

eBTC: Una versión tokenizada de Bitcoin en Ethereum con
Contratos Inteligentes, Bajas Tasa de Transacción y Alta Velocidad de Transacción.

Fundación de la Comunidad eBTC

Resumen

eBTC, eBitcoin o Bitcoin de Ethereum es una versión ERC20 tokenizada de Bitcoin en la cadena de bloques de Ethereum. Se propone resolver los problemas de costo de transacción, velocidad, escalabilidad e ineficacia del contrato inteligente de la cadena de bloques original de Bitcoin mediante el uso de la capa de cadena de bloques más eficiente, escalable e interoperable de Ethereum. Con el respaldo de una comunidad global diversa, dinámica y comprometida, eBTC tiene la intención de convertirse en un sistema electrónico de pago y efectivo de punto a punto más asequible, rápido y flexible. Tiene la intención de hacerlo conservando los ideales básicos de Bitcoin e integrándolos con el ecosistema de Ethereum. El año 2017 fue testigo del surgimiento de varias horquillas de Bitcoin, todas tratando de resolver una o más de sus preocupaciones existentes: baja velocidad de transacción, altos costos de transacción y minería centralizada. Sin embargo, ninguna de las horquillas en la actualidad tiene la capacidad de resolver efectivamente todos estos problemas. En contraste, el diseño aparente y extrañamente simple de eBTC le permite abordar de manera eficiente estos desafíos al tiempo que agrega capacidades de contrato inteligente a los ideales básicos de Bitcoin. Con una mayor concienciación y aceptación, eBTC planea convertirse en un mecanismo de procesamiento de pagos verdaderamente global, rápido, rentable y completamente descentralizado mientras continúa integrando todos los desarrollos futuros en la capa fundamental abstracta de Ethereum. Al hacerlo, eBTC representaría los valores fundamentales originales de Bitcoin, como un medio sostenible de pago electrónico y almacenamiento de valor, al tiempo que brinda la modernización necesaria a Bitcoin utilizando el ecosistema diverso de Ethereum y permite la implementación de todos los casos de uso disponibles de un sistema de pago aceptado globalmente en eBTC.

Palabras clave: eBTC, Bitcoin, Ethereum, eBitcoin, ERC20, capa fundamental abstracta, cadena de bloques, moneda digital, efectivo electrónico

Índice

Antecedentes: Introducción a la evolución cadena de bloques y la creación de eBTC	4
Asuntos y problemas existentes	5
Solución propuesta	7
eBTC: El error en el código Solidity y el intercambio	10
eBTC: Ideas respaldadas por la simplicidad y una nueva comunidad diversa y global	11
eBTC: Características Técnicas	11
eBTC vs. Ether.....	12
Suministro total, distribución y minería	12
EBTC deflacionario y Ether inflacionario	12
La capacidad de Contrato Inteligentes de eBTC y los desarrollos futuros de Ethereum	13
Conclusiones	14
Referencias.....	15

eBTC: Una versión tokenizada de Bitcoin en Ethereum con
Contratos Inteligentes, Bajas Tasa de Transacción y Alta Velocidad de Transacción.

Antecedentes: Introducción a la evolución de las cadenas de bloques y la creación de eBTC

Bitcoin fue el pionero en el sistema de pago electrónico peer-to-peer descentralizado cuando el mundo fue testigo de la aparición de un artículo titulado “Bitcoin: A Peer-to-Peer Electronic Cash System” (Nakamoto, 2008). Esta ingeniosa y resistente a los gastos dobles invención trajo dos cosas para el mundo: una moneda digital y un mecanismo de consenso distribuido. El mundo de las cripto-divisas se ha movido mucho desde entonces y nuevas tecnologías han aparecido en el ecosistema Blockchain. Uno de los más importante es la capa funcional escalable, estandarizada e interoperable de Ethereum: la cadena de bloques de Ethereum.

El consenso distribuido de Bitcoin evolucionó y llegó al mundo de una tecnología más eficiente flexible cuando Ethereum fue propuesto por primera vez por Buterin en su artículo titulado “A Next Generation Smart Contract & Decentralized Application Platform” (2013). Con este aumento de eficiencia, velocidad y flexibilidad, se hizo posible crear soluciones descentralizadas innovadoras para diversos casos de uso y de amplio alcance. La capa abstracta fundamental de Ethereum y Solidity, su propio lenguaje de programación permitió la creación de Contratos Inteligentes, de Aplicaciones Descentralizadas (DApps) y de Organizaciones Autónomas Descentralizadas (DAO). Las capacidades dinámicas de Ethereum se encuentran en sus elementos básicos: “escalabilidad, estandarización, funcionalidad completa, facilidad de desarrollo e interoperabilidad” (Buterin, 2013, p.13). Los Contratos Inteligentes aprovechan todos estos de calidad del ecosistema Ethereum.

eBTC nació como una consecuencia directa de la evolución gradual de estas dos cadenas de bloques. En esencia, surgió a la existencia como una versión ERC20 de Bitcoin que posee las amplias capacidades de la plataforma Ethereum.

Problemas y Preocupaciones Existentes

Uno de los aspectos más críticos de la implementación de Bitcoin fue eliminar la necesidad de un tercero o intermediario y, por lo tanto, los inevitables costos asociados con dichos intermediarios. Nakamoto documentó que dichos costos limitaban el mínimo tamaño práctico de las transacciones y la posibilidad de pequeños pagos casuales (2008). Mientras elaboraba sobre la implementación de Bitcoin en la Fundación P2P por primera vez, Nakamoto observó que tales intermediarios imposibilitaban los micro pagos (2009). Irónicamente, el mismo fenómeno actualmente limita el mínimo tamaño práctico de transacción en Bitcoin e inhibe a los usuarios de realizar transacciones pequeñas debido a su cada vez mayor y altamente volátil valor de mercado.

Los crecientes costos de transacción de Bitcoin han comenzado a parecerse a los mismos arreglos que inicialmente se suponía que contrarrestarían. En la actualidad, una transacción promedio de Bitcoin cuesta alrededor de \$ 2 a \$ 5 o más de alrededor de 30,000 satoshis. La velocidad de transacción de Bitcoin presenta otro desafío. El tiempo promedio de bloqueo de Bitcoin es de alrededor de 10 minutos y actualmente se necesitan 6 confirmaciones o alrededor de 60 minutos para alcanzar la finalidad de la transacción. Ambos factores limitan la adopción de Bitcoin como un medio sostenible de intercambio digital y socavan el alma ingeniosa del ecosistema de Bitcoin propuesto originalmente. Cada vez es más difícil utilizar Bitcoin como un sistema de efectivo electrónico eficiente para el uso diario. Imagine transacciones virtuales de bienes o servicios por menos de \$ 2 o cuando los tiempos de transacción son de crítica importancia.

Parece que la filosofía original de Bitcoin -que presentaba al mundo una alternativa revolucionaria contra los sistemas bancarios y financieros tradicionales- se está diluyendo con sus costos de transacción cada vez mayores, tiempos de bloqueos lentos e interminables debates sobre las bifurcaciones. Recientemente, han surgido varias horquillas de Bitcoin que intentan resolver una o más de las preocupaciones predominantes: la escalabilidad, el tamaño de bloque y la minería cada vez más antidemocrática. Pero ninguno de ellos tiene actualmente la capacidad de resolver de manera eficiente todos los problemas subyacentes que envuelven el ecosistema de Bitcoin. Por lo tanto, se necesita una modernización de Bitcoin más fundamental para realizar su visión original.

En la actualidad, existen dos horquillas documentadas de Bitcoin, a saber, *Bitcoin Cash* y *Bitcoin Gold*, mientras que un tercero, *SegWit 2X*, también se ha propuesto. El problema de los tiempos de bloqueos lentos aún no se ha abordado con cada una de estas horquillas. En general, el ecosistema actual de Bitcoin se puede describir mejor como un verdadero génesis del criptouniverso y un mecanismo digital de almacenamiento de valores altamente volátil. La tabla documenta las preocupaciones del lento tiempo de bloqueo de Bitcoin y sus horquillas más recientes y futuras.

Comparación BTC/BTG/BCH/B2X	BITCOIN BTC	BITCOIN CASH BCH	BITCOIN GOLD BTG	SEGWIT 2X B2X
Suministro	21 Millones	21 Millones	21 Millones	21 Millones
Tiempo de Bloqueo	10 Minutos	10 Minutos	10 Minutos	10 Minutos
Tamaño de Bloque	1M (2-4M)	8M (8M)	1M (2-4M)	2M (4-8M)

Figura 1: Comparación del intervalo de bloques entre Bitcoin y sus horquillas recientes y futuras (Bitcoin Gold, 2017)

Solución Propuesta

La evolución de la cadena de bloques de Bitcoin en una infraestructura de Ethereum más eficiente y flexible permitió a los desarrolladores crear aplicaciones innovadoras y descentralizadas sobre su capa de base abstracta. La capa fundamental permitió la posibilidad de crear criptomonedas verdaderamente descentralizadas y sin confianza. Esta capacidad nos permitió crear un sistema electrónico de efectivo y pago peer-to-peer en forma de eBTC. eBTC, como una versión simbólica de los ideales básicos de Bitcoin, resuelve las preocupaciones antes mencionadas al ofrecer velocidades de transacción más rápidas, menores costos de transacción y la capacidad de trabajar con contratos inteligentes para la comunidad global de cripto-entusiastas y más.

Como efectivo electrónico y sistema de pago, eBTC aspira a representar de manera sostenible los atributos principales de Bitcoin en la cadena de bloques de Ethereum sin experimentar los inconvenientes de tiempos de bloques lentos, mayores costos de transacción, minería centralizada y bifurcaciones continuas, a la vez que proporciona soporte para contratos inteligentes. Con las capacidades de contrato inteligente de Ethereum, eBTC se esfuerza por implementar todos los casos de uso disponibles que tales contratos ofrecen para promover la adopción de eBTC como un mecanismo de pago y moneda digital verdaderamente global y utilizable de manera diaria. Como eBTC existe sobre la capa fundamental de Ethereum, las características de su ecosistema -costos de transacción, velocidad de transacción y capacidad de contrato inteligente- reflejan los atributos sistemáticos de Ethereum. Una transacción eBTC cuesta alrededor de \$ 0.15 a \$ 0.5 y su tiempo de bloqueo es al menos 10 veces más rápido que Bitcoin y todas sus horquillas recientes y futuras. La siguiente tabla encapsula en su totalidad el mecanismo de transacción rápido y eficiente y varias otras características de eBTC en comparación con Bitcoin y todas sus horquillas recientes y futuras.

“Bitcoins”	BTC (Bitcoin)	BCH (Bitcoin Cash)	BTG (Bitcoin Gold)	B2X (SegWit2X)	eBTC (eBitcoin)
Suministro total	21 Millones	21 Millones	21 Millones	21 Millones	21 Millones
Plataforma	Bitcoin Original -1MB	Horquilla -8 MB	Horquilla -Equihash	Horquilla -2MB	Token ERC20 en Ethereum
Minería	Sí (ASIC & Cent.)	Sí (ASIC)	Sí (GP U)	Sí (ASIC)	No (Total en Circulación)
Lanzamiento	2009-Ene.	2017-Ago.	2017-Oct.	2017-Nov.	2017-Oct.
Tiempo de Bloqueo	~ 10 Minutos	~ 10 Minutos	~ 10 Minutos	~ 10 Minutos	~ 15 Segundos
Finalización	6 Confirmaciones (~ 60 min.)	6 Confirmaciones (~ 60 min.)	N/A	N/A	12 Confirmaciones (~ 3 min.)
Costo Promedio De Transacción	~ (\$2 – \$5)	~ (\$0.06 –\$0.3)	N/A	N/A	~ (\$0.15 – \$0.5)
Consenso	PoW	PoW	PoW	PoW	PoW (Pronto PoS)
Escalabilidad	Lightening Network (No Lanzada)	Mayor Tamaño De Bloque (No Capa Encima)	Lightenin g Network (No Lanzada)	Lightening Network (No Lanzada)	Lightening + Sharding + Plasma
Privacidad	Dandelio (No Iniciada)	N/A	N/A	N/A	zkSNARKs (en testnet)
Contratos Inteligentes	No	No	No	No	Sí
Capacidades	Pagos (Rootstock Pronto)	Pagos	Pagos	Pagos	Pagos + Contratos Inteligentes
Aceptación de pago	Alta	Media	Mínima (En progreso)	NA	Mínima (En progreso)
Estrellas GitHub	18,707	239	296	326	97
Tamaño del Mercado	~ \$120 Mil Millones	~ \$10 M.M.	~ \$3 M.M.	NA	~ \$2 Millones

Figure 2: Comparación entre Bitcoin, sus Horquillas y eBTC (Adaptado de Larsson, 2017)

eBTC propone resolver de manera efectiva las preocupaciones y problemas que continúan causando las horquillas en crecimiento en el ecosistema de Bitcoin. Con los desarrollos sostenibles y futuristas de Ethereum, eBTC continuará disfrutando y aprovechando lo mejor de las capacidades de Ethereum, mientras ofrece a la comunidad global los ideales básicos de Bitcoin en una plataforma más diversa, escalable e innovadora. eBTC, con su adopción, también impulsaría el reconocimiento de Ethereum en el universo criptográfico como un mecanismo de moneda digital y almacén de valor habilitado por Ethereum, y podría demostrar ser un activo estratégico para el ecosistema general de Ethereum.

eBTC: El error en el código Solidity y el intercambio.

La implementación original de eBTC contenía un error crítico en su código ERC20 de Solidity, que podría permitir al creador del contrato crear erróneamente más tokens que el suministro máximo de 21 millones. Si bien este fallo nunca fue explotado hizo que naturalmente la confianza en el proyecto se desplomara. Después de diligentemente tomar el control del proyecto eBTC del creador original, la Fundación eBTC decidió ejecutar un intercambio (Swap) de contrato basado en "hold and receive" (esperar y recibir) donde todos los titulares de clave privada de los tokens existentes recibirían los nuevos tokens sin errores en una proporción de 1:1 después de un determinado bloque de la red Ethereum. Después de anunciar debidamente los requisitos previos para el intercambio de antemano, la Fundación eBTC implementó un nuevo "Contrato Inteligente" (Smart Contract) ERC20 donde todos los titulares de claves privadas de los tokens recibieron los nuevos tokens libres de errores en una proporción de 1:1 con un nuevo formato excepcionalmente críptico y un nuevo contrato totalmente auditado. El contrato actual se publica en formato abierto en GitHub, gratis para que cualquiera lo revise.

A pesar de los diversos recordatorios realizados para mover y mantener los tokens eBTC en carteras que permitan la propiedad de las claves privadas, desafortunadamente, durante la implementación del swap, una parte del suministro circulante de los tokens se mantuvo en Exchanges descentralizados basados en Ethereum. Como estos Exchanges son dirigidos mediante Contratos Inteligentes y no hay control humano sobre ellos, alrededor de 2.1 millones de los nuevos tokens eBTC permanecen de forma permanente en dichos Exchanges y nunca serán parte del nuevo suministro circulante. El nuevo suministro total y circulante de eBTC es de aproximadamente 21 millones y 18.9 millones respectivamente.

eBTC: Ideas respaldadas por la simplicidad y una nueva comunidad diversa y global.

eBTC es una cripto-moneda impulsada por la comunidad y basada en tecnología de cadena de bloques y que funciona como un Token ERC20 aprovechando los mejores atributos de Bitcoin y Ethereum. Es una versión tokenizada de Bitcoin en la cadena de bloques de Ethereum y, por lo tanto, complementa de forma única a ambos. Su objetivo es representar y mantener los atributos básicos de Bitcoin, como un medio electrónico de intercambio y de almacenamiento de valores en la cadena de bloques de Ethereum, pero con una perspectiva más inteligente y más rápida.

La creación de un representante ERC20 de Bitcoin en la cadena de bloques de Ethereum puede parecer "demasiado simple", pero abre la posibilidad de implementar los ideales de Bitcoin en una tecnología de cadena de bloques existente y más evolucionada, que es más rápida, flexible y más escalable. Esto no es nada más que fruto de una idea innovadora y perturbadora. eBTC es esta idea que busca implementar la visión idealista de Bitcoin en la cadena de bloques de Ethereum, permitiendo velocidades de transacción más rápidas, menos costosas y la capacidad de albergar Contratos Inteligentes sin experimentar los problemas asociados a los horquilla y a la minería centralizada.

eBTC cree firmemente que una comunidad global, robusta y dinámica de cripto-entusiastas es fundamental para una evolución sostenible de todo el ecosistema. La Fundación eBTC está compuesta por un núcleo global, diverso y vibrante de individuos inspiradores que están incondicionalmente comprometidos con promover la causa simple, pero disruptiva, de eBTC. Además, el papel la gran comunidad eBTC es fundamental para difundir el poder de los libros de contabilidad distribuidos y difundir cómo eBTC puede cambiar la idea de cómo evoluciona la gestión de las finanzas en línea.

eBTC: Características Técnicas

eBTC vs. Ether

eBTC es un sistema de pago en efectivo y electrónico basado en Ethereum y Ethereum Ether, "el crypto-fuel de la red Ethereum" ("What is Ether", 2017) y que sirve para validar las transacciones eBTC sobre la cadena de bloques de Ethereum. Como combustible, Ether es compatible con el ecosistema general de Ethereum.

Para ser claros, el Ether nunca fue destinado a ser una moneda de Ethereum. Sino que su propósito es servir como combustible para dirigir la plataforma distribuida en Ethereum ("What is Ether", 2017). "Es una forma de pago realizada por los clientes de la plataforma a las máquinas que ejecutan las operaciones solicitadas" ("What is Ether", 2017). Por otro lado, eBTC, en su el sentido más puro, es solo una moneda digital de uso diario y un sistema de pago optimizado. Es decir, un medio más rápido y más barato de intercambio y de almacenamiento de valor.

Suministro total, distribución y minería

El suministro total y máximo de eBTC será siempre de 21 millones y será divisible hasta 8 decimales. En la creación de eBTC, todos los tokens eBTC fueron distribuidos de manera transparente a la comunidad global, diversa y comprometida de crypto-entusiastas mediante un proceso sin ICO (Oferta Inicial de Fundación). Desde el comienzo, eBTC es una moneda digital resistente a la minería y orientada a la circulación ya que su suministro total se distribuyó completamente a la comunidad y a la fundación eBTC en una proporción porcentual de 97.92 : 2.08 respectivamente.

EBTC deflacionario y Ether inflacionario

Como el suministro total de eBTC está limitado a 21 millones, esto refleja los atributos deflacionarios de Bitcoin en una cadena de bloques de Ethereum más flexible e inteligente. Es decir, con un aumento sostenible en valor de eBTC, su poder adquisitivo también se apreciará convirtiéndolo en el único representante de Bitcoin con características deflacionistas en la cadena de bloques de Ethereum. La naturaleza deflacionaria de eBTC significa además que este podría servir como un mecanismo de almacenaje de valor sostenible y apropiado en el ecosistema de Ethereum.

Irónicamente, actualmente el suministro total de Ether no tiene un límite. Esto implica un interesante fenómeno: eBTC, una moneda digital deflacionaria, funcionaría en un Blockchain descentralizado con la ayuda optimizada de un crypto-fuel inflacionario, Ether. Considerando la naturaleza inflacionaria del Eher y sus precios relativamente estables, eBTC continuaría de forma sostenible gracias a los menores costes de transacción de la red Ethereum.

La capacidad de Contrato Inteligentes de eBTC y los desarrollos futuros de Ethereum

Ser una versión tokenizada ERC20 de Bitcoin en la plataforma Ethereum ofrece a eBTC la innovadora ventaja de poder trabajar con una variedad diversa de Contratos Inteligentes habilitados por Ethereum, como DApps y DAOs. eBTC planea estratégicamente coordinar e integrar tales usos innovadores que ayudarían a convertirlo en un sistema de pago electrónico verdaderamente global y altamente accesible. Con una adopción y evolución gradual, eBTC también puede llegar a convertirse en un activo estratégico para el propio ecosistema Ethereum.

Conclusiones

Hemos discutido el diseño fundamental, el concepto y las características de implementación de eBTC como una versión tokenizada de Bitcoin en la cadena de bloques de Ethereum y que sirve como un eficaz sistema de divisas y de pago peer-to-peer electrónico más robusto y más flexible.

Hemos comenzado con la evolución de los mecanismos de consenso “trust-less” y se ha establecido cómo fue el progreso de una distribución de consenso de Bitcoin sobre la capa fundamental, abstracta, más flexible, diversa e interoperable de Ethereum.

A continuación, se ha discutido sobre cómo comenzó a existir eBTC como una consecuencia directa de la evolución de Bitcoin en lo que luego se convirtió en la cadena de bloques de Ethereum. Hemos destacado la prevaeciente preocupación sobre los lentos tiempos de bloque, mayores costes de transacción, minería centralizada y un crecimiento constante de horquillas del ecosistema de Bitcoin, que además actualmente carecen de soporte para Contratos Inteligentes. Se ha destacado cómo eBTC puede resolver todos estos problemas mientras funciona como una versión ERC20 de los ideales básicos de Bitcoin en el ampliamente capaz y continuamente optimizado ecosistema de Ethereum. También se han documentado las bases de eBTC, sus aspectos técnicos y cómo una comunidad global, comprometida y diversa es fundamental para el conocimiento y la adopción generales de eBTC. Creemos que, con adopción general y buen conocimiento, eBTC puede lograr que la comunidad global experimente una vez más Bitcoin en una cadena de bloques más flexible y eficiente sin tener que pasar por debates ideológicos y políticamente cargados sobre la horquilla de Bitcoin por su constante crecimiento.

Referencias

Bitcoin Gold. (2017). Bitcoin Gold and other forks of Bitcoin. Retrieved from <https://btcpool.org/wp-content/uploads/2017/10/BitcoinGold-Roadmap.pdf>

Buterin, V. (2013). A next generation smart contract & decentralized application platform. The-blockchain.com. Retrieved from http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Larsson, A. (2017). State of bitcoins. allcoinwiki.com. Retrieved from <https://allcoinwiki.com/bitcoin/>

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org. Retrieved from <https://bitcoin.org/bitcoin.pdf>

Nakamoto, S. (2009). Bitcoin open source implementation of p2p currency. P2P Foundation. Retrieved from <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>

What is Ether. (2017). In Ethereum.org. Retrieved from <https://ethereum.org/ether>