reorganizaciones como esta sean raras y poco profundas.

Con esta optimización, las ramas candidatas no son realmente ninguna carga. Simplemente aguardan en el disco y no requieren atención a menos que alguna vez se conviertan en la cadena principal.

> O como James planteó anteriormente, si la transmisión de la red es confiable, pero depende de un algoritmo de evolución potencialmente lenta, ¿cómo afecta eso al rendimiento?

Las transmisiones probablemente serán casi completamente confiables. Las transmisiones TCP actualmente casi nunca se descartan, y el protocolo de transmisión tiene un mecanismo de reintento para obtener los datos de otros nodos después de un tiempo. Si las emisiones resultan ser más lentas en la práctica que lo esperado, el tiempo objetivo entre bloques deberá aumentarse para evitar el desperdicio de recursos. Queremos bloques que normalmente se propaguen en mucho menos tiempo de lo que lleva generarlos, de lo contrario los nodos pasarían demasiado tiempo trabajando en bloques obsoletos.

Estoy planeando realizar una prueba automatizada con ordenadores que se envíen pagos aleatoriamente entre ellos y que lancen paquetes aleatoriamente.

> 3. El sistema bitcoin resulta ser socialmente útil y valioso, por lo que los operadores de nodos sienten que están haciendo una contribución beneficiosa al mundo por sus esfuerzos (similar a los diversos proyectos informáticos "@Home" donde las personas ofrecen voluntariamente sus recursos informáticos para buenas causas).

En este caso, me parece que el simple altruismo puede ser suficiente para mantener la red funcionando correctamente.

Es muy atractivo desde el punto de vista libertario si podemos explicarlo adecuadamente. Sin embargo, soy mejor con el código que con las palabras.

Satoshi Nakamoto

La Lista de Correo de Criptografía

15

Más Sobre Doble Gasto, Prueba de Trabajo y Comisiones de Transacción

Traducción por **Beatriz Lizarraga**

EN ESTE INTERCAMBIO, Satoshi proporciona varias aclaraciones y analiza la compensación de los mineros (los nodos) a través de las comisiones en las transacciones una vez que se ha creado todo el suministro de bitcoins.

Re: Papel del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, lunes 17 de noviembre 2008, 09:04:47 -0800

Trataré de ser rápido y lanzar el código fuente tan pronto como sea posible para que sirva de referencia y ayude a aclarar todas estas preguntas de implementación.

> Ray Dillinger (Bear) escribió:
>
> Cuando se gasta una moneda, el comprador y el vendedor firman digitalmente un registro (ciego) de la transacción.

Solo firma el comprador y no es ciego.

> Si alguien realiza un doble gasto, entonces el registro de la transacción puede ser desenmascarado revelando la identidad del tramposo.

Las identidades no se utilizan, y no depende del recurso. Todo es prevención.

> Esto se hace vía un algoritmo corta-y-elige más o menos estándar donde el comprador responde a varios desafíos con acciones secretas.

Ni desafíos ni acciones secretas. Una transacción básica es exactamente lo que ves en la figura de la sección 2. Una firma (del comprador) satisfactoria para la clave pública de la transacción previa, y una nueva clave pública (del vendedor) que debe ser satisfactoria para gastarla en la siguiente ocasión.

> También podrían recibir cadenas mientras trabajan en la que están tratando de extender, en las cuales los últimos "enlaces" son enlaces que *no* son comunes a la cadena sobre la que están trabajando.
>
> Estas las ignoran.

Correcto, si tiene la misma longitud, los enlaces se rompen manteniendo el más antiguo de los recibidos.

> Si contiene un doble gasto, crean una "transacción" que es una prueba del doble gasto, lo agregan al pool A, lo difunden y continúan trabajando.

No hay necesidad de informar de una "prueba de doble gasto" como esa. Si la misma cadena contiene ambos gastos, entonces el bloque no es válido y se rechaza.

Lo mismo si un bloque no tuvo suficiente prueba de trabajo. Ese bloque es inválido y rechazado. No es necesario hacer circular un informe al respecto. Cada nodo puede ver eso y rechazarlo antes de difundirlo.

Si hay dos cadenas competidoras, cada una con una versión diferente de la misma transacción, una tratando de dar dinero a una persona y la otra tratando de darle el mismo dinero alguien más, es el conjunto de la cadena de prueba de trabajo la que resolverá cuál de los gastos es válido.

No estamos "al acecho" del doble gasto para hacer sonar la alarma y atrapar al tramposo. Simplemente decidimos cuál de los gastos es válido. Los receptores de transacciones deben esperar unos pocos bloques para asegurarse de que la resolución haya tenido tiempo de completarse. Los tramposos pueden intentar y hacer simultáneamente doble gasto todo lo que deseen, y todo lo que lograrán es que, con unos pocos bloques, uno de los gastos se vuelve válido y los otros se serán inválidos. Cualquier doble gasto posterior se rechaza inmediatamente una vez que ya hay un gasto en la cadena principal.

Incluso si un gasto anterior aún no estaba en la cadena, si ya estaba en todos los pools de nodos, entonces el segundo gasto sería rechazado por todos los nodos que ya tienen el primer gasto.

> Si la nueva cadena es aceptada, y se dan por vencidos para agregar su enlace actual, vuelcan todas las transacciones del grupo L al grupo A (junto con las transacciones que han recibido o creado desde que comenzaron a trabajar), eliminan del grupo A esos registros de transacciones que ya son parte de un enlace en la nueva cadena, y comienzan a trabajar de nuevo tratando de extender la nueva cadena.

Correcto. También se actualizan cada vez que aparece una nueva transacción, por lo que L prácticamente contiene todo en A todo el tiempo.

> Un algoritmo de firma digital de uso intensivo de la CPU firma la cadena incluyendo el nuevo bloque L.

Es una prueba de trabajo SHA-256 estilo Hashcash (preimagen parcial de cero), no una firma.

> ¿Existe un mecanismo para garantizar que la "cadena" no consista únicamente en enlaces añadidos solo por los 3 ó 4 nodos más rápidos? Porque la emisión del registro de transacción podría pasar fácilmente por alto esos 3 ó 4 nodos y, si lo hace, y esos nodos continúan dominando la cadena, la transacción podría no ser agregada nunca.

Si estás pensando en ello como una firma digital de uso intensivo de la CPU, entonces puedes estar pensando en una carrera por terminar primero una operación larga y el que es más rápido siempre gana.

La prueba de trabajo es un hallazgo de colisión SHA-256 estilo Hashcash. Es un proceso sin memoria en el que se hacen millones de hashes por segundo, con una pequeña posibilidad de encontrar uno cada vez. El dominio de los 3 ó 4 nodos más rápidos sería sólo proporcional a su parte de la potencia total de la CPU. Cualquier oportunidad de encontrar una solución en cualquier momento es proporcional a la potencia de su CPU.

Habrá comisiones por las transacciones, por lo que los nodos tendrán un incentivo para recibir e incluir todas las transacciones que puedan. Los nodos finalmente serán compensados con las comisiones de transacción siempre y cuando el total de monedas creadas llegue al límite predeterminado.

> Además, el requisito de trabajo para agregar un enlace a la cadena debe variar (de nuevo exponencialmente) con el número de enlaces agregados a esa cadena en la semana anterior, lo que provoca un estricto control de la tasa de generación de monedas (y por lo tanto de inflación).

Correcto.

> Necesitas la agregación de monedas para escalar esto. Es necesario que haya una transacción "comprobable" donde alguien retire diez monedas individuales y cree una nueva moneda con denominación diez, etc.

Cada transacción es una de estas. Sección 9, Combinar y dividir el valor.

Satoshi Nakamoto

La Lista de Correo de Criptografía

16

Sobre Criptografía de Curva Elíptica, Ataques de Denegación de Servicio y Confirmación

Traducción por **Beatriz Lizarraga**

SATOSHI TRATA las firmas de las transacciones, añade un poco más sobre los ataques de denegación de servicio y, finalmente, retoma la velocidad de las transacciones. Un comerciante podría esperar 2 minutos después de que el consumidor haya realizado la transacción con su teléfono móvil. Luego, el comerciante (o la compañía de servicios de pago de Bitcoin que el comerciante ha elegido) vigilará las transacciones de doble gasto en la red Bitcoin. Imagine que un consumidor realiza una transacción que llamaremos "X" en el que él o ella paga 1.5 BTC desde una dirección ABC de Bitcoin que contiene 2 BTC. El saldo del consumidor cae a 0.5 BTC una vez que el pago ha sido confirmado por completo. Aquí se discuten las acciones que el comerciante debe realizar para monitorizar la red y ver si aparecen otras transacciones en las que la dirección ABC de Bitcoin está involucrada y, de ser así, si la cantidad involucrada excede de 0.5 BTC. Si las transacciones que cumplen este criterio se detectan dentro de, digamos, 2 minutos, el pago se considera no válido. Esperar 2 minutos da mucho margen para que la transacción "X" se liquide antes de que venga cualquier transacción competidora posterior de la dirección ABC de Bitcoin. Esto indica al comerciante que es muy probable que la transacción "X" se incluya en el bloque actual de la mayoría de los mineros de Bitcoin en los que están trabajando y, por lo tanto, asegura finalmente su

inclusión en la cadena de bloques.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, lunes 17 de noviembre 2008 09:06:02 -0800

> Ray Dillinger escribió:
>
> Una forma de hacer esto sería hacer que la persona que recibe la moneda genere una pareja de claves asimétricas, y dejar la mitad de la clave publicada en la transacción. Para gastar la moneda más tarde, deberá demostrar la posesión de la otra mitad de la clave asimétrica, probablemente usándola para firmar la clave provista por el nuevo vendedor.
>
> ---

Correcto, son las firmas digitales ECC (Criptografía de Curva Elíptica). Se usa un nuevo par de claves para cada transacción.

No es un pseudónimo en el sentido de que los *nyms* identifican a las personas, pero al menos es algo pseudónimo en el sentido de que la siguiente acción sobre una moneda puede ser identificada como proveniente del propietario de esa moneda.

> Mmmm. No sé si me siento cómodo con eso. ¿Estás diciendo que no hay esfuerzo para identificar y excluir los nodos que no cooperan? Sospecho que esto dará lugar a problemas y posibles ataques de denegación de servicio.
>
> ---

No se trata de identificar a nadie. Como dijiste, es inútil y puede ser fácilmente vencido con marionetas.

La credencial que establece a alguien como real es la capacidad de suministrar potencia de CPU.

> Hasta . . . ¿hasta qué? ¿Cómo sabe alguien cuándo una transacción se ha vuelto irrevocable? ¿Son tres "unos pocos" bloques? ¿treinta? ¿un centenar? ¿depende de la cantidad de nodos? ¿es logarítmico o lineal en

> número de nodos?

La sección 11 calcula el peor caso bajo ataque. Normalmente, 5 ó 10 bloques son suficientes. Si estás vendiendo algo que no merece un ataque a escala de red para robarlo, en la práctica podrías cortarlo antes.

> Pero a falta de identidad, no hay inconveniente para ellos si los gastos se vuelven inválidos, si ya han recibido los bienes por los que gastaron doblemente (acceso al sitio web, descarga, lo que sea). Los comerciantes retienen la bolsa con monedas "inválidas", a menos que esperen esos "pocos bloques" mágicos (¿y cómo pueden saber cuántos?) antes de tratar al consumidor como si hubiera pagado.
>
> Los consumidores no harán esto si gastan su moneda y les lleva una hora liquidar antes de poder hacer lo que sea por lo que pagaron. Los comerciantes no lo harán si no hay forma de cobrarle a un cliente cuando descubren que su moneda no es válida porque el cliente tiene doble gasto.

Este es un problema de la versión 2 que creo que se puede resolver muy satisfactoriamente para la mayoría de las aplicaciones.

La carrera está primero en difundir tu transacción en la red. Piensa en los 6 grados de libertad --se extiende exponencialmente. Solo llevará alrededor de 2 minutos que una transacción se extienda lo suficiente como para que un competidor que comienza más tarde tenga pocas posibilidades de obtener muchos nodos antes de que el primero supere a toda la red.

Durante esos 2 minutos, los nodos del comerciante pueden estar atentos a una transacción de doble gasto. El que gasta doblemente no podrá detonar su transacción alterna al mundo sin que la obtenga el comerciante, por lo que tiene que esperar antes de comenzar.

Si la transacción real alcanza el 90% y la transacción de doble gasto alcanza el 10%, el que genera el doble gasto solo tiene un 10% de posibilidades de no pagar, y un 90% de posibilidades de que su dinero se gaste. Eso no le merecerá la pena al estafador, con casi cualquier tipo de mercancía.

Los bienes basados en la información, como el acceso a sitios web o las descargas, no son defendibles. Nadie va a poder ganarse la vida robando accesos a sitios web o a descargas. Pueden ir a las redes de intercambio de archivos para robarlo. La mayoría de los productos de acceso instantáneo no van a suponer un gran incentivo como para robar.

Si un comerciante realmente tiene un problema de robos, puede hacer que el cliente espere 2 minutos o que espere recibir algo en el correo electrónico, cosa que muchos ya hacen. Si realmente quieren optimizar, y es una descarga grande, podrían cancelar la descarga en el medio si la transacción resulta ser de doble gasto. Si se trata de un acceso a una página web, normalmente no debería ser un gran problema permitir que el cliente tenga acceso durante 5 minutos y luego cortar el acceso si es rechazado. Muchas de estas webs tienen una versión de prueba gratuita de todas formas.

Satoshi Nakamoto

La Lista de Correo de Criptografía

17

Más Sobre el Grupo de Transacción, Difusión de Red y Detalles de Codificación

Traducción por **Arturo Monzón**

EN LA PRIMERA SECCIÓN A CONTINUACIÓN, Satoshi amplía el grupo de acción de las transacciones. A continuación, describe su experimento en el mecanismo de difusión en red donde los nodos solicitan elementos de sus vecinos. Por último, Satoshi menciona que ha estado trabajando en el código durante los últimos 18 meses.

Re: Artículo del dinero electrónico Bitcoin P2P

Satoshi Nakamoto, lunes 17 de noviembre de 2008 13:33:04 -0800

James A. Donald escribió:

Satoshi escribió:

Afortunadamente, solo es necesario mantener un grupo de transacciones pendientes para la actual mejor rama.

> Esto requiere que sepamos, es decir, un par honesto y de buen comportamiento cuyas comunicaciones y almacenamiento de datos funcionen bien, que sepa cuál es la mejor rama actual -

---

Quiero decir que un nodo sólo necesita la transacción pendiente para la mejor rama que tiene. La rama que actualmente piensa que es la mejor. Esa es la rama donde tratará de hacer un bloque, que es todo lo que el grupo necesita.

> Las transmisiones probablemente serán casi completamente confiables.

> En lugar de asumir que cada mensaje llega al menos una vez, debemos crear un mecanismo tal que la información llegue aunque sean transmitidos por mensajes que con frecuencia fallan en llegar.

Creo que tengo cubierto el mecanismo de transmisión de redes de pares.

Cada nodo envía a sus vecinos una lista de inventario de hashes de los nuevos bloques y transacciones que tiene. Los vecinos solicitan los productos que aún no tienen. Si este no llega después de un tiempo de espera, lo solicitan a otro vecino que sí lo obtuvo. Debido a que todos o la mayoría de los vecinos deberían tener cada producto, incluso si los "coms" se revuelven con uno, pueden obtenerlo de cualquiera de los otros vecinos, intentándolo de uno en uno.

El esquema de inventario de data requerida introduce una pequeña latencia, pero en última instancia ayuda a acelerar más al mantener bloques de datos extra fuera de las colas de transmisión y conservar el ancho de banda.

> Usted tiene un esquema y una propuesta para dicho diseño, que es un gran paso adelante, pero el diablo está en los pequeños detalles.

Creo que he trabajado en todos esos pequeños detalles durante el último año y medio mientras lo codificaba, y había muchos de ellos. Los

detalles funcionales no están cubiertos en el documento, pero el código fuente llegará pronto. Te envié los archivos principales. (disponibles por pedido en este momento y de pronto lanzamiento completo)

Satoshi Nakamoto

La Lista de Correo de Criptografía

18

Primer Lanzamiento de Bitcoin

Traducción por **Arturo Monzón**

EN ESTE CORREO, Satoshi anuncia el primer lanzamiento del software de Bitcoin en *sourceforge.net. Sourceforge.net* es como GitHub u otros servicios en línea que permiten a las personas compartir documentos y código fuente. Este lanzamiento ya no está disponible allí, pero ha sido copiado en las siguientes ubicaciones:

http://www.zorinaq.com/pub/bitcoin-0.1.0.rar
http://www.zorinaq.com/pub/bitcoin-0.1.0.tgz
http://we.lovebitco.in/bitcoin- 0.1.0.rar
http://www.bitcointrading.com/files/bitcoin-0.1.0.rar

Este software es de código abierto, lo que significa que el código está disponible, libre de derechos de autor para su uso, reproducción y modificación.

Bitcoin v0.1 lanzado

Satoshi Nakamoto, viernes 09 de enero 2009, 17:05:49 -0800

Anunciando el primer lanzamiento de Bitcoin, un nuevo sistema de dinero electrónico que usa una red peer-to-peer para evitar el doble gasto. Está completamente descentralizado sin servidor ni autoridad central.

Vea bitcoin.org para capturas de pantalla.

Enlace de descarga:

http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows solo por ahora. Código fuente abierto C ++ está incluido.

- Desempaquetar los archivos en un directorio
- Ejecute BITCOIN.EXE
- Se conecta automáticamente a otros nodos

Si puede mantener un nodo en ejecución que acepte conexiones entrantes, realmente estará ayudando mucho a la red. El puerto 8333 en su firewall necesita estar abierto para recibir conexiones entrantes.

El software sigue siendo alfa y experimental. No hay garantía de que el estado del sistema no deba reiniciarse en algún momento si llegar a ser necesario, aunque he hecho todo lo posible para construir en extensibilidad y control de versiones.

Puede obtener monedas haciendo que alguien le envíe algo, o encendiendo el nodo.

Options->Generate Coins para ejecutar un nodo y generar bloques. Hice que la dificultad de la prueba de trabajo fuera ridículamente fácil para empezar, así que por un tiempo y al principio una PC típica podrá generar monedas en pocas horas. Se pondrá mucho más difícil cuando la competencia haga que el ajuste automático aumente la dificultad. Las monedas generadas deben esperar 120 bloques para madurar antes de que puedan ser gastadas.

Hay dos formas de enviar dinero. Si el destinatario está en línea, puede ingresar su dirección IP y se conectará, obtendrá una nueva clave pública y enviará la transacción con comentarios. Si el destinatario no está en línea, es posible enviar a su dirección de Bitcoin, que es un hash de la clave pública que ellos le dan. Recibirán la transacción la próxima vez que se conecten y obtengan el bloque en el que se encuentra. Este método tiene la desventaja de que no envía información de comentarios, y se puede perder un poco de privacidad si la dirección es usada varias veces, pero es una alternativa útil si ambos usuarios no pueden estar en línea al mismo tiempo o si el destinatario no puede recibir conexiones entrantes.

La circulación total será de 21,000,000 de monedas. Se distribuirá a los

nodos de la red cuando hagan bloques y la cantidad se reducirá a la mitad cada 4 años.

- primeros 4 años: 10,500,000 monedas
- próximos 4 años: 5,250,000 monedas
- los próximos 4 años: 2,625,000 monedas
- los próximos 4 años: 1.312.500 monedas, etc. . . .

Cuando se agoten, el sistema puede soportar comisiones en las transacciones si fuera necesario. Está basado en la competencia de mercado abierto, y probablemente siempre haya nodos dispuestos a procesar transacciones de forma gratuita.

Satoshi Nakamoto

19

Sobre el Propósito Para el Cual Bitcoin Podría Ser Usado Primero

Traducción por **Arturo Monzón**

A PARTIR DE ESTA LECTURA, podemos extrapolar que Satoshi Nakamoto no esperaba que Bitcoin lograra tan enorme éxito muy rápidamente. Él afirma que el primer uso podría ser para micropagos o un sitio porno. Curiosamente, esos no fueron los primeros usos reales. Satoshi también sugiere que personas famosas podrían usarlo para que los fanáticos puedan enviarles mensajes personales.

También observa: "Puede tener sentido poseer algunos en caso de que se ponga de moda". Supongo que siguió su propio consejo. Un bitcoin valía más de $ 600 a principios de 2014 en comparación con los centavos en su primer año de existencia.

Re: Bitcoin v0.1 lanzamiento

Satoshi Nakamoto, sábado 17 de enero 2009, 06:58:44 -0800

Dustin D. Trammell escribió:

> Satoshi Nakamoto escribió:
>
> Sabes, creo que había mucha más gente interesada en los 90, pero después de más de una década de sistemas fallidos basados en terceros confiables (Digicash, etc.), lo ven como una causa perdida. Espero que puedan hacer la distinción de que esta es la primera vez que sé que estamos intentando un sistema sin necesidad de confianza.
>
> ---
>
> Sí, esa fue la característica principal que me llamó la atención. El verdadero truco será hacer que la gente realmente valore los BitCoins para que se conviertan en moneda.
>
> ---

Me sorprendería que dentro de 10 años no utilicemos moneda electrónica de alguna manera, ahora que conocemos una forma de hacerlo que inevitablemente no se va a venir abajo cuando el tercero de confianza pierda interés.

Podría comenzar en un nicho reducido como puntos de recompensa, tokens de donación, moneda para un juego o micropagos para sitios de adultos. Inicialmente puede ser usado en aplicaciones de prueba de trabajo para servicios que casi podrían ser gratuitos, pero no del todo.

Ya se puede usar para pago usando el correo electrónico. El cuadro de diálogo de envío se puede redimensionar e ingresar el mensaje que desee. Se envía directamente cuando se conecta. El destinatario hace doble click en la transacción para ver el mensaje completo. Si alguien famoso recibe más correos electrónicos de los que puede leer, pero aún le gustaría tener una forma para que los fanáticos se comuniquen con él, podrían configurar Bitcoin y dar la dirección IP en su sitio web. "Envía X bitcoins a mi línea de prioridad en esta IP y leeré el mensaje personalmente".

Sitios de suscripción que necesitan alguna prueba de trabajo adicional para su periodo de prueba gratuito para que no canibalice suscripciones, podría cobrar bitcoins por la versión de prueba.

Puede tener sentido solo para obtener algunos en caso de que se ponga de moda. Si suficientes personas piensan de la misma manera, eso se convierte en una profecía autocumplida. Una vez que arranque, hay tantas aplicaciones si puedes pagar sin esfuerzo unos pocos centavos a un

sitio web tan fácilmente como soltamos monedas en una máquina expendedora.

Satoshi Nakamoto

http://www.bitcoin.org

Este tema fue revisado posteriormente en el foro BitcoinTalk

Re: Porno

Publicado por satoshi, 23 de septiembre 2010, 05:56:55 PM

Bitcoin sería conveniente para las personas que no tienen una tarjeta de crédito o no quieren usar las tarjetas que tienen, o bien no quieren que el cónyuge lo vea en la factura o no confían en dar su número al "porno chicos", o miedo a una facturación recurrente.

20

"Prueba de Trabajo" Tokens y Spammers

Traducción por **Arturo Monzón**

AQUÍ HAY UNA INTERESANTE CONVERSACIÓN entre Hal Finney, un muy conocido desarrollador en la industria de la criptografía, y Satoshi Nakamoto que se centra en cómo la prueba de trabajo de Bitcoin podría usarse para limitar a los que envían correo no deseado o para recompensar a los destinatarios de correo no deseado. A Hal Finney se le atribuye la creación del primer "sistema de prueba de trabajo reutilizable", una variante de la prueba de trabajo de Bitcoin que no es necesario entender para que este tema sea comprendido. También Hal Finney fue el destinatario de la primera transacción de Bitcoin, cuyo remitente fue el propio Satoshi.

Re: Bitcoin v0.1 lanzamiento

Satoshi Nakamoto, domingo 25 de enero 2009, 08:34:34 -0800

Hal Finney escribió:

> * Los ordenadores infectados de spam pueden arder con los filtros de correo electrónico de pago por envío

Si los tokens de prueba de trabajo se vuelven útiles, y especialmente si se convierten en dinero, las máquinas ya no se quedarán ociosas. Los usuarios esperarán que sus ordenadores les generen dinero (asumiendo

> que la recompensa sea mayor que el costo de operación). Un ordenador cuyas ganancias están siendo robadas por una computadora infectada será más llamativo para su propietario que en el caso actual, por lo tanto, podríamos esperar que, en ese mundo, los usuarios trabajarán con más dedicación para mantener sus ordenadores limpios de infecciones.

Otro factor que mitigaría el spam si los tokens de prueba de trabajo tienen valor: habría un motivo de ganar dinero para que las personas creen cantidades masivas de falsas cuentas de correo electrónico para recolectar tokens de prueba de trabajo del spam. Básicamente, estarían revirtiendo los correos no deseados a los remitentes de spam con buzones de correo automáticos que recopilan su prueba de trabajo y no leen el mensaje. La proporción de buzones falsos con personas reales podría ser demasiado alta para que el correo no deseado sea rentable.

El proceso tiene el potencial de establecer el valor del token de prueba de trabajo en primer lugar, ya que los spammers que no tienen ordenadores infectados pueden comprar tokens de los recolectores. Si bien esta recompra permitiría temporalmente el envío de más spam, solo aceleraría el ciclo de autodestrucción que lleva a que demasiados recolectores exploten a los spammers.

Curiosamente, uno de los sistemas de oro electrónico (e-gold), ya tiene una forma de spam llamada "limpieza". Los spammers envían una pequeña cantidad de oro en polvo para colocar un mensaje de spam en el campo de comentario de la transacción. Si el sistema permite a los usuarios configurar el pago mínimo que están dispuestos a recibir, o al menos el mínimo que puede tener un mensaje, los usuarios pueden establecer cuánto están dispuestos a cobrar para recibir correo no deseado.

Satoshi Nakamoto

La Lista de Correo de Criptografía

21

Bitcoin Presentado en la Fundación P2P

Traducción por **Arturo Monzón**

SATOSHI ANUNCIA Bitcoin v0.1 en *p2pfoundation.ning.com.* Este es otro foro que involucra tecnología peer-to-peer. En lugar de copiar exactamente el mismo texto de su original anuncio publicado en la lista de correo Criptografía, Satoshi escribió un anuncio ligeramente diferente para su publicación aquí.

Implementación de código abierto de Bitcoin de moneda P2P

Satoshi Nakamoto, 11 de febrero 2009, 22:27

He desarrollado un nuevo sistema de pago electrónico P2P de código abierto llamado Bitcoin. Está completamente descentralizado, sin servidor central o partes de confianza, porque todo se basa en la prueba criptográfica en lugar de la confianza. Pruébalo o echa un vistazo a las capturas de pantalla y al documento del proyecto:

Descargue Bitcoin v0.1 en http://www.bitcoin.org

La raíz del problema con la moneda convencional es toda la confianza que se requiere para que funcione. Se debe confiar en que el banco central no degrade la moneda, pero el historial de las monedas fiduciarias está lleno de violaciones de esa confianza. Los bancos deben ser confiables para

guardar nuestro dinero y transferirlo electrónicamente, pero lo prestan en burbujas de crédito con apenas una fracción de reserva. Tenemos que confiar en ellos para nuestra privacidad, confiar en que no permitan que los ladrones de identidad limpien nuestras cuentas. Sus costos masivos generales hacen que los micropagos sean imposibles.

Hace una generación, los sistemas informáticos de uso compartido de múltiples usuarios tenían un problema similar. Antes de la encriptación segura, los usuarios tenían que confiar en la protección mediante contraseñas para proteger sus archivos, confiando en el administrador del sistema para guardar su información privada. La privacidad siempre puede ser anulada por el administrador en base a su criterio, desvirtuando el principio de privacidad frente a otras preocupaciones, o por orden de sus superiores. Entonces, la encriptación segura se volvió disponible para las masas y ya no se necesitaba confianza. Los datos se podían asegurar de una manera que era físicamente imposible poder acceder para otros, no importa el motivo, no importa cuán buena sea la excusa, no importa nada.

Es hora de que tengamos lo mismo para dinero. Con el dinero digital basado en pruebas criptográficas, sin la necesidad de confiar en un intermediario externo, el dinero puede ser seguro y las transacciones realizarse sin esfuerzo.

Uno de los fundamentos para construir bloques como un sistema de este tipo son las firmas digitales. Una moneda digital contiene la clave pública de su propietario. Para transferirlo, el propietario firma la moneda junto con la clave pública del próximo dueño. Cualquiera puede verificar las firmas para verificar el recorrido de la propiedad. Funciona bien para asegurar la propiedad, pero deja un gran problema sin resolver: el doble gasto. Cualquier dueño podría intentar de nuevo usar una moneda ya gastada, volviéndola a firmar a otro propietario. La solución habitual es que una empresa fiable, con una base de datos central, compruebe el gasto doble, pero eso nos devuelve al modelo de tercero de confianza. Desde su posición central, la compañía puede invalidar a los usuarios, y las tarifas necesarias para respaldar el trabajo de la compañía hacen que los micropagos no sean prácticos.

La solución de Bitcoin es usar una red peer-to-peer para verificar el doble gasto. En resumen, la red funciona como un servidor distribuido de marca de tiempo, sellando la primera transacción para gastar una moneda.

Aprovecha la naturaleza de la información, que es fácil de difundir, pero difícil de sofocar. Para detalles sobre cómo funciona, vea el documento de diseño en http://www.bitcoin.org/bitcoin.pdf

El resultado es un sistema distribuido sin un único punto de fallo. Los usuarios mantienen las claves de cifrado en su propio dinero y realizan transacciones directamente entre ellos, con la ayuda de la red P2P para verificar el doble gasto.

Satoshi Nakamoto

http://www.bitcoin.org

22

Sobre la Descentralización Como Clave para el Éxito

Traducción por **Arturo Monzón**

SATOSHI HABLA AQUÍ sobre la importancia de una moneda descentralizada como clave del éxito. Como se ha señalado anteriormente, la capacidad del gobierno para controlar el suministro de una moneda proporciona una manera fácil de financiar el gasto deficitario. Todas las monedas electrónicas controladas centralmente que han aparecido hasta ahora han sido desmanteladas por los gobiernos por diversas razones. Las razones típicas incluyen facilitar el lavado de dinero o la compra de drogas, a pesar de que el dólar estadounidense es la principal elección para estas actividades financieras.

Re: Implementación del Código Abierto Bitcoin de la Moneda P2P

Satoshi Nakamoto, 15 de febrero 2009 a las 16:42

Sepp Hasslberger escribió:

¿Podría haber sinergias con bitcoin?

http://opencoin.org/

Podría ser. Están hablando de la vieja casa de moneda central de Chaumian, pero tal vez solo porque eso era lo único disponible. Tal vez podrían estar interesados en ir en una nueva dirección.

Mucha gente descarta automáticamente la moneda electrónica por ser una causa perdida debido a todas las empresas que han fracasado desde la década de 1990. Espero que sea obvio que solo la naturaleza centralizada de esos sistemas fue lo que los condenó. Creo que esta es la primera vez que intentamos un sistema descentralizado, no basado en la confianza.

23

Sobre el Suministro de Dinero

Traducción por **Arturo Monzón**

SATOSHI EXPLICA su concepto general en este foro y hace un seguimiento sobre el problema del suministro de dinero frente a la población. Luego compara Bitcoin con metales preciosos y se refiere a una retroalimentación sobre lo que podría ocurrir con el precio cuando el número de usuarios crece más rápido que el suministro de bitcoins. Curiosamente, esto fue de hecho lo que ocurrió.

Imagínese si la población descubriera, a través de la experiencia de la vida real, lo que es vivir con una moneda que no pierda su valor, sino que en realidad gane valor. A medida que nuestra economía crece y nuestras capacidades de fabricación aumentan, los precios bajan. La única razón por la cual los precios no caen hoy - excepto en productos donde las mejoras son muy rápidas (por ejemplo, ordenadores) - es debido a la inflación monetaria causada por el gobierno.

Re: Implementación del código abierto Bitcoin de moneda P2P

Satoshi Nakamoto, 18 de febrero 2009 a las 20:50

Es una base de datos global distribuida, con adiciones a la base de datos por consenso de la mayoría, basada en el conjunto de reglas que siguen:

- Cuando alguien encuentra pruebas de trabajo para generar un bloque, obtiene algunas monedas nuevas
- La dificultad de la prueba de trabajo se ajusta cada dos semanas para apuntar a un promedio de 6 bloques por hora (para toda la red)
- Las monedas que se dan por bloque se dividen a la mitad cada 4 años

Se podría decir que las monedas son emitidas por la mayoría. Se emiten en una cantidad limitada y predeterminada.

Como ejemplo, si hay 1000 nodos, y 6 obtienen monedas cada hora, probablemente demore una semana antes de obtener algo.

Para la pregunta de Sepp, de hecho, no hay nadie que actúe como banco central o reserva federal para ajustar la oferta monetaria a medida que crece la población de usuarios. Eso habría requerido que una parte confiable determine el valor, pero no conozco una forma de que el software conozca el valor real de las cosas. Si hubiera alguna forma inteligente, o si quisiéramos confiar en que alguien administre activamente el suministro de dinero para vincularlo a algo, las reglas podrían haber sido programadas para eso.

En este sentido, es más propio de un metal precioso. En lugar de cambiar el suministro para mantener el mismo valor, el suministro está predeterminado y el valor cambia. A medida que la cantidad de usuarios crece, el valor por moneda aumenta. Tiene el potencial para un ciclo de retroalimentación positiva; a medida que los usuarios aumentan, el valor aumenta, lo que podría atraer a más usuarios para aprovechar el incremento de valor.

24

Lanzamiento de Bitcoin v0.1.3

Traducción por **Arturo Monzón**

EN ESTE LANZAMIENTO, el software ha arreglado temas de comunicación. Satoshi habla de la maduración de la cuenta regresiva para el descubrimiento de la prueba de trabajo en el bloque, es decir, la recompensa que obtienen los mineros al resolver un bloque.

[Lista Bitcoin] Bitcoin v0.1.3

Satoshi Nakamoto 2009-01-12 22:48:23

Parece que hemos terminado con los peores problemas de conexión a Internet. 0.1.3 soluciona un problema por el que las comunicaciones de tu nodo podrían desaparecer después de un tiempo. La red se está ejecutando ahora más fluidamente con esta versión.

Si has generado con éxito un bloque, verás que tienes una maduración de cuenta regresiva antes de poder gastarlo. Una vez que ha vencido, la columna de Crédito cambiará de 0.00 a 50.00. Para que un bloque sea válido, tiene que ser anunciado a la red y entrar en la cadena de bloques, por lo que Generate no se ejecuta si no estás conectado. Si generas un bloque sin estar conectado, la red no lo sabrá y continuará construyendo la cadena sin él, dejándolo atrás, y la cuenta regresiva de la maduración cambiaría a "(no aceptado)", cuando su nodo ve que no fue usado. Si resta 1 de la columna de estado, así es como cuántos bloques han sido puestos

en la cadena después del suyo.

Satoshi Nakamoto

25

Sobre Documentos de Sellado de Tiempo

Traducción por **Enrique Palacios Rojo**

AQUÍ, Hal Finney menciona que algunas personas sugirieron usar la cadena de bloques en los documentos para hacer un sellado del tiempo por medio de una función hash adicional (Ver la explicación anterior del hash criptográfico en la sección titulada *Función criptográfica hash - "una huella digital" en el Capítulo 2*).

[LISTA-BITCOIN] Bitcoin Vo.1 lanzamiento

Satoshi Nakamoto 2009-03-04 16:29:12

> Hal Finney escribió:
>
> Eso suena bien. También me gustaría poder ejecutar múltiples generadores de monedas/bloques en varias máquinas, todo por debajo de una dirección NAT única. No lo he intentado todavía así que no sé si funciona en el software actual.

La versión actual funcionará bien. Cada una se conectará en Internet, mientras que las conexiones entrantes solo llegan al host a través del puerto 8333.

Como optimización, haré un cambio "-connect = 1.2.3.4" para que sólo se conecte a una dirección específica. Se podría hacer que los nodos extras se conecten a su nodo primario, siendo sólo este el que se conecta a internet. Realmente no importa por ahora, ya que la red tendría que volverse enorme antes que haga que el ancho de banda sea insuficiente.

> Por cierto, no recuerdo si hablamos sobre esto, pero el otro día algunas personas mencionaron el sellado de tiempo seguro. Se refieren a poder probar que un cierto documento existía en un determinado momento en el pasado. Me parece que los bloques apilados del bitcoin serían perfectos para esto.
>
> ---

De hecho, Bitcoin es un servidor distribuido de sellado de tiempo seguro para transacciones. Con algunas líneas de código se podría crear una transacción con un hash extra de cualquier cosa que necesite ser sellada en el tiempo. Debería agregar un comando para el sellado del tiempo de un archivo de esta manera.

> > Más tarde quiero agregar interfaces para que sea realmente fácil de integrar en sitios web desde cualquier lenguaje del lado del servidor.
> >
> > ---
>
> Correcto, y me gustaría ver más de una interfaz de librería que podría ser llamada desde la programación o lenguajes de scripting, en el lado del cliente también.
>
> ---

Exactamente

Satoshi Nakamoto

http://www.bitcoin.org

26

Foro de Bitcointalk Mensaje de Bienvenida

Traducción por **Enrique Palacios Rojo**

SATOSHI ANUNCIA el lanzamiento de un nuevo foro dedicado a Bitcoin en *sourceforge.net*.

¡Bienvenido al nuevo foro Bitcoin!

Satoshi Nakamoto, 22 de noviembre 2009, 06:04:28 PM

¡Bienvenido al nuevo foro Bitcoin!

Aún se puede acceder al antiguo foro desde aquí:
http://bitcoin.sourceforge.net/boards/index.php

Volveré a publicar algunas conversaciones seleccionadas aquí y añadiré respuestas actualizadas a las preguntas donde pueda.

Preguntas y Respuestas - FAQ
http://bitcoin.sourceforge.net/wiki/index.php?page=FAQ

Descarga
http://sourceforge.net/projects/bitcoin/files/

27

Sobre Maduración de Bitcoin

Traducción por **Enrique Palacios Rojo**

LA MADURACIÓN es específica a los bitcoins recientemente creados como recompensas otorgadas a los mineros por su trabajo en la cadena de bloques. Una vez que un bloque tiene poca o ninguna posibilidad de convertirse en un bloque huérfano, la recompensa en forma de bitcoins es válida como para asignarlos de manera segura al minero.

¿Maduración en Bitcoin?

Satoshi Nakamoto, 22 de noviembre 2009, 06:31:44 PM

Maduración del Bitcoin

Publicado: jueves 01 de octubre, 2009 (14:12 UTC)

Desde la perspectiva del usuario, el proceso de maduración de bitcoin puede ser desglosado en 8 pasos:

1. La transacción inicial de la red que sucede cuando pinchamos sobre Genera Monedas.
2. El tiempo entre esa transacción inicial de red y cuándo la entrada del bitcoin esté lista para aparecer en el listado de todas las transacciones.

3. El cambio de entrada del bitcoin desde fuera del campo de Todas las transacciones hacia el campo dentro de Todas las transacciones.
4. El tiempo desde que aparece el bitcoin en la lista de Todas las transacciones y cuando la Descripción está lista para cambiar a Generado (50.00 maduran en x más bloques).
5. El cambio de Descripción ha Generado (50.00 maduran en x más bloques).
6. El tiempo entre el momento en que la Descripción dice Generado (50.00 maduran en x más bloques) a cuando está listo para cambiar a Generado.
7. El cambio de la Descripción ha Generado.
8. El tiempo que pasa después de que la Descripción haya cambiado a Generado.

¿Cuáles de estos pasos requieren conectividad de red, uso importante de CPU local y o uso significativo de CPU remoto? ¿Tienen nombres cada uno de estos pasos?

RE: ¿Maduración en Bitcoin?

Sirius-m, 22 de octubre 2009, 02:26 UTC

Por lo que sé, no hay transacciones de red cuando haces click en “Generar monedas”-tu ordenador solo comienza a calcular la próxima prueba de trabajo. El uso de CPU es del 100% cuando estás generando monedas.

En este ejemplo, la conexión de red es usada cuando transmiten la información sobre el bloque de prueba de trabajo que se ha creado (la cual da derecho a la nueva moneda). Generar monedas con éxito requiere una conectividad constante, para que se pueda comenzar a trabajar en el siguiente bloque cuando alguien obtiene el bloque actual antes que tú.

¿MADURACIÓN EN BITCOIN?

Satoshi Nakamoto, 22 de noviembre 2009, 06:34:21 PM

Es importante tener conectividad de red mientras estás intentando generar una moneda (bloque) y en el momento que se genera con éxito

1. Durante la generación (cuando la barra de estado dice "Generando" y se está usando la CPU para encontrar una prueba de trabajo), debe mantenerse constantemente en contacto con la red para recibir el último bloque. Si su bloque no se vincula con el último bloque, puede no ser aceptado.
2. Cuando se genera con éxito un bloque, es inmediatamente transmitido a la red. Otros nodos deben recibirlo y vincularlo para que sea aceptado como el nuevo bloque más reciente.

Piensa en ello como un esfuerzo de cooperación para hacer una cadena. Cuando agregas un enlace, primero se debe encontrar el final actual de la cadena. Si fueras a localizar el último enlace, deja pasar una hora y crea tu enlace, y entonces vincúlalo al enlace final de hace una hora, otros pueden haber agregado varios enlaces desde entonces y no van a querer usar tu enlace que ahora se bifurca en el medio.

Después de crear un bloque, el tiempo de maduración de 120 bloques es para asegurar completamente que el bloque sea parte de la cadena principal antes de que puede ser gastado. Tu nodo no está haciendo nada con el bloque durante ese periodo de tiempo, solo está esperando que se agreguen otros bloques después del tuyo. No hace falta estar online durante ese tiempo.

28

¿Cómo de anónimos son los Bitcoins?

Traducción por **Enrique Palacios Rojo**

AL CONTRARIO QUE UNA MALETA llena de billetes de 100 dólares, que se pueden mover sin dejar rastro, las transacciones de Bitcoin se registran en un libro público mayor. Aunque las direcciones de Bitcoin son anónimas por naturaleza, las transacciones realizadas en los nombres de estas direcciones no lo son.

¿CÓMO DE ANÓNIMOS SON LOS BITCOINS?

Satoshi Nakamoto, 25 de noviembre 2009, 06:17:23 PM

> ¿Pueden los nodos de la red saber el origen y el destino de las direcciones bitcoin a las que se envían las monedas? ¿Los bloques contienen una historia donde los bitcoins han sido transferidos y desde dónde?
>
> Los bitcoins se envían desde y hacia direcciones de bitcoin, que son esencialmente números aleatorios sin información que los identifique

---

Cuando se envía a una dirección IP, la transacción aún se escribe a una dirección de bitcoin. La dirección IP solo se usa para conectar el ordenador del destinatario para solicitar una nueva dirección bitcoin, dar la transacción directamente al destinatario y obtener una confirmación.

Los bloques contienen un historial de las direcciones de bitcoin a las que una moneda ha sido transferida. Si las identidades de las personas que usan las direcciones bitcoin no son conocidas y cada dirección es usada solo una vez, entonces esta información sólo revela que alguna persona desconocida ha transferido una cierta cantidad a otra persona.

La posibilidad de ser anónimo o pseudo anónimo depende de que no se revele ninguna información de identificación sobre uno mismo que lo relacione con las direcciones de bitcoin que se use. Si publica su dirección de bitcoin en la web, entonces está asociando esa dirección y cualquier transacción que se realice desde ella con el nombre con el que se ha publicado. Si ha publicado bajo un seudónimo que no se ha asociado con su identidad real, entonces sigues siendo pseudo anónimo.

Para una mayor privacidad, lo mejor es usar direcciones de bitcoin solo una vez. Se puede cambiar las direcciones con la frecuencia que se quiera utilizando Opciones->Cambiar su dirección. Las transferencias por dirección IP usan automáticamente una nueva dirección de bitcoin cada vez.

¿Pueden los nodos saber qué direcciones de bitcoin pertenecen a qué direcciones de IP?

No.

¿Hay una opción de línea de comando que ejecute el proxy sock la primera vez que se inicia Bitcoin?

En la próxima versión (versión 0.2), la línea de comando para ejecutarlo a través de un proxy desde la primera vez es:
bitcoin -proxy = 127.0.0.1:9050

El problema que tiene TOR es que el servidor IRC que Bitcoin utiliza inicialmente descubre otros nodos que prohíben los nodos de salida de TOR, como hacen todos los servidores IRC. Si ya se ha conectado antes, entonces ya ha sido trazado, pero para la primera vez, se necesitaría proporcionar la dirección de un nodo tal y como sigue:
bitcoin -proxy = 127.0.0.1:9050 -addnode = <someipaddress>

Si alguien ejecuta un nodo con una dirección IP estática que pueda aceptar conexiones entrantes se podría publicar su IP para usar para -addnode, siendo esto la mejor opción.

¿Qué sucede si se envía bitcoins a una dirección IP que tiene múltiples clientes conectados a través de una dirección de red traducida (NAT-network address translation - por sus siglas en inglés)?

Cualquiera que haya configurado su NAT para reenviar el puerto 8333 lo podrá recibir. Si tu router puede cambiar el número de puerto cuando se reenvía, puede permitir que más de un cliente lo reciba. Por ejemplo, si el puerto 8334 lo reenvía al puerto 8333 de un ordenador, entonces los que envían lo pueden mandar a "x.x.x.x:8334"

Si su NAT no puede traducir los números de puerto, entonces no hay una opción de línea de comando que cambie el puerto de entrada que vincula ese bitcoin, pero lo revisaré.

29

Algunas Preguntas Respondidas por Satoshi

Traducción por **Arturo Monzón**

EN ESTOS CORREOS, Satoshi responde a una amplia variedad de preguntas, como cuán anónimo es Bitcoin, el requisito de las copias de seguridad y lo que sucede en el caso de pérdida de monedas. Otra pregunta que se planteó fue si el código abierto de Bitcoin podría plantear un problema de seguridad ya que, por ejemplo, un minero estaba cambiando el código. Satoshi respondió que otros mineros no lo aceptarían, ya que sería una desviación del Protocolo de Bitcoin.

Re: Preguntas sobre Bitcoin

Satoshi Nakamoto, 10 de diciembre 2009, 08:49:02 PM

SmokeTooMuch escribió:

Hola, ayer me lancé sobre esta gran opción de pago.

He leído a través de muchos sitios, pero ahora tengo algunas preguntas para las que no he encontrado respuesta.

1. ¿Bitcoin es realmente anónimo? ¿Quiero decir total y completamente? ¿Mi ISP puede detectar que he enviado o recibido un pago de Bitcoin? ¿Tal vez incluso puede ver que estoy ejecutando Bitcoin en este momento?
2. Si entendí esto correctamente, mis socios de pago no pueden ver quién soy. ¿Esto significa que, ellos no pueden ver mi dirección IP real? ¿Solo la dirección de Bitcoin? ¿Incluso si él monitorea sus conexiones de red y esas cosas?
3. Si hay una manera de saber que estoy ejecutando Bitcoin para mi **ISP** o una forma de averiguar mi IP para mis socios de pago, ¿sería más seguro canalizar el tráfico de red a través de una VPN (pagada con Paysafecard, por ejemplo)? ¿Podría ser esto peligroso, porque el proveedor de VPN podrá capturar mi pago?
4. ¿Qué archivos necesitan ser respaldados con una copia de seguridad para no perder mi "dinero"? ¿Solo el wallet.dat o todo el directorio Bitcoin AppData?
5. ¿No es posible multiplicar una billetera y usarla en diferentes máquinas? De esta forma, duplicaría su dinero sin hacer nada por ello. ¿Hay medidas de seguridad para este caso?
6. Cuando alguien pierde su billetera, ¿habrá una forma de reproducir las monedas perdidas en el sistema? De lo contrario, los 21 millones máximos no serán correctos.

   (Me refiero a no recuperar las monedas perdidas para una persona, pero si se crearon todas las monedas de 21 millones, y alguien pierde su billetera con monedas de 1 millón, ¿los otros podrán crear estas monedas de 1 millón ahora o están totalmente perdidas para la red Bitcoin?)

7. He leído que actualmente hay alrededor de 130.000 bloques por ahí. En mi pc solo me muestra unos 24.000. ¿Hay algo mal o es esto un comportamiento normal?
8. Me temo que no entendí todo sobre la creación de bitcoin. ¿Cuántas monedas crea una máquina en 24 horas en promedio?
9. Sé que el puerto 8333 debe ser enviado a la máquina que ejecuta bitcoin. Ahora me pregunto si esto atañe para el TCP o el UDP.

   ¿Y se requiere este puerto para generar monedas? ¿O solo para transacciones de pago?

10. He visto que el código fuente de bitcoin está abierto para todos. ¿Puede ser esto un peligro real? Si el código es manipulado, las personas pueden crear más bitcoins que otros, ¿no? Esto sería una gran fuga de seguridad.
11. He visto un formulario para calcular las monedas que se crearán en un cierto período de tiempo. Tengo algo que hacer con la velocidad máxima y disponibilidad de CPU. Ya no puedo encontrarlo, así que te pido que me expliques la creación de la moneda. ¿Las máquinas más lentas producen tantas monedas como las de gama alta?
12. ¿Existen otros sistemas de intercambio o posibles socios de pago a excepción del nuevo estándar de libertad?
13. ¿Qué sucede cuando mi sistema falla? ¿Se guarda el monedero automáticamente o sólo cuando Bitcoin se cierra manualmente? (¿Tal vez incluso el ahorro en tiempo real cuando se crea una moneda o se realiza el pago?)
14. ¿Hay alguna manera de ver cuántos bitcoins se han generado hasta ahora? ¿Y cuántos años tiene Bitcoin?

Lo sé ... Muchas preguntas, pero estoy realmente interesado en tu servicio y quiero saberlo todo antes de empezar a usarlo más frecuentemente.

(Perdón por mi mal inglés . . .)

1-3: Para ese nivel de anonimato necesita conectarse a través de TOR, lo que será posible con la versión 0.2, que está a solo unas semanas. Voy a publicar instrucciones TOR en ese momento.

4: Versión 0.1.5: haga una copia de seguridad de todo el directorio %appdata%\Bitcoin. Versión 0.2: sólo puede respaldar wallet.dat.

5: No. Todo el diseño está pensado para prevenir eso.

6: Esas monedas nunca pueden ser recuperadas, y la circulación total es menor. Como se reduce la circulación efectiva, todas las monedas restantes valen un poco más. Es lo opuesto a cuando un gobierno imprime dinero y el valor del dinero existente disminuye.

7: Actualmente son 29,296 bloques. La circulación es el número de bloques multiplicado por 50, por lo que la circulación actual es de 1,464,800 btc.

Si solo tiene 24k bloques, no debe haber terminado la descarga del bloque inicial. Salga de Bitcoin y vuelva a iniciarlo. La versión 0.2 es mejor/más rápida en la descarga del bloque inicial.

8: Normalmente unos pocos cientos en este momento. Ahora es fácil, pero se hará más difícil a medida que la red crezca.

9: Buena pregunta, es TCP. El sitio web debe actualizarse para decir TCP puerto 8333.

El reenvío de puertos es para que otros nodos se puedan conectar a usted, por lo que le ayuda a mantenerse conectado porque puede conectarse con más nodos. También lo necesita para recibir pagos por dirección IP.

10: No, los otros nodos no aceptarán eso.

Ser código abierto significa que cualquiera puede revisar el código de forma independiente. Si fuera de código cerrado, nadie podría verificar la seguridad. Creo que es esencial que un programa de esta naturaleza sea de código abierto.

11: Máquinas más lentas producen menos monedas. Es proporcional a la velocidad del CPU.

12: Hay más por venir.

13: Utiliza una base de datos transaccional llamada Berkeley DB. No perderá datos en un bloqueo del sistema. Las transacciones se escriben en la base de datos inmediatamente cuando se reciben.

14: Por ahora, puedes multiplicar el total de bloques por 50. La red de Bitcoin lleva funcionando casi un año. El diseño y la codificación comenzaron en 2007.

Re: Preguntas sobre Bitcoin

SmokeTooMuch escribió:

Wow, muchas gracias por estas respuestas detalladas.

Pero hoy se me vino otra pregunta.

Digamos que sabemos que nuestro vecino usa Bitcoin, y también sabemos que recibirá un pago pronto (tal vez porque posee una tienda de internet y acepta bitcoin como opción de pago).

Además, sabemos que usa WLAN y su red no está protegida o está débilmente protegida. Lo mismo ocurre con la configuración del enrutador.

Ahora podemos iniciar sesión en la configuración de su enrutador, cambiar las direcciones IP para el puerto reenviado 8333 a nuestro sistema IP. Ahora nuestro cliente de bitcoin recibirá todos sus pagos.

¿Esto realmente va a funcionar?

Sé que esto es altamente criminal y el escenario es ... bueno, digamos "poco común", pero en teoría podría ocurrir, ¿no?

(No es que tenga un interés en dañar a la gente, pero sé que la gente criminal intentará muchas formas de obtener algo de dinero).

Por cierto: lo mismo debería funcionar cuando estás en un **grupo LAN** con configuración de enrutador desprotegido.

Editar: ¿O son estos escenarios totalmente imposibles porque no importa qué dirección IP usa el puerto, el pago irá a la dirección Bitcoin o IP definida por el pagador?

Eso es cierto, con la opción de enviar a IP, está enviando a quien responda esa IP. Enviar a una dirección de bitcoin no tiene ese problema.

El plan es implementar una opción de dirección IP + bitcoin que tenga los beneficios de ambos. Todavía usaría una dirección diferente para cada transacción, pero el receptor firmaría la dirección de uso único con la dirección de bitcoin dada para demostrar que pertenece al receptor previsto.

30

Sobre la "Deflación Natural"

Traducción por **Arturo Monzón**

El TEMA DE PÉRDIDAS DE MONEDAS ha sido cubierto pocas veces. Se le conoce como "deflación natural". Aquí hay dos discusiones relacionadas con este tema. Tenga en cuenta que las monedas nacionales hoy nacen de la deuda. Cuando se toma un préstamo para un automóvil o una casa, la misma cantidad de dólares es creado, y, una vez que se paga el préstamo, la moneda desaparece. Un entorno deflacionario en nuestro sistema actual significa que el valor de los activos (casas, automóviles, etc.) disminuirá, pero, dado que se han solicitado préstamos para comprarlos, se producirá una cascada de bancarrotas porque las personas poseen más de lo que pueden comprar.

Por otro lado, cuando una moneda está intrínsecamente ligada a una cantidad, los préstamos son extremadamente raros. Antes de la creación de la Reserva Federal en los EE. UU. en 1913, la mayoría de las compras se realizaban en efectivo, incluso para casas. La implicación de una moneda fija en valor, o incluso una que gana en valor con el tiempo, es importante. La gente no tendría que especular en fondos mutuos para su jubilación; en su lugar, uno podría simplemente ahorrar el dinero para hacer una compra. Esto es típicamente llamado "atesorar" por los medios financieros, pero también lo son los fondos de jubilación. Básicamente, ahorrar significa demorar el consumo de material, recursos y tiempo para que otros, incluidas las empresas que inviertan en nuevas plantas, puedan mejorar la productividad actual. Más tarde disfrutará de su jubilación debido a este retraso en el consumo. El concepto de dinero es

más abstracto de lo que la mayoría de la gente piensa.

Re: Algunas sugerencias

Satoshi Nakamoto, 13 de diciembre 2009, 04:51:25 PM

> The Madhatter escribió:
>
> Una pregunta rápida sobre "deflación natural" (como la llamo). Me di cuenta de que es posible gastar en direcciones antiguas que ya no funcionan. En esencia, las monedas no pueden ser reclamadas. ¿No habría un efecto de deflación natural debido a esto? Quiero decir, si las monedas alcanzan un máximo de 21,000,000, ¿no habría un número de monedas lentamente revertidas por debido a los errores de pago?
>
> ---

Habría un interruptor de línea de comando en tiempo de ejecución para indicarle que se ejecutará sin UI. Todo lo que necesita hacer es no crear la ventana principal. Una forma simplista sería desactivar "pframeMain->Show" y "ptaskbaricon->Show" en ui.cpp. A la red no les importa que la UI no esté allí. La única otra UI es un cuadro de mensaje en CheckDiskSpace si se queda sin espacio en el disco.

Luego, una utilidad de línea de comando separada para comunicarse con él para hacer cosas. No estoy seguro de qué nombre debería tener.

"Deflación natural"... Me gusta ese nombre. Sí, habrá una deflación natural debido a errores de pago y pérdida de datos. La creación de monedas será eventualmente lo suficientemente lento como para ser superada por la deflación natural y tendremos una deflación neta.

La segunda conversación:

Re: Bitcoins agonizante

Satoshi Nakamoto, 21 de junio 2010, 05:48:26 PM

> Hola,
>
> si alguien pierde su billetera (por ejemplo, debido a una rotura del disco) no puede recuperar sus monedas, ¿o sí?
>
> Entonces, ¿cada vez que una persona pierde monedas, se pierden para siempre? ¿Entonces la red bitcoin se reducirá lentamente con el tiempo? (¡Porque siempre habrá gente que pierde billeteras!)
>
> TIA
>
> virtualcoin

Las monedas perdidas solo hacen que las monedas de los demás un poco más valiosas. Piense en ello como una donación para todos.

> Cita de: laszlo el 21 de junio 2010, 01:54:29 PM
>
> Sin embargo, me pregunto si existe algún punto en el que la dificultad de generar una nueva base de monedas sea tan alta que, ¿tendría más sentido tratar de recuperar las llaves de las monedas perdidas o robar las monedas de otras personas? La dificultad de eso es realmente alta, así que por ahora tiene mucho más sentido generar, pero solo me pregunto ¿cuáles son las cifras reales? ¿Alguna vez se volvería más productivo? Tal vez Satoshi puede abordar estas cuestiones…

Las computadoras tienen que ser 2^200 veces más rápidas antes que eso comience a ser un problema. Alguien con mucho poder de cómputo podría ganar más dinero generando que tratando de robarlo.

31

Bitcoin Versión 0.2 Está Aquí!

Traducción por **Arturo Monzón**

SATOSHI ANUNCIA la versión 0.2 de Bitcoin.

Bitcoin versión 0.2 está aquí!

Satoshi Nakamoto, 16 de diciembre 2009, 10:45:36 PM

Bitcoin versión 0.2 está aquí!

Descargar los links:

http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.2.0-win32-setup.exe/download

http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.2.0-win32.zip/download

http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.2.0-linux.tar.gz/download

Nuevas características

- Martti Malmi
- Minimiza la opción de bandeja del sistema
- Inicio automático de arranque para que pueda mantenerlo funcionando en segundo plano automáticamente
- Nuevo diseño de diálogo de opciones para futura expansión
- Programa de instalación para Windows
- Versión Linux (probado en Ubuntu)

Satoshi Nakamoto

- Soporte multiprocesador para la generación de monedas
- Soporte proxy para uso con TOR
- Se corrigieron algunas ralentizaciones en la descarga del bloque inicial

Muchas gracias a Martti Malmi (sirius-m) por todo su trabajo de codificación y por albergar el nuevo sitio y este foro, y a New Liberty Standard por su ayuda en la prueba de la versión de Linux.

32

Recomendación Sobre Formas de Hacer un Pago Para un Pedido

Traducción por **Arturo Monzón**

HAY MÚLTIPLES TIPOS de algoritmos criptográficos utilizados en encriptación asimétrica. Aquí el punto principal de Satoshi sobre el razonamiento para usar la criptografía de curva elíptica (EDCSA) en lugar de RSA es el tamaño de la transacción (bytes). Para que el tamaño de cada transacción sea lo más pequeño posible, para que el tamaño de bloque permanezca manejable, Satoshi decidió usar EDCSA.

Re: Prueba de un principiante – ¿alguien quiere comprar una imagen por $ 1?

Satoshi Nakamoto, 29 de enero 2010 12:22:13 PM

Las formas recomendadas para hacer un pago para un pedido:

1. El comerciante tiene una dirección IP estática, el cliente lo envía con un comentario.
2. El comerciante crea una nueva dirección de bitcoin, se la da al cliente y el cliente la envía a esa dirección. Esta será la forma

estándar para que el software del sitio web lo haga.

RSA vs ECDSA: no es el tamaño del ejecutable, sino el tamaño de los datos. Pensé que no sería práctico si la cadena de bloques, las direcciones de bitcoin, el espacio en disco y los requisitos de ancho de banda fueran de magnitudes mayores. Además, incluso si usara RSA para los mensajes, aún tendría sentido hacerlo para toda la red bitcoin con ECDSA y usar RSA en paralelo solo para la parte del mensaje. En todo caso, todo lo que se ha implementado hasta ahora se ha implantado como debería.

Podemos encontrar una mejor manera para esto mucho más adelante. Podría usarse un separado (tal vez existente) correo electrónico o infraestructura IM para pasar mensajes, y en lugar de RSA, tal vez simplemente ponga un hash del mensaje en la transacción para demostrar que la transacción es para la orden descrita en el mensaje. El mensaje debería incluir un tipo de marca para que nadie pueda romper el hash y revelar el mensaje corto.

33

Sobre la Dificultad de la Prueba de Trabajo

Traducción por **Beatriz Lizarraga**

SATOSHI DISCUTE la creciente dificultad de la prueba de trabajo a medida que comienzan a participar más mineros.

La Dificultad de la Prueba de Trabajo Aumenta

Satoshi Nakamoto, 05 de febrero 2010, 07:19:12 PM

Tuvimos nuestro primer ajuste automático de la dificultad de prueba de trabajo el 30 de diciembre de 2009.

La dificultad mínima es de 32 zero bits, por lo que incluso si solo una persona ejecuta un nodo, la dificultad no será más fácil que eso. Durante la mayor parte del año pasado, estuvimos revoloteando por debajo del mínimo. El 30 de diciembre rompimos por encima y el algoritmo se ajustó hacia una mayor dificultad. Desde entonces se ha vuelto más difícil en cada ajuste.

El ajuste del 04 de febrero llevó de 1,34 veces la dificultad a 1,82 veces más difícil que el año pasado. Eso significa que solo genera el 55% de monedas a igual cantidad de trabajo.

La dificultad se ajusta proporcionalmente al esfuerzo total sobre la red. Si el número de nodos se duplica, la dificultad también se duplicará, devolviendo el total generado a la tasa objetivo.

Para aquellos con inclinaciones técnicas, la dificultad de la prueba de trabajo se puede ver buscando en "target:" en debug.log. Es un número hexadecimal sin signo de 256 bits, cuyo valor de SHA-256 tiene que ser menor que generar un bloque con éxito. Se ajusta cada 2016 bloques, generalmente dos semanas. Ahí es cuando imprime "GetNextWorkRequired RETARGET" en debug.log.

mínimo
0000000ffff0000000000000000000000000000000000000000000000000000
30/12/2009
00000000d86a0000000000000000000000000000000000000000000000000000
0
11/01/2010
00000000c4280000000000000000000000000000000000000000000000000000
0
25/01/2010
00000000be7100000000000000000000000000000000000000000000000000
0
04/02/2010
000000008cc3000000000000000000000000000000000000000000000000000
14/02/2010
0000000065465700000000000000000000000000000000000000000000000000
0
24/02/2010
0000000043b3e500000000000000000000000000000000000000000000000000
0
08/03/2010
00000000387f6f0000000000000000000000000000000000000000000000000
21/03/2010
0000000038137500000000000000000000000000000000000000000000000000
0
01/04/2010
000000002a1115000000000000000000000000000000000000000000000000
0
12/04/2010
0000000020bca7000000000000000000000000000000000000000000000000
0
21/04/2010
0000000016546f0000000000000000000000000000000000000000000000000

04/05/2010
0000000013ec530000000000000000000000000000000000000000000000000
0
19/05/2010
00000000159c240000000000000000000000000000000000000000000000000
0
29/05/2010
000000000f67c0000000000000000000000000000000000000000000000000
11/06/2010
000000000eba640000000000000000000000000000000000000000000000000
0
24/06/2010
000000000d3142000000000000000000000000000000000000000000000000
0
06/07/2010
000000000ae493000000000000000000000000000000000000000000000000
0
13/07/2010
0000000005a3f4000000000000000000000000000000000000000000000000
16/07/2010
000000000168fd0000000000000000000000000000000000000000000000000
27/07/2010
00000000010c5a000000000000000000000000000000000000000000000000
0
05/08/2010
0000000000ba18000000000000000000000000000000000000000000000000
0
15/08/2010
0000000000800e000000000000000000000000000000000000000000000000
0
26/08/2010
000000000069200000000000000000000000000000000000000000000000000
0

fecha, factor de dificultad, % cambio

2009 1.00

30/12/2009	1.18	+ 18%
11/01/2010	1.31	+ 11%

25/01/2010	1.34	+2%
04/02/2010	1.82	+36%
14/02/2010	2.53	+39%
24/02/2010	3.78	+49%
08/03/2010	4.53	+20%
21/03/2010	4.57	+9%
01/04/2010	6.09	+33%
12/04/2010	7.82	+28%
21/04/2010	11.46	+47%
04/05/2010	12.85	+12%
19/05/2010	11.85	-8%
29/05/2010	16.62	+40%
11/06/2010	17.38	+5%
24/06/2010	19.41	+12%
06/07/2010	23.50	+21%
13/07/2010	45.38	+93%
16/07/2010	181.54	+300%
27/07/2010	244.21	+35%
05/08/2010	352.17	+44%
15/08/2010	511.77	+45%
26/08/2010	623.39	+22%

34

Sobre el Límite de Bitcoin y la Rentabilidad de los Nodos

Traducción por **Beatriz Lizarraga**

LOS CORREOS ORIGINALES en este hilo cuestionaron la rentabilidad de los mineros cuando el nivel de dificultad aumenta y la cantidad de recompensas de bitcoin disminuye (era de 50 BTC al momento de estas publicaciones, pero se redujo a 25 BTC más tarde a principios de 2013. En el 2016 la recompensa se volvió a reducir a 12.5 BTC. - A este proceso se le conoce como Halving. Nota del traductor).

Re: El modelo económico actual de Bitcoin es Insostenible

Satoshi Nakamoto, 21 de febrero 2010, 05:44:24 PM

---

xc escribió:

No echéis a sudar. Nadie murió nunca de una "espiral deflacionista" :-) Estoy de acuerdo con "Yo no soy anónimo". El mercado elegirá la mejor moneda tipo bitcoin. Sin embargo, creo que las reglas en las que Satoshi fundó Bitcoin serán más que adecuadas para el futuro de una próspera economía bitcoin.

Todo el mundo sabe exactamente lo rápido que crecerá el suministro de bitcoins: está grabado a piedra en las reglas de la programación y la red bitcoin. Aunque es cierto que no existe actualmente un mercado totalmente desarrollado para dar un precio real a los bitcoins, tales mercados e intercambios están siendo desarrollados. En lo que concierne a los futuros generadores de bitcoins, la cuestión no es cuánto "exigirá ... para compensar sus gastos". La pregunta que se hará a sí mismo es "dados los valores de mercado actuales y mi capacidad para utilizar la electricidad y los recursos de la CPU, ¿me vale la pena generar bitcoins?". Si la respuesta es sí, él participa. Si es no, dejará de intentar extraer bitcoins y se centrará en intercambiar activos tangibles con bitcoins que sirven como intermediario apropiado. Si no está seguro, seguirá intentándolo por un tiempo y luego tomará una decisión final.

El número de nodos y la potencia computacional asociada de la CPU fluirá, y ese flujo competitivo permitirá que los costes se aproximen al valor (y no al revés). El valor será establecido por los mercados y por la demanda de uso de bitcoin como intermediario comercial (un dinero). En un futuro lejano, la competencia de los costes de transacción jugará un papel más importante para el potencial operador de un nodo.

Al contrario de la paradoja del argumento de ahorro que presentas, de recolectar bitcoins y guardarlos con la esperanza de ganar poder adquisitivo a través de la deflación, no es algo malo. Permitirá la acumulación del capital bitcoin y posibilitará la compra de mayores inversiones de capital. En el futuro, incluso podría haber bancos bitcoin que presten bitcoins ahorrados con tasas de interés establecidas en el mercado, disminuyendo así los efectos del acaparamiento. Todo este maravilloso ahorro, sin embargo, tiene un precio: el retraso de la gratificación de los deseos presentes. Desde la perspectiva del potencial ahorrador, la cuestión siempre será negar los deseos actuales de comprar activos tangibles reales frente a las posibilidades futuras de comprar más, más tarde. Esta preferencia temporal varía naturalmente en función de la persona y sus circunstancias.

Dado el hecho de que los bitcoins son por su naturaleza electrónica fácilmente divisibles, los precios podrán ajustarse fácilmente a las presiones deflacionarias. Si muchos están ahorrando, los precios caerán

> y la tasa de interés bajará. Esto fomenta la demanda (precios más bajos) y disminuye el deseo de ahorrar (menos interés).
>
> XC

Excelente análisis, xc.

Un precio de mercado racional para algo que se espera que aumente en valor, ya reflejará el valor presente de los incrementos de expectativas futuras. Mentalmente haces una estimación de probabilidad equilibrando las posibilidades de que siga aumentando.

En ausencia de un mercado para establecer el precio, la estimación de NewLibertyStandard basada en el coste de producción es una buena suposición y un servicio útil (gracias). El precio de cualquier producto tiende a gravitar hacia el coste de producción. Si el precio está por debajo del coste, entonces la producción se ralentiza. Si el precio está por encima del coste, las ganancias se pueden crear generando y vendiendo más. Al mismo tiempo, el aumento de la producción aumentaría la dificultad, empujando el coste de generación en el precio.

En años posteriores, cuando la nueva generación de monedas sea un pequeño porcentaje de la oferta existente, el precio de mercado determinará el coste de producción más que al revés.

Por el momento, el esfuerzo de generación está aumentando rápidamente, lo que sugiere que la gente estima que el valor presente es mayor que el coste de producción actual.

35

Sobre la Posibilidad de Colisiones de Direcciones Bitcoin

Traducción por **Beatriz Lizarraga**

LAS DIRECCIONES Bitcoin se crean a partir de un hash de las direcciones públicas, y se muestra cierta preocupación acerca de una posible colisión, en la que dos individuos podían asignar por azar una misma dirección de Bitcoin. Tenga en cuenta que un hash de 160 bits representa 2 a la potencia de 160 o 1.46×10^{48} posibilidades, y, por lo tanto, la probabilidad de que se produzca una colisión es extremadamente remota.

Re: Colisiones de direcciones Bitcoin

Satoshi Nakamoto, 23 de febrero 2010, 09:22:47 AM

NewLibertyStandard escribió:

Aunque es extremadamente improbable, ¿qué pasaría si dos clientes de Bitcoin generarán la misma dirección de Bitcoin? ¿Se entregarían los pagos a cualquier cliente que encontrará el pago primero? Si existe un mecanismo para evitar tales colisiones, por favor explíquelo.

Hay un par de claves pública/privada por separado para cada dirección de bitcoin. No tiene una sola clave privada que desbloquea todo. Las direcciones de bitcoin son un hash de 160 bits de clave pública, todo lo demás en el sistema es de 256 bits.

Si se diera una colisión, el colisionador podría gastar el dinero enviado a esa dirección. Solo el dinero enviado a esa dirección, no toda la billetera.

Si usted estuviera tratando de hacer una colisionar intencionalmente, le supondría 2^126 veces más tiempo generar una dirección de bitcoin colisionante que generar un bloque. Podría haber conseguido mucho más dinero generando bloques.

La semilla aleatoria es muy minuciosa. En Windows, utiliza todos los datos del monitor de rendimiento que miden cada bit del rendimiento del disco, las métricas de la tarjeta de red, el tiempo del CPU, la paginación, etc. desde que se inicia su ordenador. Linux tiene un colector de entropía incorporado. Además, cada vez que mueves el mouse dentro de la ventana de Bitcoin estás generando entropía, y la entropía se captura a partir del tiempo de las operaciones del disco.

36

Código QR

Traducción por **Beatriz Lizarraga**

SURGIERON DOS conversaciones relacionadas con el código QR para teléfonos móviles. Basándose en una sugerencia original del usuario *ec* en el foro, Satoshi sugirió usar el código QR para la dirección bitcoin de pagos en el punto de venta, una práctica común en la actualidad.

Re: Esquema URI para bitcoin

Satoshi Nakamoto, 24 de febrero 2010, 05:57:43 AM

Eso estaría bien en el punto de venta. La caja registradora muestra un código QR codifica una dirección e importe de bitcoin en una pantalla y lo fotografía con tu teléfono móvil.

https://bitcointalk.org/index.php?topic=177.msg1814#msg1814

Re: Bitcoin móvil

Satoshi Nakamoto, 24 de febrero 2010, 05:57:43 AM

Cita de: sirius-m el 10 de junio 2010, 01:51:16 PM

Por supuesto, puedes utilizar servicios como vekja.net o mybitcoin.com en un navegador móvil, depositando dinero allí en la medida en que

confíes en ellos.

Creo que esa es la mejor opción ahora mismo. Al igual que el dinero en efectivo, no guardas todo tu dinero neto en el bolsillo, sólo llevas dinero para gastos imprevistos mientras das una vuelta.

Podrían hacer una versión más pequeña de la web optimizada para dispositivos móviles. Si hubiera una aplicación, podría ser una interfaz para una de ellas, con la función principal de lector de código QR, o tal vez ya existe una aplicación universal de lectura de códigos QR que los sitios web puedan diseñar para aceptar escaneos.

Si hubiera una aplicación de iPhone que fuera solo una interfaz para vekja o mybitcoin, sin involucrar a una gran P2P, ¿la aprobaría Apple? y si no, ¿en base a qué? En su lugar, siempre podría ser una aplicación de Android. Sin embargo, no es realmente necesaria una aplicación, solo un sitio web adaptado a móvil.

Una interfaz web para tu propio servidor Bitcoin en casa no sería una solución para todo el mundo. La mayoría de los usuarios no tienen una dirección IP estática y es demasiado complicado configurar el reenvío de puertos.

37

Icono/Logo Bitcoin

Traducción por **Beatriz Lizarraga**

SATOSHI PRESENTA un logotipo/icono para usar con Bitcoin y lo hace libre de derechos de autor. Pero este ya no es el logo que usa bitcoin.org. El logotipo actual es este:

(See http://commons.wikimedia.org/wiki/File:Bitcoin.svg)

New icono/logo

Satoshi Nakamoto, 24 de febrero 2010 09:24:23 PM

Nuevos iconos, ¿qué opináis? ¿mejor que el antiguo?

Imagen a tamaño completo de 530 x 529 para escalar a tamaños personalizados: http://www.bitcoin.org/download/bitcoin530.png

La sombra de la perspectiva era demasiado gruesa en los tamaños más grandes. Actualicé 32, 48 y el tamaño completo.

Líbero estas imágenes al dominio público (sin derechos de autor). Solicito que los trabajos derivados se hagan de dominio público.

> Cita de: Sabunir el 25 de febrero 2010, 02:28:49 AM
>
> Excelente. Debería ser un buen recurso para los que participan en el concurso de banners. ¿Por qué dimensiones desiguales?
>
> Mi única sugerencia sería hacer que el texto de la moneda se destaque más. En pequeñas resoluciones los contornos tienden a no ser viables, por lo que una mejor opción puede ser experimentar con el contraste. Hacer el texto significativamente más oscuro que el resto de la moneda probablemente aumentaría la legibilidad. Alternativamente, podría hacer que el círculo interno sea más oscuro y el texto más claro.

Buena sugerencia. Hice la B ligeramente más clara y el fondo ligeramente más oscuro. Muy ligeramente. El primer plano ahora es exactamente del mismo color que el BC antiguo.

Está bastante bien si no puedes leer fácilmente la B en 16x16. En ese tamaño solo necesitas ver que es una moneda. No importa tanto lo que está grabado en relieve, solo que hay algún detalle, no parecería una moneda si fuera un círculo liso en blanco.

Es un poco más ancho que alto por la perspectiva oscura debajo va más hacia la derecha que hacia abajo.

Terminé y publiqué las versiones 32x31 y 48x47 en el primer mensaje. Me gusta mucho la 48.

¿Qué opináis los demás sobre el símbolo B con las dos líneas a través del exterior? ¿Podemos vivir con eso como nuestro logo?

> Cita de: Cdecker el 27 de febrero 2010, 03:24:07 AM

> ¿Qué tal una versión SVG? De esa forma, podríamos generar automáticamente versiones más pequeñas y más grandes según sea necesario.
>
> ———————————————————————————————

No sé cómo hacer un SVG, pero hice el original muy grande, más de 500 píxeles de ancho, por lo que puede ser reducido. Daré el original cuando haya terminado.

He tenido que personalizar cada tamaño de icono para que las líneas verticales se posasen cuadradas en sus píxeles, de lo contrario quedan feas, borrosas e inconsistentes. Así es el desafío de hacer íconos. El original será bueno para escalar a tamaños personalizados entre 48 y 500, pero no más pequeños.

38

Licencia GLP Versus Licencia MIT

Traducción por **Beatriz Lizarraga**

UNA SUGERENCIA para crear un logotipo de "aceptamos Bitcoin" tenía una licencia GPL. Aquí, Satoshi afirma que prefiere la licencia MIT, la misma licencia de código abierto que Bitcoin software usa.

Re: Haga su logotipo "aceptamos Bitcoin"

Satoshi Nakamoto, 24 de febrero 2010, 09:53:52 p.m.

Si tienes material de GPL, tengo que evitar usarlo. Nada en contra de GPL per-se, pero Bitcoin es un proyecto de licencia de MIT. Cualquier cosa GPL por favor marcarlo claramente como tal.

39

Sobre la Regulación de Transferencia de Moneda

Traducción por **Arturo Monzón**

EN ESTA PUBLICACIÓN, Satoshi sugiere un servicio donde los compradores y vendedores de bitcoins puedan reunirse en persona para completar la compra/venta de bitcoins y así evitar cualquier tipo de regulación. Ambas partes podrían traer un dispositivo con capacidad de acceso a Internet, o se reuniría en un lugar que tenga computadoras de acceso público (por ejemplo, una biblioteca o un cibercafé). El comprador presumiblemente pagaría en efectivo y le proporcionará al vendedor su dirección para que se pudiera completar la transferencia. Un servicio que permite a los compradores y vendedores encontrarse unos a otros existe hoy (ver por ejemplo *localbitcoins.com*).

Re: Regulaciones de Transferencia de Dinero

Satoshi Nakamoto, 03 de marzo 2010, 04:28:56 AM

Cuando haya suficiente magnitud, tal vez puede haber un sitio de intercambio que no realice transferencias, que sólo conecte compradores y vendedores para que ambos intercambien directamente, de forma similar a como funciona e-bay.

Para hacerlo más seguro, el sitio de intercambio podría actuar como un

depósito en garantía para el comprador de bitcoin. El vendedor pone el bitcoin en custodia, y el comprador envía el pago convencional directamente al vendedor. El servicio de intercambio no maneja dinero del mundo real.

Esto sería un paso mejor que e-bay. E-bay se las arregla para funcionar bien a pesar de que los bienes enviados no se pueden recuperar si el pago no se realiza.

40

Sobre la Posibilidad de Una Debilidad Criptográfica

Traducción por **Arturo Monzón**

VARIOS HILOS cubrieron diferentes problemas a los que Satoshi sugirió la misma solución. Dos de los hilos siguientes se refieren al SHA-256, que es la función hash criptográfica usada para crear el "mensaje resumen" de los bloques utilizados como libro de contabilidad público, cada uno con un conjunto de transacciones de bitcoin. SHA-256 es utilizado por la industria bancaria y otras instituciones financieras. Si alguna debilidad fuera descubierta algún día en este método de cifrado, podría afectar a toda la industria financiera, que podría verse forzada a cambiar a un nuevo método. Satoshi sugiere la misma política para Bitcoin.

El segundo hilo estaba relacionado con el descubrimiento de una gran debilidad criptográfica. Al principio, Satoshi se refiere a su publicación anterior en “SHA-256 Colisiones”, pero el usuario identificado como *llama* especifica el caso donde se descubre una debilidad importante en el código criptográfico de la curva elíptica, que se utiliza para la clave privada de Bitcoin.

Re: Tratando con Colisiones SHA-256

Satoshi Nakamoto, 14 de junio de 2010, 08:39:50 a.m.

> Cita de: lachesis el 14 de junio 2010, 01:01:11 AM
>
> Un matemático amigo mío señaló que hay muy pocos o ningún protocolo hash que haya sobrevivido durante 10 años o más. ¿Cuál sería la solución de Bitcoin si SHA256 se rompiera mañana?
>
> SHA-256 es muy fuerte. No es como el paso incremental de MD5 a SHA1. Puede durar varias décadas, a menos que haya un ataque de innovación masivo.

Si SHA-256 llega a romperse del todo, creo que podríamos llegar a un acuerdo sobre cuál sería la cadena de bloque honesta antes que comenzara el problema, conectarla y continuar desde allí con una nueva función hash.

Si la ruptura viene de forma gradual, podríamos hacer la transición a un hash nuevo de una manera ordenada. El software podría ser programado para comenzar a usar un nuevo hash después de un cierto número de bloque. Todos tendrían que actualizarse en ese momento. El software podría guardar el nuevo hash de todos los bloques antiguos para asegurarse de que no se pueda usar un bloque diferente con el mismo hash.

Re: CRISIS IMPORTANTE

Satoshi Nakamoto, 10 de julio 2010, 04:26:01 PM

> Cita de: llama el 01 de julio 2010, 10:21:47 PM
>
> Satoshi, esa sería de hecho una solución si SHA se rompiera (sin duda la crisis más probable), porque aún podríamos reconocer a los propietarios de dinero válido por su firma (su clave privada aún estaría segura).

> Sin embargo, si algo sucediera y las firmas estuvieran comprometidas (¿tal vez se resuelva la factorización de enteros, ordenadores cuánticos?), entonces incluso acordar el último bloque válido sería inútil.
>
> ---

Es cierto, si eso sucediera repentinamente. Si sucediera gradualmente, aún podemos hacer la transición a algo más fuerte. Cuando ejecuta el software actualizado por primera vez, se volvería a firmar todo su dinero con el nuevo algoritmo de firma más sólido. (creando una transacción y enviándose a uno mismo el dinero con la firma más fuerte).

Re: Hash ( ) función no segura

Satoshi Nakamoto, 16 de julio de 2010, 04:13:53 PM

SHA256 no es como el paso del bit 128 al bit 160.

Para usar una analogía, se parece más al paso del espacio de dirección de 32-bits a 64-bits. Rápidamente nos quedamos sin espacio de direcciones con computadoras de 16 bits, nos quedamos sin espacio de direcciones con computadoras de 32 bits a 4 GB, eso no significa que vamos a agotarnos de nuevo con 64 bits pronto.

SHA256 no va a ser roto por las mejoras computacionales de la ley de Moore en nuestras vidas. Si se llegara a romper, será por algún método revolucionario de craqueo. Un ataque que pudiera vencer completamente a SHA256, como para llevarlo dentro de un rango computacionalmente tratable, tiene una buena posibilidad de golpear también a SHA512.

Si vemos una debilidad en SHA256 que se aproxima gradualmente, podemos hacer la transición a una nueva función hash después de un cierto número de bloques. Todos tendrían que actualizar su software hasta ese número de bloque. El nuevo software mantendría un hash nuevo de todos los bloques antiguos para asegurarse de que no sean reemplazados por otro bloque con el mismo hash.

41

Sobre una Variedad de Tipos de Transacciones

Traducción por **Jose Manuel Arenillas**

ESTA PUBLICACIÓN es un poco más técnica que otras publicaciones aquí presentadas. No obstante, he decidido incluirla porque es útil para explicar la razón por la que la primera implementación del diseño central soportaba varios tipos de transacciones como forma de evitar grandes modificaciones a futuro.

Re: Transacciones y Scripts: DUP HASH 160 . . . EQUALVERIFY CHECKSIG

Satoshi Nakamoto, 17 de junio 2010, 06:46:08 PM

> Cita de: Gavin Andresen, 17 de junio 2010, 11:38:31 AM
>
> Estoy escribiendo una pequeña herramienta que disecciona el fichero wallet.dat de Bitcoin, principalmente porque quiero entender mejor cómo funciona Bitcoin exactamente.
>
> Y veo que las salidas de las transacciones tienen un valor (el número de bitcoins) y un puñado de bytes que se han generado a través del pequeño lenguaje de scripting parecido a Forth construido en bitcoin. Por ejemplo: ['TxOut: value: 100.00 Script: DUP HASH160 6fad...ab90 EQUALVERIFY CHECKSIG']

> Primero: me pone un poco nervioso que bitcoin tenga un lenguaje de scripting, aunque es un lenguaje de scripting realmente simple (no hay bucles, no hay punteros, nada excepto matemáticas y criptografía) Me pone nervioso porque es más complicado y la complicación es la enemiga de la seguridad. También hace más difícil crear una segunda implementación compatible. Pero creo que lo puedo asumir.
>
> Repasando el código, las nuevas transacciones se verifica poniendo la firma y la clave pública sobre la pila del intérprete y ejecutando el script TxOut (¿lo he entendido bien?).
>
> ¿Podría escribir código para crear transacciones con cualquier script válido en el TxOut?
>
> Por ejemplo, ¿podría crear una TxOut con un script de: OP_2DROP OP_TRUE. . . para crear una moneda que cualquiera pudiera gastar?
>
> Y, ¿es esta flexibilidad en los tipos de monedas creadas la razón de estar programado de esta manera?

La naturaleza de Bitcoin es tal, que una vez publicada la versión 0.1, el diseño base estará escrito en piedra para el resto de su vida. Por esta razón quise diseñarlo de tal manera que soportara cualquier tipo de transacción que pudiera pensar. El problema era que, cada una requería campos de datos y código específico así se utilizara o no, y sólo cubría un caso especial cada vez. Hubiera sido una explosión de casos especiales. La solución fue el script, que generaliza el problema de tal manera que las partes involucradas en la transacción pueden describir su transacción como un predicado que los nodos evalúan. Los nodos sólo tienen que entender la transacción hasta el punto de evaluar si las condiciones del emisor se cumplen.

El script es de hecho, un predicado. Es sólo una ecuación que devuelve verdadero o falso. Predicado es una palabra larga y poco común así que lo llamé script.

El receptor del pago comprueba el script con una plantilla. Por ahora el receptor sólo acepta dos plantillas: pago directo y dirección bitcoin. Futuras versiones podrán añadir más plantillas para más tipos de transacciones y los nodos que ejecuten esas versiones o superiores podrán recibirlas. Todas las versiones de los nodos de la red pueden verificar y

añadir cualquier nueva transacción a un bloque, aunque no sepan interpretarlas.

El diseño admite una tremenda variedad de posibles tipos de transacciones que diseñé hace años. Operaciones de depósito en garantía, contratos en condiciones de servidumbre, arbitraje de terceros, firma multipartita, etc. Si Bitcoin evoluciona a lo grande, estas son cosas que querremos explorar en el futuro, pero todas han tenido que diseñarse al principio para asegurarse de que sean posibles de usar más tarde.

No creo que, una segunda implementación compatible de Bitcoin sea una buena idea. Gran parte del diseño depende de que todos los nodos obtengan exactamente los mismos resultados así que una segunda implementación sería una amenaza para la red. La licencia de MIT es compatible con todas las demás licencias y usos comerciales, por lo que no es necesario volver a escribirla desde el punto de vista del licenciamiento.

Una segunda versión sería un gran problema de desarrollo y mantenimiento para mí. Ya es bastante difícil mantener la compatibilidad con versiones anteriores mientras se actualiza la red sin una segunda versión. Si la segunda versión fallara, la experiencia del usuario se reflejaría negativamente en ambas, aunque al menos reforzaría a los usuarios la importancia de permanecer con la versión oficial . Si alguien estuviera preparándose para bifurcarse a una segunda versión, tendría que advertir sobre los muchos riesgos de usar una versión minoritaria. Este es un diseño donde la versión mayoritaria gana si hay desacuerdo, y eso puede ser bastante feo para la versión minoritaria y prefiero no entrar en eso, y no tengo que hacerlo siempre que haya una sola versión.

Lo sé, a muchos desarrolladores no les gusta que bifurquen su software, pero en este caso tengo reales razones técnicas.

> Cita de: gavinandresen, 17 de junio 2010, 07:58:14 PM
>
> Admiro la flexibilidad del esquema de scripts en una transacción, pero mi pequeña y malvada mente inmediatamente comienza a pensar en maneras de abusar de ello. Podía codificar todo tipo de información interesante en el script TxOut, y si los clientes no pirateados validaban y luego ignoraban esas transacciones, sería un canal de comunicación

> de transmisión encubierto útil.
>
> Esa es una característica interesante hasta que se hace popular y alguien decide que sería divertido inundar la red de pagos con millones de transacciones para transferir el último video de Lady Gaga a todos sus amigos. . .

Esa es una de las razones de las comisiones. Hay otras cosas que podemos hacer si fuera necesario.

> Cita de: laszlo, 17 de junio 2010, 06:50:31 PM
>
> ¿Cuánto tiempo llevas trabajando en este diseño Satoshi? Parece muy bien pensado, no es el tipo de cosa en la que te sientas y programas sin tener muchas ideas y discusiones primero. Todo el mundo tiene las preguntas obvias buscando agujeros, pero está aguantando bien : -)

Desde 2007. Hubo un momento en el que me convencí de que había una manera de hacer esto sin necesidad de ningún tipo de confianza y no me pude resistir a seguir pensando sobre ello. Diseñarlo dio mucho más trabajo que programarlo.

Afortunadamente hasta ahora, todas las incidencias mencionadas son temas que había pensado y resuelto antes.

42

El Primer Grifo Bitcoin

Traducción por **Jose Manuel Arenillas**

GAVIN ANDRESEN, desarrollador líder de Bitcoin en aquel momento, anunció que había programado un "grifo Bitcoin" regalando 5 bitcoin por cliente. Satoshi responde que había tenido la misma idea por si a nadie más se le ocurría.

Re: Consigue 5 bitcoin gratis en freebitcoins.appspot.com

Satoshi Nakamoto, 18 de junio 2010, 11:08:34 PM

> Cita de: Gavin Andresen, 11 de junio 2010, 05:38:45 PM
>
> Para mi primer proyecto de codificación de Bitcoin, decidí hacer algo que suena realmente tonto: He creado un sitio web que regala Bitcoins. Está en: https://freebitcoins.appspot.com/
>
> Cinco ฿ por cliente, por orden de llegada, lo he abastecido con ฿ 1,100 para comenzar. Agregare más una vez que esté seguro de que está funcionando correctamente.
>
> ¿Por qué? Porque quiero que el proyecto de Bitcoin tenga éxito, y creo que es más probable que sea un éxito si la gente puede obtener unas

> cuantas monedas para probarlo. Puede ser frustrante esperar hasta que tu nodo genere algunas monedas (y eso se volverá más frustrante en el futuro), y comprar Bitcoins todavía es un poco complicado.
>
> Por favor, pruébalo y consigue algunas monedas gratis, incluso si ya tiene más Bitcoins que sabe qué hacer con ellos. Pueden conseguir algunos y volver a donarlos; la dirección es: ~~15VjRaDX9zpbA8LVnbrCAFzrVzN7ixHNsC~~

Excelente elección de un primer proyecto, buen trabajo. Había planeado hacer justo esto si alguien más no lo hacía, cuando se vuelva demasiado difícil para los mortales generar 50BTC, los nuevos usuarios podrían conseguir algunas monedas para jugar de inmediato. Las donaciones deberían poder mantenerlo lleno. La pantalla que muestra el equilibrio en el dispensador alienta a las personas a llenarlo.

Debería poner una dirección de bitcoin para donaciones en la página, para aquellos que deseen agregarle fondos, lo ideal debería ser actualizar a una nueva dirección cada vez que reciba algo.

Más adelante, a medida que el valor aumentaba. Satoshi sugirió reducir el grifo bitcoin a 1 BTC (1 bitcoin).

Re: Se necesitan donaciones para freebitcoins.appspot.com!

Satoshi Nakamoto, 16 de julio 2010, 02:02:07 AM

> Cita de: Gavin Andresen, 12 de junio 2010, 07:15:46 PM
>
> El grifo Bitcoin está aguantando muy bien la sangría ... excepto que me estoy quedando sin monedas para regalar, más de 5,000 han salido del grifo desde que lo rellené anoche.
>
> Cualquiera de vosotros, los primeros en adoptar que generaron decenas de miles de monedas en los primeros días, ¿podrían enviar unos pocos al grifo para que se regalen y que más personas puedan probar Bitcoin?

> Sé que la mayoría de ellos es probable que se pierdan (sospecho que hay muchos "busca oportunidades" que no se quedarán el tiempo suficiente para gastar sus 5 bitcoins), pero si ese es el caso, incrementará el valor del resto de bitcoin, de todos modos…
>
> La dirección de donación de la fuente es:
> ~~15VjRaDX9zpbA8LVnbrCAFzrVzN7ixHNsC~~
>
> Dependiendo de las donaciones y de cuánto dure la sangría, tendré que empezar a regalar bitcentavos...

---

5 BTC parecen mucho en estos días, probablemente una cantidad normal debería ser en torno a 1 o 2 BTC.

Este es un servicio importante para que los nuevos usuarios puedan conseguir algunos si generarlos es muy difícil.

43

¡Bitcoin 0.3 Publicado!

Traducción por **Jose Manuel Arenillas**

SATOSHI no solo es técnico en términos de lo que ofrece este nuevo lanzamiento, sino que también ofrece este argumento de ventas y marketing: *"¡Libérese del arbitrario riesgo de inflación de las monedas administradas centralmente! La circulación total de Bitcoin está limitada a 21 millones de monedas ".*

¡Bitcoin 0.3 publicado!

Satoshi Nakamoto, 6 de junio 2010, 06:32:35 PM

¡Anunciando la versión 0.3 de Bitcoin, la criptomoneda P2P! Bitcoin es una moneda digital que utiliza la criptografía y una red distribuida para reemplazar la necesidad de un servidor central de confianza. ¡Libérese del riesgo de inflación arbitrario de las monedas administradas centralmente! La circulación total de Bitcoin está limitada a 21 millones de monedas. Las monedas se liberan gradualmente a los nodos de la red en función de la potencia de CPU con la que contribuyen, por lo que puede obtener una parte de ellas al contribuir con su tiempo de CPU inactivo.

Novedades:

- Línea de comandos y control JSON-RPC
- Incluye una versión demonio sin GUI (Interfaz gráfica de usuario)
- Filtro de transacciones
- Cálculo de hash un 20% más rápido
- Visor de rendimiento de poder de minado
- Versión para Mac OS X (gracias a Laszlo)
- Traducciones al alemán, holandés e italiano (gracias a DataWraith, Xunie y Joozero)

Consíguela en http://www.bitcoin.org o lee el foro para descubrir más.

44

Sobre Segmentación o "Botón de Apagado de Internet"

Traducción por **Jose Manuel Arenillas**

Dos hilos sobre la posibilidad de segmentación o una división de la red.

Re: Anonimato!

Satoshi Nakamoto, 8 de junio 2010, 07:12:00 PM

Es difícil imaginar que Internet se dividiese en espacios herméticos. Sería como un país que se desconecte deliberada y totalmente del resto del mundo.

Cualquier nodo con acceso a ambos lados podría transmitir la cadena de bloques, por ejemplo alguien que se salte el bloqueo con un módem de acceso telefónico o un teléfono satélite. Solo haría falta un nodo. Cualquiera que quiera seguir haciendo negocios estaría motivado.

Si la red se segmentara y luego se combinará de nuevo, todas las transacciones que en la bifurcación más corta no estén también en la bifurcación más larga volverían a la cola de transacciones y serían elegibles para entrar en bloques futuros. Su número de confirmaciones

comenzaría de nuevo.

Si alguien se aprovechó de la segmentación para hacer un doble gasto, de modo que haya diferentes gastos del mismo dinero en cada lado, el gasto en la bifurcación más corta pierde, volvería a estar sin confirmar y se mantendría así.

No sería fácil aprovechar la segmentación para hacer un doble gasto. Si es imposible comunicarse de un lado a otro, ¿cómo gastar en cada lado? Si hubiera una manera, entonces probablemente otra persona también la utilice para para esparcirla sobre la cadena de bloques.

Usted debería saber si está en el segmento más corto. Por ejemplo, si su país se separa del resto del mundo, el resto del mundo es el segmento más grande. Si estás en el segmento más pequeño, debes asumir que no hay nada confirmado.

Esto trata específicamente el caso de una división de la red.

Re: ¿Qué pasa cuando la red se divide durante un periodo de tiempo prolongado y se reconecta?

Publicado por em3rgentOrdr, 01 de agosto 2010, 11:07:24 AM

Supongamos que los bitcoins están siendo usados ampliamente en todo el mundo. Supongamos que todas las conexiones de Internet entre dos países están bloqueadas (por ejemplo, China y EE. UU. van a la guerra) y la gente aún realiza transacciones dentro de cada red. Ahora, todas las transacciones dentro de cada red se emiten a todos los nodos dentro de su red, pero no a la otra red. Dentro de cada red, la cadena más larga en cada uno se consideraría válida, y la economía de Bitcoin continuaría existiendo dentro de cada red.

Ahora, después de varios años existiendo independientemente, ¿qué sucede cuando las dos redes se vuelven a conectar?

Re: ¿Qué pasa cuando la red se divide durante un periodo de tiempo prolongado y se reconecta?

Publicado por kiba, 02 de agosto, 2010 03:19:08 AM

Quizás no se vuelvan a conectar. En cambio, efectivamente tendremos dos monedas. Esto conducirá a la creación de un mercado(s) de intercambio de moneda de bitcoin Este-Oeste.

Re: ¿Qué pasa cuando la red se divide durante un periodo de tiempo prolongado y se reconecta?

Publicado por throughput, 02 de agosto 2010, 06:07:08 PM

A mí, como comerciante, solo me preocuparía si mi red es la mayoritaria, por lo que después de reconectarme, mis transacciones serán aceptadas. Por lo tanto, será suficiente para mí poder monitorizar la cantidad actual de nodos distintos. Ponerlo en un gráfico y dejar de procesar transacciones si ese número se reduce a la mitad. Puede ser un servicio en un servidor web que ejecuta un nodo de Bitcoin.

Pero ¿hay alguna forma de controlar ese número? De lo contrario, sería aconsejable agregar alguna función al estándar, que permitiría determinar en tiempo real cuál es el número de nodos distintos en ejecución.

Re: ¿Qué pasa cuando la red se divide durante un periodo de tiempo prolongado y se reconecta?

Publicado por creighto, 03 de agosto 2010, 08:01:22 PM

> Cita de: throughput el 3 de agosto de 2010, 01:33:08 PM
>
> Si…
>
> Pero lo que describes es posible solo después de que alguien se haya dado cuenta y haya probado que la división de la red está sucediendo.
>
> ¿Propones algún método para detectar el comienzo de la división de la red?

Comencé otro hilo sobre este tema en algún otro sitio, pero para un proveedor individual, un simple servicio que rastree el tiempo promedio entre bloques desde el último cambio oficial en dificultad y avise al proveedor si un solo bloque tarda más del doble que el promedio, tal vez suspendiendo la aceptación de nuevas monedas hasta que el proveedor compruebe que está sucediendo. Cada bloque en fila tome más tiempo que el promedio aumenta la confianza contra un falso positivo. Así que, si un bloque tarda el doble que el promedio, seguido de una serie de bloques que tardan un 75% más de tiempo que el promedio, entonces puedes estar bien seguro de que ya no estás en la red de la mayoría.

Re: ¿Qué pasa cuando la red se divide durante un periodo de tiempo prolongado y se reconecta?

Publicado por satoshi, 03 de agosto 2010, 10:45:07 PM

> Creighto: Estoy de acuerdo con esa idea. Tras unas pocas horas debería ser posible para el cliente darse cuenta de que el flujo de bloques ha disminuido más de lo que puede ser aceptable. Esto podría indicar que ya no está escuchando el zumbido del mundo.

> Cita de: knightmb, 03 de agosto 2010, 07:02:13 PM
>
> ---
>
> > Cita de: gavinandresen, 03 de agosto 2010, 06:38:44 PM
> >
> > O si la división durase más de lo debido (más de 100 bloques), las transacciones que implica generar monedas en la cadena más corta no serían válidas tras unirse.
> >
> > ---
>
> Información interesante, por lo tanto, aparte de algunos problemas de doble gasto, siempre que la cadena de bloques no esté separada por más de 100 bloques (o más de 16 horas),

En la práctica, las divisiones probablemente sean muy asimétricas. Sería difícil dividir el mundo por la mitad. Lo más probable es que fuera un único país frente al resto del mundo, digamos una división de 1:10. En ese caso, la cadena de la minoría tardará 10 veces más en generar 100 bloques, aproximadamente 7 días. También sería muy fácil para el cliente darse cuenta de que está escuchando muy pocos bloques y que algo debe estar mal.

> Cita de: knightmb, 03 de agosto 2010, 07:02:13 PM
>
> ¿Hay un límite programado para las bifurcaciones? Es decir, si tuviera una pequeña red dividida de la red pública, gastase algunas monedas, volviera unos días después y las sincronizará con la red pública (aparte de la generación de monedas si ocurriese) ¿las transacciones deberían estar bien?
>
> ---

No hay límite de tiempo. Asumiendo que no estaba gastando monedas generadas en la bifurcación de la minoría, o realizando doble gastos que hubiera recibido de alguien, sus transacciones se incluirían en la otra cadena posteriormente.

45

Sobre la Monopolización del Mercado

Traducción por **Enrique Palacios Rojo**

SATOSHI RESPONDE a un comentario sobre alguien que está tratando de comprar todos los bitcoins y hace referencia a los hermanos Hunt y el mercado de la plata de finales de los años setenta. Hay que tener en cuenta que la compra de los hermanos Hunt fue, en realidad un pequeño porcentaje del mercado de la plata. Lo que les condenó fue su cotización en COMEX al tener una posición apalancada en el mercado de futuros. COMEX cambió las reglas colocando un límite en la cantidad total de contratos que uno podía poseer, forzando a alguien a tener más que el límite especificado en una posición de venta, y por lo tanto provocó que los hermanos Hunt tuvieran que liquidar la posición . Ver un documento más detallado sobre este tema escrito por Mike Maloney en *WealthCycles.com:*

http://wealthcycles.com/features/the-hunt-brothers-capped-the-price-of-gold-not-50-silver

Re:¿Vulnerabilidad del BTC? (Ataque Masivo Contra El Sistema BTC. ¿Es Así Realmente?)

Satoshi Nakamoto, 09 de julio 2010, 03:28:46 PM

Cita de: usuario, 07 de julio 2010, 06:15:28 PM

> Hola. (Lo siento si no entiendo algún concepto). Qué piensas de que un intruso compre la moneda de Bitcoin y borrase todos los datos binarios. De este modo podría destruir los sistemas del Bitcoin ¿Está la red del btc protegida contra ese ataque?

Lo que el OP describió se llama "monopolizar el mercado". Cuando alguien intenta comprar toda la oferta del mundo de un activo escaso, cuanto más compran más sube el precio. En algún punto, se pone demasiado caro para que puedan comprar más. Esto está muy bien para la gente que lo poseía de antemano porque lo venden al mejor postor a precios extraordinariamente altos. A medida que el precio sube y sube, algunas personas mantienen su posición esperando a que suban aún más los precios y se niegan a vender.

Los famosos hermanos Hunt se arruinaron tratando de arrinconar al mercado de la plata en 1979:

"Los hermanos Nelson Bunker y Herbert Hunt intentaron acaparar los mercados mundiales de la plata a finales de los años setenta y principios de los ochenta, poseyendo en un momento dado los derechos sobre más de la mitad de la plata comercializable del mundo. [1] Durante esta acumulación de los Hunt los precios de la plata subieron desde los 11 dólares por onza en septiembre de 1979 a casi 50 dólares por onza en enero de 1980. [2] El precio de la plata colapsó en última instancia a menos de 11 dólares la onza dos meses después, [2] gran parte de la caída se produjo en un solo día, ahora conocido como el Jueves de la Plata, debido a los cambios hechos por los reguladores sobre las reglas en relación con la compra de materias primas con apalancamiento [3] "

http://en.wikipedia.org/wiki/Cornering_the_market

46

Sobre la Escalabilidad y los Clientes de Menor Relevancia

Traducción por **Enrique Palacios Rojo**

A MEDIDA QUE PASA EL TIEMPO, la cadena de bloques, que contiene un histórico de todas las transacciones realizadas desde enero de 2009, crece continuamente. Dado que un monedero de Bitcoin contiene varias direcciones de Bitcoin junto con sus claves privadas correspondientes y saldos, Bitcoin debe saber qué dirección o direcciones deben usarse para cubrir una transacción. Por ejemplo, supongamos que la dirección A de Bitcoin tiene 0.1 BTC, la B tiene 0.2 BTC, y la C tiene 0.3 BTC y se necesita hacer un pago de 0.5 BTC. El monedero de Bitcoin tendrá que elegir una combinación de 2 o más direcciones de Bitcoin con las que cubrir el 0.5 BTC pues ninguna de ellas individualmente tiene suficientes bitcoins para realizar el pago completo. A menos que un cliente de Bitcoin tenga la cadena completa de bloques y pueda saber el saldo actual de cada dirección, debe interactuar con un servidor que tenga la cadena de bloques. La verificación simplificada de pago, descrita por primera vez en el documento original de Bitcoin de Satoshi, permite a los clientes confiar en un servidor que participa en la red de Bitcoin y que tiene la totalidad de la cadena de bloques aunque pueda o no estar participando en el proceso de minería. Eso fue implementado más tarde y beneficia a los clientes de menor relevancia.

RE: ESCALABILIDAD

Satoshi Nakamoto, 14 de julio 2010, 09:10:52 PM

> Cita de: jib, 12 de julio 2010, 11:36:17 AM
>
> ¿Estoy en lo cierto al entender que cada nodo recibe información sobre cada transacción (como dice el documento técnico)? ¿Eso no invalida al bitcoin para utilizarlo como una moneda a gran escala?

El diseño describe un cliente de transacciones pequeñas que no necesita la cadena de bloques completa. En el diseño del PDF se llama Verificación Simplificada de Pago. El cliente de menor peso puede enviar y recibir transacciones, pero no se generan bloques. No necesita confiar en un nodo para verificar pagos, ya que aún puede verificarlos por sí mismo.

Este tipo de cliente aún no se ha implementado, pero el plan es implementarlo cuando sea necesario. Por ahora, todos ejecutan un nodo completo de red.

Os anticipo que nunca habrá más de 100.000 nodos, probablemente menos. Alcanzará un equilibrio en el momento que no valga la pena que más nodos se unan. El resto serán clientes de menor peso , que podrían ser millones.

En el tamaño de equilibrio, muchos nodos serán granjas de servidores con uno o dos nodos de red que alimentan el resto de la granja a través de una LAN.

47

Sobre Problemas en Transacciones Rápidas

Traducción por **Enrique Palacios Rojo**

AQUÍ, Satoshi explica que una empresa de procesamiento de pagos podría supervisar la red de Bitcoin por el interés de la transacción del comerciante, así como cualquier otro conflicto entre transacciones. Como los nodos sólo aceptarán las primeras transacciones y rechazarán cualquier otra transacción que entre en conflicto con aquellas, las transacciones de los comercios deberían de aceptarse primero. Si hay transacciones conflictivas son vistas por la empresa de procesamiento de pagos, se informará al comerciante que la transacción es mala. Por supuesto, si la correcta transacción es aceptada oficialmente, el comerciante puede reembolsar al cliente o procesar la venta.

Re: Bitcoin Máquina de snack (problemas de transacción rápida)

Satoshi Nakamoto, 17 de julio 2010, 10:29:13 PM

> Cita de: Insti, 17 de julio 2010, 02:33:41 AM
>
> ¿Cómo funcionaría una máquina de snacks de Bitcoin?
>
> 1. Te aproximas hacia la máquina. Introduce un bitcoin.
>
> 2.?
>
> 3. Te alejas comiendo tu rico tentempié azucarado. (¡Qué aproveche!)

No quieres tener que esperar una hora para que tu transacción se confirme.

La compañía de máquinas expendedoras no quiere regalar un montón de dulces gratis

¿Cómo funciona el paso 2?

Creo que será posible que una empresa de procesamiento de pagos proporcione como servicio la distribución rápida de transacciones con un buen sistema de confirmación en algo así como 10 segundos o menos.

Los nodos de red solo aceptan la primera versión de una transacción que reciben para incorporarla en el bloque que están tratando de generar. Cuando se transmite una transacción, si alguien más transmite un doble gasto al mismo tiempo, es una carrera para llegar a la mayoría de los nodos primero. Si una tiene una ligera ventaja, se extenderá geométricamente a través de la red de manera más rápida y llegará a mayor cantidad de los nodos.

Un ejemplo aproximado de retroceso del sobre:

1	0
4	1
16	4
64	16
80%	20%

Así pues, si un doble gasto tiene que esperar incluso un segundo, tiene una enorme desventaja.

El procesador de pagos tiene conexiones con muchos nodos. Cuando obtiene una transacción, la relanza y, al mismo tiempo, supervisa la red de posibles dobles gastos. Si recibe un doble gasto en cualquiera de sus muchos nodos de escucha, entonces alerta que la transacción es mala. Una transacción doblemente gastada no llegaría muy lejos sin que uno de los nodos oyentes la detecte. El doble gasto tendría que esperar hasta que la fase de recepción (escucha) termine, pero para entonces, la transmisión del procesador de pagos habría llegado a la mayoría de los nodos, o está va tan por delante en la propagación de que el que realiza el doble gasto que no tiene ninguna esperanza de alcanzar un porcentaje significativo de los nodos restantes.

En otra conversación posterior se revisa la escalabilidad y la tasa de transacción. Satoshi se refiere al hilo de arriba.

Re: Escalabilidad y tasa de transacción

Satoshi Nakamoto, 29 de julio 2010, 02:00:38 AM

> Cita de: Red, 22 de julio 2010 05:17:28 AM
>
> Tengo curiosidad sobre lo que opinan los desarrolladores sobre la escalabilidad. Por ejemplo, ¿podría el sistema manejar un millón de usuarios haciendo cada uno 5 transacciones al día? 5 millones de transacciones por día aproximadamente son 35.000 transacciones en un período de 10 minutos
>
> ¿Hay un cuello de botella en la propagación de 35.000 transacciones a un millón de nodos para la generación de bloques? ¿Ha sido diseñado para esta situación?

El sistema actual donde cada usuario es un nodo de red no es la configuración prevista para utilizarse a gran escala. Eso sería como si cada usuario de Usenet ejecuta su propio servidor NNTP. El diseño deja que los usuarios solo sean usuarios. Cuanto más cueste ejecutar un nodo, menos nodos habrá. Esos pocos nodos serán un gran servidor de granjas. El resto serán nodos cliente que sólo realizan transacciones y no generan bloques.

> Cita de: bytemaster, 28 de julio 2010 08:59:42 PM
>
> Además, 10 minutos es demasiado tiempo para verificar que el pago sea válido. Tiene que ser tan rápido como utilizar una tarjeta de crédito hoy en día.

Mira la conversación de la máquina de snacks, donde describo cómo un procesador de pagos podría verificar los pagos lo suficientemente bien, en realidad muy bien (con una tasa bastante menor de fraude que las tarjetas de crédito), en algo así como 10 segundos o menos. Si no me crees o no lo entiendes, no tengo tiempo para intentar convencerte, lo

siento.

http://bitcointalk.org/index.php?topic=423.msg3819#msg3819

48

Artículo de Entrada en Wikipedia Sobre Bitcoin

Traducción por **Enrique Palacios Rojo**

NO PODEMOS IMAGINAR que Wikipedia considere borrar la entrada sobre Bitcoin con el actual nivel de interés. En el momento de esta publicación (versión en Inglés), Bitcoin todavía estaba por debajo de 1 dólar, pero estaba generando suficiente interés para justificar un artículo en Wikipedia. Satoshi comenta aquí que él considera el timing un tanto extraño, en cuanto a que la cobertura sobre Bitcoin estuviera aumentando rápidamente en los medios de comunicación.

RE: Quieren borrar el artículo de Wikipedia

Satoshi Nakamoto 20 de julio de 2010, 06:38:28 PM

> Cita de: Giulio Prisco el 14 de julio de 2010, 07:21:08 AM
>
> http://en.wikipedia.org/wiki/Bitcoin
>
> Este artículo está siendo considerado para ser eliminado de acuerdo con la política de borrado de Wikipedia. Por favor, comparta sus comentarios sobre este asunto en la entrada de este artículo en Artículos para la eliminación de la página.
>
> Este artículo necesita referencias que aparezcan en otras publicaciones de confianza. Fuentes originales o fuentes relacionadas al tema no son

generalmente suficientes para un artículo de Wikipedia. Por favor, agregue citas más apropiadas de fuentes confiables.

El artículo reciente de Slashdot se debe considerar como referencia de confianza:
http://news.slashdot.org/story/10/07/11/1747245/Bitcoin-Releases-Version-03

No puedo editarlo en este momento, ¿podéis guardar el artículo de Wikipedia?

Bitcoin es una implementación de la propuesta de b-money hecha por Wei Dai
http://weidai.com/bmoney.txt en Cypherpunks
http://en.wikipedia.org/wiki/Cypherpunks en 1998 y la propuesta de Bitgold de Nick Szabo's
http://unenumerated.blogspot.com/2005/12/bit-gold.html

El timing es extraño, sólo estamos obteniendo un rápido aumento en la cobertura por parte de terceros después de haber sido temporalmente populares en la web. Espero que no haya una excesiva prisa para resolver la discusión y decidir. ¿Cuánto tiempo por lo general deja Wikipedia una pregunta como esa abierta para hacer comentarios?

Ayudaría el condensar el artículo y hacerlo que suene menos promocional tan pronto como sea posible. Solo que la gente sepa de qué se trata y que encaja en el ámbito de dinero electrónico, sin tratar de convencerles de que eso es bueno. Probablemente quieren algo que sólo identifiquen lo que es, no tratar de explicar cómo funciona.

Si públicas en
http://en.wikipedia.org/wiki/Wikipedia:Articles_for_deletion/Bitcoin
no digas por favor, que "si, el bitcoin es tan importante y especial que las reglas no deberían aplicarse" o argumentar que la regla no es muy inteligente o injusta. Eso solo lo empeoraría. Intenta enfocarlo de cómo se podría cumplir la norma.

Busca "bitcoin" en Google y mira si puedes encontrar referencias relevantes además de las de infoworld y slashdot. Puede que haya algo escrito recientemente por periodistas que obtuvieron información al respecto del artículo de slashdot.

Espero que no se borre. Si lo hace, será difícil de demostrar la

presunción. El impulso institucional es quedarse con la última decisión. (editar: o al menos eso supongo, así es como suele funcionar el mundo, pero tal vez Wiki sea diferente)

Posteriormente, el 31 de julio, el artículo fue oficialmente eliminado, y luego restaurado.

RE: Página de BitCoin en Wikipedia BORRADA!!!

Publicado por em3rgentorr, 31 de julio 2010, 02:17:41 AM

Obtenido de http://en.wikipedia.org/wiki/Bitcoin

"Esta página ha sido eliminada. El borrado y el registro de movimiento de la página se proporciona bajo la referencia.

10:42, 30 de julio de 2010 Polargeo (conversaciones | contribs) borrado "Bitcoin" (Wikipedia: Artículos para eliminación/Bitcoin)"

RE: Página de BitCoin en Wikipedia BORRADA!!!

Publicado por sirius, 30 de septiembre 2010, 04:45:26 PM

¿Qué tal si hacemos versiones en diferentes idiomas de una página eliminada sin que ellos la eliminen? Hagámoslo si podemos. Yo puedo escribir una versión en finlandés.

RE: Página de BitCoin en Wikipedia BORRADA!!!

Publicado por satoshi, 30 de septiembre 2010, 05:50:32 PM

Si lo haces, creo que debería ser un artículo muy breve y de un solo

párrafo como de 100 palabras o menos que simplemente identifique qué es Bitcoin.

Ojalá que en lugar de eliminar el artículo, pongan una restricción de longitud. Si algo no es lo suficientemente famoso, podría haber al menos una parte del artículo identificando lo que es. A menudo me encuentro con molestos enlaces rojos de las cosas que Wiki debería al menos haber tenido en cuenta.

El artículo podría ser algo tan simple como:

“Bitcoin es un descentralizado peer-to-peer /link/moneda electrónica/link/.”

La acción en Wikipedia más estándar que deberíamos hacer es tener un párrafo en una de las categorías más generales en la que somos referencia, como Moneda Electrónica o Dinero Electrónico. Podemos ponerlo ahí. Pero de nuevo ponlo corto. Sólo identificando lo que es.

RE: Página de BitCoin en Wikipedia BORRADA!!!

Publicado por ribuck, 13 de diciembre 2010, 11:23:41 AM

Parece que el artículo será restaurado. Pero un punto que sigue estando vigente es que muchas de las referencias del artículo son a páginas de este foro. Si alguien puede reemplazar la referencia al foro con una referencia a una página que no sea percibida como conflicto de intereses, eso ayudaría.

49

Sobre la Posibilidad de Robo de Monedas

Traducción por **Arturo Monzón**

COMO SE DECLARÓ ANTES, Bitcoin usa la criptografía asimétrica con un par de claves, pública y privada, como mecanismo para recibir y autorizar el gasto de bitcoins. Sin embargo, Satoshi decidió utilizar como la dirección de Bitcoin el hash de la clave pública en lugar de la clave pública en sí misma. Satoshi hizo esto por dos razones. Una era reducir el tamaño de cada transacción ya que el hash tiene solo 160 bits de largo. El segundo beneficio fue que convenientemente agregó una capa más de seguridad en caso de que algún día se descubriera un "backdoor" o falla de seguridad en el algoritmo de criptografía asimétrica utilizado por Bitcoin. Para poder gastar bitcoins, un hacker tendría que derivar primero la clave pública del hash y luego derivar la clave privada de la clave pública. La revista *Bitcoin Magazine* escribió un excelente artículo sobre este tema.[2]

Todo este hilo discute la posibilidad de que un atacante con mucha potencia informática pueda gastar los bitcoins almacenados en una dirección bitcoin. Dado que la cadena de bloques de bitcoin es un libro mayor abierto, se puede inspeccionar para identificar una dirección de bitcoin con un gran saldo, por lo que un atacante podría centrarse en esas direcciones.

---

[2] http://bitcoinmagazine.com/7781/satoshis-genius-unexpected-ways-in-which-bitcoin-dodged-some-cryptographic-bullet/

Satoshi concluyó que sería bastante difícil, ya que requeriría una fuerza bruta de ataque para encontrar una clave pública con su hash correspondiente. También muestra el valor del código fuente abierto (código que está abierto para que todos lo vean) para la seguridad, a diferencia de la fuente cerrada.

Las partes importantes de los hilos, incluida la publicación completa de Satoshi, se reproducen aquí:

Robo de Monedas

Publicado por Red, 25 de julio 2010, 05:08:03 PM

Creo que hay un error criptográfico bastante significativo en Bitcoin como está implementado actualmente. No estoy seguro de que será explotable ahora (no soy un verdadero criptohacker) pero es más que plausible que lo será en un futuro cercano.

La falla permitiría el robo anónimo de monedas desde direcciones bitcoin arbitrarias. Y no, no implica resolver ninguno de los problemas difíciles que mantienen seguros los sistemas de cifrado. Es simplemente un *potencial* fallo lógico corregible en la implementación.

Me gustaría que los bitcoins tuvieran éxito, así que preferiría no tener que saltar de un lado a otro señalando fallos en público. ¿Hay un lugar apropiado para discutir este tipo de problemas?

Re: Robo de Monedas

Publicado por Satoshi, 25 de julio 2010, 05:45:22 PM

Lo mejor es que me lo cuentes en privado para que se solucione primero.

Acabo de enviarle un correo con mi dirección de correo electrónico. (o podrías enviarme un PM aquí)

Re: Robo de Monedas

Publicado por Satoshi, 25 de julio de 2010, 07:06:23 PM

Red, ¡gracias por contarme en privado primero! Por favor, adelante y publícalo (¡y que cese el suspense para todos!)

Su punto es que las transacciones pagadas a una dirección de Bitcoin son tan seguras como la función de hash. Para hacer que las direcciones de Bitcoin sean cortas, son un hash de la clave pública, no la clave pública en sí misma. Un atacante solo tendría que romper la función hash, no ECDSA.

Re: Robo de Monedas

Publicado por Red, 25 de julio 2010, 07:09:43 PM

Gracias Satoshi,

Esto es lo que le envié.

———

La criptografía de clave pública depende del hecho de que es difícil factorizar números primos grandes. Todos saben eso. Si las transferencias de bitcoins se asignaron a una clave pública bien formada, y se requirió una firma de clave privada asociada para la futura transferencia, permitiría que las transferencias cifradas de bitcoins fueran completamente seguras.

Sin embargo, las transacciones de bitcoins no parecen funcionar de esa manera (por lo que leo). Las transacciones asignan cantidades de monedas a una "dirección de bitcoin" particular. Donde la dirección es un hash de la clave pública.

Para validar una transacción, los nodos toman la clave pública de la firma y la usan para verificar la firma real. Si la firma es válida, habrá que ver luego los hashes de la clave pública para confirmar que coincide con la dirección de bitcoin asignada en la transacción

anterior. Si ambos coinciden, por definición, la transacción es buena.

La potencial debilidad es asociar la clave pública en la firma con la dirección de bitcoin.

Hay una relación, varios a uno, entre las claves públicas y un hash dado. Ahora, si resulta difícil encontrar un par de números primos que cree un par de claves públicas/privadas seguras, donde la parte de la clave pública se hereda en una dirección de bitcoin en particular ... probablemente así lo sea.

Sin embargo, eso no es necesario.

Todo lo que necesita es CUALQUIER cosa que represente una clave pública y que el hash colisione con una gran cuenta de bitcoin. NO tiene que ser un par de claves seguras basado en primos. Simplemente tiene que funcionar una vez y permitir la transferencia del dinero robado a otra cuenta. Eso es potencialmente mucho más fácil.

Algunos hashes son más difíciles de colisionar que otros. No estoy seguro de la fuerza del hash que se usa. Sin embargo, colisionar cualquier hash es mucho más fácil si no tienes que preocuparte por el contenido que ha sido hasheado.

Debido a la naturaleza de las claves públicas, parecen datos aleatorios. Según los entiendo, no se puede saber si una clave pública está basada en matemáticas seguras a menos que tenga éxito en factorizarlo. Por lo tanto, los clientes no lo intentan. Normalmente solo hacen la validación de la firma y suponen que la clave pública se generó de manera segura porque funcionó.

NOTA: El siguiente análisis necesita una doble verificación por parte de un criptohacker real. IANACR

Por lo tanto, dependiendo del hash, puede usar uno de los algoritmos de colisión hash emergentes para generar un bloque colisionador de datos que representa una clave pública. Luego, invirtiendo la clave pública/privada, generar una clave privada asociada (pero apenas segura) que genere firmas válidas.

A continuación, tomas su par de claves inseguras, fácilmente factorizables, y generas una transacción firmada que coincida con la dirección de bitcoin de destino.

Dado que el registro de transacciones no puede validar la clave pública completa a la que se destinaron las monedas, simplemente supone que debe haber sido la presentada.

Al registrar la clave pública completa de la transferencia objetivo en la lista de bloques, puede recuperar la fuerza deseada. Sin embargo, pierde la capacidad de pasar alrededor de 34 direcciones de caracteres.

Si estoy fuera de juego, me disculpo por hacer perder su tiempo.

¡Gracias!

Red

Re: Robo de Monedas

Publicado por Red, 25 de julio de 2010, 07:22:14 PM

Satoshi señaló que mi escenario aún requiere que la función hash sea quebrada. Eso es cierto, pero me sorprendió aprender cuán exitosos han sido con eso. MD4 y MD5 son ejemplos obvios. Pero el trabajo está en marcha para colisionar SHA-1 y hermanos como SHA-256.

¿Qué hash se está utilizando en esta parte de Bitcoin?

Él también se muestra escéptico de que puedas usar algo más que no sea un par de llaves generadas.

En este punto, estoy bastante seguro de que es una simple cuestión de matemáticas. No presté la suficiente atención a este tema hasta que supe de la "firma ciega" en los documentos.

Resulta que puede tomar un documento y multiplicarlo por un número aleatorio. Luego, pedir a alguien que firme el archivo desordenado. Finalmente, divide su número aleatorio de su firma y el resultado sigue

siendo una firma válida para el documento original. ¡Quién hubiera dado cuenta de que eso podría funcionar!

De todos modos, si los pares de claves solo son seguros si están basados en pares de números primos. Entonces no cambia nada de la matemática si los números no son primos. Sólo que son mucho más fáciles de factorizar.

Estaría muy feliz de que algún tipo de criptógrafo me demostrara que soy un idiota. Incide sobre algunas características de un proyecto anterior que creé y que dependía de la misma asociación. Yo tampoco pensé en esto.

Re: Robo de Monedas

Publicado por knightmb, 25 de julio 2010, 07:34:42 PM

Muy agradable. *otra razón por la que amo el código abierto*

Como lo entiendo entonces, y por favor corrígeme si estoy equivocado.

Dado que el hash de la clave pública es más pequeño que la clave pública real en sí misma, solo se necesita encontrar una colisión que coincida con el hash y cuando se encuentre esa colisión conocerá el combo de clave pública/privada. Entonces simplemente gasta monedas usando las conocidas y los otros clientes pensarán que es una transferencia válida porque a los clientes solo les preocupa que su hash coincida con el hash de la víctima y la transacción se registre para siempre.

Actualmente el hash es de 35 caracteres de longitud, alfanumérico 26 (mayúscula) +26 (minúscula) +10 (números) = 62 posibles por carácter

Entonces tenemos
541,638,008,296,341,754,635,824,011,376,225,346,986,572,413,939,634,062,667,808,768 combinaciones posibles.

Así que creo que no tenemos mucho trabajo por hacer en comparación con ir con fuerza bruta contra la clave privada/pública principal. Nunca duele planear para el futuro: -)

Re: Robo de Monedas

Publicado por knightmb, 25 de julio 2010, 07:44:02 PM

> Cita de Red, 25 de julio 2010, 07:22:14 PM
>
> Satoshi señaló que mi escenario aún requería que se rompiese la función hash. Eso es cierto, pero me sorprendió aprender cuán exitosos han sido con eso. MD4 y MD5 son ejemplos obvios, pero el trabajo está en marcha para colisionar SHA-1 y hermanos como SHA-256.

Sin embargo, lo que a menudo no mencionan es *la generación de colisiones* todavía requiere mucho tiempo de CPU.

Si descubro que la Clave Pública 123456 genera Hash ABCD y la clave pública 654321 también genera Hash ABCD

Todavía me quedo sin la clave privada.

Pero por lo que dices, todo lo que necesito es la clave pública 654321 y puedo gastar una moneda pretendiendo ser clave pública 123456.

Re: Robo de Monedas

Publicado por Red, 25 de julio 2010, 07:52:23 PM

Por lo que me dijeron, Bitcoin está usando uno de los 160 bit hashes para generar unas direcciones bitcoin.

La familia SHA-1 de algoritmos hash son algunos de los más comúnmente utilizados. SHA-1 es un hash de 160 bit.

Aquí hay un documento que afirma encontrar colisiones SHA-1 en 2^52 operaciones de cifrado. Y el hash optimizado de forma segura tomaría 2^80 operaciones. 2^52 es todavía un tiempo considerable, pero está entrando en el rango de clúster y ordenadores infectados.

http://www.ictlex.net/wp-content/iacrhash.pdf

> Los hashes MD5 ya pueden bloquearse en segundos en las computadoras portátiles. Por eso fue retirado de las firmas basadas en certificados.
>
> Y sí, lo que estoy diciendo es **Creo** que se puede pensar en una clave pública como dos números secretos combinados juntos matemáticamente. Y la clave privada como esos dos números guardados por separado. Lo que hace que el sistema sea seguro requiere que eso dos números secretos sean números primos realmente grandes.
>
> Pero si son realmente números no primos grandes, la combinación matemática aún funciona, simplemente es más rápido romper el algoritmo.
>
> Voy a hacer un poco más de googleo y ver si puedo corroborar mis afirmaciones. Esperaba que alguien pudiera descartarlos sin más.

Robo de Monedas

Publicado por Satoshi, 25 de julio 2010, 08:01:40 PM

> Cita de knightmb, 25 de julio 2010, 07:44:02 PM
>
> Si descubro que la Clave Pública 123456 genera Hash ABCD y la clave pública 654321 también genera Hash ABCD
>
> *Todavía me quedo sin la clave privada.*
>
> Pero por lo que dices, todo lo que necesito es la clave pública 654321 y puedo gastar una moneda pretendiendo ser clave pública 123456.

Aún deberá firmarlo con la clave pública 654321. Necesita encontrar una colisión usando una clave pública para la cual conoce la clave privada.

Cuando reclamas una transacción de Dirección de Bitcoin, usted le da su clave pública que coincide con el hash, luego debe firmarlo con esa clave.

El argumento de Red es que es fácil de generar rápidamente claves

públicas inseguras que podría romper y encontrar la clave privada después de encontrar una colisión.

Señala que, si la clave pública fuese requerida de ser segura, una que debe haber requerido un trabajo significativo para encontrar los números primos, eso aumentaría la fuerza por encima de la función hash sola. Alguien que intentándolo con fuerza bruta debería tomarse un tiempo para generar una clave para cada intento.

Re: Robo de Monedas

Publicado por knightmb, 25 de julio 2010, 08:20:41 PM

> Cita de Satoshi: Satoshi, 25 de julio 2010, 08:01:40 PM
>
> Aún deberá firmarlo con la clave pública 654321. Necesita encontrar una colisión usando una clave pública para la cual conoce la clave privada.
>
> Cuando reclamas una transacción de Dirección de Bitcoin, usted le da su clave pública que coincide con el hash, luego debe firmarlo con esa clave.
>
> El argumento de Red es que es fácil de generar rápidamente claves públicas inseguras que podría romper y encontrar la clave privada después de encontrar una colisión.
>
> Señala que, si la clave pública fuese requerida de ser segura, una que debe haber requerido un trabajo significativo para encontrar los números primos, eso aumentaría la fuerza por encima de la función hash sola. Alguien que intentándolo con fuerza bruta debería tomarse un tiempo para generar una clave para cada intento.

Sí, pensé que la clave privada tenía que estar en la mezcla en alguna parte. Sin embargo, agrega otra aleatoriedad, tienes que encontrar el hash que colisiona con otra clave pública y, al mismo tiempo, la clave privada tiene que ser lo suficientemente débil para romperla. No digo que sea imposible, pero introduce 2 variables en el hallazgo de colisión inversa.

> Básicamente, uno construiría una tabla arcoíris de claves privadas débiles y luego tendría que compararlas con los hashes públicos y luego tener la esperanza que alguien tenga un hash que sea parte de ese ataque. No es imposible, por supuesto, pero ¿qué tan factible, incluso si las computadoras fueran 100 veces más rápidas en 10 años?
>
> [edit] ok, vuelve a leer lo que escribiste, la clave pública es generada desde la clave privada, no independientemente. Entonces, solo encontrar una clave pública débil es el problema.

Re: Robo de Monedas

Publicado por Satoshi, 25 de julio 2010, 08:48:01 PM

> Cita
>
> Aquí hay un documento que dice encontrar colisiones SHA-1 en 2^52 operaciones de cifrado. Y el hash optimizado de forma segura tomaría 2^80 operaciones. 2^52 es todavía un tiempo considerable, pero está entrando en el rango de clúster y ordenadores infectados.
>
> ---

2^80 es si puedes usar un ataque de cumpleaños. No puede usar un ataque de cumpleaños para esto, por lo que la dificultad está en los 2^160 bits completos. Aunque, si intentaba crackear cualquiera de las transacciones de 1 millón (2^20), podría hacer un ataque parcial de cumpleaños 2^160/2^20 = 2^140

Las direcciones de Bitcoin son el único lugar donde es usado un hash de 160 bits. Todo lo demás es SHA-256. Se calculan como:

dirección bitcoin = RIPEMD-160 (SHA-256 (clave pública))

Corrígeme si me equivoco (por favor, y con mucho gusto comeré cuervo) pero creo que sería difícil usar un ataque analítico contra RIPEMD-160 en este caso. Un ataque analítico prescribe un cierto rango o patrón de insumos para probar que aumentarán en gran medida sus posibilidades de encontrar una colisión. Aquí, no tiene ese tipo de control sobre la entrada de RIPEMD-160, porque la entrada es la salida de SHA-256. Si un ataque analítico lo ayuda a encontrar una entrada para RIPEMD-160 que produce

una colisión, ¿qué va a hacer con ella? Todavía tiene que obtener SHA-256 para generar ese valor, por lo que aún tendrá que romper SHA-256 también.

Para la fuerza bruta, RIPEMD-160(SHA-256(x)) no es más fuerte que RIPEMD-160 solo. Pero para un ataque analítico, parece que debe realizar un ataque analítico tanto RIPEMD-160 como SHA-256. Si me equivoco, entonces la fortaleza es la misma que RIPEMD-160 y el SHA-256 solo sirve como una ronda de fortalecimiento de la llave.

Re: Robo de Monedas

Publicado por Red, 25 de julio 2010, 09:04:01 PM

> Cita de: Satoshi, 25 de julio 2010, 08:48:01 PM
>
> Dirección bitcoin = RIPEMD-160(SHA-256(clave pública))
>
> Corrígeme si me equivoco (por favor, y con mucho gusto comeré cuervo) pero creo que sería difícil usar un ataque analítico contra RIPEMD-160 en este caso.
>
> ---

Creo que tienes razón en el ataque analítico. Al menos hasta donde yo entiendo (mínimamente) el genio matemático que los está analizando.

Me preocupaba que fuera más simple:

Dirección bitcoin = RIPEMD-160(llave pública)

Re: Robo de Monedas

Publicado por Red, 25 de julio 2010, 09:19:11 PM

Así que la forma en que lo leo.

Dado dos números p y q. Se supone que para RSA son primos grandes.

Entonces n = p*q

La clave pública son los dos campos (n, e). “e” es llamado el exponente público y parece ser elegido de un conjunto de valores comunes.

La clave privada también son dos campos (n, d). “d” es llamado el exponente privado del que se deriva al conocer “e”, “p-1” y “q-1”.

El truco es que es realmente difícil factorizar “n” en “p” & “q”. Por lo tanto, es igualmente difícil encontrar “p-1” y “q-1”

Lo que postulo es que, si “n” es arbitrario, y “e” es uno de los valores comunes, entonces hay muchos pares “p”, “q” diferentes que funcionarían. Cuantos menos primos sean los números, más fácil de encontrar “p” y “q”, y por lo tanto “p-1” y “q-1”. Y si tiene un gran bloque de datos arbitrarios que le dan mucha flexibilidad al intentar colisionar un hash.

(Ese es el punto donde podría estar totalmente fuera de lugar. Realmente interesado, si un cripto geek lo conoce mejor que yo.)

Leí que los algoritmos de generación de claves crean “p” y “q” de tal manera que son "muy probablemente primos", pero es demasiado trabajo para saberlo con certeza. Esto me lleva a creer que los no primos no causan FALLAS obvias. Sin embargo, podría estar equivocado.

Re: Robo de Monedas

Publicado por Red, 26 de julio 2010, 12:46:04 PM

> Cita de: Satoshi, 25 de julio 2010, 10:27:36 PM
>
> Lo siento, en realidad es ECDSA (Algoritmo de Firma Digital de Curva Elíptica, en Inglés, Elliptic Curve Digital Signature Algorithm) no RSA. No debería haber dicho "números primos". ECDSA no toma mucho tiempo para generar un par de llaves.
>
> Aprenderé cómo funcionan las curvas elípticas algún día, pero no hoy. Debería haber estudiado más matemáticas cuando estaba en la universidad. ¡Quién hubiera pensado que hubiera sido útil para algo!

Por cierto, ¡buena idea e implementación de BitCoin Satoshi!

Abre un nuevo mundo de posibilidades. Me gusta especialmente el concepto de acuerdo distribuido sin confiar en la confianza. Creo que ese es el concepto innovador.

Además, creo que la idea de la minería BitCoin es brillante. Dudo que pudieras haber conseguido la red arrancada de otra forma. No estoy de acuerdo en que sea una "forma justa" de distribuir monedas, pero ¡ojalá el mundo no sea justo! Y realmente, no creo que de ninguna otra manera hubiera generado tanto entusiasmo en el usuario.

Por cierto, concedo que no hay ningún hilo de robo de bitcoins de mi comentario anterior. El doble hash parece asegurar eso desde mi perspectiva. ¡Buena llamada!

A propósito, aún me gustaría saber qué sucede si genera claves RSA basadas en números no primos. Me imagino que hay otros sistemas que no duplican el hash. :-)

Re: Robo de Monedas

Publicado por Bitcoiner, 27 de julio 2010, 02:01:16 PM

¡Me alegro de que haya muchachos como Red a la vista! Este hilo también me hace apreciar el software de código abierto, ya que hay tantos personas inteligentes e interesadas en estos foros que pueden validar el software y colocar un grado adicional de confianza en él. ¡No estoy seguro de que Bitcoin sea demasiado exitoso si fuera de código cerrado!

Re: Robo de monedas

Publicado por bytemaster, 28 de julio 2010, 09:42:17 PM

Me parece que la solución obvia para minimizar el riesgo de cualquier

ataque potencial es hacer pequeña la potencial "recompensa". Por lo tanto, nunca guarde demasiadas monedas en una sola dirección. Si el valor económico del "premio" es menor que el costo de romperlo, entonces nadie se molestará en intentarlo. Después de decir eso, todavía pienso que es mejor mantener las cosas lo más difíciles posible para evitar robos.

Re: Robo de monedas

Publicado por knightmb, 28 de julio 2010, 10:45:16 PM

Ciertamente sería difícil tanto por suerte y como por el poder de CPU/poder de almacenamiento, hacer esto.

Si encuentra una colisión y una clave privada, eso no le haría ningún bien, ya que tendría que pegar una cuenta de las 541,638,008,296,341,754,635,824,011,376,225,346,986,572,413,939,634,062,667,808,768 posibles combinaciones de personas que usan cuentas.

Así que mírelo doble. Yo encuentro una colisión en el hash y encuentro la clave privada. Ahora tengo que esperar que mis probabilidades incluyan que alguien más está usando ese hash. Dado que hay más números posibles de cuentas hash que todas las personas nacidas en este planeta y cada uno estaba usando un millón de direcciones, el ataque por su propia naturaleza, aunque interesante, no es realmente factible a gran escala.

50

Mayor Defecto Descubierto

Traducción por **Arturo Monzón**

UN IMPORTANTE FALLO fue descubierto en el software/protocolo Bitcoin que permitía a un remitente enviar transacciones no válidas, donde el remitente creaba nuevos bitcoins. Para cuando fue corregido, se habían creado varios millones de bitcoins no válidos. Posteriormente fueron borrados de la cadena de bloques.

*** ALERTA *** Actualiza a 0.3.6

Publicado por Satoshi, 29 de julio 2010, 07:13:06 PM

Por favor, actualice a 0.3.6 lo antes posible! Solucionamos un error de implementación donde era posible que las transacciones falsas se mostrarán como aceptadas. No acepte transacciones de Bitcoin como pago hasta que actualice a la versión 0.3.6!

Si no puede actualizar a la versión 0.3.6 inmediatamente, lo mejor es cerrar su nodo Bitcoin hasta que lo haga.

También en 0.3.6, hasheando más rápido:

- optimización del caché midstate gracias a tcatm
- Crypto ++ ASM SHA-256 gracias a BlackEye

Total, generando una aceleración 2.4 veces más rápida.

Descargar:
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.6/

Usuarios de Windows y Linux: si obtuvieron la versión 0.3.5, aún necesitan actualizar a 0.3.6.

51

Prevención de Un Ataque de Inundación

Traducción por **Arturo Monzón**

LA PREOCUPACIÓN ELEVADA AQUÍ es el equivalente a un ataque de denegación de servicio en la red de Bitcoin donde una entidad podría enviar millones de transacciones, cada una transfiriendo una pequeña cantidad, 1 satoshi (0.00000001 BTC) por ejemplo. Esta publicación es más técnica que otras, y no todas las publicaciones se han copiado aquí, solo aquellas relevantes para el tema y aquellas sobre las preocupaciones abordadas por Satoshi.

Ataque de Inundación 0.00000001 BC

Publicado por Mionione, 12 de julio de 2010, 12:04:24 PM

---

hola, ¿qué pasaría si alguien envía millones de 0.00000001 BC a millones de direcciones, por favor?

=> todos los pares de redes deben almacenar todas las transacciones?
=> ¿cada destinatario/hash de 0.00000001 está almacenado en bloques sobre todos los puntos?

Realmente no entiendo cómo bitcoin puede manejar fracciones de bc

Re: Ataque de Inundación 0.00000001 BC

Publicado por Gavin Andresen, 12 de julio 2010, 12:08:45 PM

Desde el código fuente:

main.h: // Para limitar el spam en polvo, se requiere una tarifa de 0.01 si alguna salida es menor a 0.01

Re: Ataque de Inundación 0.00000001 BC

Publicado por llama, 12 de julio 2010, 02:23:46 PM

Hmm, no me había dado cuenta de que estaba ahí, y realmente no me gusta ese enfoque.

Eso prácticamente arruina la posibilidad de usar bitcoin para verdaderos micropagos. ¿No sería mejor para los clientes simplemente ignorar una IP spam? Claro que un atacante podría obtener más, pero no podría obtener millones.

Re: Ataque de Inundación 0.00000001 BC

Publicado por Gavin Andresen, 12 de julio 2010, 02:45:54 PM

Pero ¿cómo distinguirías entre una IP legítima de procesamiento de micropagos y un spam? "Quiero hacer que Bitcoin use tanto ancho de banda que nadie esté dispuesto a ejecutar más" IP?

Los micropagos realmente pequeños parecen ser un problema realmente difícil, y no creo que Bitcoin deba tratar de resolver demasiados problemas muy difíciles a la vez.

Re: Ataque de Inundación 0.00000001 BC

Publicado por Gavin Andresen, 12 de julio 2010 02:45:54 PM

Pero ¿cómo distinguirías entre una IP legítima de procesamiento de micropagos y un spam? "Quiero hacer que Bitcoin use tanto ancho de banda que nadie esté dispuesto a ejecutar más" IP?

Re: Ataque de Inundación 0.00000001 BC

Publicado por Insti, 04 de agosto 2010, 02:58:31 PM

¿Qué es exactamente este 'spam en polvo' que esta tarifa de transacción de 0.01BTC "resuelve"?

Parece hacer más daño que bien porque evita las implementaciones de micropagos, como sugiere bytemaster.

No estoy al tanto de que la red se esfuerce por el peso del volumen de transacciones existente.

Cualquiera que desee enviar muchas transacciones puede hacerlo enviando muchos x BTC a sí mismo.

Re: Ataque de Inundación 0.00000001 BC

Publicado por Satoshi, 04 de agosto 2010, 04:25:36 PM

Cita de: Insti el 4 de agosto de 2010, 02:58:31 PM

Parece hacer más daño que bien porque evita las implementaciones de micropagos, como sugiere bytemaster.

Bitcoin actualmente no es práctico para micropagos muy pequeños. No es para cosas como pago por búsqueda o para visitas a páginas sin un

mecanismo de agregación, no es para cosas que necesitan pagar menos que 0.01. El límite del spam en polvo es un primer intento de tratar intencionalmente de evitar micropagos demasiado pequeños como ese.

Bitcoin es práctico para transacciones más pequeñas que los métodos de pago existentes. Lo suficientemente pequeño como para incluir lo que podría llamarse la parte superior del rango de micropagos. Pero no pretende ser práctico para micropagos arbitrariamente pequeños.

Re: Ataque de Inundación 0.00000001 BC

Publicado por satoshi, 05 de agosto 2010, 04:03:21 PM

Olvidé añadir la parte buena de los micropagos. Aunque no creo que Bitcoin sea práctico para micropagos más pequeños en este momento, eventualmente será como el almacenamiento mientras los costos de ancho de banda continúen cayendo. Si Bitcoin alcanza una gran escala, puede que ya sea así en ese momento. Otra forma en que pueden ser más prácticos es si solo se implementa el modo para cliente y la cantidad de nodos de red se consolida en un número menor de granjas de servidores profesionales. Cualquier tamaño de micropagos que necesite eventualmente será práctico. Creo que en 5 o 10 años, el ancho de banda y el almacenamiento serán cuestiones triviales.

No pretendo que la red sea impermeable al ataque de denegación de servicio (DoS por sus siglas en Inglés). Creo que la mayoría de las redes P2P pueden ser atacadas por DoS en numerosas formas. (Como comentario adicional, leí que a las compañías discográficas les gustaría hacerlo en todas las redes de intercambio de archivos, pero no quieren romper las leyes antipiratería/anti-abuso).

Si comenzamos a atacar a DoS con un montón de transacciones desperdiciadas, tendría que comenzar a pagar una tarifa mínima de transacción de 0.01. 0.1.5 en realidad tenía una opción para configurar eso, pero lo saqué para reducir la confusión. Las transacciones gratuitas son buenas y podemos mantenerlo de esa forma si las personas no abusan de ello.

Eso nos lleva a la pregunta: si hubiera un cargo mínimo de 0.01 por cada transacción, ¿deberíamos agregar automáticamente la tarifa si es solo el

mínimo de 0.01? Sería terriblemente molesto preguntar cada vez. Si tienes 50,00 y envías 10,00, el destinatario obtiene 10.00 y te quedarán 39,99. Creo que debería agregarse automáticamente. Es trivial en comparación con las tarifas que muchos otros tipos de servicios cargan automáticamente.

> Cita de: FreeMoney, 04 de agosto 2010, 07:30:32 PM
>
> ¿Incluye disminuir más la velocidad de hash?
>
> No, en absoluto.

Re: Ataque de Inundación 0.00000001 BC

Publicado por satoshi, 05 de agosto 2010, 04:30:20 PM.

> Cita de: bytemaster.
>
> Los pagos generalmente se adelantan, digamos 1 BTC a la vez y cuando la conexión se cierra, se devolverá cualquier "cambio". Esta regla hace que sea imposible pagar una simple "búsqueda de consulta" sin más transacciones.
>
> ---

Una alternativa es usar un sistema de redondeo. Pagas, digamos, 1000 páginas o imágenes o descargas o búsquedas o lo que sea de una vez. Cuando haya agotado sus 1000 páginas, pagará por otras 1000 páginas. Si solo usa 1 página, entonces le quedan 999 que quizás nunca use, pero no es un gran problema porque el costo por cada 1000 es aún pequeño.

O podría pagar por día. La primera vez que accede al sitio en un día determinado, paga por 24 horas de acceso.

Por 1000 o por día, puede ser más fácil para los consumidores darse el gusto también. Se preocupan por cada elemento porque es más difícil saber si se puede acumular demasiado rápido. Ilimitado por 24 horas se sabe cuál será el costo. O si 1000 parece suficiente, no se preocupan de que cueste más con cada clic si calculan que 1000 es más de lo que probablemente usarán.

Re: Ataque de Inundación 0.00000001 BC

Publicado por satoshi, 05 de agosto 2010, 04:39: 58 PM

> Cita de: bytemaster, 5 de agosto 2010, 03:39:19 PM
>
> La única solución a este problema es hacer la transmisión de una transacción "no gratis". Concretamente, si quieres que lo incluya, tienes que pagarme. El resultado neto (sin juego de palabras) es que cada cliente debería pagar a otros clientes a quienes incluso envían sus transacciones, no solo a la persona que los recibe en un bloque. De esta manera, las leyes de la economía toman el control y nadie obtiene un viaje gratis en el sistema de transmisión de transacciones.
>
> No sé cómo implementarlo. La tarifa de transacción para el creador del bloque usa un truco especial para incluir la tarifa de transacción sin ningún tamaño adicional. Si hubo una transacción por cada comisión de transacción, ¿qué pasa con las comisiones para la transacción de la tarifa de transacción?

Re: Ataque de Inundación 0.00000001 BC

Publicado por satoshi, 05 de agosto 2010, 05:49:43 PM.

> Cita de: bytemaster, 05 de agosto 2010, 04:46:52 PM.
>
> Ahora la dirección de la tarifa de transacción se deja "en blanco" y el generador de bloques lo rellena.
>
> Ahora debe completarlo con la dirección de la persona que lo está solicitando para construir el bloque.
>
> ---

Si solo va a hacer que una persona trabaje en la construcción del bloque, eso podría llevar días. Ah, ¿te refieres a enviar una variación diferente a cada nodo con la tarifa de transacción escrita para ellos?

De la forma en que está ahora, es quien construye esto lo consigue.

Si necesitáramos, podríamos tener un esquema BitTorrent, toma y daca para transmisión de transacciones. Se Retransmitirá pagando la transacción, o no se transmitirá. Sin embargo, probablemente no será un problema real. Solo se necesita la retransmisión de un nodo como debería para cancelar a otros 7 que codiciosamente no están retransmitiendo.

Re: Ataque de Inundación 0.00000001 BC

Publicado por satoshi, 11 de agosto 2010, 11:28:50 PM

Sería bueno mantener los archivos blk*.dat pequeños mientras podamos.

Para la solución final no importará lo grande que sea.

Pero por ahora, aunque todavía es pequeño, es bueno mantenerlo así para que los nuevos usuarios puedan avanzar más rápido. Cuando finalmente implemente el modo solo cliente, eso ya no importará mucho.

Hay más trabajo por hacer en las tarifas de transacción. En caso de una inundación, aún podría saltar la cola y obtener sus transacciones en el siguiente bloque pagando una tarifa de transacción de 0.01. Sin embargo, no he tenido tiempo aún de agregar esa opción a la interfaz de usuario.

Escalar o no, la red de prueba reaccionará de la misma manera, pero con mucho menos desperdicio de ancho de banda y molestias.

52

Drenaje de Grifo Bitcoin

Traducción por **Arturo Monzón**

A MEDIDA QUE el valor de los bitcoins aumentaba, el grifo de Bitcoin (ver referencia anterior) era cada vez más atractivo. Gavin Andresen informa que el valor de un bitcoin ha aumentado en un factor de 10 desde que él creó el Grifo.

¿Quién es el Español Idiota Drenando el Grifo?

Publicado por Gavin Andresen, 04 de agosto 2010, 08:40:55 PM

Acabo de cerrar freebitcoins.appspot.com; parece que alguien en España es un imbécil y está obteniendo una nueva dirección IP, una dirección de bitcoin y resolviendo el captcha. Una y otra y otra vez:

Código:

79.154.133.217 - - [04/Aug/2010:12:46:55 -0700]
"POST/HTTP/1.1"200 1294 “https://freebitcoins.appspot.com/"
"Opera/9.80 (Windows NT 6.0; U; es-LA) Presto/2.6.30
versión/10.60, gzip (gfe)"

79.146.112.13 - - [04/Aug/2010:12:45:20 -0700] "POST/HTTP/1.1" 200 1294 "https://freebitcoins.appspot. com/" "Opera/9.80 (Windows NT 6.0; U; es-LA) Presto/2.6.30 versión/ 10.60, gzip (gfe)"

81.44.159.81 - - [04/Aug/2010:12:42: 20 -0700]

"POST/HTTP/1.1" 200 1294 "https://freebitcoins.appspot. com/" "Opera/9.80 (Windows NT 6.0; U; es-LA) Presto/2.6.30 versión/10.60, gzip (gfe)"

Esas direcciones IP dirigen hacia el mapa de Telefónica de España. Si fuera usted: devuélvalos, por favor:
15VjRaDX9zpbA8LVnbrCAFzrVzN7ixHNsC

Ahora que 5 bitcoins valen un poco, estoy pensando que necesito más contramedidas contra engaño. Puedo pensar en cuatro cosas para probar:

1. Límite de velocidad basado en el primer byte de la dirección IP (79. u 81. en este caso).

2. Límite de velocidad basado en la cadena USER-AGENT ("Opera / 9.8 ..." en este caso).

3. Límite de velocidad basado en los dos últimos dominios de búsqueda DNS inversa de la dirección IP (rima-tde.net en este caso).

4. Haga que se regale la cantidad estándar de 0.5 Bitcoins (los Bitcoins han subido 10 veces en valor desde que inicié el Grifo).

Si obtienes una tarifa limitada, recibirás un mensaje que te pedirá que intentes de nuevo mañana.

BitcoinFX: gracias de nuevo por las donaciones al grifo; Voy a drenar el Grifo por debajo de 500 monedas temporalmente, y lo rellenaré con sus donaciones después de que las nuevas contramedidas contra trampas estén implementadas.

Re: ¿Quién es el Español Idiota Drenando el Grifo?

Publicado por satoshi, 04 de agosto 2010 08:40:55 PM

Fallar silenciosamente se vería mal.

> Cita de: gavinandresen, 04 de agosto 2010 08:40:55 PM
>
> 1. Límite de velocidad basado en el primer byte de la dirección IP (79. o 81. en este caso).
>
> ---

Definitivamente necesario. ¿Qué tasa estás pensando? En última instancia, es mejor calificar el límite que dejar que todo se agote.

> Cita de: gavinandresen, 04 de agosto de 2010, 08:40:55 PM
>
> 3. Límite de velocidad basado en los dos últimos dominios de búsqueda DNS inversa de la dirección IP (rima-tde.net en este caso).
>
> ---

Eso podría funcionar sorprendentemente bien. Si funciona, evita que alcancen el límite de velocidad, pero el límite de velocidad está allí como última línea de defensa.

> Cita de: gavinandresen, 04 de agosto de 2010, 08:40:55 PM
>
> 4. Haga que se regale la cantidad estándar de 0.5 Bitcoins (los Bitcoins han subido 10 veces en valor desde que inicié Faucet).
>
> ---

Definitivamente es el momento de bajarlo.

53

Transacción a Una Dirección IP en Lugar de Una Dirección de Bitcoin

Traducción por **Adrián Bernabéu Escudero**

AL PRINCIPIO, se consideró la posibilidad de enviar a una dirección IP en lugar de (o quizás además de) a una dirección de Bitcoin.

Transacción de bitcoin a dirección IP

Publicado por lfm, 05 de agosto 2010, 02:22:14 PM

No puedo entender cómo enviar una transacción a una dirección IP desde la interfaz de línea de comandos de bitcoin. ¿Ya se implementó la función? (En Linux 64, por si acaso es importante).

Re: Transacción de bitcoin a dirección IP

Publicado por Satoshi, 05 de agosto 2010, 05:28:40 PM

No se ha implementado.

Resultó que a nadie le gustaba esa modalidad de transferencia, por lo que no ha tenido mucha atención este desarrollo.

54

Custodia de Depósitos y Transacciones Multi-Firma

Traducción por **Adrián Bernabéu Escudero**

LAS TRANSACCIONES requieren múltiples firmas que están integradas en el protocolo de Bitcoin y pueden ser utilizadas por los servicios de custodia. Por ejemplo, tres claves están involucradas, pero sólo dos de ellas son necesarias para firmar la transacción. En tal caso, una clave es propiedad del pagador, la segunda del beneficiario y la tercera del agente de custodia. Cuando no hay disputas o conflictos, el ordenante y el beneficiario firman la transacción para que el beneficiario pueda recibir los fondos.

Si hay una disputa, el agente de custodia revisa la disputa y, después de decidir por el pagador o por el beneficiario, firmará la transacción sobre la parte por quien el agente de custodia haya decidido. Esto es similar a un cheque bancario que requiere dos firmas de cualquiera de las tres personas, en este caso, el ordenante, el beneficiario y el agente de depósito en garantía. Los servicios de custodia para las transacciones de Bitcoin ya existen hoy en día. Los siguientes tres hilos contienen discusiones relacionadas en cómo se podría manejar el depósito en custodia y las implicaciones para Bitcoin.

Propuesta para un mecanismo de custodia semi-automatizado

Publicado por Olipro, 30 de julio 2010, 07:29:08 PM

Por lo tanto, el depósito en custodia básico funciona con dos personas que trabajan a través de un tercero para intercambiar (generalmente dinero) por algún bien o servicio.

En una transacción en la que ambas personas son honestas, el negocio de custodia puede ser esencialmente automático, ya que el comprador obtiene sus productos y aprueba liberar fondos, solo cuando hay una disputa, la interacción humana se vuelve necesaria. Por lo tanto, propongo el siguiente sistema:

1) Usted crea una transacción de custodia por una cantidad, autorizada por su llave y que contiene la clave/datos del destinatario, etc. este bloque no puede reclamarse hasta que el comprador emita un bloque subsiguiente para aprobarlo, también es imposible que el comprador lo reclame sin que el vendedor lo apruebe para ser devuelto.

2) Entra en la red, se verifica y el vendedor envía los productos, una vez que el comprador los obtiene, libera la transacción y el vendedor recibe sus bitcoins.

3) Si ocurre una disputa y ambas partes se niegan a liberar el dinero de una manera u otra, es evidente que ahora es necesario conseguir que un tercero haga el arbitraje; en esta situación, se requiere una firma tanto del comprador como del vendedor autorizando a un tercero que le otorgará la propiedad de la transacción de custodia original y luego podrá arbitrar el asunto.

Re: Propuesta para un mecanismo de custodia semi-automatizado

Publicado por satoshi, 05 de agosto 2010, 06:08:30 PM

Una transacción puede ser suscrita, lo que requiere dos firmas para ser gastadas luego. Usted suscribe un pago que requiera la firma tanto del destinatario como del remitente para gastarlo. Para liberar el depósito, usted le da al destinatario su firma por la mitad, o el beneficiario puede devolverlo entregando su mitad firmada. No hay mediador en este simple caso. El recurso es negarse a hacerlo, esencialmente quemando el dinero.

Re: Propuesta para un mecanismo de custodia semi-automatizado

Publicado por satoshi, 07 de agosto 2010, 08:04:59 PM

> Cita de: jgarzik el 05 de agosto de 2010, 07:00:30 PM
>
> Debido a ese recurso, es poco probable que se use como mecanismo de depósito en custodia : -)
>
> ---

¿De verdad? ¿Crees que las personas no podrán entender el beneficio? (Si su respuesta es un argumento donde no hay ningún beneficio en absoluto, creo que eso reforzará el caso de que las personas no podrán entenderlo).

Aquí, Satoshi crea un hilo específico con respecto al manejo de custodia.

Custodia

Publicado por satoshi, 07 de agosto 2010, 08:13:52 PM

Aquí hay un boceto del tipo de transacción de custodia en garantía que son posibles en el software. Esto no está implementado y probablemente no haya tiempo para implementarlo pronto, es sólo para informar de lo que es posible.

Custodia básica: el comprador compromete un pago en custodia. El vendedor recibe una transacción con el dinero en custodia, pero no puede gastarlo hasta que el comprador lo desbloquee. El comprador puede liberar el pago en cualquier momento después, lo que podría ser nunca. Esto no le permite al comprador recuperar el dinero, pero sí tiene la opción de quemar el dinero a pesar de que nunca lo libere. El vendedor tiene la opción de devolver el dinero al comprador.

Si bien este sistema no garantiza a las partes de una posible pérdida, eliminas el beneficio de hacer trampas.

Si el vendedor no envía los productos, no se le paga. El comprador todavía tendría el dinero y al menos al vendedor le quitas la motivación monetaria para estafar.

El comprador no puede beneficiarse al no pagar. No puede recuperar el dinero de la custodia. No puede dejar de pagar debido a una falta de fondos. El vendedor puede ver que los fondos están comprometidos con su clave y no pueden ser enviados a nadie más.

Ahora, un economista diría que un vendedor fraudulento podría comenzar a negociar, diciendo cosas como "libera el dinero y te devolveré la mitad", pero en ese punto, habría tan poca confianza y tanto rencor como para que la negociación sea probable. ¿Por qué el estafador cumpliría su palabra y te enviaría la mitad si ya está rompiendo su palabra para hacer robo? Creo que por pequeños montos, casi todo el mundo lo rechazaría en principio.

Re: Custodia

Publicado por jgarzik, 07 de agosto 2010, 09:25:40 PM

El comprador no tiene opciones, excepto quemar el dinero para limitar su utilidad, creo.

Re: Custodia

Publicado por aceat64, 08 de agosto 2010, 02:55:59 A.M

> Cita de: jgarzik, 07 de agosto 2010, 09:25:40 PM
>
> El comprador no tiene opciones, excepto quemar el dinero para limitar su utilidad, creo.
>
> ---

Tal vez podríamos trabajar en una forma para hacer el arbitraje. Si tanto el comprador como el vendedor están de acuerdo, el dinero se puede desviar a un tercero. Esa persona podría entonces arbitrar y devolver el dinero al comprador, dárselo al vendedor o robarlo (obviamente, usted querrá elegir un árbitro de confianza).

Re: Custodia

Publicado por jgarzik, 08 de agosto 2010, 03:58:03 AM

> Cita de: aceat64, 08 de agosto 2010, 02:55:59 AM
>
> ---
>
> > Cita de: jgarzik, 07 de agosto 2010, 09:25:40 PM
> >
> > El comprador no tiene opciones, excepto quemar el dinero para limitar su utilidad, creo.
> >
> > ---

> Tal vez podríamos trabajar de una manera para hacer el arbitraje. Si tanto el comprador como el vendedor están de acuerdo, el dinero se puede desviar a un tercero. Esa persona podría entonces arbitrar y devolver el dinero al comprador, dárselo al vendedor o robarlo (obviamente, usted querrá elegir un árbitro de confianza).

Así es como se opera en línea la custodia hoy en día. Comprador y vendedor acuerdan que un tercero tenga físicamente el dinero. Comprador y vendedor acuerdan las reglas que seguirá la tercera parte neutral para la resolución/canje de la transacción. El tercero neutral es quien desembolsa los fondos a una parte u otra.

Esta es una descripción bastante decente:
https://www.escrow.com/solutions/escrow/process.asp

Algunas personas pueden optar por utilizar el método de custodia firmado de Bitcoin específico ... pero el recurso de "quemar el dinero" sirve como un incentivo para *evitar* la custodia del bitcoin por completo, en lugar de ser un incentivo para usar la custodia del bitcoin honestamente.

Re: Custodia

> Publicado por aceat64, 08 agosto 2010, 05:49:44 AM

> Me gusta la sugerencia de Olipro es este hilo:
> http://bitcointalk.org/index.php?Topic=645.0
>
> El comprador y el vendedor ponen una cantidad igual de bitcoins en custodia y el vendedor no puede recuperar ambos sets hasta que el comprador lo firme. Opcionalmente, si ambas partes acuerdan que los fondos se devuelven a sus dueños originales o si ambos sets se transfieren a un árbitro acordado. Me desvié de su sugerencia de que el árbitro solo tiene el control de la mitad de los compradores, creo que deberían tener el control de ambos montos para que ambas partes sigan teniendo una participación de bitcoin en el asunto.

Re: Custodia

Publicado por jgarzik, 10 de agosto 2010, 06:53:57 PM

> Cita de: nimnul, 10 de agosto 2010, 05:51:49 PM
>
> La solución de Satoshi es buena, pero si el cliente puede recuperar el dinero, será un gran problema para los vendedores. Vea la situación actual con los pagos con tarjeta de crédito de internet y la anulación de cargos. Los recargos son un verdadero dolor de cabeza para los vendedores, bitcoin debe evitarlos a toda costa : -)
>
> ---

Pregúnteles a los dueños de negocios del mundo real si quieren contarles a sus clientes a cerca de la posibilidad de que el dinero se pierda para siempre, siendo irrecuperable para cualquiera de las partes.

Re: Custodia

Publicado por nelisky, 10 de agosto 2010, 08:20:36 P.M

Independientemente de cuáles sean las opciones técnicas, creo que un depósito en custodia siempre tendrá que existir, por definición, una entidad confiable. Puedo ver que el flujo de trabajo automatizado fácilmente cuando las cosas van bien:

- El comprador envía btc al fideicomiso, indicando la dirección del destinatario
- El vendedor ve los btc en custodia, marcados para enviar a su dirección
- El comprador puede liberar los fondos al vendedor
- La custodia va a hacerlo automáticamente después de x días
- Ambas partes pueden abrir una queja

Y eso es todo lo que será automatizado. Cuando las cosas van mal, ambas partes deben pagar una tarifa para el depósito en garantía (¿esa

> tarifa puede pagarse por adelantado para abrir una cuenta?), por lo que todos pierden algo. Así el depósito de garantía solo tendrá que mediar.
>
> Debido a que hay una tarifa *y* un intermediario humano, la posibilidad de fraude exitoso probablemente no será económicamente interesantes en el largo plazo. Alguien en quien ya se confía sería la persona ideal para esto, y tal vez por una pequeña tarifa algunos de nosotros, "tipos comunes", podríamos ayudar a afirmar las acusaciones de cualquiera de los lados, si somos próximos para ellos.
>
> Pero la solución de la quema de dinero, si bien es excelente para prevenir el fraude y económicamente viable, no hace nada para evitar la venganza y, en realidad, hace que todos pierdan si una parte es deshonesta. Ciertamente no apoyaría eso.

Re: Custodia

Publicado por satoshi, 11 de agosto 2010, 01:30:02 A.M

> Cita de: jgarzik el 10 de agosto 2010, 06:53:57 PM
>
> Pregúnteles a los dueños de negocios del mundo real si quieren contarles a sus clientes a cerca de la posibilidad de que el dinero se pierda para siempre, siendo irrecuperable para cualquiera de las partes.
>
> ---

Eso hace que suene como que de alguna manera ambas partes pueden perder, y no lo pueden recuperar, incluso si quieren cooperar.

Cuando pagas por adelantado, tampoco puedes recuperarlo. Los consumidores parecen sentirse cómodos con eso. No es peor que eso.

Cualquiera de las partes siempre tiene la opción de liberar al otro.

> Cita de: nelisky, 10 de agosto 2010, 08:20:36 PM
>
> Pero la solución de la quema de dinero, si bien es excelente para

> prevenir el fraude y económicamente viable, no hace nada para evitar la venganza y, en realidad, hace que todos pierdan si una parte es deshonesta. Ciertamente no apoyaría eso.

Entonces también debe estar en contra del sistema común de pago por adelantado, donde el cliente pierde.

Pago por adelantado: el cliente pierde y el ladrón recibe el dinero. Custodia simple: el cliente pierde, pero el ladrón tampoco recibe el dinero.

¿Están diciendo que el pago por adelantado es mejor, porque al menos el ladrón recibe el dinero, por lo que al menos alguien lo consigue?

Imagine que alguien le roba algo. No puede recuperarlo, pero si pudiera, si tuvieras un interruptor remoto con el que pudiera apagarlo, ¿lo haría? ¿Sería bueno que los ladrones supieran de todo lo que tiene, lleva un interruptor de apagado, que si lo roban, será inútil para ellos, aunque usted también lo pierda? Si lo devuelven, puede volver a activarlo.

Imagínese si el oro se convirtiera en plomo cuando es robado. Si el ladrón lo devuelve, vuelve a ser oro.

Todavía me parece que el problema puede ser presentado de una manera correcta. Por otro lado, no sea tan contundente sobre la "quema de dinero" a los efectos de la discusión sobre teoría de juegos. El dinero nunca se quema realmente. Se tiene la opción de liberarlo en cualquier momento y siempre.

Re: Custodia

Publicado por ribuck, 11 de agosto 2010, 11:13:12 AM

> Cita de: Inedible, 11 de agosto 2010, 01:52:53 AM
>
> . . . Es una lástima que no se pueda hacer nada para mitigar las intenciones maliciosas de los que ofrecen vender algo, sólo "quemar"

el pago y nunca enviar los bienes (suponiendo siquiera que existan).

Esto sería un caso de despecho, una amenaza muy real.

Por ejemplo:

- A ofrece vender un ordenador portátil
- B ofrece comprar y deposita 2000 bitcoins
- A confirma que el artículo se envió, pero nunca lo envía
- B nunca lo recibe así que nunca libera los bitcoins
- A no le importa porque su intención era hacer que B "gaste" sus bitcoins sin recompensa

---

Qué tal esto:

- A ofrece vender un ordenador portátil por 2000 bitcoins y pone 2500 bitcoins como garantía
- B quiere comprar y pone en custodia 2500 bitcoins
- A confirma que el artículo se envía pero nunca lo envía
- B nunca lo recibe así que nunca libera los bitcoins
- A ahora sí le importa porque tiene 2500 bitcoins en custodia como seguridad

En este caso, a A le interesa enviar el ordenador portátil, de lo contrario, pierde su depósito de 2500 BTC. También le conviene a B confirmar la recepción de la computadora portátil, de lo contrario, pierde su "exceso" de 500 BTC que depositó.

Las situaciones incómodas se presentarán tanto si A como B son honestos, pero un servicio de entrega no asegurado pierde o rompe la computadora portátil, o si uno de los participantes muere antes de liberar el depósito de garantía.

Y otro hilo surgió más tarde:

Cómo Hacer un Servicio de Depósito Distribuido Bitcoin

Publicado por harding, 26 de septiembre 2010, 01:16:18 AM

Resumen: Dando a BitCoin un depósito en garantía descentralizado le daría una ventaja sobre todos los demás medios de intercambio, lo que podría aumentar su tasa de adopción. Más detalles a continuación.

Para una moneda *descentralizada,* los depósitos *centralizados* se ven como la norma para BitCoin en la actualidad. Un ejemplo:

Alice quiere comprar $ 5 USD de BitCoins de Bob, pero ni Alice ni Bob confían plenamente en el otro, por lo que van a un sitio en el que ambos confían, como Mt. Gox. Ellos depositan sus respectivos dineros allí, y Mt. Gox hace el intercambio por ellos.

Sin ofender a Mt. Gox (un sitio que me gusta), pero ¿podemos prescindir de su servicio de custodia?

Una alternativa casi distribuida:

Charlie, un tercero de confianza, genera una clave privada de Bitcoin.

Luego, Charlie usa el comando Unix "split" para dividir la clave privada a la mitad, dando la mitad a Alice y la mitad a Bob.

Bob deposita 5 dólares de Bitcoins en la cuenta con la clave privada dividida de Bitcoin;

Alice verifica la transacción usando la cadena de bloques públicos;

Alice envía 5 USD a Bob por PayPal;

Bob verifica la transacción de PayPal;

Bob envía a Alice su mitad de la clave privada dividida para que Alice pueda acceder a los BitCoins que depositó anteriormente.

(Para simplificar, omito la parte de los detalles de PayPal, como quién paga la tarifa de transacción y cuánto tiempo debe esperar para evitar el reembolso de fraude. También omito cualquier incentivo para que

Bob realice el último paso).

Se pueden hacer ejemplos más avanzados casi distribuidos si sustituimos con algo más sofisticado para el comando Unix “split”. Por ejemplo: una implementación de esquema de intercambio secreto de Shamir como “ssss” [1]. Una utilidad como “ssss” permite a Alice y Bob designar un árbitro en caso de que se pongan en desacuerdo.

El problema con todo esto, por supuesto, es que debemos confiar en que Charlie no abuse de la copia completa de la clave privada que se crea.

La solución ideal sería que Alice y Bob generen la mitad de la clave privada por su cuenta. No entiendo completamente las matemáticas utilizadas en los pares de claves modernas, pero dudo que esto sea posible con el algoritmo actual.

¿Hay alguna forma alternativa para que Alice y Bob adquieran la mitad de una clave privada sin dar la clave completa a ninguna de las partes?

-Dave

[1] Ver: http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing

Re: Cómo Hacer un Servicio de Depósito Distribuido Bitcoin

Publicado por satoshi, 26 de septiembre 2010, 05:34:26 PM

Aún no está implementado, pero la red puede admitir una transacción que requiera de dos firmas. Se describe aquí: http://bitcointalk.org/index.php?topic=750.0

Es absolutamente más seguro que un pago directo sin depósito en garantía, pero no tan bueno como un depósito en garantía arbitrado por un ser humano, suponiendo que usted confíe lo suficiente en el humano.

En este tipo de depósito, un tramposo no puede ganar, pero aún es posible que usted pierda. Al menos le quita el afán de lucro por engañarlo. El vendedor está seguro de que el dinero está reservado para

él, mientras que el comprador conserva la palanca de que el vendedor no ha sido pagado hasta que se complete la transacción.

55

La Minería de Bitcoin Como un Desperdicio de Recursos

Traducción por **Adrián Bernabéu Escudero**

EL ARGUMENTO de que la minería bitcoin es un desperdicio de recursos a menudo ha sido utilizado en los medios. Si Satoshi no fuera anónimo y aún estuviera involucrado, sus entrevistas inevitablemente incluirían esta pregunta. Por lo tanto, ver la respuesta que probablemente daría, recogida en estos mensajes, resulta esclarecedor.

Acuñar bitcoin es termodinámicamente perverso

Publicado por gridecon, 06 de agosto 2010, 01:52:00 PM

Permítanme comenzar diciendo que Bitcoin es un proyecto increíble y estoy muy impresionado con la implementación y los objetivos. Al leer estos foros, parece entenderse que el debate sobre el diseño y el funcionamiento de la economía bitcoin y finalmente sirve para fortalecerlo, por lo que espero que estos comentarios se tomen con ese espíritu. *EDITAR - Más investigaciones y discusiones me han convencido de que Bitcoin es realmente altamente eficiente en comparación con la mayoría de las monedas tradicionales, porque la infraestructura requerida para respaldar una moneda fiduciaria emitida por el

gobierno representa una inversión de recursos mucho mayor que el consumo de energía de la CPU de Bitcoin. Sin embargo, estoy dejando este hilo activo porque ha estado generando muchas discusiones interesantes.*

Creo que la cantidad de energía requerida para la economía de Bitcoin representa un serio obstáculo para su crecimiento. A largo plazo, las transacciones pueden ser incluso más serias que las acuñaciones en este sentido, pero por el momento hablaré sobre la acuñación porque está delimitada y definida más precisamente. La idea de que el valor de bitcoins está de alguna manera relacionado con el valor de la electricidad requerida, en promedio, para acuñar un bloque ganador es generalmente aceptada, pero la naturaleza precisa de esta relación es polémica.

Un argumento es que cualquiera que elija generar monedas está realmente optando por comprar bitcoins con electricidad/recursos computacionales, y que debido a que algunas/muchas personas están haciendo esa elección, los bitcoins tienen al menos ese "valor" para los generadores, de quien se puede suponer que maximizan su utilidad. Un argumento enfrentado es que el costo de producción es diferente al valor de mercado, y la medida más objetiva es el precio actual de conversión del mercado a una moneda más líquida y ampliamente negociada, como el dólar estadounidense.

Mi opinión es que estos dos argumentos pasan por alto el punto y el problema real, que es la perversidad fundamental de desperdiciar grandes cantidades de energía y cálculos en la generación de los bloques ganadores para el proceso de acuñación. El proceso de acuñación existe debido a la necesidad de "imprimir" realmente la moneda, y ciertas propiedades deseables de cripto-matemática para hacer predecible el comportamiento de la moneda. El hecho de que el proceso de acuñación actual requiere un gran impulso de energía de trabajo computacional es altamente desafortunado y tiene la consecuencia perversa de que bitcoin puede estar "destruyendo riqueza", en el sentido de desperdiciar energía produciendo un objeto digital que vale menos que los recursos invertidos en él.

Como se señala a menudo, una moneda no necesariamente tiene, o necesita tener, algún valor inherente; un medio de intercambio es una herramienta útil y puede tener valor puramente como consecuencia de

una convención social. El costo de producción de bitcoins en el consumo de electricidad representa un desperdicio, una "carga termodinámica" que la moneda tiene que soportar. Considere una moneda digital hipotéticamente alternativa llamada "compucoin", que compra ciclos de CPU desde nodos en la red. El valor de mercado de esta moneda convergerá muy de cerca con el costo de la electricidad requerida para generar ciclos de CPU. En lugar de calcular el costo de los ciclos de la CPU, las monedas podrían intercambiarse por el valor de los ciclos de la CPU, esto crearía una base racional para el valor de la divisa y la integraría con un mercado existente. Imagino que las alternativas a Bitcoin (muchas de ellas probablemente compartiendo una gran cantidad de código fuente de Bitcoin), inevitablemente surgirán porque el actual proceso de acuñación de Bitcoin hace que la moneda sea "cara" en términos de requerimiento de energía. Creo que esto lo coloca en una desventaja competitiva frente a otras monedas y solo puede obstaculizar su adopción generalizada y su valor a largo plazo. * Editar: como se mencionó anteriormente, ahora soy mucho más optimista sobre Bitcoin a largo plazo. ¡Sin embargo, todavía creo que los compucoins serán una buena idea!

Re: Acuñar bitcoin es termodinámicamente Perverso

Publicado por satoshi, 07 de agosto 2010, 05:46:09 PM

Es la misma situación del oro y la extracción de oro. El costo marginal de la extracción de oro tiende a mantenerse cerca del precio del oro. La extracción de oro es un desperdicio, pero ese desperdicio es mucho menor que la utilidad de tener oro disponible como medio de intercambio.

Creo que el caso será el mismo para Bitcoin. La utilidad de los intercambios posibilitados por Bitcoin superará con creces el costo de la electricidad utilizada. Por lo tanto, no tener Bitcoin sería el desperdicio neto.

> Cita de: gridecon, 06 de agosto 2010, 04:48:00 PM
>
> Como punto general, tampoco estoy de acuerdo con la idea de que la gran carga computacional para la generación de monedas es, de hecho, una necesidad del sistema actual. Según entiendo, la creación de divisas se mide fundamentalmente por TIEMPO, y si esa es la variable de control fundamental, ¿cuál es la necesidad de que todos "tiren tantos dados como sea posible" dentro de ese período de tiempo dado? La "cadena de pruebas" para la posesión de monedas y las transacciones no depende del método para generar monedas.

La influencia de cada nodo en la red es proporcional a su potencia de CPU. La única forma de mostrarle a la red la cantidad de energía de la CPU que tienes es usándola realmente.

Si hay algo más que cada persona tiene en una cantidad finita con lo que podríamos contar para una-persona-un-voto, no puedo pensar en nada similar. Direcciones IP ... es mucho más fácil de obtener muchos de ellos que las CPU.

Supongo que sería posible medir la potencia de la CPU en ciertos momentos. Por ejemplo, si el desafío de potencia de la CPU fuera sólo ejecutarse para un promedio de 1 minuto cada 10 minutos. Todavía podría demostrar su poder total en momentos determinados sin ejecutarlo todo el tiempo. Aunque no estoy seguro de cómo podría ser implementado. No hay forma de que un nodo que no estaba presente en ese momento sepa que una cadena anterior se generó realmente en un ciclo de trabajo con descansos de 9 minutos, no de forma consecutiva.

La prueba de trabajo tiene la buena propiedad de que puede transmitirse a través de intermediarios que no son de confianza. No tenemos que preocuparnos por una cadena de custodia de comunicación. No importa quién te diga que cadena es la más larga, la prueba de trabajo habla por sí misma.

Re: Acuñar bitcoin es termodinámicamente perverso

Publicado por satoshi, 09 de agosto 2010, 09:28:39 PM

El calor de su computadora no se desperdicia si necesita calentar su hogar. Si usa calor eléctrico en el lugar donde vive, entonces el calor de su computadora no es un desperdicio. Es igual coste si genera calor con su computadora.

Si tiene otra calefacción más barata que la eléctrica, entonces el desperdicio es solo la diferencia en el coste.

Si es verano y estás usando aire acondicionado, entonces es el doble.

La generación de Bitcoin debería estar donde sea más barato. Tal vez sea en climas fríos donde haya calor eléctrico, donde sería esencialmente gratis.

Re: Acuñar bitcoin es termodinámicamente perverso

Publicado por throughput, 10 de agosto 2010, 12:27:30 PM

Creo que la discusión finalmente ha perdido los aspectos éticos de motivar a los creadores de botnets para que inviertan aún más recursos en su negocio en caso de que los BTC generados proporcionen el valor, comparable con los usos actuales de botnets.

¿Qué pasa si la operación de Bitcoin supera a las demás actividades? ¿Cómo se puede imaginar que el proceso de construcción de botnets se realice de una manera que, beneficie a la comunidad?

Cita de: jgarzik, 06 de agosto 2010, 07:53:25 PM

La participación en la red como un nodo honesto ayuda a todos.

> Sí, pero solo cuando no va en contra de la voluntad del propietario de la computadora, él paga la factura de la electricidad.
>
> Si es así, entonces pierde dinero REAL por un consumo de energía extra causado por una carga de CPU del 100%.
>
> Entonces, Bitcoin motiva el comportamiento de robar poder de cómputo en los ordenadores de propietarios inocentes.
>
> Bueno, ahora puede intentar comparar el daño social con los beneficios, pero ¿realmente siente que tiene el derecho moral de hacerlo?

RE: ACUÑAR BITCOIN ES TERMODINÁMICAMENTE PERVERSO

Publicado por Gavin Andresen, 10 de agosto 2010, 09:26:14 PM

> Cita de: throughput, 10 de agosto 2010, 12:27:30 PM
>
> Entonces, Bitcoin motiva el comportamiento de robar poder de cómputo en los ordenadores de propietarios inocentes.

Claro, exactamente de la misma forma que la existencia de tarjetas de crédito motiva la conducta de robar números de tarjetas de crédito de usuarios inocentes que tienen tarjetas de crédito.

O la existencia de cuentas bancarias motiva a los piratas informáticos a intentar entrar en su sistema para averiguar su número de cuenta bancaria.

O la existencia de automóviles motiva a algunas personas a robar gasolina de propietarios inocentes de estaciones de servicio.

Creo que los beneficios de Bitcoin superarán el daño, y además creo que **soy** capaz de hacer ese juicio moral. Podría estar equivocado, y podría lamentar haberme involucrado alguna vez, pero si sólo hiciera algo que

estuviera 100% seguro de que iba a funcionar lo mejor posible, nunca lograría algo nuevo e interesante.

56

Sobre un Tipo Alternativo de Cadena de Bloques con Sólo Registros Hash

Traducción por
Enrique Palacios Rojo | Adrián Bernabéu Escudero
Beatriz Lizarraga | Alex Viñas Salles

AQUÍ, se discute una sugerencia que Satoshi consideró interesante. Esta sugerencia se basa en dar menos información en la cadena de bloques, con la intención de proporcionar un mayor nivel de privacidad.

No es una sugerencia

Editado por Red, 10 de agosto 2010, 05:45:45 AM

Como algunos habrán notado, una de las cosas que me molesta de Bitcoin es que todo el historial de transacciones es completamente público. Entiendo totalmente los beneficios de cómo esto simplifica las cosas y hace que sea fácil para todos probar que las monedas son válidas.

Esto no es una sugerencia para un cambio en bitcoin. Más bien es una pregunta sobre qué podría ser posible y qué no podría ser posible.

La pregunta a grandes rasgos es, si la lista de registros en el bloque que ¿Podría haberse implementado de una manera que no almacenará las

transacciones completas? Específicamente, *quizás* sería posible almacenar sólo los hashes de los puntos de entrada y salida en la lista del bloque. Estos estarían con un sellado del tiempo (certificado) en la lista de registros del bloque exactamente como se está haciendo ahora.

La principal diferencia es que sería responsabilidad del receptor de la moneda almacenar la transacción completa. Y quizás tenga que almacenar las transacciones previas (X) en profundidad para mostrar la trazabilidad.

Entonces, cuando este último quiera transferir las monedas al siguiente receptor, crearía una transacción exactamente como se hace ahora, excepto que tendría que incluir los antecedentes en la transacción para su validación también. Para la validación, cada antecedente de los puntos de entrada se les aplicará el hash y validará como que existen en la lista del bloque. Los puntos de entrada serían hasheados e identificados en la lista del bloque como que aún no se han gastado. Entonces la transacción sería validada como se hace actualmente.

Si todo está validado correctamente, los hashes adicionales de entrada/salida se agregaran al bloque. Esto cierra los puntos de entrada de la transacción, y marca los nuevos hashes de los puntos de salida como no gastados.

Una vez que un nodo complete el bloque (ganando el concurso de hash), luego transmite el bloque de hashes y las transacciones relacionadas + antecedentes a los otros nodos para su confirmación y aceptación.

un ejemplo aproximado sería:

{block-9

hash-a, hash-b, hash-c, hash-x

}

{block-12

hash-a, hash-y, hash-c, hash-d

}

{block-17

hash-b, hash-d, hash-e, hash-z, hash-f

}

{Transaction

{in-points: hash-x, hash-y, hash-z}

{address, signature and other transactions stuff}

{out-points: hash-payed, hash-change

}

{generating-block

hash-x, hash-y, hash-z, hash-payed, hash-change

}

Entonces, básicamente, si el hash del punto de entrada/salida existe dos veces en la lista del bloque, se ha gastado. Si existe solo una vez es que no se ha gastado.

Así pues, después del bloque-17:

a, b, c & d se han gastado

e, f, x, y, z no se han gastado

La transacción gasta x, y & z, y crea el hash-pagado & hash-cambio, por lo que la transacción es válida.

Una vez generado el bloque:

a, b, c, d, x, y, & z se han gastado

e, f, pagados, cambio no se han gastado

====

El Objetivo:

El objetivo es proporcionar la misma seguridad del sistema existente, pero evitando crear un gráfico público de cada transacción que se correlaciona fácilmente. En este caso, los hashes ni siquiera tienen que asociarse en el bloque. El bloque podría simplemente ordenar todos los hashes en orden ascendente.

En efecto, quiero crear monedas de oro de verdad. Puedo darte mis monedas, pero ninguna persona en el mundo no sabría que yo te las transferí. Puedes dárselos a la siguiente persona y demostrar que son monedas de oro, porque tienes el pedigrí de las monedas Y cada generación en el árbol genealógico fue certificada ante notario en el registro público.

====

La Pregunta:

Satoshi demostró que se puede eliminar transacciones de la lista del bloque a través de la estructura de árbol de Merkle, sin comprometer la seguridad. Creo que mi verdadera pregunta es:

"¿Qué es lo primero que se puede eliminar en las transacciones?"

Se podría argumentar que los nodos podrían recordar todo de todas maneras (la web nunca olvida). Pero si se estructuró el protocolo para que los nuevos nodos solo reciban una lista de hash del bloque, sólo podrían recordar desde ese momento en adelante. Eso le daría un poco de privacidad adicional. (Tal vez)

====

¿Algún comentario? ¿Hay alguna manera obvia de que la gente pueda engañar y hacerse rica?

Re: No es una sugerencia

Anunciado por Insti, 10 de agosto 2010, 09:34:14 AM

En tu sistema, en lugar de sólo obtener transacciones de la cadena de bloques, solo tengo que mirar cada transacción (que veré de todos modos) y registrarlas en mi servidor secreto.

Solo defiendes la seguridad a través de la oscuridad.

Re: No es una sugerencia

Anunciado por Red, 10 de agosto 2010, 02:09:36 PM

> Comentado por: Insti, 10 agosto 2010, 09:34:14 AM
>
> Solo defiendes la seguridad a través de la oscuridad.
>
> ---

Ya mencioné eso. No contaría con esto para la seguridad monetaria. Me gustaría que el sistema sea equivalente al actual.

Sin embargo, se sabe que la oscuridad de la privacidad agrega valor. Tus vecinos, o el FBI podrían ver todo lo que haces todo el día. Pero probablemente no lo hagan. Si te vuelves "de interés", seguro que podrían comenzar a vigilarte desde ese momento en adelante

Pero parece que lo que más se pide por parte de las instituciones legales es "¡déjenme examinar los registros de todos!" (Llamadas telefónicas, antenas telefónicas, conexiones de correo electrónico, conexiones de Facebook, transacciones de tarjetas de crédito/débito, historial de Google, historial del navegador). Los otros sistemas son "seguridad a través de autoridad". Bitcoin no tiene eso

Por cierto, preferiría no transmitir cada transacción a cada nodo. Pero eso es para otra conversación.

Por cierto, esta es la forma en que funcionan la mayoría de los

servicios de notaría digital. Se les envía un hash de un documento firmado y lo registran de permanentemente. Luego crean una cadena hash como lo hace Bitcoin. Publican periódicamente el valor actual de la cadena hash en un periódico u otro medio redundante sin conexión.

No hay que enviar los documentos privados/transacción al notario para que los registre y certifique. El notario solo está certificando que algo que coincide con este hash existía ya en ese punto en el tiempo.

Re: No es una sugerencia

Anunciado por Insti, 10 de agosto 2010, 03:06:16 PM

> Comentado por Red, 10 de agosto 2010, 02:22:09 PM
>
> Por cierto, esta es la forma en que funcionan la mayoría de los servicios de notaría digital. Se les envía un hash de un documento firmado y lo registran de permanentemente. Luego crean una cadena hash como lo hace Bitcoin. Publican periódicamente el valor actual de la cadena hash en un periódico u otro medio redundante sin conexión.
>
> No hay que enviar los documentos privados/transacción al notario para que los registre y certifique. El notario solo está certificando que algo que coincide con este hash existía ya en ese punto en el tiempo.
>
> ---

Tampoco tienes que demostrar al notario que tienes X BTC en tu cuenta para gastar.

Aunque recientemente estuve leyendo sobre pruebas de conocimiento cero (http://en.wikipedia.org/wiki/Zero-knowledge_proof) si pudieras usar algo así para demostrar que tu cuenta tenía X BTC sin revelar nada más, podría ser lo que estás buscando.

Me preocupa que lo que quieres sea teóricamente imposible.

Re: No es una sugerencia

Publicado por Red, 10 de agosto 2010, 05:29:44 PM

> Comentado por Insti, 10 de agosto 2010, 03:06:16 PM
>
> Aunque recientemente estuve leyendo sobre pruebas de conocimiento cero (http://en.wikipedia.org/wiki/Zero-knowledge_proof)

¡Interesante idea para volver sobre ella! Gracias. No había pensado en esto.

Re: No es una sugerencia

Publicado por Satoshi Nakamoto, 11 de agosto 2010, 12:14:22 AM

Este es un tema muy interesante. Si una solución fuera encontrada, una mucho mejor, más fácil, más conveniente implementación de Bitcoin podría ser posible.

Originalmente, una moneda puede ser solo una cadena de firmas. Con un servicio de sellado de tiempo, las firmas antiguas podrían localizarse finalmente antes de que se las pierda el rastro desde el origen o que las monedas se mantengan individualmente o en su denominación de valor. Es la necesidad de verificar la ausencia de doble gasto que requiere un conocimiento global de todas las transacciones.

El desafío de esto es, ¿cómo se demuestra que no existen otros gastos? Un nodo debe conocer todas las transacciones para poder verificarlo. Si solo conoce el hash de los puntos de entrada/salida, no puede verificar las firmas para ver si un punto de salida se ha gastado previamente. ¿Has reparado en ello?

Es difícil pensar en cómo aplicar pruebas de cero conocimientos en este caso.

Estamos tratando de demostrar la ausencia de algo, lo que parece requerir conocerlo todo y verificar que ese algo no esté incluido.

Re: No es una sugerencia

Publicado por Red, 11 de agosto de 2010, 04:58:50 AM

Satoshi: Sé que sabes la primera parte de lo que estoy escribiendo, pero quiero que otros puedan seguir y corregir cualquier concepto erróneo que pueda tener.

Estaba viendo la implementación actual del árbol Merkle tratando de descubrir cuándo se podrían eliminar las transacciones sin perder seguridad.

En términos de gráfico de transacción, las transacciones representan los nodos. Los bordes del gráfico de transacción están representados por los puntos de entrada que apuntan a transacciones previas usando una clase de estructura BlockHash->TransHash->OutPoint. Es la existencia de un punto de entrada que marca un punto de salida anterior gastado.

Por lo tanto, para que una transacción sea válida, lo más que se muestra por cada punto ingreso de una transacción de AMBOS, un punto de salida anterior existente Y, que no exista un punto de ingreso previo que haga referencia a ese punto de salida. Por lo tanto, para cada punto de salida, hay cero o uno puntos de ingreso haciendo referencia hacia él. cero = no gastado. uno = gastado.

Eso también significa que no se puede eliminar ninguna transacción de la lista de bloqueo, hasta que ambos puntos de salida sean gastados. De lo contrario, las monedas desaparecerán.

Sin embargo, puede eliminar todas las transacciones de doble enlace tan pronto como esté seguro de que el segundo bloque de enlace se mantendrá. (posibilidad más temprana).

Sin embargo, a medida que elimina transacciones y las reemplaza con su hash del árbol de Merkle, pierde la estructura de gráfico presente

> en la lista de bloque. En efecto, todas las transacciones recuperadas de la lista de bloque tienen un valor no utilizado, simplemente porque aún existen. Ya no pueden demostrar su validez por ascendencia ya que esa parte del gráfico fue eliminada.
>
> Lo que me hizo pensar, ¿hay alguna forma de probar la validez si nunca se ponen todas las transacciones en el gráfico para empezar?

Cita de: satoshi, 11 de agosto de 2010, 12:14:22 AM

El desafío es, ¿cómo se demuestra que no existen otros gastos? Parece que un nodo debe conocer todas las transacciones para poder verificarlo. Si solo conoce el hash de los puntos de entrada/salida, no puede verificar las firmas para ver si un punto de salida había sido gastado antes. ¿Tienes alguna idea sobre esto?

> La clave es codificar la información de transacción como parte del hash de punto de salida. Por lo tanto, en lugar de crear un hash de transacción único, representa la transacción como dos hashes de salida. (Originalmente consideré una estructura como un *punto de entrada/transacción/punto de salida*, usando hashes, pero resultó ser innecesario).
>
> Solo los validadores de transacciones necesitan conocer la dirección de bitcoin asociada con un hash de punto de salida grabado. Eso proviene de la transacción antecedente presentada para un punto de ingreso de la transacción actual. La transacción antecedente y el punto de salida son hasheados y se presumen AMBOS válidos y no gastados si ese hash aparece una, y sólo una vez en la lista de bloque.
>
> La transacción actual debe estar firmada por la clave de la dirección en las transacciones antecedentes, por supuesto. Si esto resulta válido, se generarán dos nuevos hashes de salida y se insertarán en el bloque actual. Los hashes del punto de ingreso se marcan gastados para incluirlos también en el bloque actual. (Si existe un hash dos veces, se gasta.) Si desea representar la transacción como una unidad (y el gráfico de transacción actualmente visible), los hashes del punto de ingreso y los del punto de salida podrían agruparse. Sin embargo, esto no es estrictamente necesario para probar la validez.

Cita de: satoshi, 11 de agosto 2010, 12:14:22 AM

Estamos tratando de demostrar la ausencia de algo, lo que parece requerir conocerlo todo y verificar que algo no esté incluido.

En este caso, estamos tratando de probar la existencia de UN hash coincidente y la ausencia de DOS hashes coincidentes. Requiere conocerlos a todos para probarlo.

Creo que las prohibiciones contra el doble gasto son tan fuertes como en la versión actual.

==== ¡PRECAUCIÓN! ====

Sin embargo, debe considerar el caso en el que un nodo causa daños al agregar deliberadamente "hashes de cancelación" aleatorios. En este caso, el nodo no podría obtener acceso a las monedas, ya que no tiene hashing de transacción firmada a un hash de punto de salida no gastado como válido. Sin embargo, el propietario actual tampoco podría gastar las monedas. El punto de ingreso se daría ya por gastado.

Eso significa que las condiciones de validación son EXACTAMENTE LAS MISMAS que con la implementación actual. Todos los nodos de validación deben examinar y validar todas las transacciones representadas en un bloque antes de aceptarlo y desarrollarlo.

Si existen hashes en el bloque propuesto que no están representados por transacciones válidas, el bloque debe ser rechazado. Eso es exactamente lo mismo que el sistema actual, si alguna transacción no es válida, el bloque debe ser rechazado.

Tenía la esperanza de que la condición para pasar todas las transacciones a todos los validadores podría debilitarse, pero no consigo ver cómo (todavía) sin depender de la delegación de confianza.

Una característica interesante es que esto simplifica el proceso de validación. Todo lo que se necesita hacer es analizar la lista de bloqueo (de hashes) una vez. Como cada hash es analizado simplemente lo

> busca en un hash-set. Si no existe, añádelo. Si existe, lo borras. Cuando haya terminado de analizar la lista de bloques, tendrá el conjunto mínimo de puntos de salida válidos y no gastados. Incluso podría ser capaz de mantener todo el conjunto en la memoria. (¡Al menos un momento!)

Cita de: satoshi, 11 de agosto 2010, 12:14:22 a.m.

Es difícil pensar en cómo aplicar pruebas de cero conocimientos en este caso.

> ¡También es difícil para mí! :-) ¡Aunque fue interesante volver a leerlo!
>
> Esperaba que generara una idea de cómo los nodos pueden demostrar que "siempre siguen" las reglas generadoras de bloques, en ausencia de que todos necesiten tener el conjunto de todas las transacciones para verificar.
>
> No fue así. :-)

RE: NO ES UNA SUGERENCIA

Publicado por satoshi, 11 de agosto 2010, 09:07:59 PM

Todavía pensando en esta idea. . .

El único trabajo que la red necesita hacer es decir si un gasto de un punto de salida es el primero o no.

Si estamos dispuestos a que los clientes mantengan el historial por su propio dinero, es posible que la red no tenga que almacenar parte de la información, como, por ejemplo:

- el valor
- la asociación de puntos de entrada y salida en una transacción

La red rastrearía un grupo de puntos de salida independientes. Sin saber a qué transacciones o cantidades pertenecen. Un cliente puede averiguar si un punto de salida se ha gastado y puede enviar un punto de entrada satisfactorio para marcarlo. La red mantiene el punto de salida y el primer punto de entrada válido que lo demuestra. El punto de ingreso firma un hash de su próximo punto de salida asociado y un condimento, por lo que se puede mostrar de forma privada que la firma está firmada por el próximo punto de salida si conoces el condimento, pero públicamente la red no sabe cuál es el próximo punto de salida.

Creo que los clientes tendrían que mantener una copia de toda la historia de las monedas originales generadas. Alguien que envíe un pago tendría que enviar datos al destinatario, además de comunicarse con la red para marcar los puntos gastados y verificar que el gasto sea el primer gasto. Tal vez la transferencia de datos podría hacerse como un adjunto de correo electrónico.

El hecho de que los clientes tengan que mantener todo el historial reduce el beneficio de la privacidad. Alguien que maneja mucho dinero podría ver mucho historial de transacciones. La forma en que se expande retrospectivamente podría terminar viendo la mayoría de la historia. Las denominaciones podrían ser granulares para limitar la dispersión, pero una empresa que maneje mucho dinero podría terminar viendo gran parte de la historia.

Re: No es una sugerencia

Publicado por Red, 12 de agosto 2010, 01:10:19 AM

> Cita de: satoshi, 11 de agosto de 2010, 09:07:59 PM.
>
> Todavía pensando en esta idea …

Es una idea un poco retorcida, ¿no? :-)

Resulta que la noción de una notarización cancelable se generaliza muy bien.

Por ejemplo, este sistema no está limitado a las transacciones de bitcoin. Dado que los contratos firmados se mantienen de forma externa, con reglas adicionales de validación/notarización, puede implementar fácilmente cosas como pagarés/cheques de reclamos.

Si alguien te dio 5$, podrías darle 5$ que te debo. Su hash de lo que le debo sería autenticado en la lista de bloques (con hashes). Cuando le devuelva el dinero, puede pedirles que firmen el pagaré para su confirmación. Luego haga que el notario inserte una cancelación del hash de deuda. Entonces, nadie podría mostrar una copia de seguridad con una copia del pago de la deuda y exigir un pago doble.

> Cita de: satoshi, 11 de agosto de 2010, 09:07:59 PM
>
> ---
>
> Creo que los clientes tendrían que mantener una copia de toda la historia de las monedas originales generadas. El hecho de que los clientes tengan que mantener todo el historial reduce el beneficio de la privacidad.
>
> ---

Yo también pensé esto al principio. Pero luego me convencí de lo contrario.

Es realmente una cuestión de cuánta confianza deposita en los verificadores y en el proceso de verificación. A la gente le gusta la sensación de que tener todas las transacciones disponibles, les permite rastrear las raíces de su dinero hasta su creación. Sin embargo, eso no es necesario.

Si tiene confianza en el proceso que validó las transacciones durante la creación del bloque (> 50% de acuerdo de CPU). Y si está seguro de que los bloques previos no pueden ser cambiados (tú lo compruebas esto). Entonces solo necesita verificar que los puntos de salida relacionados no hayan sido gastados. Las características de seguridad permanecen en la lista de bloqueo y el procedimiento, incluso si las transacciones se almacenan externamente y los anteriores no se almacenan en absoluto. Mostraste esto demostrando que las transacciones antiguas se pueden eliminar utilizando el árbol de Merkle para mantener la coherencia.

> Cita de: satoshi, 11 de agosto de 2010, 09:07:59 PM
>
> Alguien que maneja mucho dinero podría ver mucho historial de transacciones. La forma en que se expande retrospectivamente podría terminar viendo la mayoría de la historia. Las denominaciones podrían ser granulares para limitar la dispersión, pero una empresa que maneje mucho dinero podría terminar viendo gran parte de la historia.
>
> Es cierto que la privacidad está directamente relacionada con visibilidad. Si hay un punto central como una casa de cambios, puede relacionar muchos puntos de salida. Pero si nos alejamos de la noción de que cada moneda debe remontarse a la creación, los horizontes de observación estarán mucho más cerca.
>
> ___
>
> Es realmente extraño acostumbrarse a la idea de que esta moneda es válida simplemente porque el proceso no permite que se incluya de otra manera. Pero en realidad, así es exactamente cómo funciona la generación de bitcoins. La transacción no tiene entradas, pero todos deciden que el punto de salida debe ser válido sólo porque de lo contrario, no estaría en el bloque. :-)

RE: NO ES UNA SUGERENCIA

Publicado por satoshi, 12 de agosto 2010, 02:46:56 AM

> Cita de: Red, 12 de agosto 2010, 01:10:19 AM
>
> > Cita de: satoshi, 11 de agosto 2010, 09:07:59 PM
> >
> > Creo que los clientes tendrían que mantener toda la historia original de las monedas generadas. El hecho de que los clientes tengan que mantener todo el historial reduce el beneficio de privacidad.

> Yo también pensé esto al principio. Pero luego me convencí de lo contrario.
>
> ---

¿Vuelves a hablar sobre el sistema Bitcoin aquí existente?

Hablaba sobre el sistema hipotético que estaba describiendo, si la red no conoce los valores y el origen de las transacciones, entonces no puede verificarlas y responder por ellas, por lo que los clientes tendrían que mantener todo el histórico.

Si un cliente no estuvo presente hasta hace poco, las dos formas de convencerlo de que una transacción tiene un pasado válido es:

1) Mostrándole el histórico completo de la moneda original generada.

2) Mostrándole el histórico completo de un bloque extremadamente profundo, entonces confiará en que, si tantos nodos dicen que el histórico hasta ese momento era correcto, entonces debe ser cierto.

Pero si la red no conocía todos los valores y el origen de las transacciones, no podría hacer la 2), no lo creo.

Re: No es una sugerencia

Publicado por Red, 12 de agosto 2010, 04:25:51 AM

> Cita de: satoshi, 12 de agosto 2010, 02:46:56 AM
>
> ---
>
> > Cita de: Red, 12 de agosto 2010, 01:10:19 AM
> >
> > Yo también pensé esto al principio. Pero luego me convencí de lo contrario.
> >
> > ---
>
> ¿Vuelves a hablar sobre el sistema Bitcoin aquí existente?
>
> ---

Sí, estoy hablando del sistema hipotético.

La forma en que propuse el sistema, cada vez que se genera un bloque, cada nodo de validación debe aceptar o rechazar ese bloque al validar las transacciones y confirmar los valores hash en el bloque. En efecto, el mismo trabajo que se está haciendo con el sistema actual más los controles de hash de punto de salida. Como los otros validadores ya estaban compitiendo para generar el bloque, ya tienen (al menos la mayoría) las transacciones.

Al igual que con el sistema actual, si las transacciones no se validan (más los hashes de punto de salida incluidos) los otros nodos rechazarán el bloque. Si el bloque no obtiene aceptación por al menos el 50% de la potencia de la CPU, no hace la lista de bloque.

Entonces, la presencia de los hashes en la lista de bloques significa que al menos el 50% de los validadores existentes en ese momento vieron y validaron todas las transacciones y los hashes de punto de salida que contiene.

Por lo tanto (salvo en bloqueos de hashes) si alguien presenta una transacción antecedente que coincide con un punto de salida no gastado, debe ser válida.

El antecedente de ese antecedente debe haber sido válido también, de lo contrario el antecedente habría sido rechazado. Y así una y otra vez.

Para que ese no sea el caso, debes postular que hubo un período de tiempo en el que los bloques no se validaban contra los hashes del punto de salida. Pero eso es plausiblemente inverosímil con el sistema de competencia de CPU.

> Cita de: satoshi, 12 de agosto 2010, 02:46:56 AM
>
> Si un cliente no ha estado presente hasta hace poco, las dos formas de convencerlo de que una transacción tiene un pasado válido es:
>
> 1) Mostrándole el histórico completo de la moneda original generada.
>
> 2) Mostrándole el histórico completo de un bloque extremadamente profundo, entonces confiará en que, si tantos nodos dicen que el histórico hasta ese momento era correcto, entonces debe ser cierto.

Si un cliente se unió a la red recientemente, lo hizo asumiendo que los validadores anteriores siguieron las reglas y que todos los bloques preexistentes son válidos. (Nadie se uniría a una red con fama de corrupta).

Por supuesto, en el sistema actual, si las transacciones nunca se purgaron, un nuevo nodo podría validar todos los bloques anteriores para la auto-consistencia. Pero aún no podrían probar la verdad absoluta. Una red de robots podría haber tomado el relevo y borrado algunas transacciones dejando "una nueva verdad" y usuarios insatisfechos. Equivalente al caso 1) anterior.

En el sistema actual, si las transacciones se purgaron del árbol de Merkle, entonces tienes el caso 2) anterior. Los recién llegados deben confiar en el proceso. Falta algo, no tienen por qué preocuparse. Todos deben suponer que fue válido.

Lo único que digo es que, si confías en el proceso de la competencia de validación de bitcoins (¡y nosotros lo hacemos!), entonces realmente no necesitas "un 2) bloque extremadamente profundo" para ser muy profundo. Alguien dijo en otro hilo que los clientes rechazan cualquier cambio en los bloques con más de dos horas de antigüedad. Entonces podemos tener absoluta confianza en todos los bloques enterrados a 12 profundidades.

Entonces, si una transacción no se gasta y se entierra en profundidad 12, podemos purgar todos sus antepasados. Añaden paños calientes, pero ninguna validación adicional. Tenemos que confiar en ellos. Simplemente no hay forma de retroceder y cambiar el rumbo.

Después de eso, cada bloque sucesivo presupone que todos los bloques precedentes son verdaderos. De lo contrario, sería un fork y no un bloque sucesivo. Por lo tanto, para cualquier transacción validada contra puntos de salida en un bloque anterior, si esos puntos de salida existen y no se han gastado, se deben suponer válidos. Si se presume que son válidos, se debe suponer que sus antepasados son válidos, incluso si se purgan.

En el sistema propuesto, exactamente las mismas cosas son verdad.

Si un hash de un punto de salida antecedente no se gasta y está enterrado a 12 bloques de profundidad, entonces no se gasta en absoluto. Nada puede cambiar ese hecho. No tiene sentido controlar a sus antepasados. Puede finalizar la validación de la transacción, cancelar los hashes de punto de entrada y crear nuevos hashes de punto de salida.

Curiosamente, si un hash de punto de salida antecedente no se gasta y se sepulta a MENOS DE 12 bloques de profundidad, entonces está RELATIVAMENTE no utilizado. Curiosamente, todavía no tiene sentido controlar a sus antepasados. Lo único que podría cambiar la validez del antecedente es un cambio de rama a una cadena más larga. Si un antecesor de un antecedente que usted está validando esta transacción contra la que cambiada, esta transacción también se intercambiará.

Es una de esas tramas cutres de película de la máquina de tiempo. Cuando alguien retrocedió en el tiempo y desapareció a mi antepasado. ¡Ahora no existo!

=====

Así que lo que digo es que, en AMBOS sistemas (existentes y propuestos), lo único que los validadores deben hacer es validar que los puntos de salida de los antecedentes existen y que no se han utilizado (para la cadena de bloque actual). El proceso asegura que todo lo demás permanece relativamente o absolutamente válido.

El resto simplemente son paños calientes.

- PD -

Sé que esto es demasiado largo y redundante, pero estoy cansado de editar. :-)

Re: No es una sugerencia

Publicado por satoshi, 13 de agosto 2010, 07:28:47 PM

Aun no estoy comprendiendo tu idea. ¿Es que acaso se esconde alguna información de la red pública? ¿Qué ventaja tiene?

Si al menos el 50% de los nodos validan suficientes transacciones, haciendo que las transacciones viejas se descarten, entonces, todo el mundo vería todo y podría guardar una copia.

¿Podrían los nodos públicos ver el valor de las transacciones? ¿Podrían ver de qué transacción anterior procede el valor? Si pueden, entonces ellos sabrían todo. Si no pueden, no podrían verificar que el valor proviene de una fuente lícita, dado que no podrías tomar en cuenta su cadena para verificar la procedencia de esta.

¿Se esconde la dirección de bitcoin? ¿Eso es todo? OK, quizás ahora lo veo, si eso es todo.

Crypto puede ofrecer una manera de "llave ciega". He investigado un poco y, quizás haya algo ahí. Las "firmas de grupo" puede que estén relacionadas.

En el área general podemos encontrar algo: http://www.users.zetnet.co.uk/hopwood/crypto/rh/

Lo que necesitamos es una manera de generar variaciones ciegas adicionales de la clave pública. Las variaciones ciegas/obscuras tendrían que tener las mismas propiedades que la clave pública raíz, como el hecho de que la clave privada pueda generar una firma para cualquiera de las anteriores. Otros podrían no decir si una clave ciega es relacionada con la clave raíz, u otras claves ciegas provenientes de la misma clave raíz. Estas serían las propiedades del cegamiento. Ceguera, en pocas palabras, si x = (x * gran_número_entero_aleatorio) mod m.

Cuando pagas a una dirección de Bitcoin, generarías una nueva clave ciega para cada uso.

Entonces, tendrías que ser capaz de firmar con una clave de tal manera que no se pueda decir que las dos firmas provienen de la misma clave

privada. No estoy seguro si siempre, al firmar con una clave pública ciega diferente ya le daría esta propiedad. Si no, creo que un grupo de firmas podrían valer. En las firmas de grupo, es posible que algo sea firmado sin saber quién lo ha firmado.

Por ejemplo, digamos que un ataque militar sin mucha popularidad ha sido ordenado, pero nadie en la historia quiere ser recordado como la persona que lo ordenó. Si diez líderes tienen claves privadas, uno de ellos podría firmar la orden, y ninguno de estos sabría quién ha sido.

Re: No es una sugerencia

Publicado por Red, 13 de agosto 2010, 09:48:56 PM

Voy a contestar en dos partes.

> Cita de: satoshi, 13 de agosto 2010, 07:28:47 PM
>
> Aun no estoy entendiendo que quieres conseguir con tu idea.
>
> ---

Eso ha sido mi culpa, porque estaba intentando hacer demasiados casos de una tirada. Tampoco estaba intentando introducir muchas "funcionalidades" nuevas de golpe para el análisis.

Mi objetivo mental es incrementalmente restringir el horizonte de la visibilidad de una transacción. Tanto en el tiempo como en el espacio. El significado del tiempo se refiere solo a los nodos que están funcionando en un instante en particular. Espacio, que significa que menos que el conjunto de todos los nodos ejecutándose en el momento. De manera óptima, una transacción sólo sería conocida por el remitente y el receptor. De tal manera que todas las pruebas desaparecerían.

Yo te entrego un billete de 10$. Y cada uno se marcha para siempre. Mientras que nadie haya observado que te entregaran ese billete en ese momento, nadie puede llegar a descubrir qué ha ocurrido, ni aun pudiendo examinar el billete mismo.

Cita de: satoshi, 13 de agosto 2010, 07:28:47 PM

¿Esconde algún tipo de información para la red pública? ¿Cuál es la ventaja?

Si al menos 50% de los nodos validan las transacciones suficientes como para poder descartar transacciones antiguas, entonces todos vieron todo y podrían tomar nota.

Inicialmente, esperaba que todas las transacciones fueran validadas solo entre las partes involucradas. En realidad, la generación de bloques por los nodos anotaría los hashes que les dijeron las partes.

Sin embargo, en el último momento me di cuenta de que dado que los hashes no eran firmas o de otra manera verificados, esto, hacía que fueran fácilmente de falsificar un "cancelar el hash del punto de salida anterior". No podría robarle monedas a nadie, pero sí que se podrían invalidar.

Puedes ver tres distintas maneras de avanzar sobre el detalle de las claves. 1) Dejar que todos los verificadores puedan ver las transacciones, minimizando lo que es guardado. 2) Aparecer con una manera de minimizar el número de validadores que necesitan ver cada transacción. 3) crear una clave única para cada uso. Firmando los hashes (¡En el último momento!)

1) Inicialmente escribí sobre el primer episodio, porque introducía menos variables a la vez. Quería asegurarme de que anotar los hashes no era un ERROR obvio.

Intente cuantificar cuánta privacidad se podría ganar. Es mínima en el peor de los casos (todo el mundo guarda todo de todas maneras), pero es considerable en caso nominal. La mayor parte de la gente no guarda nada que no sea necesario para ellos mismos.

Con este incremento, el beneficio es, que cualquier nueva amenaza solo podría observar las transacciones que ocurren luego que se han unido. No pueden mirar hacia atrás en el tiempo, a no ser que encuentren a un "*early adopter*" que hubiera guardado todo y le convenciera para que compartiera toda la historia con él. Por lo que protección mínima, pero al menos su Ex no va a estar husmeando

después del hecho. :-)

2) Sin embargo, es posible minimizar el horizonte de espacio con un uso inteligente del DHT (*Distributed Hash Table, por sus siglas en Inglés - network storage- almacenamiento de la red*).

Todos los detalles aún no están terminados, pero puedes visualizarlo al partir la lista de bloques, digamos que 1024 bloques iguales, cada uno con 10 nodos validadores redundantes. En vez de una única lista de bloques con 10,000 nodos validadores redundantes. Cada uno escogido aleatoriamente de un conjunto de nodos responsables de un segmento del espacio del hash.

En lugar, garantizar que el 50% del todo el poder CPU es necesario, para falsificar cualquier cosa, que pueda intentar conseguir un consenso del 100% y replicar en la cadena una suma-comprobación de la cadena de bloques. (Sería parecido a publicar la comprobación de las 1024 sumas en el periódico cada día).

Esto restringe la visibilidad de un atacante para saber qué hash quisiera cancelar (Solo veo 1/1024 de las transacciones), y eso limita su ventana de tiempo para enviar una cancelación fraudulenta, que cuando controla el 100% de los verificadores de un cubo, lo que le daría una ventana de tiempo mayor en ese caso.

Por lo que hay un camino potencial para ganar privacidad al restringir alguna visibilidad. Esto, conlleva unos riesgos potenciales.

3) En realidad, debo darte méritos por dar chispa a la mejor idea de caso de uso. ¡Enhorabuena! Inicialmente descarte la idea de firmar los hashes de punto de salida, porque se parecía mucho como las actuales direcciones de Bitcoin. Asumí que la clave pública requerida en la firma asociaría demasiadas cosas a la vez.

Sin embargo, si solo usa una clave pública una vez donde firmas una combinación del hash punto de salida y el número de bloque actual. Luego, cuando el hash de punto de salida es inicialmente creado, este se registra con una clave pública. Cuando es gastado, el hash se verifica al tener una firma distinta pero relacionada por la misma clave.

Creo que esto resolvería el problema por completo. No habría más

asociaciones posibles por que las dos simples instancias de uso del hash de punto de salida en la lista del bloque TIENEN QUE estar relacionados. Añadir un segundo uso como identificador no aporta nada.

Para simplificar el tema del “número de bloque actual”, quien envía puede presentar firmas durante los 3-4 bloques siguientes. El validador solo anotaría el apropiado en el bloque.

Esto solo añade más bits a la lista del bloque, más de lo que esperaba. Creí que el hash solo era la óptimo.

====

¿Cuál es la construcción de crypto más pequeña que siga estas propiedades? Quizás seas capaz de considerar eso en vez de un hash y una firma completa.

1) Te doy algo que parece arbitrario

2) Te doy algo que parece fácilmente relacionable con tu #1 pero sin relación al #1 de alguien más

3) Nadie puede averiguar #2 desde #1

====

Por ejemplo

1) Te doy Z donde Z = X * Y y tanto X e Y son grandes números primos

2) Te doy la dupla (X, Y)

3) Nadie puede factorizar X e Y desde Z

En ese caso, cuando envías una transacción offline, la remitente encierra (X, Y) para cada punto de entrada.

El receptor crearía en privado un nuevo (X, Y) para cada nuevo punto de salida.

El receptor entonces transmite cada uno de los puntos de entrada (X, Y) para cancelarlos. Se transmite cada Z del punto de salida para

crearlos.

¿Eso funciona? O, ¿es demasiado ingenuo?

Re: No es una sugerencia

Publicado por Red, 13 de agosto 2010, 10:20:50 PM

Cita de: satoshi, 13 de agosto 2010, 07:28:47 PM

Crypto puede ofrecer una manera de "llave ciega". He investigado un poco y, quizás haya algo ahí. Las "firmas de grupo" puede que estén relacionadas.

En el área general podemos encontrar algo: http://www.users.zetnet.co.uk/hopwood/crypto/rh/

Lo que necesitamos es una manera de generar variaciones ciegas adicionales de la clave pública. Las variaciones ciegas/obscuras tendrían que tener las mismas propiedades que la clave pública raíz, como el hecho de que la clave privada pueda generar una firma para cualquiera de las anteriores. Otros podrían no decir si una clave ciega es relacionada con la clave raíz, u otras claves ciegas provenientes de la misma clave raíz. Estas serían las propiedades del cegamiento. Ceguera, en pocas palabras, si x = (x * gran_número_entero_aleatorio) mod m.

Cuando pagas a una dirección de Bitcoin, generarías una nueva clave ciega para cada uso.

Entonces, tendrías que ser capaz de firmar con una clave de tal manera que no se pueda decir que las dos firmas provienen de la misma clave privada. No estoy seguro si siempre, al firmar con una clave pública ciega diferente ya le daría esta propiedad. Si no, creo que un grupo de firmas podrían valer. En las firmas de grupo, es posible que algo sea firmado sin saber quién lo ha firmado.

Por ejemplo, digamos que un ataque militar sin mucha popularidad ha sido ordenado, pero nadie en la historia quiere ser recordado como la persona que lo ordenó. Si diez líderes tienen claves

> privadas, uno de ellos podría firmar la orden, y ninguno de estos sabría quién ha sido.

Esto es una idea muy buena. Creo que ya veo por donde vas con ella.

Me ha costado varios intentos poner todas las piezas en conjunto. Soy un poco lento.

Estoy en lo correcto, estabas sugiriendo que se pudiera firmar un hash de punto de salida con una clave ciega de un solo uso.

Donde la clave pública ciega es equivalente a la clave pública de la transacción de una dirección de Bitcoin. Digamos que el par de llaves pública/privada de la dirección bitcoin fue P/p. Las claves públicas ciegas podrían ser P1, P2, P3…Pn. Donde cada quien puede validar cualquier cosa firmada con la clave privada (p).

Así que después de la creación cuando se emite el hash del punto de salida para validación, este aparecería firmado por P1. Sin embargo, cuando el receptor emita el punto de salida para una cancelación, este sería firmado por P2, o cualquiera diferente de P1 (ya que esta se encuentra emitida al público). Ambas firmas calculadas serían las mismas, pero la clave pública podría cambiar. Esto significa que solo alguien que posea la clave privada común podría haberlo generado.

¡Eso es de genio!

57

Sobre el Alto Coste De La Minería

Traducción por
Alex Preukschat | Roberto Fernández Hergueta

ESTE HILO DISCUTE el aumento en la dificultad de la minería tras un aumento del poder de procesamiento, cuando el incremento de poder de computación es seguido por un descenso de la potencia de cómputo. Entonces, los mineros que quedan en la red tendrían que enfrentarse a un nivel de dificultad mucho más alto, lo que aumenta el tiempo por bloque hasta el siguiente ajuste.

Este problema no ha afectado a Bitcoin, pero sí afectó mucho a algunas criptodivisas alternativas como Feathercoin. Una solución llamada Gravity Well de Kimoto, fue desarrollada para divisas alternativas. El siguiente hilo aborda este potencial problema.

Satoshi se refiere específicamente a la respuesta del mercado sobre el coste de la minería.

Escenario de desastre potencial

Publicado por gebler, 14 de agosto 2010 12:43:54 PM

La dificultad para generar bitcoins es ajustada periódicamente usando

un método que ha funcionado bastante bien hasta ahora. Sin embargo, me temo que hay escenarios plausibles donde el método actual se comportaría de bastante mal.

Un escenario sería el siguiente:

1) A medida que los bitcoins se vuelven más conocidos, la competencia entre mineros aumentará, con los consiguientes aumentos en dificultad. Esta mayor dificultad eventualmente haría que el minado de bitcoins no fuera rentable para aquellos que no tienen acceso a buenos precios de energía o acceso barato a una combinación eficiente de hardware/software.

2) Algunos usuarios de bitcoins pueden continuar minando bitcoins incluso aunque no sea rentable para ellos. Esto podría deberse por ideología, porque es divertido o simplemente por ignorancia. Pero es bastante plausible que la gran mayoría de bitcoins se minen por aquellos que se benefician de hacerlo. Digamos que el 99% de todos los bitcoins son finalmente creados por mineros rentables.

3) La competencia entre los mineros rentables bajará el margen de beneficio, hasta el punto en que siga siendo rentable seguir minando pero poco. Digamos que el margen de beneficio típico durante un período de ajuste de dificultad (2016 bloques) sea del 10%.

4) Desde que el minado de bitcoins es un proceso descentralizado y no coordinado, podemos esperar fluctuaciones aleatorias en la actividad de minado. Esto no afecta la dificultad durante un periodo específico del bloque 2016, por lo que la actividad de minado podría, por ejemplo, incrementarse en un 20% durante un período sin hacer que el minado sea rentable dentro de ese período.

Dadas las suposiciones anteriores, tenemos un desastre previsible en el siguiente ajuste de dificultad. Como la producción de bitcoins fue un 20% por encima de meta, la dificultad se ajustará al alza en un 20%. Pero el margen de ganancia fue solo del 10%, así los que operan con fines de lucro, ahora perderían dinero si continúan minando. Así que dejarán de minar, y como constituyen el 99% de la capacidad de minado, entonces generar los próximos 2016 bloques supone un esfuerzo 100 veces mayor de lo normal. Todo lo que depende de la generación de bloques se ralentizará y esta lentitud persistirá durante mucho tiempo, ya que los próximos 2016 bloques tardarán 100 veces

más tiempo para generarlos (casi 4 años en lugar de dos semanas).

Ahora, si esto sucediera, supongo que un nuevo cliente podría ser liberado para restablecer la dificultad a algún número sensible y comenzar a usar un mejor algoritmo para el ajuste de dificultad. Pero sería mucho mejor hacerlo proactivamente antes de que se convierta en un problema (quizás con un "flag day" predeterminado activando el nuevo algoritmo en un momento determinado en el futuro, dando al nuevo cliente la oportunidad de propagarse).

Una simple (¿?) modificación del algoritmo podría aplicar el ajuste después de una cierta cantidad de tiempo, en lugar de en un cierto número de bloques. El cambio podría ser sincronizado para tener efecto en el próximo bloque, por lo que la sincronización de tiempo entre los clientes no necesitaría ser súper exacta para poner a la gran la mayoría de ellos de acuerdo sobre cuándo aplicar la nueva dificultad.

Además, el ajuste de dificultad probablemente debería tener en cuenta los ajustes del número de bitcoins minados (ahora 50, reducido a la mitad cada 4 años). Reducir a la mitad el número de bitcoins generados cada vez es equivalente a duplicar la dificultad en cuanto a la rentabilidad, y esa caída drástica en la rentabilidad es innecesaria si puede ser evitada fácilmente.

No estoy seguro si el actual algoritmo de ajuste ya toma eso en cuenta de alguna manera, pero no puedo ver ningún obvio ajuste al respecto en el código fuente.

Re: Escenario de Desastre Potencial

Publicado por satoshi, 15 de agosto 2010, 04:37:16 PM

Algunos lugares donde gravitaría la generación :

1. lugares donde es más barato o gratis
2. personas que quieren ayudar por razones ideológicas
3. personas que quieren obtener algunas monedas sin el inconveniente de hacer una transacción para comprarlas.

Hay lugares legítimos donde es gratis. La generación es básicamente libre en cualquier lugar que tenga calefacción eléctrica, ya que el calor del ordenador compensa la calefacción eléctrica con su placa base. Muchos pisos pequeños tienen calefacción eléctrica sin ser inconveniente.

¿Qué tan caro es el combustible para la calefacción? Con el precio del petróleo tan alto, actualmente es más caro que la electricidad, entonces la generación tendría coste negativo.

También hay adolescentes aprovechando la factura de electricidad de sus padres, empleados tomando recursos de sus empleadores, botnets (computadoras infectadas), etc.

El caso 3 entra en juego para pequeñas cantidades. Los costes generales de hacer un intercambio no tienen sentido si solo necesitas un poco de dinero en los bolsillos para micropagos fortuitos. Creo que esta es una buena ventaja frente al dinero fiduciario, en lugar de que todo el señoreaje vaya una gran entidad, dejándolo en cantidades convenientes a personas que necesiten recuperar una pequeña cantidad de cambio.

58

Sobre el Desarrollo de un Sistema de Alerta

Traducción por **Alex Viñas Salles**

SATOSHI DISCUTE sobre el desarrollo de un sistema de alerta donde los mensajes importantes pueden ser enviados a través de la red de Bitcoin solo para aquellos que posean una clave privada, y, en este caso, Satoshi tiene una. Por ejemplo, esta podría usarse para comunicar a todos los mineros sobre una importante actualización del software después de que un error (bug) haya sido encontrado.

Desarrollo de un sistema de alerta

Publicado por satoshi, 22 de agosto 2010, 11:55:06 PM

He estado trabajando en escribir un sistema de alerta. Las alertas se difunden a través de la red y pueden aplicar a una amplia versión de números. Los mensajes de alertas son firmados con una clave privada que solo yo tengo.

Los nodos pueden hacer dos cosas para responder a las alertas:

- Poner un mensaje de atención en la barra de estado.
- Hacer que los métodos de control de dinero de las interfaces json-rpc devuelvan un error.

En los casos del error de desbordamiento, o una bifurcación donde los usuarios pueden desconfiar de los pagos recibidos, las alertas deberían guardar versiones antiguas que son mayormente seguras hasta que ocurra la actualización. Los usuarios manuales deberían darse cuenta de la atención mostrada en la barra de estado cuando comprueben los pagos recibidos, y el modo seguro de json-rpc detiene a las webs automatizadas puedan realizar cualquier tipo de intercambio hasta que son actualizadas.

Los métodos json-rpc que devuelven errores durante una alerta son:

- sendtoaddress
- getbalance
- getreceivedbyaddress
- getreceivedbylabel
- listreceivedbyaddress
- listreceivedbylabel

En una respuesta sobre el sistema de alerta:

Re: Desarrollo de un sistema de alerta

Publicado por satoshi, 24 de agosto 2010, 11:51:12 PM

Si es tan paranoico que se está poniendo histérico por esto, entonces seguramente es lo suficientemente paranoico que si aparece un mensaje de advertencia en la barra de estado, verificará el sitio web y el foro.

Creo que después que otro error aparezca, como el de desbordamiento, es importante que las webs automatizadas paren de enviar órdenes hasta que los administradores pueden comprobar que está ocurriendo y decidir qué hacer. Si decide que ha sido una falsa alarma, y quiere arriesgarse, usted puede el switch “-disablesafemode”.

Re: Desarrollo de un sistema de alerta

Publicado por satoshi, 25 de agosto 2010, 03:17:37 PM

No puedo hacer acciones arbitrarias de forma remota. ¿Quizás, alguno de ustedes está respondiendo a quienes han sugerido que un sistema de alerta debería hacer algo más?

Si hay una alerta, los siguientes métodos json-rpc devuelven un error:

- sendtoaddress
- getbalance
- getreceivedbyaddress
- getreceivedbylabel
- listreceivedbyaddress
- listreceivedbylabel

Los 14 métodos restante funcionan correctamente.

Creo que la opción más segura tiene que habilitarse por defecto. Si quiere que su servidor siga haciendo trading e ignorar una alerta diciendo que el dinero que está recibiendo puede ser dinero procedente del error de inundación, aun pudiendo activar el switch más tarde, perderá la posibilidad de poder culpar a alguien en caso de que se pierda el dinero.

En el peor caso, si deja las alertas habilitadas, su web parará el trading hasta que actualice o añada el switch -disablesafemode.

Ser sorprendido por un tiempo de inactividad temporal cuando su nodo, de lo contrario estaría en riesgo, es mejor que sorprenderse por un ladrón quitándole todo tu inventario.

Algún día cuando ya no hayamos encontrado errores por mucho tiempo y haya sido completamente revisado por seguridad sin encontrarse nada, esto puede ser reducido. No estoy defendiendo que esto funcione así para siempre. Aún es un software beta.

Re: Desarrollo de un sistema de alerta

Publicado por satoshi, 25 de agosto 2010, 04:56:15 PM

> Una frase de: jimbobway, 25 de agosto 2010, 04:45:22 PM
>
> > Una frase de: BioMike, 23 de agosto 2010, 05:15:43 AM
> >
> > @mizerydearia, Creo que el botón de comillas es mucho más fácil de encontrar que el de respuesta.
> >
> > ¿Entonces, teóricamente este es el primer sistema de control donde <algún gobierno> pueda arrestar a Satoshi y demandarle que entregue su llave (o quitársela del ordenador) y poder apagar completamente toda la red?
> >
> > ¿O eso no es posible? ¿Hasta dónde podría llegar <algún gobierno>?
>
> Algunas preguntas retóricas para Satoshi:
>
> - ¿Puede resistirte al ahogamiento simulado?
> - ¿Puede aguantar shocks eléctricos?
> - ¿Todas las formas de tortura?
> - Por último, ¿por alguna casualidad no serás Jack Bauer? Seriamente.

Con respecto al sistema de alerta, a quien le importa? Lo más que puede llegar a hacerse con la clave es, desactivar temporalmente los seis comandos json-rpc hasta que los dueños de la web añadan el switch -disablesafemode o actualicen. Todos los nodos seguirán funcionando y generando, por lo que la red se mantiene correctamente. Si no estoy disponible, cualquier niño puede hacer un script para averiguar cómo poder añadir dos caracteres y crear una nueva versión que desactive el sistema de alerta. Solo sería una inconveniencia temporal.

> Cita de: BioMike, 23 de agosto 2010, 05:15:43 AM
>
> ¿Entonces, teóricamente este es el primer sistema de control donde <algún gobierno> puede arrestar a Satoshi y demandarlo a que entregue su llave (o quitársela del ordenador) y poder apagar completamente toda la red?

Esto me hace pensar que la gente que escribe no sabe muy bien de lo que están hablando. No pueden “apagar la red por completo”.

Re: Desarrollo de un sistema de alerta

Publicado por satoshi, 25 de agosto 2010, 04:56:15 PM

> Cita de: BioMike, 25 de agosto 2010, 06:23:45 PM
>
> ---
>
> > Cita de: satoshi, 25 de agosto 2010, 04:56:15 PM
> >
> > Esto me hace pensar que la gente que escribe no sabe muy bien de lo que están hablando. No puede “apagar la red por completo”.
> >
> > ---
>
> Nunca me he opuesto a este cambio/idea, solo estaba preguntando si esto sería posible, y hasta dónde podrían llegar?
>
> ¿Qué hay de malo en querer estar informado? :-)
>
> ---

Mis disculpas, tu post era de hecho una pregunta y no una afirmación.

59

Sobre la Definición de Dinero y Bitcoin

Traducción por **Alex Viñas Salles**

SATOSHI RESPONDE a un hilo sobre Bitcoin y la visión de Murray Rothbard sobre el dinero. Rothbard formaba parte de la Escuela de Economía Austriaca, una escuela de economía donde muchos de sus fundadores procedían de la Viena del siglo XIX. Su rasgo distintivo es su creencia de que el funcionamiento de la economía en general es la suma de las decisiones y acciones de todos los individuos en conjunto. En contraste a la mayoría del resto de escuelas de economía, la escuela austriaca creía que ningún ente central podría estimar correctamente el resultado de la oferta agregada ni de la demanda de cualquier bien o servicio. Si los planificadores centrales cambian cualquier parámetro económico que controlan (típicamente aplicable a al tipo de interés establecida por un banco central), cómo pueden estimar correctamente el resultado de la suma de todas las decisiones de consumo de la gente, así como todas las decisiones de empresas e inversores. Da igual cuantas gráficas y estadísticas se aporten, la diferencia entre las expectativas y los resultados finales son inevitables y darán lugar a alteraciones temporales.

Bitcoin NO viola el Teorema de Regresión de Mises

Publicado por xc, 27 de julio 2010, 02:09:27 AM

La Regresión Monetaria y el Surgimiento del Dinero de la Economía de Trueque

Todo el propósito del teorema de regresión es ayudar a explicar una aparente paradoja del dinero: ¿cómo tiene valor el dinero como medio de intercambio, si se valora porque sirve como medio de intercambio? Menger y Mises ayudaron a entenderlo explicando, que el tiempo es lo esencial que falta en la paradoja del dinero.

Como explica Rothbard en Hombre, Economía y Estado (p. 270), "...el precio del dinero, al *final* del día X es determinado por las utilidades marginales del dinero y los bienes, mientras estos existieran al *principio* del día X. Pero la utilidad marginal del dinero se basa, como hemos visto anteriormente, *en una matriz previamente existente de precios de dinero*. El dinero es demandado y considerado útil porque tiene precios ya existentes. Por lo tanto, el precio de un bien en el día X es determinado por la utilidad marginal del bien en el día X, y la utilidad marginal del dinero en el día X, que a su vez depende de los precios de los bienes en el día X-1. **El análisis económico de los precios por lo tanto no es circular. Si los precios de hoy dependen de la utilidad marginal del dinero del día de hoy, este último depende de los precios del dinero de ayer."** [énfasis añadido]

Luego Rothbard explica que para que el dinero emerja de la economía del **trueque,** tiene que tener un valor preexistente a este bien. Este valor de este bien surge por la demanda del trueque por el potencial de ese dinero en **consumo directo** (a saber, ornamentación). Este valor **es la semilla** de las futuras estimaciones sobre el valor del dinero como medio de cambio. El surgimiento de un mercado natural del dinero es así totalmente explicado.

La Economía Monetaria

Sin embargo, una vez que la economía se ha monetizado y una memoria de los ratios de precios de bienes y servicios ha sido establecida, el dinero puede perder su valor directo de mercancía y aun así usarse como dinero (medio indirecto de cambio). Rothbard explica (p. 275):

"Por otro lado, si no se sigue desde este análisis que, si un dinero existente fuera a perder su uso directo no podría usarse como dinero. Así, si el oro, después de establecerse como dinero, repentinamente perdiera su valor para ornamentación o uso industrial, no necesariamente perdería su caracterización de dinero. Una vez que un medio de cambio se ha establecido como dinero, **los precios del dinero se continúan poniendo**. Si en el día X el oro pierde su uso directo, aun así, habría un histórico de precios establecidos en el día X-1, y dichos precios forman la base de la utilidad marginal del oro en el día X. Similarmente, el histórico de precios determinado el día X, compone la base de la utilidad marginal del dinero en el día X+1. De X en adelante, el oro podría ser demandado simplemente por su valor de intercambio, y en absoluto para su uso directo. Por lo tanto, mientras sea absolutamente necesario que el dinero se **origine como una mercancía** con usos directos no es absolutamente necesario que los usos directos continúen luego que el dinero ha sido establecido."

Esto explica la historia del dinero fiduciario. Originalmente surgieron como nombres simples para pesar el dinero mercancía (plata) que se desarrolló en la economía pre-monetaria del trueque. Aun perdiendo sus lazos con el valor directo del producto por la intervención del estado, el dinero de papel retuvo el status de dinero gracias a su **histórico de precios anterior**. Este factor es tan fuerte, que la relación entre el oro y el dólar, por ejemplo, es de alguna forma inversa. El oro ya no circula como un medio de cambio común. Los precios se establecen en dólares, no en oro. La mayoría de las personas que desean operar con oro, lo hacen basándose en el ratio del dólar/oro. ("Hey, ¿te compro ese sofá de 100$ en oro?" "OK, el ratio usd/oro es 1000$/oz, dame un 1/10 oz de oro.") Las leyes de curso legal, impuestos y todo el ambiente regulado financiero mantienen esta inercia de precios en dólares, haciendo muy difícil retornar al uso directo del oro, a pesar de la naturaleza destructiva e inflacionaria del dinero fiduciario.

El Surgimiento de la Economía de Bitcoin

Los primeros negocios en la economía de Bitcoin fueron casas de cambio (NewLibertyStandard, BitcoinMarket, BitcoinExchange,…) Esto no fue casualidad, sino que nace a raíz de la explicación anterior. Para que Bitcoin sirva como medio de cambio sin tener un valor como

mercancía para usos más allá del intercambio indirecto, tiene que haber un histórico de precios. Las casas de cambio del mercado cubren esa necesidad y dan a los usuarios de Bitcoin acceso a esa información. Por lo que Bitcoin, puede servir como un dinero intermediario para paypal dólares/pecunix/euros. ¿Pero, por qué existe una demanda de Bitcoin sobre dólares? Esto es una valoración subjetiva basado en sus propiedades como anonimato, sistema de compensación descentralizado, confianza criptográfica, ratio de crecimiento predeterminado y definido, deflacionario, divisible, bajas comisiones por transacción etc.... inherente al sistema Bitcoin.

El punto esencial es que una vez que un intercambio puede darse entre Bitcoin y dinero (USD), el proveedor de servicios tiene una manera de evaluar los Bitcoins como un potencial medio de intercambio. La regresión del dinero se cumple, porque, si tiramos hacia atrás lo suficiente, llegamos al dinero como mercancía tradicional: BITCOINS -> USD -> ORO y PLATA MONETIZADOS [empieza la economía monetaria] -> [termina la economía del trueque] MERCANCÍA ORO Y PLATA.

Por supuesto, si hubiera una gran catástrofe, y el histórico de precios se destruyera, probablemente el Bitcoin NO surgirá directamente como dinero (asumiendo que los Bitcoins tienen valor limitado fuera del intercambio). El dinero fiduciario con cero valor directo de trueque, tampoco lo haría. Las materias primas como el oro y la plata que tienen un amplio reconocimiento como valor directo de trueque, podrían surgir primero. La economía entonces sería monetizada con unos ratios de precio en oro y plata. Entonces, los Bitcoins, siendo valorados por sus propiedades intrínsecas como dispuestas a intercambio, pueden convertirse en la forma predominante para comerciar. Inicialmente, los creadores de valor continuarán poniendo sus ratios de valor precio en términos del dinero “real” (ratio onza de oro/BTC), pero con el tiempo, los precios de Bitcoin (BTC) pueden surgir (ver vekja.net como ejemplo). Estamos en esa fase inicial.

Por lo tanto, siempre que se produzca un intercambio de BTC y USD/Euros/etc., el conocimiento de las relaciones de precios existentes puede utilizarse en la economía de Bitcoin. Con el tiempo, a medida que los Bitcoins se vuelven cada vez más comerciables, estos ratios de precios fiat<->BTC generarán relaciones directas de precios de BTC. La economía de Bitcoin surge de esta forma. El teorema de la regresión de Mises se satisface.

XC

Edit: clara posibilidad de que bitcoin surja directamente como dinero de una economía de trueque.

RE: Bitcoin NO viola el Teorema de Regresión de Mises

Publicado por satoshi, 27 de agosto 2010, 05:32:07 AM

Si te sirve de ejemplo, imagínate que hay un metal común tan escaso como el oro pero con las siguientes propiedades:

- Color gris aburrido
- No es buen conductor de la electricidad
- No es particularmente fuerte, pero tampoco es dúctil, ni fácilmente maleable
- No es válido para nada práctico u ornamentación.

Y una propiedad especial, la propiedad mágica:

- Puedes transportarlo a través de un canal de comunicaciones

Si de alguna manera adquiriera algún valor por razón que sea, entonces cualquiera que quiera transferir valor a distancia podría comprar algunos gramos, transferirlos, y que el destinatario lo venda.

Quizás podría tener un valor inicial de circulación como has sugerido, haciéndole ver a la gente su utilidad como medio de intercambio. (Yo claramente querría algunos). Quizás como coleccionista pero, cualquier otro motivo arbitrario podría ser bueno.

Creo que las características tradicionales del dinero fueron escritas asumiendo que hay en competición varios objetos en el mundo que son escasos, que automáticamente cuenten con un valor intrínseco el cual se impondrá sobre el resto de objetos que no tengan dicho valor. Pero, si no hubiera nada en el mundo con valor intrínseco que pueda ser usado como dinero, escaso pero sin valor intrínseco, creo que la gente terminaría aceptándolo.

(Estoy usando la palabra escaso refiriéndome sobre la oferta potencial limitada)

Otro post sobre el mismo asunto:

RE: BITCOIN NO VIOLA EL TEOREMA DE REGRESIÓN DE MISES

Publicado por epaulson, 17 de agosto 2010, 06:45:18 PM

Ha habido mucho debate sobre qué son los Bitcoins – a saber dinero versus producto. Además, ha habido un gran debate sobre inflación versus deflación en relación con el Bitcoin, sobre si la gente los prestaría a terceros, a que tipos de interés, etc.

Creo que la decisión más correcta de Bitcoin es que son acciones de una empresa común llamada Bitcoin Enterprise que estamos construyendo. Es como ser parte de una empresa (ahora mismo una empresa de tamaño pequeño) y estamos siendo pagados en acciones de la compañía. Hay un número limitado de Bitcoins, como también hay un número limitado de acciones en una compañía (Salvo nuevas emisiones/etc.).

El principal valor del Bitcoin actualmente es la esperanza de que en algún día estos valgan significativamente más de lo que valen ahora mismo. Para que eso ocurra, Bitcoin Enterprise en su totalidad, debe ganar valor añadido. La manera más obvia es facilitar a los comercios de internet el cambiar bitcoins por otros bienes. El esfuerzo computacional colectivo de todos los empleados/dueños ayuda a asegurar que el cambio es bueno al guardar una copia de cada transacción. El esfuerzo individual de algunos Bitcoiners está ayudando a que el cambio a Bitcoin sea más fácil y útil.

En relación con los préstamos/créditos de Bitcoins, para mí son análogos a los préstamos/créditos sobre acciones. La primordial razón para pedir Bitcoins prestados es porque usted piensa que están sobrevaluados y terminarán valiendo menos de lo actual en el

momento que toque devolverlos. Cuando pide que le presten Bitcoins, puedes venderlos ahora (hacer el trueque), confiando que costarán menos dinero recomprarlos luego para que pueda devolverlo a su prestatario (probablemente más una comisión).

En esencia, los Bitcoins son una "directa oferta pública" de acciones de la Bitcoin Enterprise.

RE: LOS BITCOINS SON COMO LA MAYORÍA DE LAS ACCIONES DE BOLSA COMUNES

Publicado por satoshi, el 27 de agosto 2010, 04:39:26 PM

Los bitcoins no tienen dividendos o potenciales futuros dividendos, por lo que no son como una acción.

Más como un coleccionable o producto.

60

Sobre el Requerimiento de Comisión en una Transacción

Traducción por **Alex Viñas Salles**

EL CONSEJO DE SATOSHI es permitir que algunas transacciones sean procesadas, aunque no tengan incluidas la comisión en la transacción. Ahora mismo, los mineros aún están siendo recompensados con bitcoins, aunque está programado para terminar cuando se hayan minado los 21 millones de bitcoins, que será a mediados del siglo XXII. Cuando llegue ese momento, las comisiones de transacción serán obligatorias para que los mineros puedan ser recompensados apropiadamente por el uso de sus recursos.

¿Siempre se paga una comisión por transacción?

Publicado por jgarzik, 07 de septiembre 2010, 03:17:34 AM

Para reflejar precisamente el procesamiento de una transacción tiene un coste asociado al consumo de recursos de la red, propongo que la comisión de transacción sea obligatoria para todas las transacciones a partir del día X (Donde X sea en los próximos meses).

RE: ¿SIEMPRE SE PAGA UNA COMISIÓN POR TRANSACCIÓN?

Publicado por satoshi, 07 de septiembre 2010, 04:32:21 AM

Otra opción puede ser reducir el número de transacciones gratis permitidas en cada bloque antes que los costes por transacción sean obligatorios. Los nodos solo cogerán unos pocos KB de transacciones gratuitas por bloque antes de requerir un costo mínimo por transacción de al menos de 0.01.

El umbral, probablemente debería ser menor que el que es actualmente.

No creo que el umbral deba llegar nunca a 0. Siempre deberíamos aceptar algunas transacciones gratuitas.

RE: ¿SIEMPRE SE PAGA UNA COMISIÓN POR TRANSACCIÓN?

Publicado por satoshi, 08 de septiembre 2010, 05:30:14 AM

Actualmente, pagar el coste de la transacción es controlado manualmente a través del -pattxfeeswitch. Sería muy fácil hacer que, automáticamente, el software comprobará el tamaño de los bloques recientes para ver si debería existir un coste o no. Estamos aún muy lejos de llegar a ese umbral, no lo necesitamos activarlo aún. De todas maneras, es una buena idea ver cómo funcionan las cosas controladas manualmente primero.

No es muy importante el hecho de que alcancemos el umbral. Las transacciones gratuitas simplemente tardarían más en introducirse dentro de un bloque.

Hice un recuento aproximado de 4000 bloques desde alrededor del 74000 al 78000. Esto es excluyendo las transacciones de recompensa por bloque:

Serían en promedio 2 transacciones por bloque, 17 transacciones por hora, que son 400 transacciones por día.

El promedio de bytes por bloque eran 428 bytes, o 214 bytes por transacción.

El umbral actual es 200KB por bloque, o alrededor de 1000 transacciones por bloque. Creo que debería reducirse a 50KB por bloque. Eso sería aún 100 veces más que el promedio de transacción por bloque.

El umbral puede ser fácilmente cambiado en el futuro. Podemos decidir incrementarlo cuando sea la hora de hacerlo. Es una buena idea mantenerlo en valores bajos, e incrementarlo según sea necesario. Si ahora llegamos al umbral, casi sería algún tipo de congestión y no sería un caso real. Mantener el umbral bajo ayudaría a limitar el espacio que se despreciaría en el disco.

RE:¿SIEMPRE SE PAGA UNA COMISIÓN POR TRANSACCIÓN?

Publicado por satoshi, 23 de septiembre 2010, 04:08:35 PM

> Una frase de satoshi, 08 de septiembre 2010, 05:30:14 AM
>
> El umbral actual es 200KB por bloque, o alrededor de 1000 transacciones por bloque. Creo que debería reducirse a 50KB por bloque. Eso sería aún 100 veces más que el promedio de transacción por bloque.
>
> ---

He implementado este cambio en SVN rec 157.

La razón por lo que lo hice tan alto fue para permitir un gran número de transacciones sin llegar a necesitar la comisión por transacción. El umbral estaba alrededor de 26.000 BTC para transacciones hechas de las 50 monedas BTC generadas. Aunque fuera 100 veces más fácil generar un respaldo en aquellos tiempos, solo algunas personas llegaron a encontrar esa comisión a ese nivel. El nuevo umbral lo deja alrededor de los 11,000 BTC para enviar monedas generadas. Solo se podría alcanzar con bitcoins generados. Si ha comprado sus bitcoins, serán denominados en transacciones más grandes, con lo que ni se acercaría al límite de los costes por transacción, a no ser que los comprara con cientos de

direcciones diferentes. Si llegas al nivel del coste por transacción, sólo tiene que pagar una vez para agrupar sus transacciones pequeñas.

61

Sobre Sitios con CAPTCHA y Requisitos de Paypal

Traducción por **Jose Antonio Bravo**

ALGUIEN PROPONE unas cuantas formas posibles en las cuales Bitcoin puede ser útil. La respuesta de Satoshi se dirige al que se refiere a páginas web que tienen tanto CAPTCHA como requisitos de PayPal.

La Lista de Nicho

Publicado por kiba, 23 de septiembre 2010, 04:00:16 PM

Esta es la Operación Crecimiento Económico. Nuestra misión es hacer crecer la economía bitcoin haciendo que todos se especialicen en un grupo reducido de bienes y servicios.

En resumidas cuentas, anuncie lo que quiere consumir y lo añadiré a la lista. Entonces alguien anunciará que intentará entrar en ese nicho. Puede también haber competencia dentro de nichos también, pero habrá otros nichos por completar.

Haremos que esas personas sean "responsables" de sus nichos, trabajando torpemente, alentando, comenzando un hilo y luego decepcionandose cuando el servicio no funcione en línea etc.

Nichos deseados:

1. Anuncios clasificados al estilo de Craiglist para ámbito local
2. Sitio al estilo de "Mechanical Turk" con una lista de trabajos sencillos para que los haga la gente. Sugerido por noagendamarket en el tema ¿Tipo de Cambio Estable? del Foro Económico.
3. Tienda de suministro de cerveza. Malta, levadura, lúpulo, etc.
4. Tienda de plantas para vender hierbas y otras cosas.
5. Academia Hacker. Video educativo gratuito. Clases con tarifa plana. Tutores personales a los que se paga según se avanza.
6. Sitio de citas que acepte bitcoins.
7. Servicio sencillo de encriptación y backup.

Nichos completados o en los que se está trabajando:

1. Centro de coordinación de anuncios al estilo de http://projectwonderful.com. Sugerido por mskwik. (He utilizado projectwonderful para hacer algo de dinero. Me pregunto si puedo ganar más dinero en un centro de coordinación de anuncios en bitcoin) noagenda ofreció una gran recompensa por esto, y lo está haciendo Biomike.
2. Sitio de descargas al estilo de rapidshare y otros hosts lamentables. Captcha inoportuno y paypal requerido. Bitcoin puede tal vez asumir ambos roles y optimizar el proceso completo. Sugerido por Kiba. Hecho por Hippich. Finalmente aparecieron 3 competidores.
3. Sitio para trabajadores por cuenta propia. Hecho por whichspace.
4. Sistema de pedidos de pizza. Puedes pedirla en la web, desde la línea de comandos, desde tu smartphone, por sms… Hecho por mizerydearia.

RE: LA LISTA DE NICHO

Publicado por satoshi, 6 de octubre 2010, 11:10:31 PM

Cita de: kiba, 23 de septiembre 2010, 04:00:16 PM

1. Sitio de descargas al estilo de rapidshare y otros hosts lamentables. Captcha inoportuno y paypal requerido. Bitcoin puede tal vez asumir ambos roles y optimizar el proceso completo.

Me repito aquí, pero hay un software open source para eso, por lo que solo sería cuestión de echar mano de un mecanismo de pago de Bitcoin. Uno bueno que he encontrado es de Mihalism Multi Host. Está diseñado como un host libre, así que sólo necesitaría algunos ajustes para relajar las restricciones con usos de pago.

62

Sobre Mensajes Cortos en la Cadena de Bloques

Traducción por **Jose Antonio Bravo**

LA CADENA DE BLOQUES es el libro de registro público de todas las transacciones de bitcoins y está compartido dentro de la red peer-to-peer. En este momento, contiene sólo sus propias transacciones. En este hilo, alguien propone añadir otra información dentro de cada transacción contenida en la cadena de bloques que sería el equivalente de la sección "Observaciones" en los cheques bancarios. A diferencia de éstos, sin embargo, estas observaciones serían públicas y por tanto visibles para todos. Satoshi expresó su preocupación por que alguien pudiera publicar en estas observaciones información que hubiera de mantenerse privada, como un número de cuenta de cliente.

Sin embargo, esta característica estaba siendo considerada para una actualización futura de Bitcoin, pero aún no disponible todavía en el momento en que se escribió la versión en Inglés de este libro. A esa fecha, solo un servicio de terceros como *blockchain.info* permitía a los usuarios añadir información textual extra, pero no era parte de la cadena de bloques en sí.

Los mineros tienen la capacidad de añadir cierto texto extra en el bloque. De hecho, el primer bloque creado por Satoshi Nakamoto, el bloque 0, tiene el siguiente mensaje en su interior:

"The Times 03/enero/2009 El ministro de Hacienda al borde del segundo rescate bancario"

El mensaje está codificado en ASCII pero es fácil de obtener para aquellos que saben cómo hacerlo.

Sugerencia: ¿Permitir que puedan mandarse mensajes cortos junto con bitcoins?

Publicado por ShadowOfHarbringer, 23 de octubre 2010, 03:11:17 PM

Bitcoin es estupendo, pero le falta algo que las transferencias bancarias habituales tienen: título de pago.

Quizás sería posible incluir mensajes cortos (<= 512 bytes) en cada transacción.

El mensaje podría estar encriptado con claves privadas/públicas de forma que sólo el receptor pueda leer sus contenidos.

¿Qué te parece?

PD.

Podría estar equivocado, pero los mensajes también podrían utilizarse para aumentar la aleatoriedad del proceso de hashing, ¿no? Si no es así, olvídalo.

Re: Sugerencia: ¿Permitir que puedan mandarse mensajes cortos junto con bitcoins?

Publicado por satoshi, 23 de octubre 2010, 07:02:57 PM

ECDSA no puede encriptar mensajes, solamente realizar firmas.

Sería imprudente tener registrados de forma permanente mensajes de texto sin formato que pudieran ver todos. Sería como esperar a que sucediera un accidente.

Si se hiciera un sistema de mensajes, tendría que ser un sistema separado y en paralelo a la red bitcoin. Los mensajes no deberían ser grabados en la cadena de bloques. Los mensajes podrían firmarse con los pares de claves de la dirección de bitcoin para demostrar de quién son.

63

Sobre el Manejo de un Ataque por Inundación de Correo no Deseado

Traducción por **Arturo Monzón**

EN ESTE INTERCAMBIO, Satoshi habla sobre la introducción de cambios en el software que haría más económicamente difícil a quien "envíe correo basura" a la red con múltiples transacciones.

Transacción/Ataque de inundación por correo no deseado actualmente en curso

Publicado por jgarzik, 19 de noviembre 2010, 07:02:38 PM

Aparentemente, alguien está "probando" la red principal de bitcoin inundándola con transacciones de 0.01 BTC desde A->A y B->B, donde A y B son dos claves públicas aleatorias. Puede verlo en http://theymos.ath.cx:64150/bbe

Hemos alcanzado el límite de transacciones gratis en cada bloque, para muchos bloques ahora, parece ser ~ 219 transacciones gratuitas por bloque. Las transacciones "reales" no aparecen como denegación de servicio en este momento, presumiblemente debido a la lógica que prioriza en parte, en función del valor de transacción.

<soapbox>
Las transacciones gratuitas solo piden un nivel permanente de spam. Debería haber un costo para cada transacción, incluso si solo es 0.001 BTC o más.
</soapbox>

Re: Transacción/Ataque de inundación por correo no deseado actualmente en curso

Publicado por Satoshi, el 19 de noviembre 2010, 11:50:24 PM

> Cita de: creighto el 19 de noviembre 2010, 08:29:12 PM
>
> Quizás además de la regla de prioridad de maduración recientemente implícita, debe haber una regla de maduración mínima sin una comisión de transacción. Dicho de otra manera, tal vez una regla de generación que dice que una transacción gratis debe tener 3 bloques de profundidad antes de poder ser transferida nuevamente de forma gratuita. Esto aún permitirá a los usuarios reales gastar de manera inmediata nuevos fondos si es necesario, al mismo tiempo que permite a los usuarios reales reorganizar los fondos para satisfacer sus necesidades sin un costo adicional. Creo que esto inhibiría significativamente el tipo de ataque de spam que se está llevando a cabo actualmente.

Estoy haciendo algo así. La prioridad es una versión más formal del concepto que está describiendo.

> Cita de: FreeMoney, el 19 de noviembre 2010, 05:39:44 PM
>
> ---
>
> Tal como está ahora v0.3.15 tiene mucho espacio para transacción libre y ese espacio se da primero a las transacciones con el mayor [maduración]*[valor]/[tamaño], ¿correcto? ¿Sería razonable hacer que una parte arbitraria del espacio libre requiera [maduración]*[valor]/[tamaño]>C?

> Tal vez configure C para que la transacción estándar de 1BTC pueda ingresar al área principal gratis en el siguiente bloque. Y un .1 puede entrar después de esperar alrededor de 10 bloques. Y haga que el área que permite [maduración]*[valor]/[tamaño]<C permita aproximadamente una docena de transacciones más o menos.
>
> ---

Sí, así. Y el área sin requisitos de prioridad es 3K, alrededor de una docena de transacciones por bloque.

Acabo de subir SVN rev 185, que tiene un requisito de prioridad mínimo para las transacciones gratuitas. Las inundaciones de transacciones se componen de monedas que se vuelven a gastar una y otra vez, por lo que dependen de sus propias 0 configuraciones de transacción repetidamente. Las transacciones de 0 configuración tienen prioridad 0, por lo que las transacciones gratuitas como esta tendrán que esperar a que una transacción entre en un bloque a la vez.

La versión 0.3.15 no inscribe transacciones con 0 configuración a menos que eso sea todo lo que le queda, por lo que los usuarios normales generalmente no deberían tener un problema con esto.

Creo que este es un buen pequeño compromiso para hacer la tarifa predeterminada 0.01. No se trata tanto de pedir que las transacciones gratuitas solo puedan usarse en monedas con alta frecuencia de transacciones. Si estás utilizando transacciones gratuitas, estás tomando beneficio y tiene que haber algún límite en la frecuencia con la que puede usarla con las mismas monedas.

Siempre hemos dicho que las transacciones gratuitas pueden ser procesadas más lentamente. Usted puede ayudar a garantizar que sus transacciones se procesen rápidamente agregando -paytxfee=0.01.

64

Tecnicismos Sobre los Pools de Minería

Traducción por **Jose Antonio Bravo**

EN ESTE HILO, se discute el concepto de cómo funciona el minado de Bitcoin mediante pools y cómo debería hacerse para evitar que los tramposos se conviertan en parte de un pool sin contribuir. Hoy por hoy, los pools mineros son los mayores contribuidores al minado. Los pools mineros no fueron inicialmente un concepto que describiera Satoshi Nakamoto. Aparecieron posteriormente como sugerencia de alguien en el fórum cuando la dificultad de minado comenzó a aumentar en la medida que se incrementó el interés en Bitcoin. La mejor analogía de un pool minero en Bitcoin son compañeros de trabajo que comparten billetes de lotería.

Minado cooperativo

Publicado por slush, 27 de noviembre 2010, 01:45:41 PM

Hola a todos,

desde que bitcointalk fue hackeado hace unos meses, perdí temporalmente el acceso a este fórum. Ahora he recuperado el acceso, pero no me planteo continuar más con el apoyo al pool en este hilo, por varias razones. Sobre todo porque los novatos no pueden postear, no puede funcionar como un soporte completo al cliente; he recibido muchas quejas sobre esto particularmente. En ese caso, es un fórum estilo “spaghetti” y es muy complicado seguir la discusión.

Hace unos días comenzamos un sistema de tickets para el soporte oficial del pool en http://support.bitcoin.cz. Este sistema de soporte está integrado también con support@bitcoin.cz, así que escribir un correo electrónico a support@bitcoin.cz es la forma correcta si necesitas una respuesta rápida y autorizada de uno de los administradores del pool en cualquier momento. Por ahora estamos procesando una gran cantidad de correos electrónicos atrasados allí, pero nuestra meta es contestar a todos los tickets en 24 horas. En http://support.bitcoin.cz hay también una base de conocimiento en la que vamos completando de más y más preguntas y respuestas todos los días.

Me gustaría invitarle también a IRC #mining.bitcoin.cz, donde hay mucha gente en línea, preparada para charlar y proporcionar ayuda básica con todas las cosas.

Dejaré este hilo abierto para debate no-oficial, pero está fuera de mis posibilidades de tiempo seguir el debate aquí.

Únete a nosotros en http://mining.bitcoin.cz!
EDITADO 27.12.2010: página wiki sobre minado en pool
EDITADO 17.03.2011: DaCoinMinster publicó script de GreaseMonkey que ajusta la página web sobre pool - es una herramienta de tercero, úsala bajo tu propio riesgo.

¿Qué es el Minado en Pool?

El minado en pool es una forma para que múltiples usuarios trabajen juntos acuñando bitcoins, y compartan los beneficios de una manera justa.

¿Qué necesito?

Los bitcoins se crean generalmente sólo en cantidades de 50 cada vez, pagándose los 50 a una sola persona. Además, la carrera para obtener el premio de 50 BTC en un bloque determinado es altamente competitiva.

Si se pone a minar por su cuenta, podría pasar mucho tiempo antes de que pueda recibir un retorno. El minado en pool le permite recibir en

su lugar pagos más pequeños, más frecuentes y más estables. Si tiene un ordenador más lento, o un minero CPU, entonces el minado en pool puede ser la única manera en que minará siempre bitcoins.

¿Cómo empiezo?

Necesita menos de 10 minutos para comenzar a minar en un pool. Visite: http://mining.bitcoin.cz y siga las instrucciones.

Publicación original:

Una vez la gente comenzó a utilizar ordenadores habilitados con GPU para minar, la minería se hizo muy difícil para otras personas. Estoy en bitcoin hace pocas semanas y no he encontrado un bloque todavía (estoy minando con tres CPUs). Cuando mucha gente tiene CPUs lentas y minan por separado, todos compiten entre ellos Y contra los ricos cabrones con GPU ;-), porque todos cuentan con hashes sha256 del mismo rango. ¡Dos CPUs separadas con 1.000 khash/s no son lo mismo que una máquina de 2.000 khash/s! Pero la nueva característica del cliente bitcoin oficial llamada 'getwork' permite ahora el trabajo de muchos ordenadores juntos, de forma que no compiten. Dado que ahora hay un minero de CPU independiente (¡gracias a jgarzik!) y el parche 'getwork' es ahora un cliente oficial, tengo una idea:

¡Unan a los pobres mineros CPU en un grupo y aumenten sus posibilidades de encontrar un bloque!

¿Cómo debería funcionar esto? Habría una página web en la que podrías registrarte, introducir la dirección de tu wallet y obtener la URL y tu rpcusuario/rpccontraseña personal para tus mineros CPU/GPU. Cuando comiences tu propio minado con esas credenciales, el servidor te enviará trabajo que no está siendo calculado todavía por otros miembros del grupo.

Pero cuando tu cliente encuentra un hash ganador, no obtienes la recompensa completa por bloque (50 BTC - "de ese momento"), sino solamente una parte proporcional, la cual calculaste. Cuando ofrezcas 1.000 khash/s durante un día, y el rendimiento del grupo completo sea de 20.000 khash/s y cueste dos días encontrar un bloque, tu

recompensa será (50/20/2=)1,25 BTC.

¿Ventajas? Cuando tienes un pobre ordenador independiente, necesitas esperar muchas semanas o incluso meses para encontrar una recompensa completa de 50 BTC. Cuando te unas a un grupo como éste, recibirás constantemente cantidades pequeñas de bitcoins cada día o cada semana (dependiendo del rendimiento completo del grupo).

¿Desventajas? Necesitas confiar en que la autoridad central (yo) no robará el bloque para sí mismo. Pero estoy bromeando por unas semanas y estoy asombrado con la idea de bitcoin, así que no planeo robar nada en este momento :-).

~~Otro problema posible es que alguien pida trabajo nuevo muy a menudo, pero en realidad no cuente hashes reales. En este caso parecería que tiene una CPU muy potente y obtendría una gran parte de la recompensa si el grupo encuentra un bloque. Pero hay una defensa sencilla frente a los tramposos: el servidor central enviará a veces trabajo que lleve a un hash 'ganador'. El trabajador que no devuelva ese hash como coincidencia será expulsado permanentemente (inicio de sesión/contraseña y dirección IP)~~. Esto se ha resuelto de forma satisfactoria dejando a los mineros calcular la prueba de trabajo. No es posible de ninguna manera pertenecer a un grupo y no contar hashes.

¿Está interesado?

Re: Minado cooperativo

Publicado por ribuck, 27 de noviembre 2010, 10:21:02 PM

> Cita de grandilu, 27 de noviembre 2010, 10:21:27 PM
>
> ---
>
> Me parece que el minado cooperativo es una tarea dura, porque la honestidad de los participantes tiene que comprobarse. ¿Qué evita que alguien ejecute una versión modificada del cliente, que estuviese generando bitcoins solamente para él, mientras recibe bitcoins de otros?

<suspiro>

O no he sabido explicar muy bien por qué no hay posibilidad de hacer trampa, o estoy equivocado. Pero si estoy equivocado, nadie ha publicado una objeción específica. Así que trataré de explicarlo nuevamente, presentando un diseño específico que muestre que un cliente deshonesto no puede hacer trampa.

Supongamos que opero un servidor minería agrupado como pool, y recluto algunos clientes que desean unir al pool el minado de ellos.

Mi servidor le pide a cada cliente que haga algo de hashing. Pide a cada cliente que envíe cualquier hash que encuentre que esté por encima de un cierto límite de dificultad. El servidor escoge una dificultad que es un cuadragésimo (1/40) del nivel de dificultad “oficial” anual.

Mi servidor recibe un flujo constante de hashes candidatos enviados por los clientes mineros remotos. De vez en cuando, uno de esos hashes cumple con el nivel de dificultad oficial y mi servidor puede generar un bloque, lo que hace ganar 50 bitcoins a mi servidor.

Ahora distribuyo bitcoins a los clientes mineros remotos, a razón de un bitcoin por cada hash que se envió para el bloque actual que estuviera en o por encima de 1/40 del nivel oficial de dificultad.

A la larga, esperaría distribuir 40 monedas de cada 50 que genera mi servidor, aunque habría fluctuaciones de bloque a bloque. ¡Nada en este esquema requiere que los clientes sean honestos, porque no hay forma de que un cliente deshonesto pueda engañar!

El cliente está calculando hashes que van a generar 50 BTC para mi servidor. Esos mismos hashes no son de ninguna utilidad para un cliente deshonesto. No se pueden ser usados para generar 50 BTC para el cliente deshonesto, porque se necesita un código hash diferente para codificar el pago de los bitcoins generados para alguien más. Y si el cliente deshonesto trata de hacer trampa generando hashes que van a pagar los bitcoins generados por ellos mismos, entonces los códigos hash que envían no se validarán en mi servidor y no distribuiré ninguna parte de los pagos a ellos.

Por tanto, este sistema no requiere absoluta confianza del cliente.

Este sistema tampoco requiere que el cliente de minería tenga fe en que el servidor sea honesto. Si el servidor anuncia que está pagando 1BTC por cada hash que es al menos 1/40 del nivel de dificultad oficial, entonces cada cliente que envía un hash "fácil" para un bloque que se generó puede verificar que recibió su bitcoin. Cualquier fraude aparecería inmediatamente.

RE: MINADO COOPERATIVO

Publicado por satoshi, 28 de noviembre 2010, 04:03:30 PM

La descripción de ribuck ha dado en el clavo.

Los operadores de pool pueden modificar su getwork para tomar un parámetro adicional, la dirección a la que envían su parte.

Lo más fácil para el operador del pool sería esperar hasta que se encuentre el siguiente bloque y dividirlo proporcionalmente como sigue:

intentos del usuario/intentos totales de todos

Eso sería más fácil y seguro para empezar. También tiene la ventaja de que múltiples aciertos del mismo usuario pueden combinarse en una transacción. Muchos de sus aciertos generalmente serán de las mismas personas.

El modo de gratificación instantáneo sería pagar una cantidad fija por cada intento inmediato, y el operador toma el riesgo de la aleatoriedad de tener más o menos intentos antes de que se encuentre un bloque.

Sea como sea, el usuario que envía el acierto que resuelve el bloque debe obtener una cantidad extra por encima del resto, como de 10 BTC.

Los nuevos usuarios podrían realmente no necesitar en realidad el software Bitcoin. Podrían descargar un minero, crear una cuenta en mtgox o mybitcoin, ingresar su dirección de depósito en el minero y señalarlo en el servidor del grupo de cualquier persona. Cuando el minero

anuncia que encontró algo, un momento después aparecen algunas monedas en su cuenta.

Mineros escritores se aseguran mejor que nunca de tener falsos-positivos intentos. Los usuarios dependerán de eso para verificar si el operador del pool los está engañando. Si el minero dice erróneamente que encontró algo, los usuarios buscarán en su cuenta, no encontrarán nada, y se enfadarán con el operador del pool.

65

Sobre el Uso de Bitcoin por WikiLeaks

Traducción por **Alex Viñas Salles**

A FINALES DEL 2010, los gobiernos mundiales presionaban a WikiLeaks cortando todas sus posibles fuentes de ingresos, principalmente las donaciones electrónicas realizadas a través de tarjetas de crédito y PayPal.

Cuando PayPal anunció que bloquearía el servicio a WikiLeaks, Satoshi escribió que, en su opinión, Bitcoin aún no estaba preparado para reemplazarlo.

http://www.wired.com/threatlevel/2010/12/paypal-WikiLeaks/

¿Información de contacto de WikiLeaks?

Publicado por genjix, 10 de noviembre 2010, 12:49:16 PM

Hola, me gustaría enviar una carta a WikiLeaks sobre Bitcoin desde que desafortunadamente han tenido varios problemas con incautaciones de fondos en el pasado.

http://wikileaks.org/media/support.html

¿Alguien sabe dónde enviarles un mensaje?

Re: Información de contacto de WikiLeaks?

Publicado por wumpus, 04 de diciembre 2010, 08:47:59 AM

PayPal acaba de bloquearles, también están intentando que varios bancos estadounidenses hagan lo mismo. Este, sería un buen momento para abrir donaciones a través de bitcoin.

Re: ¿Información de contacto de WikiLeaks?

Publicado por RHorning, 04 de diciembre 2010, 10:17:44 PM

> Cita de: Hal, 04 de diciembre 2010, 08:43:07 PM
>
> Mirando el lado positivo, si Bitcoin ha sido conocida como la moneda de WikiLeaks, siendo atacada por gobiernos de todas partes del planeta, al menos, volveremos a tener nuestra página de Wikipedia!
>
> ---

Esto es muy cierto. Así no habría escasez de "fuentes confiables" sobre Bitcoins en ese punto. Probablemente sería portada de todos los periódicos mundiales, así como objeto de extensos debates en talk show de radio y otras redes de comunicación también.

Yo ya estoy en el punto de, “adelante” en relación con WikiLeaks. Fijaros que firmo con mi nombre real en vez de un pseudo anónimo y estoy dispuesto a decir “adelante”, a pesar de poder ser asociado con el proyecto Bitcoin. He tenido a la policía en mi casa sin mi permiso, haciendo todo tipo de cosas estúpidas, así que para mí, esa línea ya ha sido traspasada. También estoy conectado políticamente con el suficiente número de personas como para que, si me pasara algo, se dieran cuenta y actuarán.

Es moralmente correcto apoyar a WikiLeaks, y si aceptan unos pocos de mis Bitcoins, no sólo quiero donar, también predicar por el mundo que pueden hacer donaciones a WikiLeaks a través de Bitcoin.

No puede hablar por todo el mundo en la comunidad de Bitcoin, pero estoy hablando por mí mismo en este aspecto, y no tengo ningún miedo a lo que me puede hacer el gobierno de los Estados Unidos por estar apoyando financieramente a WikiLeaks. Si ocurriera algo, demostraría que ya no vivo bajo un gobierno constitucional. Si el gobierno de los Estados Unidos quiere lanzar esa piedra sobre su tejado, que así sea. En caso de que el gobierno de los Estados Unidos me mate o me encarcele, yo mismo establecería una manera para que la comunidad lo averiguara. No creo que llegue a ese punto, pero no me importa si es así.

Si tuviera que "votar" en este asunto, alentaría a que la comunidad tome cartas en el asunto, como lo hicimos con EFF, y aconsejaría a WikiLeaks que pongan en su web direcciones de Bitcoin para realizar donaciones. Eso traería nueva sangre a la comunidad, y puede ser beneficioso para WikiLeaks también. Dejemos a WikiLeaks la decisión de usar o no Bitcoin. En cuanto al interés del gobierno sobre Bitcoin, sabíamos que tarde o temprano iba a ocurrir, ¿así que por qué estamos luchando contra algo inevitable? Cualquier cosa más allá de una investigación discreta, lo único que conseguirá es despertar más interés en Bitcoin en la gente, lo que terminará ayudando al proyecto aún, más. El proyecto no puede morir, solo puede ralentizarse un poco el ritmo de crecimiento en este momento, y lo más probable es que su adopción se vea acelerada gracias a cualquier tipo de publicidad que se hiciera.

La única posible preocupación que tengo es el estado actual del protocolo. Si eso, con el gran flujo de gente nueva en la comunidad de Bitcoin también sería beneficioso, y lo peor que pudiera ocurrir es que Bitcoin se rompa de tal manera, que una nueva criptomoneda surja para resolver los problemas que tenga Bitcoin. La idea es que una criptomoneda pueda persistir, y esta idea es muy difícil de censurar.

Básicamente, adelante. Fomentemos que WikiLeaks utilice Bitcoin, estoy dispuesto a asumir los riesgos o consecuencias de dicho acto.

- Robert S. Horning

Logan, Utah

Re: ¿Información de contacto de WikiLeaks?

Publicado por Satoshi, 05 de diciembre 2010, 09:08:08 AM

> Cita de: RHorning, 04 de diciembre 2010, 10:17:44 PM
>
> Básicamente, adelante. Fomentemos que WikiLeaks utilice Bitcoin, estoy dispuesto a asumir los riesgos o consecuencias de dicho acto.

No, “adelante”, no.

El proyecto necesita crecer gradualmente para el que software pueda ser fortalecido por el camino.

Hago este llamamiento a WikiLeaks para que no intenten utilizar Bitcoin. Bitcoin es una pequeña comunidad beta en su infancia. No sacarían más que un simple intercambio de monedas, y el fuego de esta situación, probablemente nos destruiría en el estado actual.

66

Sobre un Servidor de Nombre de Dominio Distribuido

Traducción por **Alex Viñas Salles**

ALGUIEN SUGIRIÓ crear un clon de Bitcoin (una moneda alternativa) con el fin de crear una red distribuida, de punto a punto, para crear un sistema de nombres de dominios - DNS (por sus siglas en Inglés de "Domain Name Server System"). Además de contener monedas, almacenar transacciones en la cadena de bloques, también contendría información DNS, así como actualizarse a través de nuevas transacciones.

Esta moneda alternativa aún existe al día de hoy y se llama Namecoin (ver http://namecoin.org/), la que permite a las personas registrar un nombre de dominio que finalice con ".bit" y asociarlo con una dirección IP. Satoshi comparte su opinión sobre este tipo de sistemas. Uno de los mayores beneficios de tener un sistema de nombres de dominios descentralizado, es el poder resistir intentos gubernamentales de interrumpir las comunicaciones de sus ciudadanos a través de internet, como hemos visto el 2011 en Egipto.

Re: BitDNS y Generalizando Bitcoin

Publicado por satoshi, 09 de diciembre 2010, 09:02:42 PM

Creo que BitDNS podría ser una red completamente separada con una cadena de bloques separada, pero compartiría la potencia de la CPU con Bitcoin. La única superposición sería hacer que los mineros puedan buscar pruebas de trabajo para ambas redes simultáneamente.

Las redes no necesitarían ninguna coordinación. Los mineros se suscribirían a ambas redes en paralelo. Explorarían el SHA de tal manera que si encuentran el punto, potencialmente resuelvan ambos a la vez. Una solución puede ser solo para una de las redes si una red tiene una dificultad menor.

Creo que un minero externo podría llamar a la función getwork en ambos programas y combinar el trabajo. Podría empezar obteniendo el trabajo en Bitcoin para usarlo en BitDNS en un trabajo combinado.

En vez de tener una fragmentación, las redes pueden compartir y aumentar el poder computacional total (CPU). Así se resolvería el problema de tener múltiples redes, y el peligro para ambas, si el poder computacional disponible se une sólo a una red. En su lugar, todas las redes del mundo podrían compartir poder computacional combinado (CPU), para incrementar el poder total de la red. Sería más fácil para las redes más pequeñas, comenzar utilizando una base de mineros ya existente.

Re: BitDNS y Generalizando Bitcoin

Publicado por nanotube, 09 de diciembre 2010, 09:20:40 PM

> Cita de: satoshi el 09 de diciembre 2010, 09:02:42 PM
>
> Creo que BitDNS podría ser una red completamente separada con una cadena de bloques separada, pero compartiría la potencia de la CPU con Bitcoin. La única superposición sería hacer que los mineros

> puedan buscar pruebas de trabajo para ambas redes simultáneamente.
>
> ---

Suena extremadamente bien en la teoría…

> Cita de: satoshi, 09 de diciembre 2010, 09:02:42 PM
>
> Las redes no necesitarían ninguna coordinación. Los mineros se suscribirían a ambas redes en paralelo. Explorarían el SHA de tal manera que si encuentran el punto, potencialmente resuelvan ambos a la vez. Una solución puede ser solo para una de las redes si una red tiene una dificultad menor.
>
> Creo que un minero externo podría llamar a la función getwork en ambos programas y combinar el trabajo. Podría empezar obteniendo el trabajo en Bitcoin para usarlo en BitDNS en un trabajo combinado.
>
> ---

Entonces el minero tendría que básicamente hacer “trabajo extra”, y si no hay recompensa por parte de bitdns minados que provienen del trabajo extra (que desde luego, ralentizaría el trabajo de la red principal de Bitcoin), ¿cuál sería el incentivo de un minero para incluir bitdns (y cualquier otro tipo de cadenas paralelas (sidechains)?

Con muchas ganas de escuchar tus pensamientos sobre el tema : -)

Re: BitDNS y Generalizando Bitcoin

Publicado por satoshi, 09 de diciembre 2010, 10:46:50 PM

> Cita de: nanotube, 09 de diciembre 2010, 09:20:40 PM
>
> Entonces el minero tendría que básicamente hacer “trabajo extra”, y si no hay recompensa por parte de bitdns minados que provienen del trabajo extra (que desde luego, ralentizaría el trabajo de la red principal de Bitcoin), ¿cuál sería el incentivo de un minero para incluir

bitdns (y cualquier otro tipo de cadenas paralelas (sidechains)?

El incentivo es obtener las recompensas por la cadena paralela, con el mismo trabajo.

¿Mientras está generando bitcoins, por qué no obtener también de manera gratuita unos nombres de dominio por el *mismo trabajo*?

Si actualmente generas 50 BTC a la semana, ahora podría obtener 50 BTC y también algunos dominios.

usted tiene una pieza de trabajo. Si la resuelve, va a resolver un bloque tanto en Bitcoin como en BitDNS. El concepto, es que las dos pruebas de trabajo están atadas conjuntamente por un árbol de Merkle. Para entregarlo a Bitcoin, rompe la rama de BitDNS, y para entregarlo a BitDNS, se rompe la rama de Bitcoin.

En la práctica, para readaptarlo para Bitcoin, la parte de BitDNS tendría que tener, quizás, unos 200 bytes extras, lo cual no es gran problema. Está hablando de 50 dominios por bloque, lo que reduciría los 200 bytes por bloque para poder ser compatible con las versiones anteriores. Podríamos programar un bloque en un futuro lejano para que cuando Bitcoin se actualice a una versión de estructura más moderna del árbol de Merkle, si lo que de verdad importa, es ahorrarnos unos cuantos bytes.

Nótese que las cadenas están por debajo de este nuevo árbol de Merkle. Esto es, cada Bitcoin y BitDNs tienen sus propios enlaces a la cadena dentro de los bloques. Esto se invierte de la asignación del servidor de marca de tiempo común, donde la cadena que está por encima del árbol Merkle, porque se crea una cadena maestra común. Esto es, dos asignaciones de marcas de tiempo que comparten una cadena.

Re: BitDNS Y Generalizando Bitcoin

Publicado por satoshi, 10 de diciembre 2010, 05:29:28 PM

Acumular todos los sistemas quorum de pruebas de trabajo bajo un mismo conjunto de datos no es escalable.

Bitcoin y BitDNS pueden usarse por separado. Los usuarios no tendrían por qué descargarse ambas para poder usar una u otra. Es posible que los usuarios de BitDNS no quieran descargar todo lo que las siguientes redes no relacionadas decidan acumular.

Las redes necesitan tener destinos diferentes. Los usuarios de BitDNS pueden ser libres de agregar cualquier característica de datos sin importar el tamaño, dado que relativamente pocos nombres de dominios registrados son necesarios, mientras que los usuarios de Bitcoin podrían ser cada vez más tiranos a la hora de limitar el tamaño de los bloques de la cadena, para que sea fácil de manejar para muchos usuarios y pequeños dispositivos.

El miedo a comprar dominios de manera segura con Bitcoins es una cuestión falsa. Es fácil intercambiar Bitcoin por otros productos no tan repudiables.

Si aun sigues preocupado por esto, que sepas que es criptográficamente posible hacer un intercambio sin riesgo. Las dos partes establecen transacciones en las dos cadenas, de tal manera que cuando se firman las transacciones, la parte que firme la segunda transacción activará la liberación de ambas transacciones en las cadenas. La otra parte firmante no puede liberar la transacción hasta que libere la otra, y viceversa.

RE: BITDNS Y GENERALIZANDO BITCOIN

Publicado por Hal, 10 de diciembre 2010, 07:14:04 PM

Satoshi, ¿estas respaldando la idea de que cadenas de bloques adicionales crearían su propio tipo de monedas, intercambiando estas con bitcoins en las casas de cambio? ¿Las monedas de cadena específica serían utilizadas para recompensar a los mineros de esas cadenas, además de comprar una serie de derechos o privilegios sobre un dominio de esa cadena?

Re: BitDNS y Generalizando Bitcoin

Publicado por satoshi, 10 de diciembre 2010, 07:55:12 PM

> Cita de: Hal, 10 de diciembre 2010, 07:14:04 PM
>
> ---
>
> cadenas de bloques adicionales crearían su propio tipo de monedas, intercambiando estas con bitcoins en las casas de cambio? ¿Las monedas de cadena específica serían utilizadas para recompensar a los mineros de esas cadenas, además de comprar una serie de derechos o privilegios sobre un dominio de esa cadena?
>
> ---

Exacto, el tipo de cambio entre el dominio y el bitcoin sería flotante.

Un intervalo mayor de 10 minutos sería lo apropiado para BitDNS.

Hasta ahora, en esta discusión ya ha habido bastantes requisitos de datos para gestiones internas. Sería mucho más fácil si pudieras usar libremente el espacio que necesita sin preocuparse por costes muy altos para adquirir espacio en la cadena de Bitcoin. Algunas transacciones:

Cambiar el registro de IP.

Cambio de nombre. Un dominio objeto podría dar derecho a un dominio, pudiéndose cambiar el nombre a tu gusto, siempre y cuando que ya no exista ese nombre. Esto incentivaría a los usuarios a liberar nombres que ya no quieren. Los dominios generados empiezan en blanco, para que los mineros puedan venderlos a la gente que quiere registrar lo que quieran.

Renovaciones. Pueden ser gratuitas, o quizás requieran consumir otro dominio objeto para renovarlos. En ese caso, las monedas de dominios objeto (¿domaincoins?) podrían representar el derecho a poseer un dominio durante un año. La comisión se lo llevan los mineros en las comisiones del siguiente bloque.

Re: BitDNS y Generalizando Bitcoin

Publicado por Hal, 10 de diciembre 2010, 08:12:02 PM

OK, entonces si va a haber bitdnscoins (aka DCCs, DomainChain Coins) tienen que ser útiles para algo. Si no, los mineros de BitDNS van a llenar cada bloque con sus propios nombres para el dominio, en vez de reemplazarlos con los nombres de los otros usuarios a cambio de una comisión de una transacción realizada en una moneda sin uso.

Las reglas tienen que obligarte a gastar una cantidad x de bitdnscoins/DCCs para poder registrar tu dominio y/o hacer transacciones en BitDNS. Esa es la única manera de hacer que la moneda tenga valor y sea atractiva.

(Podríamos hacer como en Bitcoin y decidir que solo se creen un total de 22 millones DCCs, por lo que su escasez haría que tuvieran valor, como los bitcoins. Pero, eso parece débil.)

Re: BitDNS y Generalizando Bitcoin

Publicado por Satoshi, 10 de diciembre 2010, 08:19:39 PM

Estoy de acuerdo. Todas las transacciones, cambios de IP, renovaciones, etc., tendrían que tener una comisión para los mineros.

Puedes considerar una cierta cantidad de trabajo para generar un dominio, en vez de una cantidad fija en circulación. El trabajo por dominio podría ir ligado al crecimiento de la Ley de Moore. De tal manera que el número de dominios se podría crecer con la demanda, así como el número de personas que lo utilizan.

Re: BitDNS y Generalizando Bitcoin

Publicado por dtvan, 11 de diciembre 2010, 07:43:08 AM

Después de leer todo el hilo, tengo un par de comentarios que creo que puedan ser útiles:

1) Todas las personas del hilo están decididas a reemplazar toda la infraestructura actual DNS de una tacada, siendo esto, bajo mi punto de vista, el enfoque erróneo. El problema real con el sistema DNS al día de hoy, es que alguien es dueño de la raíz. Al final del día, tienes que confiar en ICANN. El sistema DomainChain/BitDNS debería estrictamente enfocarse en establecer la posesión del nombre de los dominios. Todo lo que hay que rastrear es quien es el poseedor de la clave A que posee el dominio foo.bar. Una vez que hayamos establecido dicha confianza compartida, podemos apoyar diferentes infraestructuras DNS que pueden implementarse independientemente para este proyecto. Cualquier sistema nuevo que se cree utilizará DomainChain/BitDNS para establecer que llave posee el dominio, y permitir escribir archivos sobre el mismo dominio a ese individuo. Esto funciona correctamente, dado que todos los participantes en el sistema pueden validar que todos los archivos que han buscado son válidos. Ahora mismo es muy fácil desanimarse por todos los detalles de cómo funcionaría el manejo de los registros DNS, cuando todo lo que hay que hacer es establecer una autoridad distribuida de confianza para que pueda crear la raíz de DNSSEC, un nuevo DNS p2p o lo que sea.

También, estoy pensando, que podría usarse para resolver el problema de CA con HTTPS, dado que, al firmar tu certificado con la misma llave, demostrarías que has llegado al servidor correcto. Pero, estoy divagando…

2) Limitar el TLDs debería ser un requisito. Si este sistema no interopera con la actual infraestructura DNS, evitando colisiones en los nombres, minará la confianza que se está tratando de generar. Aunque no estoy muy seguro sobre si estoy listo para usar un sistema DNS distribuido si alguien nuevo puede registrar www.mylocalbank.com y causar estragos. Humildemente, sugiero .web como el TLD a usar, pero

cualquier cosa funcionaría siempre y cuando sea corto y no esté actualmente en uso.

Ahora mismo el foco debería estar en sacar adelante la idea y llevarla a cabo de tal manera que no genere conflicto con el sistema existente. Si el sistema llega a ser dominante en algún momento y necesite abordar TLDs adicionales, este es un "problema" que puede ser tratado entonces.

3) Personalmente, creo que expirar los nombres de dominios es el camino a seguir. Aun con los actuales precios caros de renovación al día de hoy, hay una gran cantidad de basura ahí fuera. No puedo imaginar lo malo que llegaría a ser si tuvieras un dominio para toda la vida. No es pedir mucho, que si quieres renovar el dominio, tienes que renovarlo periódicamente, especialmente esto no tendría que ser el timo que es el sistema actual.

Me gustaría acabar, diciendo que es un tema bastante emocionante. He leído cantidad de ideas diferente sobre cómo resolver el problema de los DNS, y esta es la primera vez que creo que una idea podría resolverlo (y no para reemplazar a ICANN con un nuevo dictador benevolente).

Re: BitDNS y Generalizando Bitcoin

Publicado por satoshi, 10 de diciembre 2010, 08:19:39 PM

@dtvan: tres puntos excelentes

1. Los registros de IP no necesitan estar en la cadena, solo tiene que registrar la función no el DNS. Y ya tienes el problema de CA resuelto, listo.
2. Escoge un TLD, .web +1
3. El vencimiento y los costos significativos son muy importantes

---

Cita de: Joe, 11 de diciembre 2010, 10:53:58 AM

Sin embargo, si pienso más sobre el tema, ahora apoyo la inclusión de coinbases adicionales / sistemas de rastreo sobre la red principal. La

> razón para hacer esto no es para diluir el poder de CPU entre distintas redes. Queremos una red fuerte, así que la red debería ser versátil.

Evitar la fragmentación del poder computacional CPU ya no es un problema. Redes/cadenas independientes pueden compartir poder computacional sin necesidad de compartir mucho más. Ver http://bitcointalk.org/index.php?topic=1790.msg28696#msg28696 y http://bitcointalk.org/index.php?topic=1790.msg28715#msg28715

> (Nota, dos de los anteriores posts de Satoshi están incluidos en este hilo)
>
> Otro hilo tratando el mismo el tema apareció:

Re: Confusión en las comisiones de BitDNS

Publicado por galeru, 09 de diciembre 2010, 07:45:38 PM

Bastante del debate actual sobre incluir BitDNS o BitX asume que los mineros incluirán transacciones o no, basándose en algunas condiciones muy finas, mientras que ninguna parte del código standard incluya algún tipo de implementación que permita a los no programadores poder tomar decisiones de ese calibre. ¿Cómo podría yo, usuario, averiguar qué tipo de comisiones pueden ir en cada transacción?

Re: Confusión en las comisiones de BitDNS

Publicado por jgarzik, 09 de diciembre 2010, 11:07:04 PM

> Cita de: davout, 09 de diciembre 2010, 09:08:55 PM
>
> ---
>
> Me pregunto sobre el siguiente ejemplo:
>
> Si transmito una transacción, enviando X monedas a alguna dirección.

> Esta no es incluida en los bloques durante un tiempo porque no tiene una comisión.
>
> ¿Hay alguna manera de cancelar la transacción y transmitirla de nuevo esta vez con una comisión?
>
> ---

Mira la discusión sobre el tiempo de bloqueo (https://bitcointalk.org/index.php?topic=1786.msg22119#msg22119) para reemplazar la transacción.

RE: CONFUSIÓN EN LAS COMISIONES DE BITDNS

Publicado por satoshi, 09 de diciembre 2010, 11:58:54 PM

Sin hora de cierre.

Hay un posible diseño para un futuro lejano:

Intencionadamente se escribe un doble gasto. Puede escribirlo con la misma entrada y salida, pero esta vez incluyendo una comisión. Cuando su doble gasto se incluye en el bloque, el primer gasto se vuelve inválido. El pagador no se da cuenta, porque en el momento en que la nueva transacción es válida, la vieja se vuelve inválida, simplemente la nueva transacción ocupa su lugar.

Es más fácil decir que de implementar. Habría una cantidad importante de trabajo para desarrollar la opción de que un cliente escriba correctamente un doble gasto, manejando las dos versiones en la cartera (wallet) hasta que se escoja una, manejando todas las cuestiones. Cada suposición que existe en el código asume que no intentas hacer un doble gasto.

Sería necesario hacer algunos cambios en la parte del minero de Bitcoin también, para poder hacer posible un doble gasto dentro del pool de transacciones, pero solo estrictamente si las entradas y salidas concuerdan, y la comisión de la transacción es más alta. Actualmente, el doble gasto no puede aceptarse en el pool de transacciones, por lo que

cada nodo es testigo de que transacción ha tenido lugar antes y han trabajado sobre esta para incluirla en el bloque.

67

Artículo de *PC World* sobre Bitcoin y WikiLeaks Pateando el Avispero

Traducción por **Alex Viñas Salles**

A LA LUZ DE LOS PROBLEMAS que WikiLeaks estaba trayendo en primer plano y el posible rol que Bitcoin podría desempeñar ayudando a financiar WikiLeaks, *PC World* publicó un artículo relacionado con Bitcoin. Claramente, Bitcoin estaba empezando a generar atención en la prensa. Lo que es interesante, son los comentarios de Satoshi en referencia a WikiLeaks "pateando el avispero". Aquí está el link al artículo de PC World, junto con los comentarios de Satoshi.

"¿Podría el Escándalo de WikiLeaks, Llevar a Una Nueva Moneda Virtual?"

http://www.pcworld.com/article/213230/could_wikileaks_scandal_lead_to_new_virtual_currency.html

Re: Artículo de PC World sobre Bitcoin

Publicado por satoshi, 11 de diciembre 2010, 11:39:16 PM

Hubiera estado bien acaparar toda esta atención en otro contexto. WikiLeaks ha dado una patada al avispero, y ahora el enjambre viene hacia nosotros.

68

Último Post de Satoshi en el Foro: Lanzamiento de Bitcoin 0.3.19

Traducción por **Alex Viñas Salles**

DIECINUEVE HORAS después del post sobre el "Avispero", Satoshi escribió su último post en el fórum antes de retirarse de la "vida pública". Hizo el post en *bitcointalk.org*. Fue su último post antes del que hizo en marzo de 2014 en el foro p2pfoundation.

Añadidos algunos límites a la denegación de servicio, eliminado el modo seguro (0.3.19)

Publicado por satoshi, 12 de diciembre 2010, 06:22:33 PM

Hay más trabajo que hacer en cuanto a la denegación de servicio, pero estoy montando algo rápido de lo que tengo hasta ahora, por si acaso es necesario, antes de aventurarnos en ideas más complejas. Esta versión es la versión número 0.3.19.

-Añadidos algunos controles de denegación de servicio

Como Gavin y yo hemos dicho claramente en otras ocasiones, el software no es resistente a un ataque de denegación de servicio. Esto es una

mejora, pero aún así existen más formas de atacar que las que puedo contar.

Dejo la parte de -limitfreerelay como un switch por ahora y ahí está en caso de ser necesaria.

-Eliminación de las alertas de “modo seguro”

Las alertas sobre el “modo seguro” fueron una medida temporal después del bug de desbordamiento de la versión 0.3.9. Podemos decir que solo queremos que los usuarios puedan solo ejecutar con “-disablesafemode”, pero es mejor no tenerlo por el mero hecho de las apariencias. Nunca fue planeado como característica para el largo plazo. El modo seguro aún puede ser activado al ver una cadena invalida más larga (mayor prueba de trabajo total).

Versión

http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/

El 14 de marzo del 2014, fue el último post de Satoshi en el foro p2pfoundation, realizado el 7 de marzo del 2014:

No soy Dorian Nakamoto

Esto fue en respuesta a la revista que publicó haber identificado a Satoshi Nakamoto, creador de Bitcoin, como un hombre que vivía en California con el nombre de Dorian Satoshi Nakamoto.

69

Correos Electrónicos a Dustin Trammell

Traducción por **Jose Luis Abia**

LOS SIGUIENTES son intercambios directos de correo electrónico entre Satoshi Nakamoto y Dustin Trammell, quien generosamente los ha puesto a disposición para su publicación.

Email 1—Sellado de tiempo y maduración de bitcoin

Este primer intercambio se refiere al servicio de registro del sellado de tiempo y a la madurez de la minería de Bitcoin. Estos se discutieron más tarde en un foro público, pero Satoshi se refirió a ellos primero en una conversación privada con Dustin Trammell.

De: "Satoshi Nakamoto" satoshi@vistomail.com

Para: dtrammell@dustintrammell.com
Fecha: martes, 13 de enero 2009, 02:33:28 +0800
Asunto: Re: Bitcoin v0.1 lanzado

> Actualmente estoy leyendo tu documento. En la sección del sellado de tiempo del servidor, mencionas noticias y Usenet, por lo que pensé que podrías estar interesado en esto si aún no lo has visto:
>
> http://www.publictimestamp.org/

Gracias, no lo había visto. Se ve que está muy bien presentado.

Hubo uno más antiguo que se estuvo ejecutando durante mucho tiempo y que publica sus hashes en Usenet. Me sorprende que este no use Usenet, aunque es un poco difícil acceder a Usenet de manera automática estos días. Si pudieran obtener una revista o periódico para publicar sus hashes, sería mucho más fácil en la corte para sus propósitos. Bitcoin y todos los servidores de sellado de tiempo comparten la funcionalidad básica de recopilar elementos periódicamente en bloques y convertirlos en hashes en una cadena.

> Por cierto, actualmente también estoy ejecutando el código alfa en una de mis estaciones de trabajo. Hasta el momento tiene dos mensajes "Generados", sin embargo, el campo "Crédito" para ellos es 0.00 y el saldo no ha cambiado. ¿Se debe esto al requisito de edad/madurez para que una moneda sea válida?

Correcto, el campo de crédito permanece a 0.00 hasta que madure, entonces será 50.00. ¿Crees que sería más claro si dejara en blanco el campo de crédito hasta que madure? Debo poner algo de texto en los detalles de la transacción (cuando haces doble click en él) explicando cómo funciona. (¿Era obvio que puedes hacer doble click en una línea para obtener más información?)

Asegúrate de actualizar a v0.1.3 si aún no lo has hecho. Esta versión realmente ha estabilizado las cosas.

Satoshi

Email 2—Continuación

De: "Satoshi Nakamoto" satoshi@vistomail.com

Para: dtrammell@dustintrammell.com
Fecha: martes, 13 de enero 2009, 15:55:13 +0800
Asunto: Re: Bitcoin v0.1 lanzado

> De hecho, publique los bloques de hash en un grupo de Google llamado 'proof-hashes', por lo que el resultado es similar si se publicara en Usenet.
>
> http://groups.google.com/group/proof-hashes
>
> Desde que administro ese grupo, y su único propósito es archivar hashes de prueba de trabajo, siéntete libre de unirte a una cuenta para que tu sistema publique también allí si lo deseas.

Bien, estaba buscando un grupo como ese en Usenet en un punto para ver qué usaría si lo necesitara, y nada encajaba realmente. Estoy seguro de que es mucho más fácil publicar en grupos de Google.

Hay algunos escenarios en los que un Usenet o grupo de Google podría usarse como una defensa suplementaria. Bitcoin está en su punto más vulnerable al principio, cuando la potencia total de CPU de la red es pequeña. Eso se compensa con el hecho de que el incentivo para atacar también es bajo cuando es pequeña.

Con suerte funcionará la solución fácil de solo crecer y superar esa etapa. De lo contrario, hay formas en que un grupo de Google podría ayudar, si es que realmente llegara a esa situación.

> La moneda electrónica y la criptografía son dos cosas que me interesan mucho, por lo que supondrás que me atrajo este proyecto inmediatamente cuando lo vi publicado en la lista de correo electrónico de Criptografía. Siéntete libre para pedirme comentarios o para probar nuevas funciones. Estaré encantado de ayudarte.

¡Definitivamente tenemos intereses similares!

Sabes, creo que había mucha más gente interesada en los 90´s, pero después de más de una década de fallos en sistemas basados en la Confianza de Terceras Partes (Digicash, etc.), lo ven como una causa perdida. Espero que puedan distinguir, que esta es la primera vez que sé que estamos intentándolo con un sistema que no está basado en la confianza.

> Cuando las monedas están maduras, ¿se generará una nueva transacción de "crédito" o ¿se actualizará ésta en el campo de crédito en la línea de transacción?
>
> ---

La línea de transacción existente cambiará.

> Al abrir la versión 0.1.3, las cuatro entradas de mi transacción aún dicen 'sin confirmar', pero ahora las descripciones dicen 'Generado (no aceptado)'.
>
> ¿Esto significa que algún otro nodo había extendido la cadena primero y mis monedas se generaron en una rama muerta? Si es así, ¿por qué la con anterioridad el software no detectó esto inmediatamente y comenzó a generar monedas en la rama ganadora? ¿Error en 0.1.0?
>
> ---

Tienes razón, lo siento. Es el error que se solucionó en 0.1.3.

El hilo de comunicaciones se bloquearía, por lo que deberías conectar, pero se silenciará al cabo de un rato. Cuando encuentres un bloque, no podrás transmitirlo a la red, por lo que no entraría en la cadena. No estarías recibiendo nada para saber que la red continuaba sin ti, hasta que la reiniciaras.

Este error también es lo que causó que bitcoin.exe fallara al cerrarse. El hilo de comunicaciones se bloqueaba y no podías salir. Bitcoin realiza un apagado cuidadoso en caso de que se encuentre en medio de una transacción importante, pero actualmente es completamente seguro matarlo.

Esto está todo arreglado en 0.1.3. Si me das tu IP, te enviaré algunas

monedas.

> Otra pregunta que tenía... ¿Qué impide que el único nodo con la mayor potencia de CPU genere y conserve la mayoría de los BitCoins?
>
> Si cada nodo funciona independientemente de todos los demás, si uno es significativamente más potente que los demás, ¿no es probable que este nodo llegue a la solución correcta antes que otros nodos? Un nodo con poca potencia puede tener suerte de vez en cuando, pero si tienen una ventaja de potencia significativa, yo esperaría que la mayoría de los BitCoins sean generados por el nodo más potente?

No es como una carrera en la que si un automóvil es el doble de rápido, siempre gana. Un SHA-256 que tarda menos de un microsegundo, y cada invitado tiene una posibilidad independiente de éxito. La probabilidad de que cada computadora encuentre una colisión de hash es linealmente proporcional a su potencia de CPU. Una computadora que es la mitad de rápida obtendría la mitad de monedas.

> Voy a ver este tema y ver cómo va…..

Hazme saber cómo va. Si tienes algún problema con ello, envíame tu archivo debug.log. A menudo puedo descubrir qué salió mal solo con eso.

Satoshi

Email 3— Sobre el potencial de Bitcoin

Este intercambio parece indicar que Satoshi no esperaba una aceptación tan rápida de Bitcoin.

De: "Satoshi Nakamoto" satoshi@vistomail.com

Para: dtrammell@dustintrammell.com
Fecha: viernes, 16 de enero 2009, 03:15:14 +0800
Asunto: Re: Bitcoin v0.1 lanzado

> He tenido esa dirección por un tiempo, aunque espero que mi cliente dhcp tenga éxito renovandola y no perdiendo mi dirección. Ella cambia de vez en cuando, pero esa dirección debería ser buena por un tiempo.
>
> ---

Hay al menos un nodo cuya IP entrante que cambia continuamente dentro de la misma clase B. Quizás cada vez que se ejecuta el programa. No esperaba eso.

¿Te importa si pongo en CC el resto de esto a la lista bitcoin o a la de criptografía? Por cierto, la lista bitcoin es:

bitcoin-list@lists.sourceforge.net
página de suscripción/darse de baja:
http://lists.sourceforge.net/mailman/listinfo/bitcoin-list
Archivos:
http://sourceforge.net/mailarchive/forum.php?forum_ name=bitcoin-list.

> Dustin D. Trammell escribió:
>
> ---
>
> > Satoshi Nakamoto escribió:
> >
> > Sabes, creo que había mucha más gente interesada en los 90´s, pero después de más de una década de fallos en sistemas basados en la Confianza de una Tercera Parte (Digicash, etc.), lo ven como una causa perdida. Espero que puedan distinguir, que esta es la primera vez que sé que estamos intentándolo con un sistema basado en la no confianza.
> >
> > ---
>
> Sí, esa fue la característica principal que me llamó la atención. El verdadero truco será hacer que la gente realmente valore los BitCoins para que se conviertan en moneda.
>
> ---

Hal aludió de alguna manera la posibilidad de que se pudiera ver como una inversión a largo plazo. Me sorprendería que dentro de 10 años no utilicemos la moneda electrónica de alguna manera, ahora que sabemos una forma de hacerlo que inevitablemente no se va a atascar cuando el TTP se enfríe.

Incluso si no despega de inmediato, ahora está disponible para uso de cualquier persona que venga con un plan que necesita algún tipo de token o moneda electrónica. Podría comenzar en un sistema cerrado o un nicho pequeño como puntos de recompensa, donación de fichas, moneda para un juego o micropagos para sitios de adultos. Una vez que se pone en marcha, hay tantas aplicaciones por las que podrías pagar sin mucho esfuerzo unos centavos a un sitio web tan fácil como echar monedas en una máquina expendedora.

Ya se puede usar para pagar por el envío de correos electrónicos de pago. El envío de textos es redimensionable y se puede incluir el mensaje del tamaño que se desee. Se envía directamente al conectarse. El destinatario hace doble click en la transacción para ver el mensaje completo. Si alguien famoso recibe más correos electrónicos de los que puede leer, y aún le gustaría mantener una forma para que los fans se comuniquen con él, podrían configurar Bitcoin y dar la dirección IP en su sitio web. "Enviar X bitcoins a mi línea caliente en esta IP y leeré el mensaje personalmente".

Los sitios de suscripción que necesitan alguna prueba de trabajo adicional para su versión prueba gratuita y para que no se canibalicen las suscripciones podrían cobrar bitcoins por esta versión de prueba.

Satoshi.

Email 4— Sobre ataques y direcciones IP involucradas en el envío de bitcoins

De: "Satoshi Nakamoto" satoshi@vistomail.com

Para: dtrammell@dustintrammell.com
Fecha: viernes, 16 de enero 2009, 03:46:30 +0800
Asunto: Re: Algunos pensamientos. . .

Yo agrupo los ataques en dos clases:

1) Ataques que solo pueden ser realizados por alguien que esté dentro de la cadena de comunicación.

2) Ataques que cualquiera puede hacer en Internet desde cualquier lugar.

Tipo 1 te expone a personas de tu casa o empresa en tu LAN local, a los administradores de los ISP intermedios, y a la LAN en el lado del destinatario. El tipo 2 te expone a mil millones de personas que pueden elegir ser atacantes y obtener una economía de escala cuando desarrollan una técnica para atacar a múltiples víctimas.
Enviar una nueva clave pública, por solicitud de IP, por lo que sí, se es vulnerable al tipo 1 “hombre en el medio”. Si eso es una preocupación, enviar a una dirección de Bitcoin no tiene esa vulnerabilidad, aunque hay una pequeña elección en relación a la privacidad. Tengo la sensación de que la mayoría de las personas recibirán direcciones de Bitcoin de sitios web que no son SSL y correos electrónicos sin firmar, que ya son vulnerables a los tipos 1 y 2 a través de DNS tóxicas.

Una solución sería usar las direcciones IP y Bitcoin en el envío (tal vez 1.2.3.4-1Kn8iojk...), donde el destinatario use la clave pública de la dirección Bitcoin para firmar la nueva clave pública y probar que estás enviando a quién crees que eres. Si el sistema comienza a utilizarse con fines comerciales reales, ciertamente lo implementare. Otra solución es usar SSL.

Por ahora, es bastante obvio que si envías algo a una IP, no das ninguna otra información de identificación sobre el destinatario, por lo que estás enviando a ciegas a quien responda esa IP.
Otra característica para más adelante es una opción para encriptar tu

billetera.

> Sí entiendo cómo se hace eso correctamente, simplemente calculas la transacción dentro de la cadena de bloques y dejas que el supuesto destinatario la 'descubra', ¿correcto?.

Eso es correcto.

> Una alternativa podría ser permitir que los nodos de la red proporcionen un servicio de resolución, donde preguntan por la dirección de red de una dirección de BitCoin, y si ese nodo está conectado, y una vez que la red acuerda por consenso sobre dicha dirección, la aplicación de envío de BitCoin se conecta directamente allí.

Sería bueno solo necesitar la dirección de Bitcoin y tener la IP resuelta antes de salir a escena. Podría tener problemas de privacidad o denegación de servicio. Ciertamente antes de que otro método de envío sea implementado, ahora hay mucho tiempo para pensar detenidamente en el diseño y asegurarse de que sea de la mejor manera.

Satoshi

Email 5— Sobre la pérdida potencial y la necesidad de copias de seguridad

De: "Satoshi Nakamoto" satoshi@vistomail.com

Para: dtrammell@dustintrammell.com
Fecha: sábado, 17 de enero 2009, 02:32:48 +0800
Asunto: Re: Algunos pensamientos. . .

> Una cosa que viene a la mente sobre este tema es el de la potencial pérdida de BitCoins si tienes un fallo en el sistema. La aplicación no parece almacenar ningún dato en el directorio en el que se ejecuta, así

> que supongo que está almacenado en el registro y en otros lugares (aún no he descifrado el ProcessExplorer para verificarlo), por lo que puede ser una buena idea el que la aplicación pueda exportar todo lo que necesita para la recuperación a un archivo del que se podría hacer una copia de seguridad fuera del sistema.
>
> ---

Los archivos están en "%appdata%\Bitcoin", ese es el directorio para hacer una copia de seguridad. Los datos se almacenan en una base de datos transaccional DBM, por lo que deben estar a salvo de pérdidas si se produce un accidente o un fallo de energía.

%appdata% es de acceso restringido para cada usuario. La mayoría de los nuevos programas como Firefox almacenan sus archivos de configuración allí, a pesar del viento en contra de Microsoft al cambiar el nombre del directorio con cada versión de Windows y estar lleno de espacios y tanto tiempo ejecutándose fuera de la pantalla.

> Otra cosa que noté hoy es que si cierras la aplicación, parece que no cierra limpiamente los conectores de red (los TCP RST comienzan a volar). Probablemente es un elemento de baja prioridad para la lista de tareas a realizar (:
>
> ---

Justo ahora agregue el código en la siguiente versión para eso.

Satoshi

Email 6— Satoshi envió bitcoins

De: "Satoshi Nakamoto" satoshi@vistomail.com

Para: dtrammell@dustintrammell.com
Fecha: lunes, 19 de enero 2009, 00:54:32 +0800
Asunto: Re: Transferencias de Bitcoins

Debería ser tu dirección de Bitcoin de casa con la que lo recibiste. No hay forma de que sepa de quién es, así que lo mejor que puedes hacer es

decir en cuál de tus direcciones se recibió.

Puedes crear varias direcciones y dar una dirección diferente a cada persona y etiquetarlas para ayudar a determinar quién te la está enviando.

No conoce más nombres que los que le dices. El nombre impreso allí es lo que está asociado en tu libreta de direcciones para esa dirección, ya sea bajo el botón Libreta de direcciones o el botón "Cambiar ..." a la derecha de su dirección de Bitcoin.

Hola Satoshi,

Después de esa primera transferencia de 25.00, no me enviaste otros 100.00 ¿verdad? Me envié 100.00 desde mi aplicación BitCoin en el trabajo a la de mi casa utilizando la dirección de BitCoin en lugar de la de IP. Mi aplicación en casa recibió una transferencia de 100.00, sin embargo, los detalles de la transacción dicen:

"Recibido con: Satoshi 12higDjoCCNXSA95xZMWUdPvXNmkAduhWv".

Esa no es mi dirección BitCoin del trabajo, así que supongo que esto significa que recibí el pago codificado con un bloque que fue computado por tu cliente. De ser así, ¿cómo sabía tu nombre además de la dirección de BitCoin que lo generó? No recuerdo que haya un lugar en mi formulario de solicitud para poner siquiera mi nombre.

--

Dustin D. Trammell
dtrammell@dustintrammell.com
http://www.dustintrammell.com

70

Última Correspondencia Privada

Traducción por **Jose Luis Abia**

SUPUESTAMENTE, Gavin Andresen es la última persona que tuvo un intercambio privado con Satoshi Nakamoto. Tuvo lugar cuatro meses después de su publicación final en el foro de bitcointalk.org de diciembre de 2010. Gavin Andresen tuvo algunos intercambios privados de correo electrónico con Satoshi después de su retiro de la vida pública. Sin embargo, Gavin ha decidido que sólo compartiría públicamente el último correo electrónico de Satoshi.

Correo electrónico de Satoshi

Gavin Andresen, 26 de abril 2011

Martes 26 de abril 2011, Satoshi Nakamoto <satoshin@gmx.com> escribió:

Desearía que no siguieras hablando de mí como una figura misteriosa en la sombra, la prensa simplemente lo trata como una especie de moneda pirata. En cambio, podrías incidir más en la idea de que es un proyecto de código abierto y dar más énfasis a las contribuciones de tus

colaboradores; lo que ayudaría a motivarlos.

Debes leer el artículo de Forbes. . . sí, tampoco estoy contento con el tono de " dinero pirata excéntrico".

Mayor énfasis para el resto de los colaboradores es una muy buena idea.

Sobre un tema completamente diferente: hice algo que espero que sea inteligente, pero podría ser estúpido.

Me han contactado por http://www.iqt.org/, - que es una empresa de "inversión estratégica" financiada por el gobierno de EE. UU., y parte de lo que hacen es realizar una conferencia anual sobre tecnologías emergentes para las agencias de inteligencia de EE. UU. Este año, el tema es "Movilidad del dinero".

Me preguntaron si estaría dispuesto a hablar sobre Bitcoin, y me comprometí a dar una presentación de 50 minutos y participar en un panel de discusión.

Espero que hablando directamente con "ellos" y, lo que es más importante, escuchar sus preguntas/inquietudes, piensen en Bitcoin de la forma en que yo lo hago, simplemente como algo mejor, más eficiente, dinero menos sujeto a caprichos políticos. No como una poderosa herramienta del mercado negro que será utilizada por los anarquistas para derrocar Al Sistema.

Puede ser realmente estúpido si solo aumenta la visibilidad de Bitcoin en su radar, pero creo que es demasiado tarde para eso; Bitcoin ya está en su radar.

Planeo publicar esto en los foros pronto, porque "Gavin visita secretamente a la CIA" daría lugar a todo tipo de teorías de la conspiración. "Gavin visita abiertamente a la CIA" creará suficientes teorías de la conspiración tal y como están las cosas.

71

Bitcoin y Yo (Hal Finney)

Traducción por **Jose Luis Abia**

DESDE QUE ÉL FUE EL RECEPTOR de la primera transacción de Bitcoin y alguien que participó desde el principio, vale la pena agregar esta maravillosa publicación de Hal Finney en el foro *bitcointalk.org* con fecha del 19 de marzo de 2013.

Bitcoin y yo (Hal Finney)

Hal Finney, 19 de marzo 2013, 08:40:02 PM

Pensé que escribiría sobre los últimos cuatro años, un momento memorable para Bitcoin y para mí.

Para aquellos que no me conocen, soy Hal Finney. Me inicié en la criptografía trabajando en una versión anterior de PGP, en estrecha colaboración con Phil Zimmermann. Cuando Phil decidió comenzar PGP Corporation, yo fui uno de los primeros empleados. Hubiera trabajado en PGP hasta mi jubilación. Al mismo tiempo, me involucré con los Cypherpunks. Lideré, entre otras actividades, el primer remailer anónimo basado en criptografía.

Avanzado rápido hasta finales del 2008 y el anuncio de Bitcoin. Me he dado cuenta de que los criptógrafos que peinan canas (que ya contaba con más de 50 años) tienden a volverse cínicos. Yo era más idealista; siempre me ha apasionado la criptografía, el misterio y la paradoja de todo esto.

Cuando Satoshi anunció Bitcoin en la lista de correo de Criptografía, obtuvo una respuesta más bien fría en el mejor de los casos. Los criptógrafos han visto demasiados novatos con grandes planes para ser, en realidad, totalmente absurdos, de modo que reaccionan instintivamente.

Yo fui más positivo. Hace tiempo que he estado interesado en los sistemas de pago criptográfico. Además, tuve la suerte de conocer y mantener amplia correspondencia tanto con Wei Dai y con Nick Szabo, ambos reconocidos por haber ideado esquemas que más tarde se materializaron con Bitcoin. Yo mismo había intentado crear mi propia criptomoneda basada en la prueba de trabajo, llamada RPOW (Reusable Proof-of-Work, Prueba de Trabajo Reutilizable en español). Así que Bitcoin me pareció algo fascinante.

Cuando Satoshi anunció el lanzamiento de la primera versión del software, lo descargue de inmediato. Creo que fui la primera persona, después de Satoshi en ejecutar Bitcoin. Miné el bloque 70 y algo, y fui el primer destinatario de una transacción de bitcoin, cuando Satoshi me envió diez monedas como prueba. Durante los siguientes días mantuve con Satoshi conversaciones por correo electrónico y le reporté varios fallos que acabó solucionando.

Hoy en día, la verdadera identidad de Satoshi se ha convertido en un misterio. Pero en ese momento, yo pensaba que estaba tratando con un joven de ascendencia japonesa, extraordinariamente inteligente y sincero. He tenido la suerte de conocer a muchas personas brillantes a lo largo de mi vida, así que reconozco los signos.

Después de unos días, Bitcoin ya funcionaba muy estable, así que lo dejé correr. Eran los días en que la dificultad era de 1, y se podían encontrar bloques fácilmente con una CPU, no hacía falta ni una GPU. Miné varios bloques en el transcurso de los siguientes días, pero finalmente decidí apagarlo, porque mi ordenador se recalentaba y el ruido constante del ventilador me resultaba molesto. En retrospectiva, me gustaría haberlo mantenido encendido más tiempo, pero por otro

lado me considero increíblemente afortunado por haber estado allí desde el principio. Es como un vaso que podemos ver medio lleno o medio vacío.

No volví a saber de Bitcoin hasta finales de 2010, cuando me sorprendí al descubrir que el proyecto no sólo seguía en marcha, si no que los bitcoins habían pasado a tener valor monetario. Desempolvé mi viejo monedero, y me sentí aliviado al comprobar que mis bitcoins seguían allí. Al ver que la cotización aumentaba, decidí guardar esas monedas en una cartera offline, donde con suerte van a preservar su valor para mis herederos.

Hablando de herederos, tuve una sorpresa en 2009, cuando de repente me diagnosticaron una enfermedad mortal. A principios de ese año, me encontraba en un estado formidable, había perdido mucho peso y corría mucho. Había corrido varias medias maratones y comencé a entrenar para correr una maratón completa. Estaba preparado para participar en carreras de más de 20 millas, y cuando pensaba que estaba todo listo, en ese momento empezó todo a salir mal.

Mi cuerpo comenzó a fallar. Arrastraba mi forma de hablar, perdía fuerza en mis manos, y mis piernas tardaron en recuperarse de lo esfuerzos. En agosto de 2009, me diagnosticaron Esclerosis Lateral Amiotrófica (ELA), también llamada la enfermedad de Lou Gehrig, por el famoso jugador de béisbol que la padeció.

La ELA es una enfermedad que mata a las neuronas motoras, que conducen las señales desde cerebro a los músculos. Inicialmente se manifiesta como debilidad y luego aumenta gradualmente hacia la parálisis. Por lo general es mortal en 2 a 5 años. Mis síntomas eran leves al principio y pude seguir trabajando, pero la fatiga y la imposibilidad de hablar me obligaron a retirarme a principios del 2011. Desde entonces, la enfermedad ha continuado su inexorable progresión.

Hoy, estoy casi totalmente paralizado. Me alimento con una sonda y mi respiración es asistida a través de otro tubo. Uso el ordenador usando un sistema comercial de rastreo ocular que cuenta además con un sintetizador de voz, así que esta es mi voz ahora. Paso todo el día en mi silla de ruedas eléctrica. He desarrollado un interfaz utilizando una placa de arduino para ajustar la posición de mi silla de ruedas con sólo mover mis ojos.

Ha sido un gran cambio, pero mi vida no es tan mala. Todavía puedo leer, escuchar música y ver televisión y películas. Recientemente descubrí que incluso puedo escribir código. Soy muy lento, probablemente 50 veces más lento que antes. Pero todavía sigo amando la programación y me pongo metas. Actualmente estoy trabajando en algo que Mike Hearn sugirió, utilizando las características de seguridad de los procesadores modernos, diseñado para admitir "*Trusted Computing*" (Computación de la Verdad), para fortalecer las billeteras de Bitcoin. El producto está casi listo para lanzarlo. Solo tengo que hacer la documentación.

Y por supuesto, los giros de los precios de los bitcoins me resultan divertidos. Al fin y al cabo, tengo ahorros en el juego aunque mis bitcoins son más producto de la suerte que de mérito personal, con poco valor para mí. He vivido el crash de 2011. Lo he visto antes. Lo que fácil viene, fácil se va.

Esa es mi historia. Me considero un afortunado. A pesar de la ELA, mi vida es muy satisfactoria. Pero mi esperanza de vida es limitada. Las discusiones que he leído sobre cómo dejar en herencia tus bitcoins adquiere un interés más personal que académico para mí. Mis bitcoins se almacenan en nuestra caja de seguridad, y mi hijo e hija son conocedores de la tecnología. Creo que están lo suficientemente seguros. Me siento cómodo con mi legado.

Hal Finney †

---

† (Hal Finney falleció el 28 de agosto del 2014, a causa de la ELA - Nota del traductor)

72

Conclusión

Traducción por **Jose Luis Abia**

SATOSHI NAKAMOTO reunió muchos conceptos matemáticos y de software existentes para crear Bitcoin. Desde entonces, Bitcoin ha sido un experimento continuo, sigue evolucionando y se actualiza regularmente. Hasta el momento, ha demostrado su utilidad y ha revolucionado la industria financiera y monetaria, en particular el sistema de pago electrónico, y está siendo aceptado en todo el mundo. Bitcoin, en sí mismo, puede o no sobrevivir hasta el año 2140, cuando todos los bitcoins hayan sido minados, pero la idea de la distribución de igual a igual de una divisa con oferta limitada y descentralizada está aquí para quedarse.

La capacidad de transferir dinero digitalmente solo ha sido posible muy recientemente en la historia humana, pero esto va más allá de un cambio mecánico en el uso del dinero, es una nueva forma de realizar la misma acción. Pero oro y plata o cualquier alguna otra no hinchable entidad no puede transmitirse directamente por vía electrónica y, por lo tanto, requieren del concepto de un delegado que puede tergiversar su cantidad si se hicieran demasiadas copias (es decir, este delegado puede estar hinchado). Cuanto mayor cantidad hay de cualquier moneda, esta se vuelve menos valiosa, y menos, en términos de bienes y servicios reales, es capaz de comprar.

Luego, a fines de 2009, Satoshi presentó Bitcoin. El concepto de una moneda digital descentralizada, de fuente abierta y con un libro de contabilidad abierto, ha sido actualizado. Curiosamente, a diferencia del oro y la plata, que solo pueden existir en el mundo físico, los bitcoins solo pueden existir en el

mundo electrónico.[3] Por eso, en esencia, se puede argumentar que los metales preciosos y Bitcoin se complementan muy bien.

El hecho de que Bitcoin sea un software de código abierto cuyas transacciones deben ser confirmadas por todos los miembros de la red y que opera con un libro de contabilidad público lo convierte en el polo opuesto de un sistema de moneda cerrada y controlada centralmente. Independientemente de si los reguladores están involucrados en un sistema cerrado o no, dichos sistemas son tan susceptibles a corrupciones y sobornos a los líderes del gobierno como cualquier otra institución controlada por el gobierno. Cómo son escasos, los metales preciosos, el oro y la plata son una excelente opción para usarse como dinero, pero su incapacidad de ser transferidos electrónicamente requiere algún tipo de forma representativa e intermediaria, capaz de ser manipulada por un tercero. El transporte de una gran suma de oro y plata también es engorroso y caro. Sin embargo, los metales preciosos mantendrán su valor durante grandes acontecimientos, como apagones en la red eléctrica, y sin duda se convertirán en la moneda elegida en un escenario de Mad Max. Para aquellos temerosos de tal eventualidad, poseer una cierta cantidad de oro y plata es apropiado. En cualquier caso, todas las monedas fiduciarias (es decir, decretadas por el gobierno) a lo largo de la historia siempre mueren, y no debe esperar que la moneda de su país sea una excepción a esta regla.

Este libro ha presentado todas las conversaciones y discusiones más relevantes en las que participó el creador de Bitcoin. Si un grupo o un individuo, la persona conocida como Satoshi Nakamoto se expresó de manera clara y concisa y naturalmente entendía muy bien la base de Bitcoin. Sus diversos escritos parecen indicar que no esperaba que Bitcoin despegara tan rápido como lo hizo. Satoshi reunió varios conceptos existentes para crear esta tecnología formidable que actualmente revoluciona la forma de cómo el sistema monetario es conceptualizado. Él ha abierto una caja de pandora, y

---

[3] Hasta ahora, transportar bitcoins en el mundo físico implica algún tipo de artefacto, como una billetera de papel con la dirección de Bitcoin y una clave privada inscrita en ella. O, alternativamente, requiere cierta confianza en un tercero, por ejemplo, el fabricante de una moneda física con una clave privada secreta de Bitcoin junto con una dirección visible de Bitcoin.

muchas mentes brillantes están trabajando más allá de Bitcoin para revolucionar otros sistemas basados en sus preceptos.

Si Bitcoin representa dinero está sujeto a debate, pero de que es una moneda, un medio de cambio, es indiscutible. El oro y la plata son una reserva de valor a largo plazo debido a su suministro limitado y su utilidad. Bitcoin también tiene un suministro limitado -los 21 millones de bitcoins planeados al 2140- y hasta ahora ha demostrado ser muy útil como una forma sencilla de pago a través de Internet, su medio natural.

Satoshi cubrió muchos de los argumentos que vemos debatiéndose, una y otra vez, en los medios de comunicación desde que Bitcoin ha crecido en popularidad. Aunque nos hubiera encantado escucharlo hablar en persona, este libro nos da la posibilidad de revisar fácilmente las muchas opiniones que compartió durante su "vida pública". El mayor impacto de Bitcoin ha sido permitir que la población del mundo reconsidere cómo debería funcionar una moneda. Abre la puerta a la humanidad a un nuevo sistema monetario, un renacimiento electrónico.

¡Gracias!

"Bitcoin: Un Sistema de Dinero Electrónico Peer-to-Peer" por Satoshi Nakamoto

Traducción por **Jose Luis Abia**

Resumen. Una versión puramente peer-to-peer de dinero electrónico que permitiría que los pagos en línea se envíen directamente de una parte a otra sin tener que pasar por una institución financiera. Las firmas digitales proporcionan parte de la solución, pero los principales beneficios se pierden si un tercero de confianza es aún requerido para evitar el doble gasto. Proponemos una solución al problema de doble gasto utilizando una red peer-to-peer. La red marca el tiempo de las transacciones al tiempo que las va hasheando (hacer una transformación criptográfica), que va dentro de una cadena continua de prueba de trabajo basados en hashes, formando un registro que no puede modificarse sin rehacer la prueba de trabajo. La cadena más larga no solo sirve como prueba de la secuencia de eventos ocurridos, sino, como prueba de que proviene del mayor conjunto de potencia de CPU. Siempre que la mayor potencia de CPU esté controlada por nodos que no están cooperando para atacar la red, generarán la cadena más larga y superarán a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes se transmiten según el mejor esfuerzo, y los nodos pueden salir y unirse a la red a voluntad, aceptando la cadena de prueba de trabajo más larga como prueba de lo sucedido mientras ellos no estaban.

1. Introducción

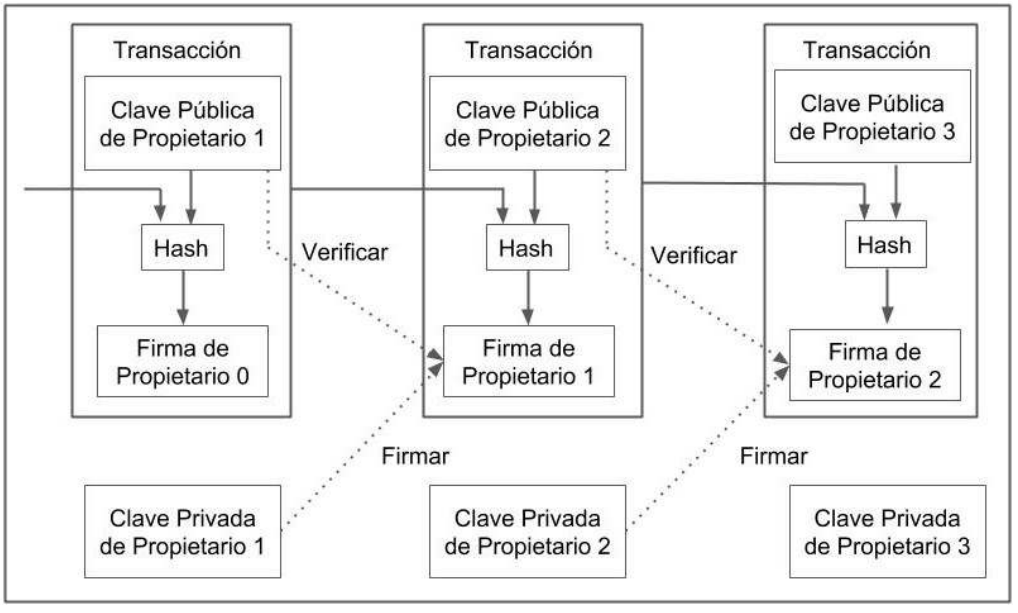
El comercio en Internet ha llegado a depender casi exclusivamente de las instituciones financieras, las cuales sirven como terceros de confianza, para procesar los pagos electrónicos. Mientras que el sistema funciona suficientemente bien para la mayoría de las transacciones, aún sufre de las debilidades inherentes del modelo basado en confianza. Transacciones completamente irreversibles no son realmente posibles, debido a que las instituciones financieras deben mediar para resolver disputas. El costo de la mediación incrementa los costos de transacción, limitando el tamaño mínimo práctico por transacción y eliminando la posibilidad de realizar pequeñas transacciones casuales, y hay un costo más amplio en la incapacidad de hacer pagos no reversibles por servicios no reversibles. Con la posibilidad de revertir, la necesidad de confianza se expande. Los comerciantes deben tener cuidado de sus clientes, molestándoles por más información de la que ellos en otro caso necesitarían. Un cierto porcentaje de fraude se acepta como inevitable. Estos costos e incertidumbres en los pagos pueden ser evitados si la persona utiliza dinero físico, pero no existe un mecanismo para hacer pagos por un canal de comunicación sin un tercero confiable.

Lo que se necesita es un sistema de pagos electrónicos que esté basado en pruebas criptográficas en vez de en confianza, permitiendo a las dos partes interesadas realizar transacciones directamente sin la necesidad de un tercero confiable. Las transacciones que son computacionalmente poco factibles de revertir protegerían a los vendedores de fraude, del mismo modo que mecanismos rutinarios de depósito de garantía podrían ser fácilmente implementados para proteger a los compradores. En este trabajo, proponemos una solución al problema del doble gasto utilizando un servidor de marca de tiempo punto a punto distribuido para generar una prueba computacional del orden cronológico de las transacciones. El sistema es seguro mientras que los nodos honestos colectivamente controlen más poder de procesamiento (CPU) que cualquier grupo de nodos con intención de atacar.

2. Transacciones

Definimos una moneda electrónica como una cadena de firmas digitales.

Cada dueño transfiere la moneda al próximo propietario al firmar digitalmente un hash de la transacción previa y la clave pública del próximo dueño y agregando estos al final de la moneda. El beneficiario del pago puede comprobar las firmas para verificar la cadena de propiedad.



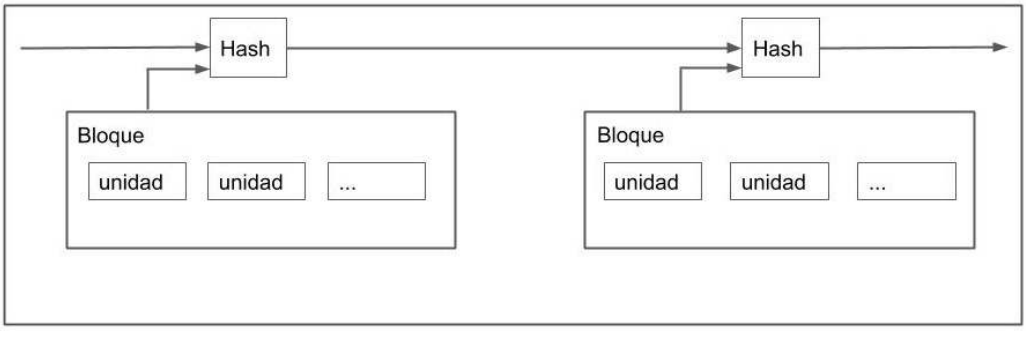
El problema por supuesto está en que el beneficiario no puede verificar si alguno de los dueños previos no realizó un doble gasto de la moneda. La solución común es introducir una autoridad central confiable, o casa de la moneda, que revisa si cada transacción tiene doble gasto o no. Después de cada transacción, la moneda debe ser devuelta a la entidad para generar una nueva moneda, de modo que solo las monedas generadas directamente por esta institución son en las que se confía de no tener doble-gasto. El problema con esta solución es que, el destino del sistema monetario entero depende de la compañía que gestiona la casa de la moneda, con todas las transacciones teniendo que pasar por ellos, tal y como actuaría un banco.

Necesitamos una forma para que el beneficiario de la transacción pueda saber que los dueños previos no firmaron ninguna transacción anterior. Para nuestros propósitos, la primera transacción es la que cuenta, así que no nos importarán otros intentos de doble gasto posteriores. La única forma de

confirmar la ausencia de una transacción es estando al tanto de todas las transacciones. En el modelo de la casa de la moneda, ésta casa era la que estaba al tanto de todas las transacciones y decidía cuales llegaban primero. Para lograr esto sin un intermediario de confianza, las transacciones deben ser anunciadas públicamente [1], y necesitamos un sistema para que los participantes estén de acuerdo en una historia única del orden en que estas transacciones fueron recibidas. El beneficiario necesita una prueba de que al tiempo de cada transacción, la mayor parte de nodos de la red coincide en que fue el primero recibido.

3. Servidor de Marca de Tiempo

La solución que proponemos comienza con un servidor de marca de tiempo. Este sistema funciona al realizar el hash de un bloque de datos, poniéndole fecha y haciéndolo público ampliamente, tal y como se haría en un periódico o en una publicación de Usenet [2-5]. La marca de tiempo prueba que la data, obviamente, debe de haber existido en ese momento para poder incluirse dentro del hash. Cada marca de tiempo incluye en su hash la marca de tiempo previa, formando una cadena, de modo que cada marca de tiempo adicional refuerza las anteriores.

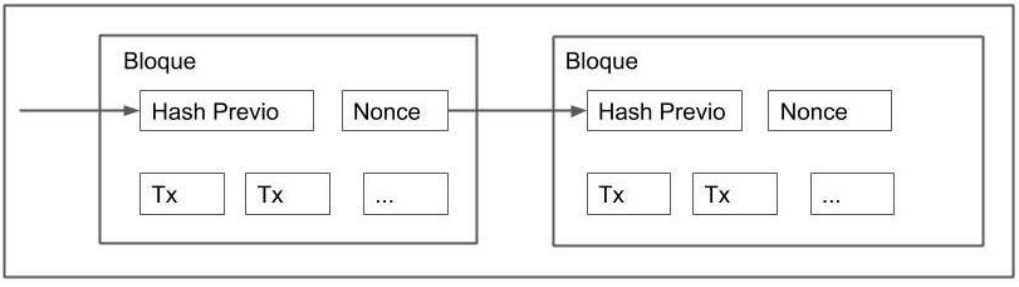


4. Prueba de Trabajo

Para implementar un servidor de marca de tiempo distribuido en un esquema peer-to-peer (P2P), necesitaremos utilizar un sistema de prueba de

trabajo similar al Hashcash de Adam Back [6], en vez de usar una publicación en un periódico o en Usenet. La prueba de trabajo implica la búsqueda de un valor, tal que, al calcular un hash, como SHA-256, éste empiece con un número determinado de bits con valor cero. El trabajo promedio requerido será exponencial al número de bits requeridos con valor cero, y que puede ser verificado ejecutando un solo hash.

Para nuestra red de marca de tiempo implementamos la prueba de trabajo incrementando el valor de un campo nonce en el bloque, hasta que el valor es encontrado y que dé el número requerido de bits con valor cero para el hash. Una vez que el esfuerzo de CPU se destina para satisfacer la prueba de trabajo, el bloque no puede ser cambiado sin rehacer el trabajo. A medida que más bloques se van encadenando, el trabajo para cambiar un bloque incluiría rehacer todos los bloques posteriores a éste.



La prueba de trabajo también resuelve el problema de determinar cómo representar la decisión por mayoría. Si esta mayoría se basará en una dirección IP, un voto, podría ser alterada por alguien capaz de asignar muchas IPs. La prueba de trabajo es esencialmente a “una-CPU-un-voto”. La decisión de la mayoría es representada por la cadena más larga, la cual tiene la prueba de trabajo con mayor esfuerzo invertido. Si el mayor poder de CPU es controlado por nodos honestos, la cadena honesta crecerá más rápido y dejará atrás cualquier otra cadena competidora. Para modificar un bloque pasado, un atacante tendría que rehacer la prueba de trabajo del bloque y de todos los bloques posteriores, y luego alcanzar y superar el trabajo de los nodos honestos. Luego demostraremos que la probabilidad de que un atacante más lento alcance la cadena más larga, disminuye exponencialmente a medida que bloques subsecuentes son incorporados.

Para compensar el incremento de la velocidad del hardware y el interés variable de ejecutar nodos en el tiempo, la dificultad de la prueba de trabajo es determinada por una media móvil dirigida por un número promedio de bloques por hora. Si estos se generan muy rápido, la dificultad se incrementa.

5. La Red

Los pasos para el ejecutar la red son los siguientes:

1. Transacciones nuevas son comunicadas a todos los nodos.
2. Cada nodo agrupa las nuevas transacciones en un bloque.
3. Cada nodo se esfuerza en encontrar una difícil prueba de trabajo para el bloque.
4. Cuando un nodo encuentra una prueba de trabajo, difunde el bloque a todos los nodos.
5. Los nodos aceptan el bloque si todas las transacciones en el bloque son válidas y no ya gastado.
6. Los nodos dan su consentimiento a cada bloque y empiezan a trabajar en crear el próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash previo.

Los nodos siempre consideran la cadena más larga como la correcta y empiezan a trabajar en extenderla. Si dos nodos emiten versiones diferentes del próximo bloque simultáneamente, algunos nodos puede que reciban uno u otro primero. En ese caso, trabajan en el primero que reciban pero guardan la otra rama en caso de que esta se vuelva más larga. El empate se rompe cuando se encuentra la próxima prueba de trabajo y una rama se vuelve más larga que la otra; los nodos que estaban trabajando en la otra rama posteriormente se cambian a la que ahora es más larga.

La difusión de nuevas transacciones no necesariamente necesita llegar a todos los nodos. En el momento que éstas llegan a muchos nodos, acabarán entrando en un bloque antes de que pase mucho tiempo. La difusión de bloques también es tolerante a la pérdida de mensajes. Si un nodo no recibe un bloque, lo pedirá cuando reciba el próximo bloque y se dará cuenta de que ha perdido uno.

6. Incentivo

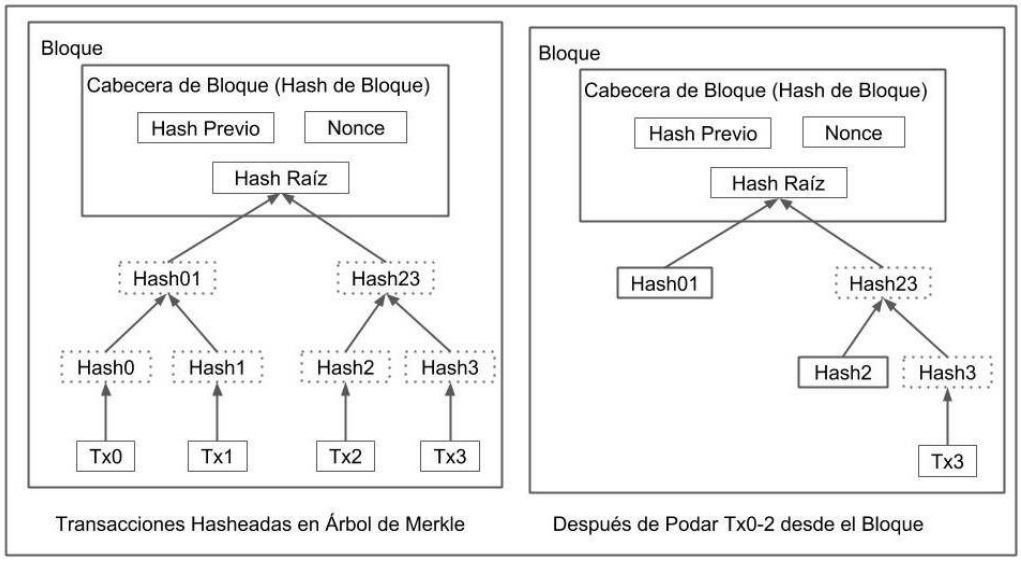
Por convención, la primera transacción en el bloque es una transacción especial que genera una nueva moneda cuyo dueño es el creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red, y provee una forma inicial de distribuir y poner en circulación las monedas, dado que no hay una autoridad central para crearlas. Esta adición estable de una cantidad constante de monedas nuevas es análoga a los mineros de oro que gastan recursos para ponerlo en circulación. En nuestro caso, los recursos son el tiempo de CPU y la electricidad que se gastan.

El incentivo también puede establecerse con los costes de transacción. Si el valor de salida de una transacción es menor que la entrada, la diferencia será una tarifa de transacción que se añadirá al valor del incentivo del bloque que la contiene. Una vez que un número predeterminado de monedas han entrado en circulación, el incentivo puede evolucionar enteramente a tarifas de transacción y estar completamente libres de inflación.

El incentivo también puede ayudar a animar a los nodos a mantenerse honestos. Si un atacante egoísta es capaz de reunir más potencia de CPU que el resto de los nodos honrados, éste tendría que elegir entre utilizarlo para defraudar a la gente robando sus pagos, o usarlo para generar monedas nuevas. Debería encontrar más rentable jugar siguiendo las reglas, ya que éstas le favorecen con más monedas que nadie más combinado, que intentando socavar el sistema y la validez de su propia riqueza.

7. Reclamando Espacio en Disco

Una vez que la última transacción está enterrada bajo suficientes bloques, las transacciones gastadas anteriores a esta pueden ser descartadas para ahorrar espacio en disco. Para facilitar esto sin romper el hash del bloque, las transacciones se comprueban en un árbol de Merkle [7] [2] [5], incluyendo sólo la raíz en el hash de dicho bloque. Los bloques viejos pueden compactarse al sacar ramas del árbol. Los hashes interiores no necesitan ser guardados.

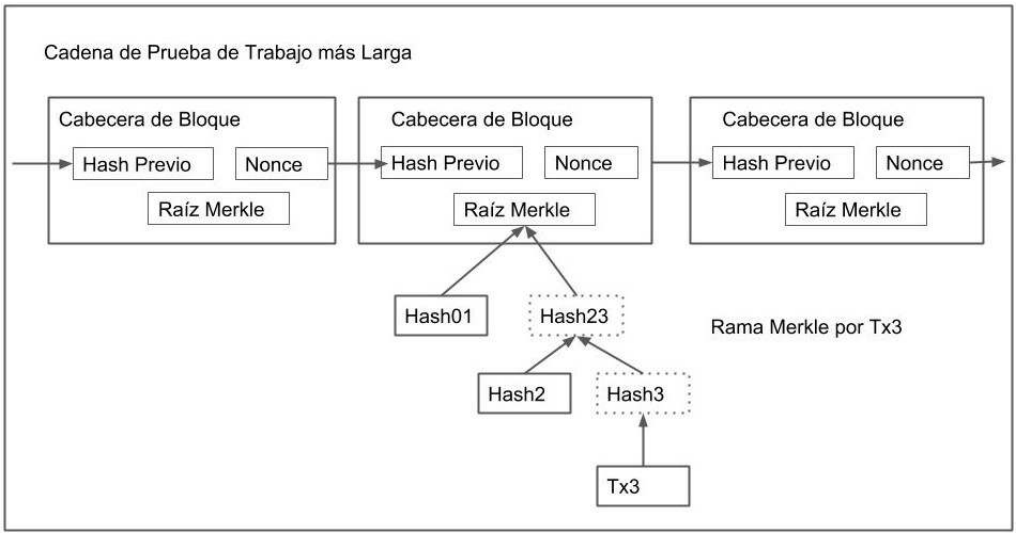


La cabecera de un bloque sin transacciones será de unos 80 bytes. Si suponemos que cada bloque se genera cada 10 minutos, 80 bytes * 6 * 24 * 365 = 4.2MB por año. Con ordenadores vendiéndose generalmente con 2GB de RAM en 2008, y la Ley de Moore prediciendo un crecimiento actual de 1.2GB por año, el almacenamiento no debe ser un problema aun si las cabeceras de los bloques deben permanecer en memoria.

8. Verificación de Pagos Simplificado

Es posible verificar pagos sin ejecutar un nodo completo en la red. Un usuario solo necesita mantener una copia de las cabeceras de los bloques de la cadena más larga de la prueba de trabajo, la cual se puede obtener buscando en los nodos de la red hasta que esté convencido de tener la cadena más larga, y obtener la rama del árbol de Merkle enlazando la transacción con el bloque en que ha sido fechado. Aunque no puede verificar la transacción por sí mismo, pero enlazándolo a algún lugar de la cadena, puede ver que un nodo de la red la ha aceptado, de modo que los bloques añadidos después de confirmar aún más esta aceptación por parte de la red.

Como resultado, la verificación resulta fiable a medida que los nodos honestos controlen la red, pero se vuelve más vulnerable si la red es dominada por un atacante. Mientras que los nodos de la red puedan verificar las

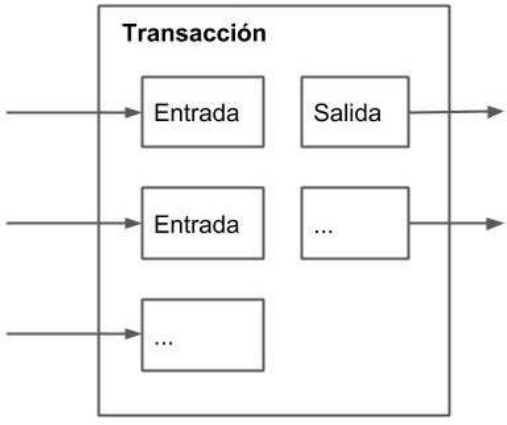


transacciones por sí mismos, el método simplificado puede ser engañado por transacciones fabricadas por un atacante mientras éste pueda dominar la red. Una estrategia para protegerse es aceptar alertas de los nodos de la red cuando detecten un bloque inválido, pidiéndole al usuario que se baje el bloque completo y las transacciones alertadas para confirmar la inconsistencia. Los negocios que frecuentemente reciban pagos querrán ejecutar sus propios nodos para tener una seguridad más independiente y una verificación más rápida.

9. Combinando y Dividiendo Valor

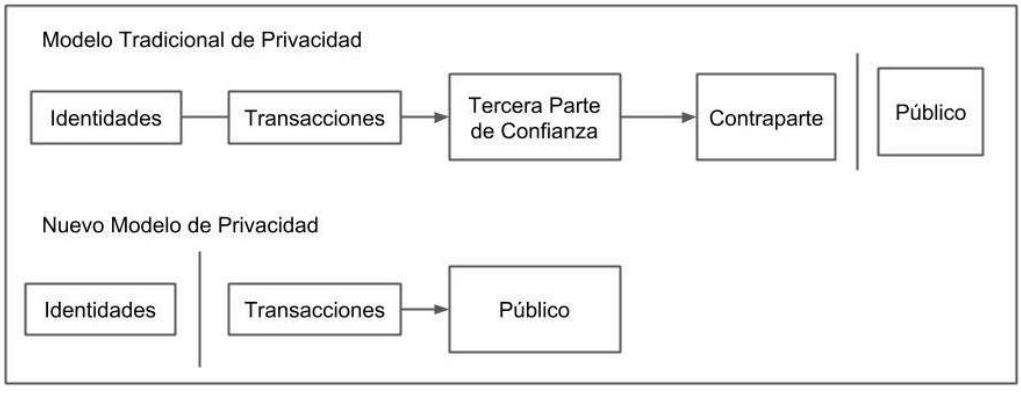
Aunque sería posible manipular monedas individualmente, sería difícil realizar transacciones separadas por cada céntimo de una transferencia. Para permitir que el valor se divida y se combinen, las transacciones contienen múltiples entradas y salidas. Normalmente habrá o una sola entrada, de una transacción previa más grande, o múltiples entradas combinando cantidades más pequeñas, y al menos dos salidas: una para el pago, y una para devolver el cambio, si es que hay alguno, de vuelta al emisor.

Hay que tener en cuenta que este sistema se abre el abanico, de modo que una transacción puede depender de varias transacciones, y estas a su vez depender de muchas más, lo que no es ningún problema. Nunca existe la necesidad de extraer una copia completa única de la historia de las transacciones.



10. Privacidad

El modelo bancario tradicional, logra su nivel de privacidad, al limitar el acceso a la información a las partes involucradas y al tercero de confianza. La necesidad de anunciar todas las transacciones públicamente se opone a este método, pero la privacidad aún puede mantenerse rompiendo el flujo de información en otro lugar: manteniendo las claves públicas anónimas. Públicamente puede verse que alguien está enviando una cierta cantidad a otra persona, pero sin información que relacione la transacción con nadie en particular. Esto es similar al nivel de información que se muestra en las bolsas de valores, donde el tiempo y el tamaño de las transacciones individuales, la "cinta", son públicos, pero sin decir quiénes son las partes.



Para establecer un sistema de seguridad adicional, un nuevo par de claves debería ser usada para cada transacción para evitar que sean vinculadas a un

mismo propietario. Algunos enlaces aún son inevitables con transacciones de múltiples entradas, las cuales necesariamente revelan que sus entradas fueron propiedad del mismo dueño. El riesgo estaría en que si la identidad del dueño de una clave es revelada, entonces los vínculos podrían revelar otras transacciones que pertenecieron al mismo dueño.

11. CÁLCULOS

Consideramos el escenario en el que un atacante intenta generar una cadena alterna más rápida que la cadena honesta. Aún si esto se lograse, no abriría el sistema a cambios arbitrarios, tales como crear valor de la nada o apropiarse del dinero que no pertenecen al atacante. Los nodos no aceptarían una transacción inválida como pago, y los nodos honestos nunca aceptarán un bloque que las contenga. Un atacante puede únicamente intentar cambiar solo sus propias transacciones para recuperar el dinero que ha gastado recientemente.

La carrera entre una cadena honesta y la cadena de un atacante puede ser caracterizada como un Camino Aleatorio Binomial. El caso de éxito ocurre cuando la cadena honesta logra extenderse con un bloque adicional e incrementa su ventaja en +1, mientras el caso fallido tendría lugar si el atacante adquiere la ventaja de un bloque y la cadena del atacante adquiere la ventaja de un bloque y reduce la brecha en -1.

La probabilidad de que un atacante en desventaja pueda alcanzarnos, es análogo al problema de la Ruina del Jugador. Supóngase que un jugador con crédito ilimitado empieza en déficit y juega potencialmente un número infinito de intentos para intentar llegar a un punto de equilibrio. Podemos calcular la probabilidad de que llegase al punto de equilibrio, o que llegue a alcanzar a la cadena honesta, como sigue [8]:

p = probabilidad de que un nodo honrado encuentre el próximo bloque

q = probabilidad de que el atacante encuentre el próximo bloque q

q_z = probabilidad de que el atacante llegue a alcanzar desde z bloques atrás.

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Dada nuestra hipótesis de que p > q, la probabilidad cae exponencialmente mientras que el número de bloques que el atacante debe alcanzar incrementa. Con las probabilidades en contra, si no hace una jugada afortunada desde el principio, sus oportunidades se vuelven extremadamente pequeñas a medida que se queda más atrás.

Ahora consideremos cuánto necesita esperar el beneficiario de una nueva transacción antes de tener la certeza suficiente de que el emisor no puede cambiarla. Asumimos que el remitente es un atacante que quiere convencer al receptor de que ha pagado, pero luego pretende cambiar la operación para recuperar los fondos. El receptor será alertado cuando eso sucede, pero el remitente tendrá la esperanza de que sea ya demasiado tarde.

El beneficiario genera un nuevo par de claves y entrega la clave pública al emisor poco después de hacer la firma. Esto previene que el emisor prepare una cadena de bloques antes de tiempo, y pueda estar trabajando en ella continuamente hasta que tenga la suerte de adelantarse lo suficiente, y luego ejecutar la transacción en ese momento. Una vez que la transacción es enviada, el emisor deshonesto empieza a trabajar en secreto en una cadena paralela que contiene una versión alterna de su transacción.

El beneficiario espera hasta que la transacción haya sido añadida a un bloque y que z bloques hayan sido enlazados después de la transacción. Él no sabe la cantidad exacta de progreso que ha logrado el atacante, pero asumiendo que los bloques honestos tardaron el promedio esperado de tiempo por bloque, el progreso potencial del atacante será una distribución de Poisson con un valor esperado de:

$$\lambda = z\frac{q}{p}$$

Para obtener la probabilidad de que el atacante logre su objetivo, multiplicamos la densidad de la distribución de Poisson por la cantidad de progreso que pudo haber hecho, por la probabilidad de que pudiera alcanzar ese punto:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Reorganizamos para evitar la suma de la cola infinita de la distribución…

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Convertimos a código C…

```
#include <math.h>
double AttackerSuccessProbability(double q, int
z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k &lt;= z; k++)
    {
      double poisson = exp(-lambda);
      for (i = 1; i &lt;= k; i++)
           poisson *= lambda / i;
      sum -= poisson * (1 - pow(q / p, z - k));
}
return sum;
}
```

Ejecutamos algunos resultados, podemos ver que la probabilidad cae exponencialmente con z.

```
q=0.1
z=0  P=1.0000000
z=1  P=0.2045873
z=2  P=0.0509779
z=3  P=0.0131722
z=4  P=0.0034552
z=5  P=0.0009137
z=6  P=0.0002428
z=7  P=0.0000647
z=8  P=0.0000173
z=9  P=0.0000046
z=10 P=0.0000012

q=0.3
z=0  P=1.0000000
z=5  P=0.1773523
z=10 P=0.0416605
z=15 P=0.0101008
z=20 P=0.0024804
z=25 P=0.0006132
z=30 P=0.0001522
z=35 P=0.0000379
z=40 P=0.0000095
z=45 P=0.0000024
z=50 P=0.0000006
```

Resolvemos para P menor que 0.1%…

```
P > 0.001
q=0.10 z=5
q=0.15 z=8
q=0.20 z=11
q=0.30 z=24
q=0.35 z=41
q=0.40 z=89
q=0.45 z=340
```

12. Conclusión

Hemos propuesto un sistema de transacciones electrónicas que no depende de la confianza. Comenzamos con la descripción de la infraestructura habitual en la que funcionan las monedas compuestas por firmas digitales, el cual provee un fuerte control sobre la propiedad, pero queda incompleto si no existe un método para evitar el gasto doble. Para solucionarlo, proponemos una red peer-to-peer (P2P) que utiliza la prueba de trabajo para registrar una historia pública de transacciones que, rápidamente llega a ser computacionalmente irresoluble para un atacante que quiera cambiarla, si los nodos honestos controlan la mayoría de poder de CPU. La red es robusta por su simplicidad no estructurada. Los nodos pueden trabajar todos al mismo tiempo con poca coordinación. No necesitan ser identificados, dado que los mensajes no son enrutados a ningún lugar en particular, y solo necesitan ser entregados sobre la base de un esfuerzo colectivo. Los nodos pueden dejar y volver a la red a voluntad, aceptando la cadena de prueba de trabajo como prueba de lo sucedido mientras estuvieron ausentes. Votan con su poder de CPU, expresando su aceptación de los bloques válidos, trabajando en extender la red y rechazando bloques inválidos al rechazar trabajar en ellos. Cualquier regla necesaria o incentivos pueden hacerse cumplir con este mecanismo de consenso.

Referencias

1. W. Dai, “b-money,” http://www.weidai.com/bmoney.txt, 1998.

2. H. Massias, X.S. Avila, and J.-J. Quisquater, “Design of a secure timestamping service with minimal trust requirements,” In 20th Symposium on Information Theory in the Benelux, May 1999.

3. S. Haber, W.S. Stornetta, “How to time-stamp a digital document,” In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

4. D. Bayer, S. Haber, W.S. Stornetta, “Improving the efficiency and reliability of digital time-stamping,” In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

5. S. Haber, W.S. Stornetta, “Secure names for bit-strings,” In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

6. A. Back, “Hashcash – a denial of service counter-measure,” http://www.hashcash.org/papers/hashcash.pdf, 2002.

7. R.C. Merkle, “Protocols for public key cryptosystems,” In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

8. W. Feller, “An introduction to probability theory and its applications,” 1957.

TÉRMINOS & DEFINICIONES

TRADUCCIÓN POR **ARTURO MONZÓN**

1. **Algoritmo de Firma Digital de Curva Elíptica (ECDSA -Elliptic Curve Digital Signature Algorithm) -** En criptografía, el Algoritmo de Firma Digital de Curva Elíptica (o ECDSA por sus iniciales en inglés) ofrece una variante del Algoritmo de Firma Digital (Digital Signature Algorithm o DSA), que emplea criptografía de curva elíptica.

2. **Archivo Compartido Distribuido (Distributed File Sharing)** - Un sistema en el que los archivos se comparten en varias computadoras que actúan como consumidores y como proveedores de información.

3. **Bloque (Bloque)** - Una porción de datos que contiene varias transacciones de Bitcoin que los mineros trabajan en su creación.

4. **Bloque Génesis (Genesis Block)** – El primer bloque de la cadena de bloques.

5. **BTC** – El acrónimo que representa la moneda Bitcoin.

6. **Cadena de Bloque (Block Chain)** - La cadena de bloques de Bitcoin que se comparte a través de una red peer-to-peer (punto a punto), entre todos los mineros y los nodos interesados (computadoras/ordenadores). Contiene todos los bloques desde la creación de Bitcoin el 3 de enero de 2009.

7. **Comisión de Transacción (Transaction Fee)** – Este es el costo que los remitentes de bitcoins pagan a los mineros para que incluyan sus transacciones en la siguiente cadena de bloques.

8. **Criptografía (Cryptography)** – El estudio de técnicas por el cual las comunicaciones están aseguradas.

9. **Criptografía De Curva Elíptica (Elliptic Curve Cryptography)** - Una criptografía de clave pública basada en la estructura algebraica de curvas elípticas sobre un número finito de elementos (campos finitos). Las curvas elípticas también se usan en varios algoritmos de factorización de enteros que tienen aplicaciones en criptografía.

10. **Dirección Bitcoin (Bitcoin Address)** - Una larga serie de dígitos a los que la cadena de bloques asociará los bitcoins. Es la salida del hash de la clave pública. Cualquier bitcoin que lo contiene sólo puede ser transferido a otra dirección de Bitcoin por la persona que posee su clave privada correspondiente.

11. **Encriptación (Encryption)** – El proceso de codificar mensajes o información de tal forma que solo la parte autorizada lo puede leer o acceder a él.

12. **Encriptación Asimétrica (Asymmetric Encryption)** – Un tipo de encriptación (cifrado) que involucra dos claves, una clave privada y una clave pública. El texto encriptado con la clave privada se debe descifrar con la clave pública y viceversa. La clave pública se deriva fácilmente de la clave privada pero lo inverso es casi imposible.

13. **Hash Criptográfico (Cryptographic Hash) –** Un algoritmo que crea una serie de números de longitud fija a partir de una entrada que tiene una longitud arbitraria. El algoritmo de salida se puede definir como el equivalente de la "huella digital" de un documento**.**

14. **Hash, Función Hash (Hash, Hash Function)** - Hash es la salida de longitud fija de un algoritmo criptográfico o función hash. Hash es la "huella dactilar" de un documento, donde el documento, que puede ser de cualquier longitud, es el texto codificado por la función hash.

15. **Libro Mayor (Ledger)** – En contabilidad, este es el libro principal o archivo de computadora para registrar y sumar transacciones monetarias por cuenta. Incluye un saldo inicial, débitos, créditos y un saldo final.

16. **Mineros (Miners)** - Inicialmente llamados nodos, estos son dispositivos con hardware especializado que compiten en la creación del próximo bloque y, por lo tanto, en cobrar las recompensas asociadas con él. Las recompensas se componen de nuevos bitcoins que el protocolo permite a los mineros crear, junto con la suma de todas las comisiones de transacción contenidas en este bloque.

17. **Monedero (Wallet)** – El software que contiene una lista de direcciones Bitcoin y sus correspondientes claves privadas.

18. **Nonce** – (Viene de "Number used only once" – Número usado solo una vez - *nota del traductor*) Número dentro de un bloque que un minero incrementa hasta que él u otro minero obtiene el resumen del mensaje con las características requeridas por el protocolo Bitcoin para constituir un "ganador" de ese bloque.

19. **Protocolo (Protocol)** – Un procedimiento establecido que mineros y clientes tienen que seguir. Es dictaminado por el software de código abierto de Bitcoin el cual todos los mineros ejecutan.

20. **Prueba de Trabajo (Proof-of-Work, PoW)** – Esto es como una competencia donde cada minero compite. El primer minero en obtener el Nonce que genera el resumen del mensaje con la característica definida por el protocolo Bitcoin es el ganador.

21. **Red Punto a Punto o P2P (Peer-to-Peer Network)** - Una arquitectura de red descentralizada y distribuida donde los nodos individuales (computadoras/ordenadores) en la red actúan como proveedores y consumidores de recursos. Esto está en contraste con un modelo de cliente-servidor centralizado donde los clientes solicitan recursos del servidor.

22. **Resumen de Mensaje (Message Digest)** - Es el resultado de una función de cifrado hash.

23. **Satoshi** – La más pequeña denominación de Bitcoin. Es equivalente a 10^{-8} bitcoin, y por lo tanto hay 100.000.000 satoshis en 1 bitcoin.

24. **SHA256** – Un tipo de algoritmo de hash criptográfico. Es actualmente usado por el software Bitcoin.

25. **Sistema de Número Hexadecimal (Hexadecimal Number System)** - Mientras que el sistema de numeración decimal se basa en 10, el sistema hexadecimal se basa en 16, y el sistema emplea los símbolos del 0 al 9 para representar los números del 0 al 9 y los símbolos A, B, C, D, E y F (en minúsculas o mayúsculas) para representar los números del 10 al 15. Los números hexadecimales tienen el prefijo 0x, por lo que el decimal 16 es 0x10 en hexadecimal, el decimal 17 es 0x11, y así sucesivamente.

26. **Software De Código Abierto (Open Source Software)** - Código de software (modelo) que se comparte y está disponible para que cualquier persona lo pueda ver, inspeccionar y modificar para poder reproducir los programas ellos mismos.

ÍNDICE

F

G

H

I

L

M

N

O

P

Colaboradores

Coordinadores Traductores

Arturo Monzón
@monzon_arturo
linkedin.com/in/arturomonzon

Apasionado e interesado en seguir aprendiendo sobre Blockchain, Fintech y Transformación Digital. Cuenta con una experiencia de 19 años en el primer banco del sistema financiero del Perú (Banco de Crédito), donde trabajó en las áreas de tesorería, riesgos, asesoría de inversión, banca minorista y banca pequeña empresa (pyme). Actualmente sigue el programa directivo de "Banca Digital" en el Instituto de Estudios Bursátiles (IEB) de Madrid, España, y, es consultor en banca y finanzas. Ha participado en eventos relacionados a Blockchain en Perú, Colombia, Chile y España. Bachiller en Ingeniería Industrial y Magíster en Finanzas por la Universidad del Pacífico (Perú).

Alex Preukschat
@AlexPreukschat

Apasionado por la continua transformación social propiciada por la tecnología y de la nueva economía P2P. Desde 2012 es asesor de desarrollo estratégico y, gestión de proyectos del ecosistema Blockchain. A lo largo de su carrera ha trabajado en el sector financiero (FinTech) y turismo en facetas vinculadas a tecnología, marketing digital

y desarrollo de negocio en distintos países. Nodo Coordinador de Blockchain España (BlockchainEspana.com) y SSIMeetup.org, Autor coordinador del best seller "Blockchain: la revolución industrial de Internet" (LibroBlockchain.com) y autor de la primera novela gráfica del mundo sobre Bitcoin (BitcoinComic.org - Bitcoin: la caza de Satoshi Nakamoto), así como de juegos móviles, inspirados en el mundo de las criptomonedas, desde MoneyFunGames.com. Estudió en la Universidad Pontificia Comillas-ICADE E-4 en Madrid/España y ESB Reutlingen/Alemania.

IÑIGO MOLERO MANGLANO
@Imolman

Licenciado en Derecho y Master en Periodismo. Consultor en Comunicación y tecnología Blockchain. Muchos años ligado al tercer sector como responsable de Comunicación en ONG´s y en Redes de Asociaciones Internacionales. Ha participado también en distintos proyectos europeos, auspiciados por la Comisión Europea, y otros de índole internacional, liderando las tareas de Comunicación. Colaborador y analista en OroyFinanzas.com, co-autor del libro "Blockchain: la revolución industrial de Internet", cofundador de #Blockchain4GoodRocks Madrid, y asesor en EthicHub.

Colaboradores traductores

Adrián Bernabéu Escudero
linkedin.com/in/adrian-bernabeu-escudero

Socio cofundador de CryptoInvest, cofundador del vehículo de inversión privado Manhattan Bull, ponente habitual en TheCube Madrid, colaborador de la Escuela de Inversión, formador, emprendedor, amante de los negocios. Apasionado de la tecnología Blockchain, Bitcoin y criptomonedas. Licenciado en la Universidad Politécnica de Valencia y egresado en la primera promoción del postgrado "Experto en Bitcoin y Blockchain" de la Universidad Europea de Madrid.

Alex Viñas Salles
@VinyasAlex

Graduado en International Degree in Management por la Universidad de Navarra. Actualmente Consultor Financiero para importantes entidades en Nfq Advisory Solutions, trabajando en proyectos regulatorios y sobre tecnología Blockchain. Impulsor y colaborador en tecnologías disruptivas como Blockchain o Sistemas descentralizados. Interesado en los laboratorios de ideas y desarrollos para aplicaciones prácticas de la tecnología de los Smart Contracts, sobre nuevas redes P2P y redes permisionadas. Gran apasionado del nuevo paradigma que viene de la mano de las criptomonedas

descentralizadas, así como todos los proyectos focalizados en descentralizar cualquier sector de la economía.

Beatriz Lizarraga Mariezcurrena

@bealiza

Especialista en marketing y desarrollo de negocio, cuenta con una larga trayectoria en medios de comunicación, así como en agencias de publicidad. En los últimos años ha dirigido procesos de transformación digital. Consultora, emprendedora y Nodo Comunicación Blockchain España, es una entusiasta de la economía del token y de la transformación digital. Licenciada en Publicidad y Relaciones Públicas por la Universidad Complutense de Madrid, Master Internet Business (MIB) en ISDI y Curso Especializado en Blockchain en ICEMD/ESIC.

Enrique Palacios Rojo

@henryfyodor
linkedin.com/in/enriquepalaciosrojo

Licenciado en Ciencias Económicas y Empresariales por la Universidad Complutense de Madrid con más de 15 años de experiencia nacional e internacional en el sector financiero en áreas relacionadas con la tesorería, regulación y mercado de capitales y actualmente en la pasarela de pagos éticos Fairbill intentando buscar nuevas soluciones aplicando nuevas tecnologías especialmente blockchain. Con formación de postgrado en la 1ª promoción de Banca Digital y Fintech por la Universidad

Internacional de la Rioja -UNIR- me entusiasman todos los proyectos que aporten valor a la sociedad y mejoren las habilidades de las personas, en especial aquellos que tengan que ver con la educación y el deporte.

IVÁN DURÁN FABEIRO

Administrativo banca. Apasionado del Bitcoin, expectante ante los próximos cambios de paradigma que vamos a vivir y muy agradecido por tener la oportunidad de aportar mi granito de arena en la difusión. Productor de Caribian Drim. Hijo de María y padre de Mateo.

JOSE ANTONIO BRAVO MATEU

@jabravo

Licenciado en Ciencias Económicas y Empresariales por la Universitat de València (1993). Master en Contabilidad. Máster en Dirección Contable y Financiera por la Universitat Oberta de Catalunya (2006), y Máster en Tributación y Asesoría Fiscal por la Universidad a Distancia de Madrid (2012). Durante más de 20 años ha desarrollado tareas de contabilidad, auditoría interna y tributación de empresas, y desde hace 5 años desarrolla en paralelo la actividad de asesoramiento tributario y contable a profesionales autónomos y microempresas. Interesado en nuevas tecnologías, a partir de 2014 participó en los primeros meetups sobre Bitcoin, y colaboró en la creación de Avalbit (Asociación Valenciana del Bitcoin y las Criptomonedas).

JOSE LUIS ABIA ELVIRA
@joseluisAE
linkedin.com/in/joseluisabiaelvira

Ingeniero de Telecomunicaciones de la "Escuela Técnica Superior de Ingenieros de Telecomunicaciones" (E.T.S.I.T.), Universidad Politécnica de Madrid. Freelance con más de 30 años de experiencia en la gestión de programas de tecnologías avanzadas en las áreas de telecomunicaciones, electrónica profesional, comunicaciones por satélite y de defensa. Certificaciones en estándares ISO 9001, ISO 27000 e implementación DoDI 8500 (MAC 1, 2 y 3). Apasionado por las nuevas tecnologías y el futuro de la humanidad. Fundador de comunidades abiertas: HackMadrid%27, BlockMad, TechBusiness3.0, una activa colaboración en comunidades de Blockchain, Programación Funcional, Haskell, Rust y Computación Cuántica. Cofundador de Epsilon Hack Services & Training.

JOSE MANUEL ARENILLAS
@jochemin
linkedin.com/in/jose-manuel-arenillas-5193221a

Aita de Ane. Administrador de sistemas. Interesado en Bitcoin desde hace años. Me gasté 1 BTC en la despedida de soltero de un amigo, se lo recuerdo de vez en cuando y no podía dejar pasar esta oportunidad de dejarlo por escrito. He minado, tradeado y ahora enfocado en aprender y transmitir. Leyendo sobre Bitcoin cada día. Un placer haber colaborado en esta traducción para posibilitar su lectura en español.

ROBERTO FERNÁNDEZ HERGUETA

@rfhergueta

Director global de Blockchain y responsable de negocios digitales emergentes en everis (NTT Data Company). Matemático de formación y apasionado por la tecnología y su contribución a la mejora de la sociedad. Más de 17 años de experiencia en proyectos de desarrollo de negocio, innovación y estrategia con clientes estratégicos, tanto a nivel nacional como internacional. Miembro de la junta directiva y del equipo promotor del consorcio nacional Blockchain: Alastria. Colaborador de diferentes escuelas de negocio como Imperial Business School, ESADE, ESIC, … donde imparte clases sobre la realidad del nuevo mundo descentralizado y los nuevos modelos de marketing del siglo XXI. Coautor del libro "Blockchain: la revolución industrial de Internet" del Grupo Planeta, liderado y coordinado por Alex Preukschat.

Uno de los valores más transcendentes del Bitcoin es que nos hace reflexionar y repensar como funcionan los fundamentos de nuestra sociedad. Que mejor que hacerlo a través de un libro que fue construido colectiva y descentralizadamente desafiando los esquemas editoriales tradicionales.

Rodolfo Andragnes y **Diego Gutiérrez Zaldívar** (CEO y Co-fundador de RSK Labs)
- Co-fundadores de ONGs Bitcoin Argentina e Iberoamérica

Un viaje en el tiempo para vivir de primera mano como se gestó uno de los grandes cambios en la humanidad. Una joya. Imposible de hacer en ninguno de los cambios tecnológicos anteriores.

Joaquín Moreno - BizDev LATAM ConsenSys

El libro para comprender una genialidad llamada Bitcoin, desde los textos de su misterioso creador: Satoshi Nakamoto.

Mauricio Tovar - Co-Director grupo de investigación InTIColombia
de la Universidad Nacional de Colombia y miembro de Blockchain Colombia

---

El Libro de Satoshi es un esfuerzo colectivo de la comunidad de Blockchain España, que ha traducido al español, para toda la comunidad de habla hispana, la famosa obra de Phil Champagne "The Book of Satoshi". El libro recoge los escritos e intercambio de opiniones realizadas por Satoshi Nakamoto a lo largo de dos años, antes de desaparecer de la vida pública.

ALIANZA BLOCKCHAIN IBEROAMÉRICA
BITCOIN IBEROAMÉRICA
BLOCKCHAIN ESPAÑA