Moeda **eBitcoin – *eBTC***: UMA VERSÃO TOKENIZADA DA BITCOIN EM *ETHEREUM*

eBitcoin: Uma versão Tokenizada da Bitcoin na rede *Ethereum*, com contratos inteligentes, taxas de transação mais baixas e maior velocidade de transação.

Fundação da Comunidade *eBTC*.

Resumo

eBTC, eBitcoin ou *Ethereum* Bitcoin é uma versão Token (tokenizada) ERC20 da Bitcoin na blockchain *Ethereum*. A *eBTC* propõe-se a resolver os custos, a velocidade da transação, a escalabilidade e questões relacionadas com a ineficácia do Contrato-Inteligente (Smart-Contract) da blockchain original da Bitcoin usando a blockchain *Ethereum* , que é mais eficiente, escalável e interoperável. Suportada por uma comunidade global diversificada, dinâmica e comprometida, a *eBTC* é uma moeda digital que pretende tornar-se num sistema de pagamento eletrónico *peer-to-peer* (pessoa a pessoa) mais acessível, mais rápido e mais flexível. Pretende fazê-lo mantendo os ideais fundamentais da Bitcoin, integrando-os no ecossistema *Ethereum*.

No ano de 2017 testemunhou-se o surgimento de bifurcações (*forks*) múltiplas da Bitcoin, todas tentando resolver uma ou mais questões existentes relacionadas com a baixa velocidade de transação, altos custos de transação e mineração centralizada. No entanto, nenhuma das bifurcações tem, atualmente, a capacidade de resolver efetivamente estas questões. Em contraste, o design aparentemente simples e diferente d*a eBTC* permite que ela responda de forma eficiente a estes desafios, ao mesmo tempo que adiciona as capacidades de contrato inteligente (smart-contracts) aos ideais fundamentais da Bitcoin.

Com a crescente consciencialização e aceitação, *a eBTC* pretende tornar-se num mecanismo de processamento de pagamentos verdadeiramente global, rápido, económico e totalmente descentralizado, continuando a integrar todos os desenvolvimentos futuros da plataforma base e abstrata do *Ethereum*. Ao fazê-lo *a eBTC* representa os valores fundamentais e originais da Bitcoin, como um meio sustentável de pagamento eletrónico e de armazenamento de valor, trazendo a necessária modernização para a Bitcoin, usando o ecossistema diversificado do *Ethereum* e permitindo a implementação de todos os tipos de uso disponíveis num sistema de pagamento globalmente aceite em *eBTC*.

Palavras-chave: *eBTC*, Bitcoin, *Ethereum*, eBitcoin, ERC20, plataforma *Ethereum* (abstract foundational layer), cadeia de blocos (blockchain), moeda digital (digital currency), dinheiro eletrónico (electronic cash)

Resumo 2
Antecedentes: Uma introdução à evolução de *Blockchains* e à criação da *eBTC* 4
Preocupações e problemas existentes 5
Solução proposta 7
eBTC: Fundamentos apoiados pela simplicidade e uma comunidade global dinâmica e diversa 11
eBTC: Características técnicas 12
eBTC vs *Ether* 12
Oferta total, distribuição e mineração 12
eBTC deflacionário e *Ether* inflacionário 12
Capacidade de Contrato Inteligente *eBTC* e Desenvolvimento Futuro da *Ethereum* 13
Conclusão 14
Referências 15

eBTC: uma versão Tokenizada da Bitcoin em *Ethereum* com contratos inteligentes, taxas de transação baixas e maior velocidade de transação

Antecedentes: Uma introdução à evolução de *Blockchains* e à criação da *eBTC*

A Bitcoin foi pioneira no sistema de dinheiro eletrónico pessoa-a-pessoa descentralizado e confiável quando o mundo assistiu ao surgimento de um artigo intitulado *Bitcoin: A Peer-to-peer Electronic Cash System* (Nakamoto, 2008). Esta invenção engenhosa e resistente à dupla despesa (doble-spending) trouxe duas coisas novas ao mundo: uma moeda digital e um mecanismo de consenso partilhado. O mundo das cripto-moedas mudou muito e apareceram novas tecnologias no ecossistema blockchain. A principal referência é a plataforma da *Ethereum* - *Ethereum*'s Blockchain, que é escalável, padronizada e interoperável.

O consenso distribuído da Bitcoin evoluiu e deu ao mundo uma tecnologia mais eficiente e flexível quando foi proposto pela primeira vez o *Ethereum* por Buterin, no seu artigo intitulado *"A Next Generation Smart Contract & Decentralized Application Platform"*(2013). Com mais eficiência, velocidade e flexibilidade, tornou-se possível criar soluções descentralizadas inovadoras para situações de uso diverso e abrangente. A solidez e linguagem de programação possibilitou à plataforma *Ethereum*, a criação de contratos inteligentes, aplicativos descentralizados (DApps) e organizações autónomas descentralizadas (DAOs). As forças dinâmicas do *Ethereum* estão nos seus elementos principais: "escalabilidade, padronização, completude, fácil desenvolvimento e interoperabilidade" (Buterin, 2013, p.13). Os contratos inteligentes possuem todos estes atributos de qualidade do ecossistema *Ethereum*.

A *eBTC* foi introduzida como uma consequência direta da evolução progressiva de ambos os blockchains. Na sua essência, surgiu como uma versão ERC20 da Bitcoin, que possui as vastas capacidades do ecossistema *Ethereum*.

A *eBTC* emergiu como consequência direta da evolução gradual de ambas as cadeias de blocos. Em síntese, surgiu como uma versão ERC20 da Bitcoin que possui as vastas capacidades da plataforma *Ethereum*.

Preocupações e problemas existentes

Um dos aspectos mais críticos da implementação da Bitcoin foi remover a necessidade de confiança de terceiros e, portanto, os custos de transação inevitáveis associados a tais acordos intermediários. Nakamoto documentou que tais custos de transação limitavam o tamanho mínimo da operação prática e a possibilidade de pequenos pagamentos ocasionais (2008). Ao elaborar a implementação da Bitcoin na P2P Foundation pela primeira vez, Nakamoto observou que tais intermediários tornaram os micro-pagamentos impossíveis (2009). Ironicamente, o mesmo fenómeno atualmente limita o tamanho mínimo da operação prática da Bitcoin e inibe os usuários de transacionar pequenas transações devido ao seu valor de mercado, cada vez maior e altamente volátil.

Os crescentes custos de transação da Bitcoin começaram a assemelhar-se aos mesmos "arranjos" que inicialmente deveriam ser contrariados. Atualmente, uma transação Bitcoin média custa cerca de US $ 2 a 5 $ ou mais, cerca de 30.000 satoshis. A velocidade de transação Bitcoin apresenta outro desafio. O tempo médio de calculo de um novo bloco Bitcoin é de cerca de 10 minutos e, atualmente, leva 6 confirmações ou cerca de 60 minutos para alcançar a finalidade da transação. Ambos os fatores limitam a adoção da Bitcoin como meio sustentável de troca digital, que prejudica a alma engenhosa do ecossistema Bitcoin proposto originalmente. Está a tornar-se mais desafiador usar a Bitcoin como um eficiente sistema de moeda eletrónica de uso diário. Imagine vender virtualmente mercadorias ou serviços de valor inferior a 2 US $, ou quando os tempos das transações são de relevância crítica.

Aparentemente a filosofia original da Bitcoin, que apresentou ao mundo uma alternativa revolucionária contra os sistemas bancários e fiduciários tradicionais, dilui-se com os seus custos de transação cada vez maiores, tempos de bloqueio lento e debates intermináveis sobre bifurcações da moeda. Múltiplas bifurcações da Bitcoin aconteceram recentemente, tentando resolver uma ou mais das principais preocupações: escalabilidade, tamanho de bloco e mineração cada vez mais antidemocrática. Mas nenhuma delas tem capacidade, atualmente, para resolver eficientemente todos os problemas subjacentes envolvendo o ecossistema Bitcoin. Uma modernização Bitcoin é fundamental e necessária para fazer cumprir a sua visão original.

Atualmente existem duas bifurcações documentadas da Bitcoin, a Bitcoin Cash e a Bitcoin Gold, enquanto uma terceira, a SegWit 2X, também foi proposta. A questão dos tempos de bloco lentos ainda não foi abordada por cada uma destas bifurcações. No geral, o atual ecossistema da Bitcoin pode ser descrito melhor como uma verdadeira génese do universo da criptomoeda e um mecanismo de armazenamento de valor digital altamente volátil. A tabela documenta as preocupações com os blocos lentos da Bitcoin e as suas mais recentes e próximas bifurcações.

Comparação BTC/BTG/BCH/B2X	**BITCOIN BTC**	**BITCOIN CASH BCH**	**BITCOIN GOLD BTG**	**SEGWIT 2X B2X**
Supply	21 Million	21 Million	21 Million	21 Million
Block Time	10 Minutes	10 Minutes	10 Minutes	10 Minutes
Block Size	1M (2-4M)	8M (8M)	1M (2-4M)	2M (4-8M)

***Figura 1*:** Comparação do Intervalo de Blocos entre Bitcoin e os seus mais recentes e próximas bifurcações (Bitcoin Gold, 2017).

Solução proposta

A evolução da blockchain da Bitcoin na plataforma *Ethereum* permite criar aplicativos inovadores e descentralizados mais eficientes e flexíveis. Esta plataforma permite a possibilidade de criar cripto-moedas verdadeiramente descentralizadas, capacidade que permitiu criar um sistema de dinheiro digital e pagamento eletrónico *peer-to-peer* sob a forma da *eBTC*. A *eBTC*, como uma versão tokenizada dos ideais fundamentais da Bitcoin, resolve as preocupações acima mencionadas, oferecendo velocidades de transação mais rápidas, custos de transação mais baixos e a capacidade de trabalhar com contratos inteligentes para a comunidade global de cripto-entusiastas e mais além.

Como moeda digital e sistema eletrónico de pagamento, a *eBTC* aspira representar, de forma sustentável, os atributos principais da Bitcoin na blockchain *Ethereum*, sem experimentar os problemas de tempos de bloco lentos, custos de transação mais elevados, mineração centralizada e *forks* contínuos, além de oferecer suporte para contratos inteligentes. Com as capacidades de contratos inteligentes da *Ethereum*, a *eBTC* esforça-se para implementar todos os casos de uso disponíveis, tais como contratos para promover a adoção d*a eBTC* como um mecanismo de pagamento e moeda digital verdadeiramente global e de uso quotidiano.

Como a *eBTC* foi fundada na plataforma *Ethereum*, as características do seu ecossistema - custos de transação, velocidade de transação e capacidade de contrato inteligente - refletem os atributos do sistema *Ethereum*. Uma transação *eBTC* custa cerca de US $ 0,15 a US $ 0,5 e o seu tempo de bloco é, pelo menos, 10 vezes mais rápido do que o da Bitcoin e de todos os seus mais recentes e futuros *forks*. A tabela abaixo encapsula o mecanismo de transação rápido e eficiente e vários outros recursos da *eBTC* em comparação com a Bitcoin e todos os seus últimos e futuros *forks* (bifurcações).

"Bitcoins"	**BTC (Bitcoin)**	**BCH (Dinheiro Bitcoin)**	**BTG (Ouro Bitcoin)**	**B2X (SegWit2X)**	***eBTC* (eBitcoin)**
Oferta total	21 Milhões	21 Milhões	21 Milhões	21 Milhões	**21 Milhões**
Plataforma	Bitcoin Original ―1MB‖	Fork Bitcoin ―8 MB‖	Fork Bitcoin ―Equihash‖	Fork Bitcoin ―2MB‖	**ERC20 Token on *Ethereum***
Mineração	Sim (ASIC & Cent.)	Sim (ASIC)	Sim (GPU)	Sim (ASIC)	**Não (T. em circulação)**
Lançamento	2009-Jan.	2017-Ago.	2017-Out.	2017-Nov.	**2017-Out.**
Tempo de boqueio	~ 10 Minutos	~ 10 Minutos	~ 10 Minutos	~ 10 Minutos	**~ 15 Segundos**
Finalidade	6 Confirmações (~ 60 min.)	6 Confirmações (~ 60 min.)	NA	NA	**12 Confirmações (~ 3 min.)**
Taxa média de custo	~ ($2 – $5)	~ ($0.06 – $0.3)	NA	NA	**~ ($0.15 – $0.5)**
Consenso	PoW	PoW	PoW	PoW	**PoW (brevemente PoS)**
Escala	Sistema elétrico (não implementado)	Maior tamanho de bloco Sem camada no topo	Sistema elétrico (não implementado)	Sistema elétrico (não implementado)	**Iluminação + Sharding + Plasma**
Privacidade	Dandelion (not live)	NA	NA	NA	**zkSNARKs (na testnet)**
Contratos smart	Não	Não	Não	Não	**Sim**
Capacidade	Pagamentos (brevemente Rootstock)	Pagamentos	Pagamentos	Pagamentos	**Pagamentos + Contratos smart**
Nível de aceitação de pagamento	Elevado	Médio	Mínimo (em desenvolvimento)	NA	**Mínimo (em desenvolvimento)**
Estrelas GitHub	18,707	239	296	326	**97**
Cap. Mercado	~ $120 Biliões	~ $10 Biliões	~ $3 Biliões	NA	~ $2 Milhões

Tabela 2: Comparação entre Bitcoin, os seus *Forks*/Bifurcações e *eBTC* (adoptado por Larsson, 2017)

A *eBTC* propõe resolver, de forma efetiva, as preocupações e problemas que continuam a causar constantes *forks* no ecossistema Bitcoin. Com os desenvolvimentos sustentáveis e futuristas da *Ethereum*, a *eBTC* continuara a aproveitar o melhor dos recursos da *Ethereum*, oferecendo à comunidade global os ideais fundamentais da Bitcoin numa plataforma mais diversificada, escalável e inovadora. A *eBTC* também impulsionara o reconhecimento do *Ethereum* no universo cripto como uma moeda digital e um mecanismo de reserva de "valor", podendo revelar-se num ativo estratégico para o ecossistema geral da *Ethereum*.

eBTC: o erro de solidez do Token e o Swap

A implementação original d*a eBTC* continha um erro crítico no seu código ERC20, que poderia permitir que o criador do contrato criasse, incorretamente, mais tokens do que o suprimento máximo de 21 milhões. Embora a falha nunca tenha sido explorada e aparentemente não tivesse sido intencional, naturalmente, que a confiança no projeto caiu. Depois de assumir diligentemente os direitos sobre o projeto da *eBTC,* em detrimento do criador original, a Fundação *eBTC* decidiu executar um contrato em que todos os titulares de chaves privadas dos tokens existentes receberiam os novos tokens sem erros num Rácio 1:1, após um bloco *Ethereum* pré-especificado. Depois de anunciar previamente os pré-requisitos para o swap, a Fundação *eBTC* implementou a nova arquitetura de contrato inteligente ERC20, onde todos os titulares de chaves privadas dos tokens existentes receberam tokens novos e sem erros numa proporção de 1:1 de acordo com o rigoroso escrutínio e um novo contrato completamente auditado. O contrato atual é publicado como fonte aberta no GitHub, gratuitamente, para qualquer um avaliar.

Apesar dos avisos d*a eBTC* para mover e manter os tokens em carteiras que permitam a propriedade privada, uma parte do fornecimento circulante dos tokens foi infelizmente realizada em trocas descentralizadas baseadas em *Ethereum* durante a implementação do swap. Devido ao facto de os smart contracts potenciarem este tipo de troca e também por não haver controlo humano sobre o mesmo, cerca de 2,1 milhões dos novos tokens *eBTC* são permanentemente mantidos por tais trocas e nunca seriam parte da oferta em circulação. O novo suprimento total em circulação d*a eBTC* é de cerca de 18,9 milhões em 21 milhões, respetivamente.

eBTC: Fundamentos apoiados pela simplicidade e uma comunidade global dinâmica e diversa

A eBTC é uma criptomoeda comunitária e movida pelo blockchain, que funciona como um token ERC20 alavancando os melhores atributos da Bitcoin e *Ethereum*. É uma versão tokenizada da Bitcoin no blockchain *Ethereum* e, portanto, complementa exclusivamente ambos. Pretende representar e sustentar os atributos fundamentais da Bitcoin como meio eletrónico de troca e armazenamento sustentável de valor, mas com uma perspetiva mais inteligente e rápida pela sua integração na plataforma *Ethereum.*

A criação de um representante ERC20 da Bitcoin na blockchain *Ethereum* pode parecer "simples", mas descobrir a possibilidade de implementar os ideais da Bitcoin numa tecnologia de cadeias de blocos (blockchains) existente e mais evoluída, rápida, flexível e mais escalável, não é senão um processo de pensamento inovador e disruptivo. A *eBTC* é este processo de pensamento que busca implementar a visão idealista da Bitcoin na cadeia de blocos *Ethereum*, permitindo velocidades de transação mais rápidas, custos de transação mais baixos e capacidades de contratos inteligentes sem experienciar problemas de bifurcação e mineração centralizada.

A *eBTC* acredita firmemente que uma comunidade global robusta e dinâmica de cripto-entusiastas é fundamental para uma evolução sustentável de todo o ecossistema. A Fundação *eBTC* é composta por um corpo global diversificado e vibrante de indivíduos inspiradores, que estão firmemente empenhados em promover uma causa simples, mas disruptiva, a *eBTC*. Além disso, o papel da comunidade *eBTC* é fundamental para espalhar a palavra sobre o poder d*a eBTC* e como esta podera mudar a forma como poderemos evoluir na conduta das transações financeiras on-line.

eBTC: Características técnicas

eBTC* vs *Ether

A *eBTC* é um sistema de pagamento e dinheiro eletrónico na plataforma *Ethereum* e o *Ether* - a criptomoeda para a rede *Ethereum* ("O que é *Ether*", 2017), serve para validar as transações *eBTC* na cadeia de blocos *Ethereum*. Como combustível, a *Ether* apoia o ecossistema *Ethereum* geral.

Para esclarecer, o *Ether* nunca foi concebido para ser uma moeda *Ethereum*. Em vez disso, o seu objetivo é servir como combustível para operar na plataforma de aplicação *Ethereum* ("*O que é Ether*", 2017). - É uma forma de pagamento feita pelos clientes da plataforma às máquinas que executam as operações solicitadas‖ ("*O que é Ether*", 2017). Por outro lado, *a eBTC*, no seu sentido mais puro, é apenas uma moeda digital utilizável diariamente e um sistema de pagamento otimizado, ou seja, um meio de troca mais rápido e mais barato.

Oferta total, distribuição e mineração

O suprimento total e máximo d*a eBTC* será no máximo de 21 milhões e divisível por 8 casas decimais. Na génese, todos os tokens d*a eBTC* foram distribuídos de forma transparente, sem ICO, para a comunidade global diversificada e comprometida de entusiastas de cripto. Desde o início *a eBTC* é uma moeda digital resistente à mineração e à circulação, já que a globalidade da sua oferta foi totalmente distribuída para a comunidade e para a Fundação *eBTC* com uma percentagem de 97,92: 2,08, respectivamente.

***eBTC* deflacionário e *Ether* inflacionário**

Como a oferta total da *eBTC* é limitada a 21 milhões, reflete os atributos deflacionários da Bitcoin, numa cadeia de blocos *Ethereum* mais flexível e inteligente. O que quer dizer que com um aumento sustentável do valor da *eBTC*, o seu poder de compra seria reconhecido como o único representante da Bitcoin, na cadeia de blocos *Ethereum*, com características deflacionárias. A natureza deflacionária d*a eBTC* também significa que

poderia servir como um de mecanismo de valor sustentável e apropriado do ecossistema *Ethereum*.

Ironicamente, o suprimento total de *Ether* é atualmente ilimitado. Isso significa um fenómeno interessante: a *eBTC*, uma moeda digital deflacionária, funcionara num sistema de blocos descentralizado com a assistência otimizada por uma criptomoeda inflacionária, o *Ether*. Considerando a qualidade inflacionária do *Ether* e os seus preços relativamente estáveis, a *eBTC* ira continuar de forma sustentável, a experienciar os baixos custos de transação da rede *Ethereum*.

Capacidade de Contrato Inteligente *eBTC* e Desenvolvimento Futuro da *Ethereum*

Sendo uma versão tokenizada do ERC20 da Bitcoin na plataforma *Ethereum*, a *eBTC* tem a inovadora vantagem de trabalhar com uma ampla gama de contratos inteligentes, DApps e DAO habilitados para *Ethereum*. A *eBTC* estrategicamente planeia coordenar e integrar tais inovações, que usam casos que ajudariam a torná-la num sistema de pagamento de dinheiro eletrónico verdadeiramente global e altamente acessível. Com a adoção e a evolução gradual, a *eBTC* também pode tornar-se um ativo estratégico para o ecossistema *Ethereum*.

Conclusão

Discutimos o design fundamental, o conceito e os recursos de implementação d*a eBTC* como uma versão tokenizada da Bitcoin na cadeia de blocos *Ethereum*, que serve como sistema de dinheiro eletrónico e pagamento eletrónico *peer-to-peer* eficiente, robusto e mais flexível. Começamos com a evolução dos mecanismos sem consenso de confiança (trust- less mechanisms) e estabelecemos o progresso do consenso distribuído da Bitcoin na plataforma mais flexível, diversa e interoperável da *Ethereum*.

Discutiu-se que *a eBTC* surgiu como uma consequência direta da evolução da Bitcoin, que mais tarde se tornou conhecida como cadeia de blocos de *Ethereum*. Destacamos as preocupações prevalentes dos tempos de bloco lentos, dos custos de transação mais elevados, da mineração centralizada e das crescentes bifurcações do ecossistema de Bitcoin - que atualmente carecem de suporte ao contrato inteligente – e como *a eBTC* pode resolver todas estas questões enquanto atua como uma versão ERC20 dos ideais fundamentais da Bitcoin no ecossistema, amplamente capaz e continuamente otimizado da *Ethereum*. Documentámos também os fundamentos d*a eBTC*, os seus aspectos técnicos e a importância da sua comunidade global, comprometida e diversificada, como fundamento para a consciencialização e adoção geral da *eBTC*. Acreditamos que com a adoção e conscientização, *a eBTC* pode permitir que a comunidade global experimente também o Bitcoin, mas numa cadeia de blocos mais flexível e eficiente sem ter que passar pelos debates ideológicos e politicamente carregados sobre as constantes bifurcações (f*orks)* da Bitcoin.

Referências

Bitcoin Gold. (2017). *Bitcoin Gold and other forks of Bitcoin*. Retrieved from https://btcgpu.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*