[WHITE PAPER]
VERSIÓN EN ESPAÑOL

Bitcore BTX

The future is NOW!

Bitcore BTX

Una Solución de Pago Dirigida Genuinamente por la Comunidad

¿ESTÁ LISTO PARA EL FUTURO?

Escrito por
Christina

Gráficos por
DgCarlosLeon

Traducido al Español por
Iván León - Ubikalo

Ponte en contacto con el equipo fundador de Bitcore:

JON, STEVE y CHRIS

info@bitcore.cc | www.bitcore.cc

Contents

1 Bitcore – Una Solución de Pagos Dirigida Genuinamente por la Comunidad

Bitcore es una criptomoneda diseñada para hacer la visión del Bitocoin original a prueba del futuro.

Bitcore mantiene las ventajas centrales del Bitcoin's – pero el equipo fundador de Bitcore está tomando audázmente la tecnología original del Bitcoin llevándola hacia el futuro. Bitcore, originalmente un fork híbrido de Bitcoin, se caracteriza por un mecanismo de concenso proof-of-work e implementa todas las Propuestas de Mejoramiento de Bitcoin (BIP´s-Bitcoin Improvement Proposals) del protocol de Bitocoin.

A través de su estructura delgada y una comunidad activa, Bitcore es más ágil en la implementación de innovaciones necesarias que otras monedas. En la cadena de bloques de Bitcore, el SegWit (Segregated Witness) se activó completamente 4,5 meses antes que en la cadena de bloques de Bitcoin, haciéndolo **totalmente compatible con el Lightning Network.**

Y lo más importante, **Bitcore implementa una verdadera descentralización y empoderamiento del usuario**:

- El Algoritmo de minado **ASIC-resistant** de Bitcore reestablece la participación comunitaria y contrarresta los efectos de la centralización del minado.
- La aplicación de Bitcore de filtros Bloom[i] reduce significativamente el almacenamiento requerido **para correr un nodo entero de cadena de bloques**, permitiendo que más usuarios individuales se empoderen completamente y lleguen a ser pariticipantes de Bitcore via SPV/Billeteras ligeras.
- El novedoso proceso de airdrop de Bitcore resulta definitivamente en una **distribución más equitativa de las monedas**, alentando el uso de Bitcore como medio de pago. La decisión de la comunidad de Bitcore de olvidarse de la Oferta Inicial de Monedas (ICO) ha mantenido a los especuladores al margen.
- Bitcore es mas rápido que Bitcoin, más rápido incluso que Paypal, permitiéndole convertirse en una opción real de **pagos de uso diario**, gracias a la implementación a tiempo del SegWit y a otras decisiones de diseño. En la Lightning Network se pueden soportar teóricamente un número ilimitado de transacciones offline. Las **comisiones bajas de Bitcore** de alrededor de us$0,003 por transacción lo hace más adecuado para el uso diario y hace factible los micropagos.
- Bitcore es un **proyecto de código de fuente abierta**: producido colaborativamente, compartido libremente, publicado transparentemente y desarrollado para ser un bien común más que la propiedad o negocio de una sola compañía o persona[ii].

"Bitcore: El Fork más inteligente del Bitcoink"

-- Jimmy Song[iii], Desarrollador Central Bitcoin

En resumen:

Bitcore es la **solución original para pagos digitales de igual a igual conducida por la comunidad**, adaptada a las necesidades del mañana. Si Satoshi Nakamoto hubiese conocido en 2008 lo que nos ha enseñado la experiencia a la comunidad crypto en los últimos 10 años, Bitcoin[iv] se hubiese visto como el Bitcore actual desde el mismo inicio. Hoy, Bitcore ofrece a todos la oportunidad de ser parte de la vision original de Satoshi, fresca y sin manchas por los cuestionables desarrollos económicos del pasado.

2 De Bitcoin a Bitcore

> *"Una version purista del dinero electrónico de igual a igual permitiría pagos online que serían enviados directamente de una de las partes a la otra sin pasar por una institución financiera. Las firmas digitales proveen parte de la solución, pero los beneficios principales están perdidos si una tercera parte de confianza es requerida para prevenir el doble gasto. Nosotros proponemos una solución al problema del doble gasto usando una red de igual a igual."*

-- Satoshi Nakamoto, 2008

Es esta la declaración que dió nacimiento a concepto modero de la criptomoneda y de hecho al de la finanza descentralizada. Hasta el momento en que Satoshi Nakamoto diseñó el concepto original del Bitcoin, todo el mundo financiero se basaba en autoridades centrales, o más exactamente: **Puntos Centrales de Falla.** La seguridad del dinero de todo el mundo estaba supeditado en la seguridad y salud económica del banco o institución financiera que controlaba los fondos.

Cada caso de falla de seguridad, conducta inadecuada o bancarrota en el mundo financiero significaba que aquellos que confiaron en esas instituciones para proteger sus ahorros podían potencialmente ser dejados sin sus fondos necesarios.

Sin necesidad de inventar alguna clase de tecnología no existente ya, Satoshi Nakamoto combinó los paradigamas existentes en una forma novedosa para resolver este problema: Un Libro Mayor Distribuido y asegurado por prueba de trabajo (proof-of-work) que proveería de ahora en adelante un marco en el cual los participantes se verían forzados a mantenerse honestos, sin intervención –y con la potencial manipulación- de cualquier autoridad central.

El proceso incentivado llamado “minado” era y es central en el funcionamiento de este sistema. Un grupo de reglas aseguran que el sistema **opere autónomamente y sosteniblemente** esencialmente sin ninguna orden de “líderes” o de hecho de ninguna clase de individuos u organización. Esto se hizo a propósito con la idea de mantener el principio de decentralización: Si una compañía era la responsable de asegurar una operación sin contratiempos, entonces esa entidad representaría un potencial punto de falla – el cual derrotaría el propósito del protocolo.

En este documento (Whitepaper), daremos una mirada más de cerca a las características del protocolo original del Bitocoin – y las formas en las que Bitcore también ha preservado, avanzado y mejorado estas características originales del Bitocoin.

Esto servirá para demostrar por qué y cómo el protocolo de Bitcore es una **poderosa criptomoneda alternativa** que ayuda a facilitar algunos casos prácticos para las criptomonedas que no han sido realizables con la tecnología cripto existente.

2.1 Bitcore como Código de Fuente Abierta

Bitcoin y Bitcore son esfuerzos **genuinos de código de fuente abierta.** La comunidad de Bitcore siente que se está en sincronía con el espíritu descentralizado, participativo y enfocado en la comunidad de Bitcore.

En particular, el desarrollo de Bitcore sólo fue posible debido a la conformidad del Bitcoin con las siguientes características de la fuente abierta, como lo estipula la Iniciativa de Fuente Abierta[v] - y, a su vez, la base de código Bitcore está sujeta a las mismas condiciones y grados de libertad:

1. Redistribución gratuita

2. Inclusión del código fuente

3. Permiso para trabajos derivados, modificaciones y su distribución.

4. Integridad del código fuente del autor.

5. Sin discriminacion contra personas o grupos.

6. Sin discriminación contra campos de esfuerzo.

7. Aplicabilidad de la licencia sin necesidad de ejecución de otra licencia.

8. Licencia no específica para un product.

9. Sin restricciones de otro software a través de la licencia.

10. Neutralidad de la tecnologia de la licencia.

Al adherirse a estos estandares del software libre, Bitcore habilita a la comunidad de código abierto a acceder, modificar y desarrollar su código, sin discriminación por identidad, pasado, intención o industria.

2.2 Distribución: Cambio Uno-a-uno, Fork Híbrido y Airdrop

Los fork clásicos copian la cadena de bloques de Bitcoin en un bloque y un punto en el tiempo específico. Bitcore, sin embargo, ha creado una nueva moneda con una cadena de bloques vacia, con el propósito específico de separar a Bitcore del Bitcoin y establecerlo como una entidad separada.

16.2 millones de monedas Bitcore (BTX) fueron pre-minadas (un número equivalente a los Bitcoin existentes al momento de la creación de la cadena de bloques Bitcore) listas para su distribución en la comunidad.

La distribución de los BTX en la prospective comunidad usuaria se realizó en 3 fases:

- Cambio Uno-a-uno
- Fork Híbrido
- Airdrop

2.2.1 Cambio Uno-a-uno

Durante los primeros 6 meses de existencia de Bitcore, desde Abril del 2017 a Noviembre del 2017, los usuarios de Bitcoin pudieron cambiar sus Bitcoin (BTC) a Bitcore (BTX) en un radio de 1:1

Este cambio se implementó usando una base de datos y la función signmessage de Bitcoin[vi].

De los 16.2 BTX preminados, 590.000 fueron reclamados en este primer paso de distribución. La oportunidad para el cambio 1:1 finalizó el 2 de Noviembre del 2017.

2.2.2 Fork Híbrido

El 2 de Noviembre del 2017, en el bloque #492.820 del protocol Bitcoin, se tomó una instantánea de la cadena de bloques. La distribución de los restantes 15.8 millones de BTX continuó de manera diferente a la usada en la primera fase de Cambio 1:1.

A todas las direcciones de la cadena de bloques de Bitcore cuyas direcciones se correspondieran con las direcciones de la cadena de bloques de Bitcoin y que tuvieran al menos 0.01 BTC les fueron acreditadas con un monto del 50% en BTX, en relación con la cantidad de BTC que tuvieran en la respectiva dirección. En otras palabras, la proporción del financiamiento fue de 0,5 BTX por cada 1,0 BTC.

Los días siguientes, se procesaron aproximadamente 5 millones de transacciones, y alrededor de 8 millones de BTX fueron distribuidos entre todas las direcciones elegibles. Está fue no sólo una forma práctica de distribuir BTX, sino también sirvió para demostrar que la cadena de bloques BTX es capaz de procesar un gran número de transacciones en una cantidad relativamente pequeña de tiempo.

Así que cerca de 8 millones de los 16 millones de BTX preminados fueron distribuidos a la comunidad. De los restantes 8 millones, el 10% fue almacenado por el equipo de Bitcore con el propósito de usarlos para desarrollos técnicos futuros.

2.2.3 Airdrop

El 90% de los 8 millones de BTX restantes fueron distribuidos finalmente en una serie de Airdrops semanales, entregados de acuerdo al un programa diferencial.

En el airdrop inicial, se distribuyó un bono del 25% sobre el balance que tenía la cartera BTX de cada usuario. Luego, los siguientes airdrops se llevaron a cabo con el siguiente programa (con el porcentaje basado en el balance de la cartera BTX de cada usuario):

+5% cada lunes en enero 2018

+6% cada lunes en febrero 2018

+7% cada lunes en marzo 2018

+8% cada lunes en abril 2018

+9% cada lunes en mayo 2018

Con esta última fase se completó la distribución de los BTX preminados.

2.2.4 Ejemplo de Airdrop

He aquí un ejemplo que servirá para ilustrar este proceso de airdrop:

Alicia tiene 20 BTX en su cartera. Ella registró su cartera para el airdrop de enero, cuando el bono era del 5%. Por lo tanto ella era elegible para recibir el 5% sobre su balance de BTX en el airdrop de enero:

20 BTX * 5% = 1 BTX

Por lo tanto Alicia recibió 1 BTX adicional y su balance total subió a 21 BTX después del airdrop de enero

2.2.5 ¿Por qué Fork Híbrido y Airdrop?

La diferencia crucial entre este modelo y el modelo tipico del “fork” es la siguiente: En lugar de distribuir la misma cantidad de monedas disponibles emitidas en el momento de la instantánea de la cadena de bloques de Bitcoin, solo se distribuyeron el 50% de BTX de esta manera. Y el 50% restante fue distribuido sólo a usuarios activos. De esta forma el equipo de Bitcore se aseguró que los titulares activos de grandes montos de Bitocoin, también conocidos como ballenas, no se convirtieran automáticamente en “ballenas Bitcore”, y así sesgar el equilibrio de poder dentro de la comunidad Bitcore, así como también limitar la disponibilidad de Bitcore de una forma que podría hacer daño en las futuras operaciones del ecosistema. En lugar de eso, el equipo Bitcore logró manejar el objetivo de una **distribución más equitativa de las monedas** que antes de realizar el fork de Bitcoin, y en concordancia con los ideales de decentralizacion y participación de la comunidad Bitcore.

2.3 Sin ICO

Ya que es un fork Híbido, el lanzamiento de bitcore no fue diseñado o capitalizado por una Oferta Inicial de Monedas (ICO)

Esta fue una decisión consciente de la comunidad Bitcore con la intención de fomentar oportunidades y la participación iguales entre todos los usuarios potenciales de BTX alrededor del mundo. En los últimos años las tendencias y desarrollos de la criptosfera han demostrado que las ICO atraen especuladores, incrementando la volatilidad de la criptomoneda ofrecida y desechando luego su uso cotidiano. Para ir más allá, las ICO conminan a una afluencia de inversionistas privados ricos que "compran" a su manera un poder y una influencia desproporcionada sobre las comunidades cripto. Y por último pero no menos importante, se aplican diferentes marcos regulatorios a las ICO cuyos equipos están establecidos en diferentes países y en muchas de ellas de manera explícita se excluye a ciudadanos de ciertos países en la participación de dichas ICO.

Estas limitaciones arbitrarias no son aceptables para la comunidad Bitcore. Nos esforzamos para crear un cripto ecosistema útil que sea igualmente acsequible para cualquier interesado, sin importar su locación y nacionalidad.

Para ser tan independiente de las regulaciones locales como sea posible, hemos escogido operar como un consorcio de individuos interesados sin fines de lucro. La membresía en el equipo fundador y la participación en la comunidad Bitcore depende solamente de los niveles de habilidad del individuo, sus intereses y compromiso, sin fronteras geográficas arbitrarias.

3 Solución y Especifícaciones Técnicas

Bitcore incluye innovaciones clave que lo hacen particularmente adecuado como medio de pago diario, tanto en el contexto personal como en el comercial. Cada una de estas innovaciones, así como su rol en el incremento en la eficiencia y usabilidad de Bitcore serán detalladas en esta sección.

Para una mirada rápida, las especificaciones claves de Bitcore están resumidas a continuación:

Nombre **Bitcore**

Ticker **BTX**

- Lanzado el 24 de Abril de 2017
- Suministro máximo de monedas 21 millones
- Tamaño de bloque 10MB (20MB con el SegWit)
- 2.5 min tiempo de bloque promedio (average blocktime)
- Tamaño de la cadena de bloque actual aproximadamente 950 MB
- Algoritmo de minado (mining algorithm)Timetravel10 (GPU)
- SegWit y Bloom online
- Algoritmo de reorientacion de dificultad suave Smooth diff64_15

- Distribución justa: Cambio BTC y Airdrops

"[Bitcore] innova limpiando las cosas"

-- Jimmy Song[vii], Desarrollador Central Bitcoin

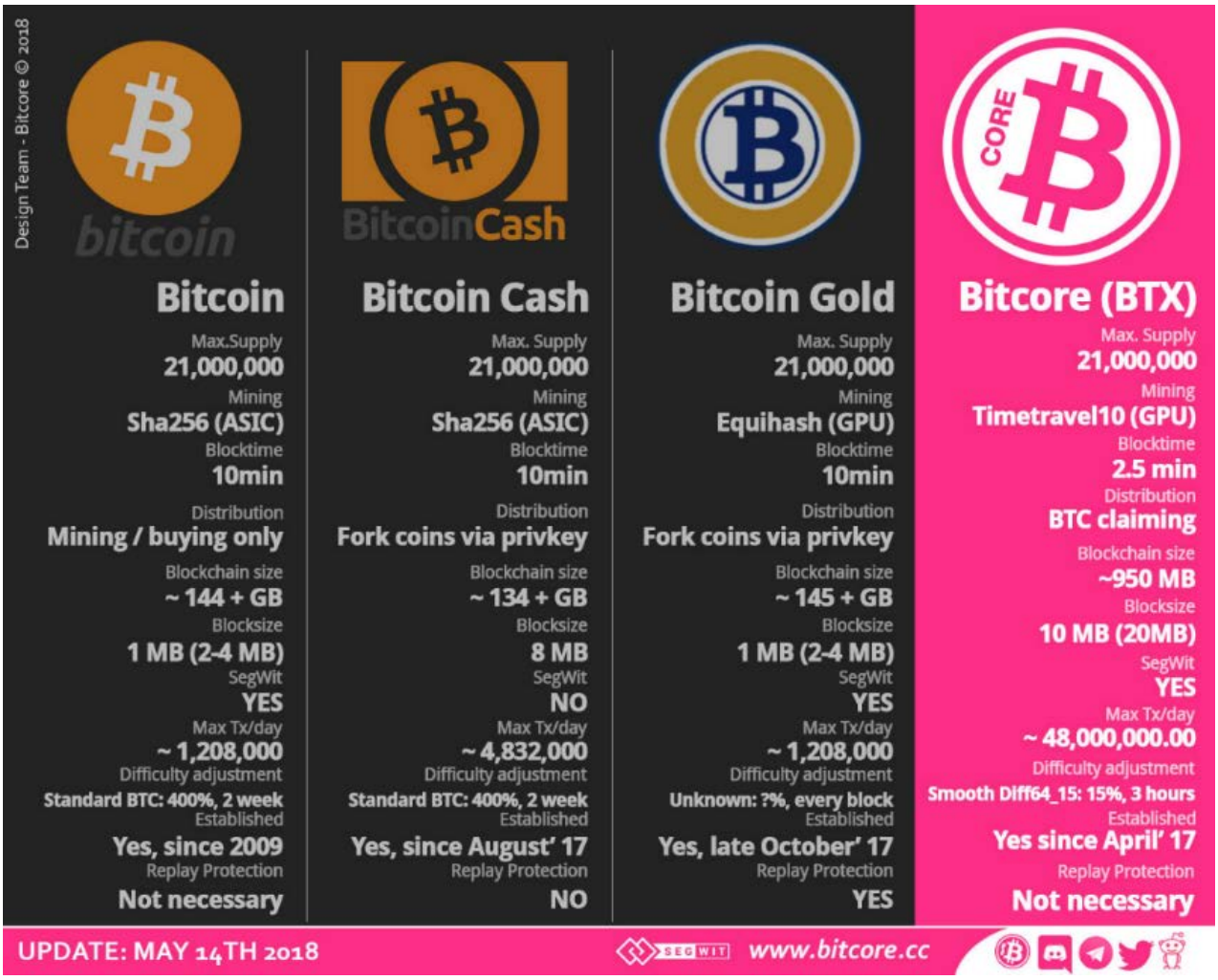

Figure 1: Bitcoin, Bitcoin Cash, Bitcoin Gold and Bitcore - comparison chart.

3.1 Suministro de monedas

El número máximo de monedas que serán producidas en la plataforma Bitcore está pautado para ser de 21 millones. Este número fue escogido deliberadamente para igualar el número de monedas del protocolo Bitcoin al momento del fork híbrido.

Este número limitado en el suministro de monedas es el resultado del algoritmo de reducción a la mitad de Bitcoin que reduce la recompensa de la base de monedas para los mineros en un 50% cada 210.000 bloques, reduciendo por lo tanto el número de nuevas monedas minadas cada cuatro años, hasta que alcance aproximadamente el cero para el año 2140.

La recompensa de bloques de Bitcore es idéntica a la recompensa de bloques de Bitcoin los primeros 10.000 bloques,: 12,5 BTX por bloque, con un tiempo de bloque de 10 minutos. Posteriormente, una actualización disminuye la recompensa a 3,125 BTX por bloque con un tiempo de bloque promedio de 2,5 minutos.

Bitcore aplica el mismo algoritmo de reducción a la mitad a sus recompensas coinbase, pero en intervalos de 840.000 bloques. Por lo tanto el suministro de Bitcore está limitado de la misma manera que el suministro de Bitcoin.

La siguiente gráfica muestra la reducción a la mitad de la recompensa de bloque de Bitcore:

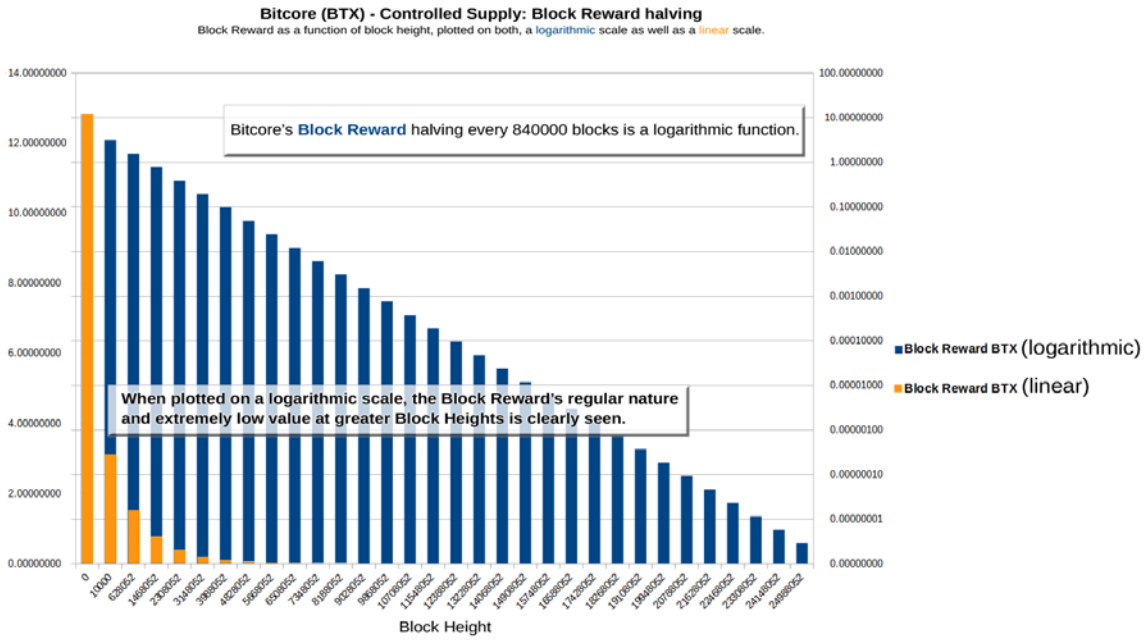

Figura 2: Recompensa de bloque disminuyendo a la mitad en el tiempo.

Esta reducción a la mitad de la recompensa ajustada a intervalos de bloques conlleva a un número final predeterminado de monedas, concepto llamado suministro controlado.

3.2 Blockchain y Algoritmos

Bitcore usa un algoritmo proof-of-work tal como el de Bitcoin. Sin embargo, el ajuste de dificultad se resuelve de forma innovadora, empleando el algoritmo de reorientación de dificultad suave Core Shield 64_15 tal como se describe más abajo.

Otra diferencia crucial con el Bitcoin son los tiempos de bloques reducidos del Bitcoin, una cuarta parte de los tiempos de bloques del Bitcoin, los cuales están haciendo a Bitcore más utilizable y más seguro, como se detalla más adelante en esta sección. Al mismo tiempo, el tamaño del bloque es significativamente más grande, contribuyendo nuevamente a una velocidad de transacción mayor y una mejor usabilidad.

Finalmente la activacion del SegWit – 4,5 meses antes que la cadena de bloques de Bitcoin – y la compatibilidad con el Lightning Network hace que Bitcore sea un medio de pago ideal para las necesidades del mañana de individuos y de negocios.

3.2.1 Reorientación de Dificultad con Core Shield 64_15

En criptomonedas basadas en proof-of-work, la reorientación de la dificultad – en otras palabras, el ajuste en la dificultad con la cual los mineros pueden encontrar el siguiente bloque – tiene como propósito principal el asegurar tiempos de bloques consistentes. Sin la reorientación de dificultad, los tiempos de bloques disminuirían al aumentar el número de mineros activos en la cadena de bloques en determinado momento ya que esto incrementaría la probabilidad de que el valor hashing correcto sea encontrado entre este gran número de mineros.

Por lo tanto, en la reorientación de la dificultad, el nivel de dificultad para descubrir el siguiente bloque aumenta cuando hay muchos mineros activos en el protocolo, y disminuye cuando hay pocos mineros activos.

En Bitcoin, el nivel de dificultad es ajustado cada 2016 bloques. Con un tiempo de bloque de aproximadamente 10 minutos, esto equivaldría a un ajuste cada dos semanas - una tasa bastante lenta que no responde a aumentos o disminuciones a corto plazo en la actividad minera. Sin embargo, estas fluctuaciones de la actividad minera a corto plazo se observan con frecuencia cuando los mineros cambian entre Bitcoin y sus forks, buscando la mejor relación entre el esfuerzo de extracción (determinado por la dificultad) y la recompensa.

En orden para resolver este reto, Bitcore ha reemplazado el método de reorientación de la dificultad del Bitcoin con un algoritmo novedoso, llamado Core Shield 64_15.

En el Core Shield 64_15, la dificultad del bloque se reajjusta cada 64 bloques. Con un tiempo de bloques de Bitcore de solo 2,5 minutos, los reajustes de dificultad se llevan a cabo cada 2 horas y 40 minutos. Esto hace que la dificultad de bloque de Bitcore sea más sensible que la de Bitcoin pero al mismo tiempo se evitan ajustes demasiado turbulentos a corto plazo: La dificultad no cambiará en más de un 15% en cada reajuste, llevándose a cabo cambios graduales en lugar de cambios dramáticos.

El algoritmo de reorientación de dificultad de Bitcore es por lo tanto no sólo más eficiente, sino que conduce a tiempos de bloques más predecibles y además asegura la red contra ataques de doble gasto que pueden tener más probabilidades de tener éxito en tiempos de dificultad hash desproporcionadamente baja.

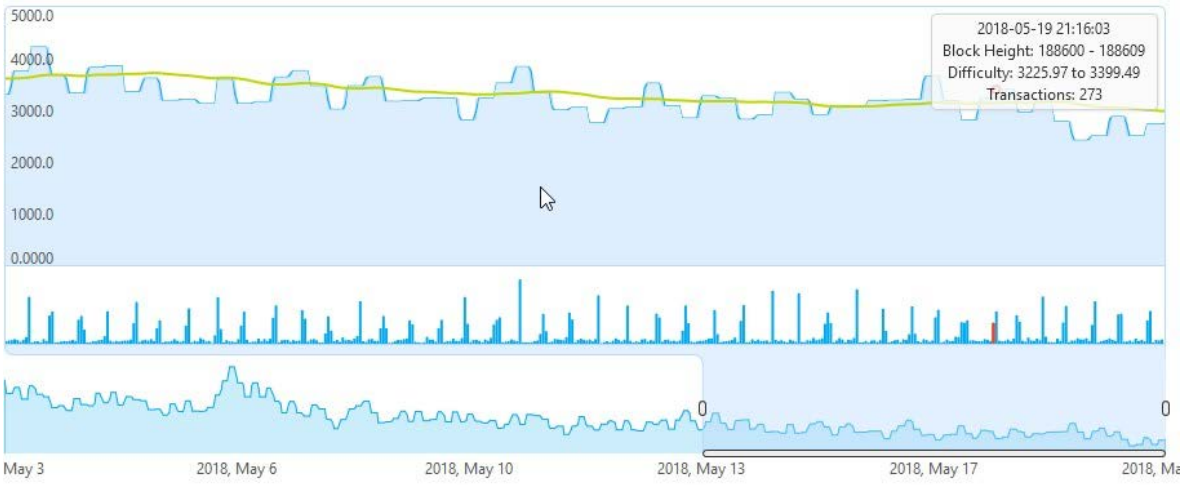

Figura 3: Reorientación de Dificultad en Bitcore (datos de mayo 2018).

3.2.2 Tiempos de Bloque Más Cortos

El protocolo de Bitcore está diseñado para rendir un bloque cada 2,5 minutos – una cuarta parte del tiempo de bloque del Bitcoin de 10 minutos.

Tiempos de bloque más cortos son ventajosos por numerosas razones diferentes.

La primera es que se permiten **confirmaciones más rápidas.** Cada transacción en la cadena de bloques empieza su existencia con una transacción sin confirmar, la cual eventualmente es recogida por los mineros que compiten para crear el siguiente bloque. Cada vez que un bloque válido es creado en la cadena de bloques, las transacciones que contiene se consideran confirmadas.

Dado que varios bloques válidos con diferentes transacciones pueden existir en paralelo dentro de la cadena de bloques, solo la creación de bloques adicionales prueban que una transacción se ha convertido en parte de la cadena activa, por ejemplo, la cadena existente más larga. Esta política es parte del mecanismo de concenso proof-of-work para impedir los ataques de doble gasto realizados por nodos maliciosos: La cantidad de trabajo (y por tanto de energía) para crear un solo bloque con una transaccón fraudulenta puede ser algo manejable por el atacante. Sin embargo, esta transacción fraudulenta a la larga no será parte de la cadena activa a menos que el atacante pueda gastar una cantidad mucho más significativa de trabao para crear el suficiente número de bloques para lograr que esta sea la cadena más larga.

Por esta razón, muchos comerciantes y otras entidades que aceptan pagos con criptos esperan por más de un bloque válido antes de aceptar como confirmada a una determinada transacción. En general, los pagos de grandes montos tienen mayor riesgo de ser falsificados, y por lo tanto se requieren tiempos de confirmación mayores por la seguridad del comerciante.

Los tiempos de bloques de 10 minutos fueron escogidos originalmente por Satoshi Nakamoto para asegurar la red Bitcoin según su tamaño de hace casi 10 años. Desde entonces, la red ha crecido considerablemente, haciendo más difícil para los actores maliciosos el poder introducir transacciones fraudulentas en la red.

Vitalik Buterin, fundador de Etherum, argumenta que los tiempos de bloques *más cortos* son preferibles por encima de los más tiempos largos[viii] porque ellos proveen una mayor granularidad de información: Las cadenas activas correctas serán detectadas más rápidamente y con preferencia sobre las cadenas incorrectas y se lograría mucho antes un nivel de seguridad aceptable para las transacciones de tamaño pequeño y mediano. Sin embargo, el acortamiento en los tiempos de bloques incrementa el riesgo de centralización de las cadenas de bloque basadas en proof-of-work, ya que se le otorga más poder a grandes participantes que podrían engañar a la red. Asi que los tiempos de bloques no pueden reducirse arbitrariamente, pero se puede lograr con un diseño cuidadoso y manteniendo en mente estas tendencias conflictivas.

A la luz de estas consideraciones, Bitcore ha decidido disfrutar totalemente el privilegio y los beneficios que vienen con una reducción modesta del tiempo de bloques a 2,5 minutos.

3.2.3 Tamaño de Bloque Más Grande

Actualmente los bloques de Bitcore tiene un tamaño de 10 MB, eso sin tener en cuenta el espacio adicional que proviene del 're-pesaje' de los datos debido a SegWit, el cual aumenta el tamaño a 20 MB. Por lo tanto Bitcore puede producir 80 MB en bloques (40 MB de los cuales corresponden a SegWit) en el mismo intervalo de tiempo en el que Bitcoin produce 2 MB (1 MB sin el SegWit)

Bloques más grandes contienen más transacciones, lo que a un tiempo de bloque constante equivale a un rendimiento de transacción más rápido. El rendimiento de transacción siempre ha sido un tema crítico en relación con la habilidad de la criptomoneda para competir con las soluciones de pago fiat: VISA puede manejar 1.700 transacciones por segundo (TPS) y PayPal 11 TPS por lo menos.

Con el SegWir activado Bitcoin puede manejar alrededor de 11 TPS, aunque ha tenido repuntes con hasta 20 Transacciones por Segundo durante cortos períodos de tiempo.

Para lograr una amplia adopción de los metodos de pago criptos, la escalabilidad de la red de cadena de bloques obviamente debe mejorar, y el rendimiento debe aumentar. Dos soluciones a este reto se discuten comúnmente: Incrementar el tamaño del bloque o introducir una solución de escalamiento off-chain como el Lightning Network.

La comunidad Bitcore ha optado por incrementar el tamaño del bloque a 20 MB, llevando la capacidad de procesamiento de 80 MB por cada 10 minutos o aproximadamente 224.000 transacciones en 10 minutos. Con SegWit, el potencial máximo del tamaño del bloque se incrementa aún más, hasta los 20 MB, llevando la capacidad de procesamiento de 80 MB por cada 10 minutos o 208.000 transacciones en 10 minutos.

Dado el promedio de 224 bytes/transacción, la cadena BTX es teóricamente – si todos los nodos de la red hicieran disponible todo su- capaz de manejar 350 TPS o 550 TPS bajo condiciones óptimas, aún sin tomar en cuenta el factor de que algunas transacciones pudieran ser conducidas off-chain via Lightning Network.

Bitcore ya probó su capacidad para manejar gran cantidad de transacciones en cortos intérvalos de tiempo cuando 5 millones de transacciones fueron procesadas en poco días el 2 de noviembre del 2017, cuando ocurrió la activación del fork híbrido (ver sección 2.2 del presente documento)

3.2.4 Activation de Segregated Witness (SegWit)

El Segregated Witness (SegWit) fue activado el 17 de abril del 2017, con el bloque #3.000 – 6 meses antes que el Bitcoin. Antes de la activación, los mineros Timetravel10 de Bitcore empezaron con la creación exitosa de bloques que cumplían con el SegWit.

SegWit prove multiples beneficios inmediatos:

- Eliminación de la maleabilidad no deseada en la transacción
- Incremento de la capacidad
- Pesaje de data basada en como afecta el desempeño del nodo
- Firma de cobertura de valor
- Escalada lineal de las operaciones sighash
- Seguridad incrementada para el multisig
- Seguridad “almost-full-node” más eficiente
- Versión de script

3.2.5 Compatibilidad con Lighting Network

El Lighting Network[ix] es una red de transferecia que opera en una capa sobre la cadena de bloques de Bitcore. Por su funcionalidad al usar contratos inteligentes, permite pagos instantáneos entre todos los participantes de la red, obviando la necesidad de esperar por confirmación, tal como se describe en las secciones previas de este documento.

Adicionalmente a los pagos instantáneos, el Lightning Network confiere otras ventajas:

- Escalabilidad aumentada como efecto secundario de los pagos instantáneos
- Costos más bajos, haciendo que esta solución sea más atractiva para los micropagos también
- Permite intercambios atómicos entre cadenas cruzadas, off-chain, con reglas de concenso de cadenas de bloques heterógenas

Bitcore es totalmente compatible con el Lighting Network y por lo tanto es capaz de soportar pagos instantáneos así como los micropagos.

.

3.2.6 Bajas Comisiones

Con una comisión promedio de us$0,0003 por kilobyte y una comisión media de us$0,0002 por kilobyte, las comisiones de Bitcore son marcadamente menores que las comisiones de las grandes criptomonedas (ver Figura 4). Mientras que 1 kilobyte equivale aproximadamente a 3 transacciones, esto correspode a una comisiones de cerca de us$0,0001 o 0.01 centimo de dólar por transacción.

Esta estructura de comisiones favorables contribuye para que el Bitcore sea utilizable para las transacciones de todos los días e incluso para los micropagos.

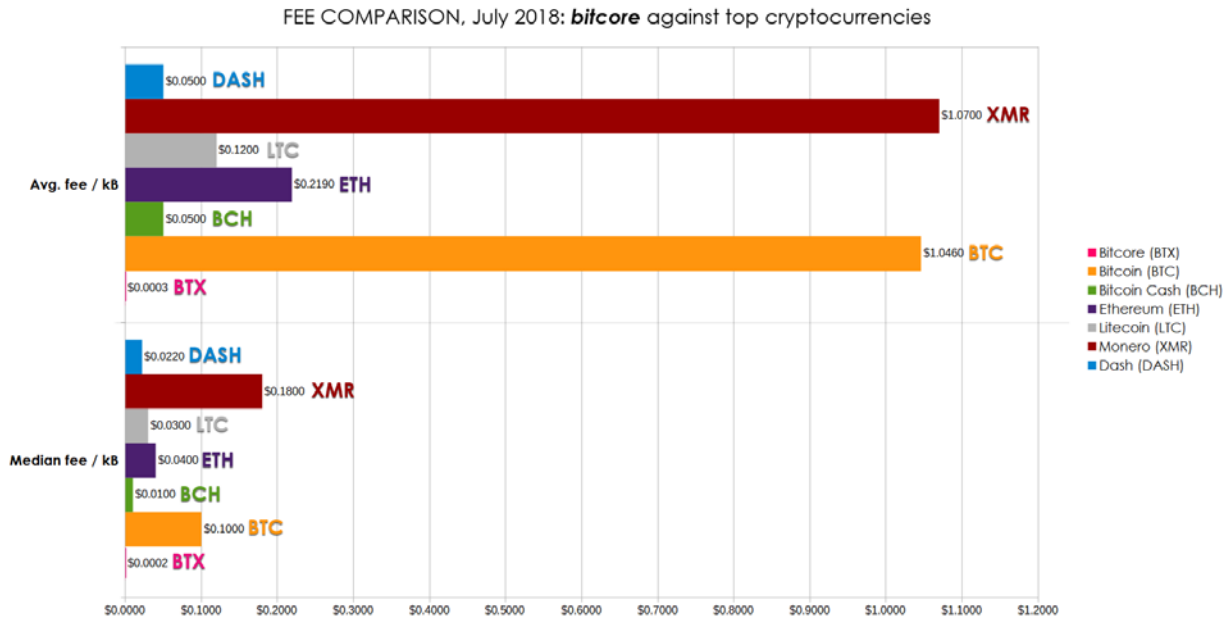

Figura 4: Table comparativa, Bitcore contra otras criptomonedas.

Bitcore tiene una comisión minima requerida de 0.0001 BTX por kilobyte; la comisión recomendada, destinada para apoyar a los mineros, es actualmente (Julio 2018) de cerca de 0.001 BTX por kilobyte. Como los bloques de Bitcore aún no están llenos, no existe una ventaja en términos de incremento en la velocidad de transacción pagando una comisión más alta; sin embargo, este si podría ser el caso en el futuro al incrementarse la carga en la red Bitcore.

4 Comunidad y Mapa de Ruta (Roadmap)

4.1 Comunidad

Bitcore ofrece un amplio rango de ventajas tecnológicas, tales como transacciones veloces y bajos costos de transacción, que lo hacen particularmente útil para aplicaciones de todos los días. Sin embargo, Bitcore no vive sólo por su tecnología: Una fortaleza y una ventaja considerable de Bitcore es su multifacética y diversa comunidad.

Desde su propio inicio, Bitcore se ha enfocado en fomentar una comunida activa y sin restricciones por fronteras geográficas. Esto se ve reflejado , entre otras cosas, en la decisión de Bitcore de no realizar una Oferta Inicial de Monedas (ICO) e ir a favor de un modo de distribución más descentralizado y con igualdad de oportunidades (ver sección 2.2) – una decisión basada en el voto de la comunidad.

La localización y la nacionalidad no son lo único irrelevante en el contexto de la membresía de la comunidad de Bitcore, sino también el idioma. Es por esto que Bitcore ha estado presente en muchos canales de Redes Sociales en muchos países e idiomas diferentes desde el principio.

Hay muchas sub-comunidades activas en una gran variedad de idiomas. Notablemente especiales son el desarrollo y la prominencia de las comunidades Turcas e Hispanohablantes dentro de Bitcore. Uno de los objetivos de Bitcore es reforzar dichas iniciativas regionales, las cuales contribuyen masivamente al fortalecimiento de Bitcore.

4.2 Mapa de Ruta (Roadmap)

Bitcore, como se detalló anteriormente, es un proyecto guiado exclusivamente por la comunidad.

No hay una autoridad central o un comité ejecutivo responsable de ciertos logros diseñados para satisfacer a los accionistas o inversores institucionales.

En lugar de eso, el desarrollo de Bitcore está guiado por las necesidades y las visiones de los miembros de su comunidad. La historia de Bitcore ha mostrado que este modo de operación y estrategía es conducente a la innovación y a la implementación veloz de las mejoras necesarias.

Aunque no hay un Mapa de Ruta (Roadmap) definido centralmente para los próximos años, el equipo de desarrollo de Bitcore está por supuesto constantemente trabajando en implementar nuevas características, tal y como las requiera la comunidad. Actualmente los proyectos planeados y activos pueden verse en el sitio web de Bitcore, https://bitcore.cc.

5 Equipo

Chris
Desarrollador Central C++ y Qt

Chris es el desarrollador principal. Él ha trabajado en varias otras monedas como BitSend, BitCloud entre otras.

Jon
Sistema, Administrador de Servicios y Talento All-Round

Jon es el desarrollador de API, de Electrumm y de infraestructura para Bitcore, y es el responsable por el mantenimineto de nuestra red de servidores. Él fue la principal fuerza detrás del desarrollo y ejecución del fork híbrido y de los airdrops semanales.

Steve
Embajador de Marca & Redes Sociales

Steve supervisa el contacnto con las casas de cambio (exchanges) y los sitios de listados, y es nuestro hombre número uno para contatos de negocios.

David
Publicaciones & Diseño Gráfico

David es la mente artística detrás de Bitcore. Él también está trabajando en publicaciones en medios y apoya el flujo de trabajo del equipo principal.

Ivo
Gerente Principal del Proyecto para Servicios y Negocios

Ivo está ayudando al crecimiento de Bitcore legal y técnicamente.

Thomas
Gerente de Intercambios

Thomas es nuestro gerente de correo electrónico y de intercambios responsable por la mayor parte de nuestras comunicaciones oficiales con los servicios y plataformas de intercambio (exchanges).

Greg (GM)
Experto en Minería y Gerente de Pool

Administrador del Pool de Minería y soporte de mineria en el canal de Telegram.

DgCarlosLeon
Soporte y Diseño Gráfico

Comunicaciones de Bitcore en Reddit y soporte en el área gráfica.

Fahim Altınordu
Soporte

Gerencia de casas de cambio internacional y Turco.

Jose Martin
Gerente de la Comunidad Española

Hampus
Soporte

Hampus está organizando campañas insignia y maneja nuestras cuentas en muchos foros de monedas altarnativas (altcoin).

Brad
Soporte

Brad es el encargado del Facebook de Bitcore.

Ugur
Soporte

Ugur esta manejando la comunidad turca de Bitocre y ayuda con el trabajo de soporte en Telegram.

Eric
Soporte en Telegram y Facebook

Klaas
Soporte

Klaas prove soporte en Telegram y foros de monedas alternativas (altcoin).

Ibrahim Acir
Equipo desarrollados (Turquía)

6 Descargo de Responsabilidad Legal

Esta presentación no es, y nada en ella debe interpretarse como una oferta, invitación o recomendación de una persona, o una solicitud para comprar. La inversión en criptomonedas es altamente especulativa con una volatilidad comparable con los vehículos de inversión tradicionales y puede no ser la apropiada para su situación financiera particular. A los inversionistas potenciales les aconsejamos que acudan a sus consejeros financieros, contadores u otros consejeros confiables para asesorarse en cuanto a si Bitcore es una inversión adecuada para sus restricciones y objetivos financieros. El El rendimiento pasado de Bitcore no es garantía de rendimiento futuro.

Fuentes:

[i] https://blog.medium.com/what-are-bloom-filters-1ec2a50c68ff
[ii] Citing CoinCenter's definition of open source, https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects
[iii] https://medium.com/@jimmysong/bitcoin-diamond-super-bitcoin-bitcore-what-you-need-to-know-f49c35688a39
[iv] https://bitcoin.org/bitcoin.pdf
[v] https://opensource.org/osd
[vi] See https://www.reddit.com/r/Bitcoin/comments/18qy88/bitcoin_message_signing_and_verification/ for further details on message signing in Bitcoin.
[vii] https://medium.com/@jimmysong/bitcoin-diamond-super-bitcoin-bitcore-what-you-need-to-know-f49c35688a39
[viii] https://blog.ethereum.org/2015/09/14/on-slow-and-fast-block-times/
[ix] https://lightning.network/