eBTC : Une version tokenisée de Bitcoin sur Ethereum avec des Smart Contracts, de faibles coûts de transaction et une vitesse de transaction plus élevée

eBTC's Community Foundation

Résumé

eBTC, eBitcoin ou Bitcoin d'Ethereum est une version tokenisée ERC20 de Bitcoin sur l'Ethereum Blockchain. Il propose de résoudre les problèmes de coût de transaction, de rapidité, d'évolutivité et d'inefficacité de la chaîne de blocage Bitcoin originale en utilisant la couche de chaîne de blocage Ethereum plus efficace, évolutive et interopérable. Soutenu par une communauté mondiale diversifiée, dynamique et engagée, eBTC a l'intention de devenir un système de paiement et d'encaissement électronique pair-à-pair plus abordable, plus rapide et plus flexible. Il a l'intention de le faire en conservant les idéaux fondamentaux de Bitcoin et en les intégrant à l'écosystème d'Ethereum. L'année 2017 a vu l'émergence de multiples forks de Bitcoin qui tentent tous de résoudre une ou plusieurs de ses préoccupations existantes : faible vitesse de transaction, coûts de transaction élevés et minage centralisé. Pourtant, aucun des forks n'a actuellement la capacité de résoudre efficacement tous ces problèmes. En revanche, la conception apparente et étrangement simple d'eBTC lui permet de relever efficacement ces défis tout en ajoutant des capacités de contrats intelligents aux idéaux fondamentaux de Bitcoin. Avec une prise de conscience et une acceptation croissante, eBTC prévoit de devenir un mécanisme de traitement des paiements véritablement global, rapide, rentable et entièrement décentralisé tout en continuant à intégrer tous les développements futurs prévus par la fondation d'Ethereum. Ce faisant, eBTC représenterait les valeurs fondamentales initiales de Bitcoin, en tant que moyen durable de paiement électronique et de stockage de valeur, tout en apportant à Bitcoin la modernisation nécessaire en utilisant l'écosystème diversifié d'Ethereum et en permettant la mise en œuvre de tous les cas d'utilisation disponibles d'un système de paiement accepté mondialement dans eBTC.

Mots clés : : eBTC, Bitcoin, Ethereum , eBitcoin, ERC20 , couche d’abstraction fondamentale, blockchain, crypto-monnaie, monnaie électronique

Table des matières

eBTC : Une version tokenisée de Bitcoin sur Ethereum avec des Smart Contracts, de faibles coûts de transaction et une vitesse de transaction plus élevée

Contexte : Introduction à l'évolution des blockchains et à la création d'eBTC

Bitcoin a été le pionnier du système de paiement électronique décentralisé en peer-to-peer en contexte d'absence de confiance. Lorsque le monde a assisté à la naissance d'un papier intitulé Bitcoin : Un système de paiement électronique en peer-to-peer (Nakamoto, 2008). Cette invention ingénieuse résistant à la double-dépense a apporté deux choses au monde : une monnaie numérique et un mécanisme de consensus distribué. Le monde de la cryptographie a beaucoup évolué depuis lors et de nouvelles technologies sont apparues dans l'écosystème des blockchains. La mention principale est la couche d'abstraction fondamentale évolutive, standardisée et interopérable d'Ethereum : la blockchain Ethereum.

Le consensus distribué de Bitcoin a évolué et fourni au monde une technologie plus efficace et plus flexible lorsque Ethereum a été proposé pour la première fois par Buterin dans son article intitulé « *A Next Generation Smart Contract & Decentralized Application Platform* » (2013). Avec une efficacité, une rapidité et une flexibilité accrues, il est devenu possible de créer des solutions décentralisées innovantes pour des cas d'utilisation variés et de grande envergure. La couche d'abstraction fondatrice d'Ethereum et Solidity, son langage de codage, ont permis la création de smart contracts intelligents, d'applications distribuées (DApps) et d'organisations autonomes décentralisées (DAOs). Les forces dynamiques d'Ethereum résident dans ses éléments de base : l'extensibilité, la standardisation, l'exhaustivité des fonctionnalités, la facilité de développement et l'interopérabilité (Buterin, 2013, p. 13). Les contrats intelligents bénéficient de tous ces attributs de qualité de l'écosystème Ethereum.

eBTC s'est ouvert comme conséquence directe de l'évolution progressive de ces deux blockchains. En substance, il est apparu sous la forme d'une version ERC20 de Bitcoin possédant les vastes capacités de la plate-forme Ethereum.

Préoccupations et problèmes existants

L'un des aspects les plus importants de la mise en œuvre de Bitcoin consistait à éliminer la nécessité d'un tiers de confiance et, par conséquent, les coûts de transaction inévitables associés à de tels arrangements intermédiaires. Nakamoto a documenté que ces coûts de transaction limitaient la taille minimale pratique des transactions et la possibilité de petits paiements occasionnels (2008). En élaborant pour la toute première fois la mise en œuvre de Bitcoin sur « *P2P Foundation* », Nakamoto a observé que de tels intermédiaires rendaient les micropaiements impossibles (2009). Ironiquement, le même phénomène limite actuellement la taille minimale pratique des transactions sur Bitcoin et empêche les utilisateurs d'effectuer de petites transactions en raison de sa valeur de marché toujours croissante et très volatile.

Les coûts de transaction croissants de Bitcoin ont commencé à ressembler à ceux qu'elle était censée contrer. Actuellement, une transaction Bitcoin coûte en moyenne entre 2 et 5$ ou augmentent autour de 30 000 satoshis. La vitesse de transaction de Bitcoin représente un autre défi. Le temps moyen de validation d'un block sur Bitcoins est d'environ 10 minutes et il faut actuellement 6 confirmations, soit environ 60 minutes, pour atteindre le caractère définitif de la transaction. Ces deux facteurs limitent l'adoption du bitcoin comme un moyen pérenne d'échange de valeur numérique, ce qui sape l'âme ingénieuse de l'écosystème du bitcoin proposé à l'origine. L'utilisation de Bitcoin en tant que système d'encaissement électronique efficace pour un usage quotidien devient de plus en plus difficile. Imaginez que vous traitiez virtuellement des biens ou des services de moins de 2 $ ou que la vitesse de transaction soit d'une importance cruciale.

Il semble que la philosophie originelle de Bitcoin - qui offrait au monde une alternative révolutionnaire contre les systèmes bancaires traditionnels et les systèmes de monnaie fiat - se dilue avec ses coûts de transaction sans cesse croissants, ses temps de validation de blocs lents et ses débats interminables. De multiples forks de Bitcoin ont émergé récemment, tous essayant de résoudre une ou plusieurs de ses préoccupations dominantes : l'extensibilité, la taille du bloc et le minage de moins en moins démocratique. Mais aucun d'entre eux n'a actuellement la capacité de résoudre efficacement tous les problèmes sous-jacents qui engloutissent l'écosystème des Bitcoins. Une modernisation plus fondamentale du bitcoin est donc nécessaire pour concrétiser sa vision originelle.

A l'heure actuelle, il existe deux forks de Bitcoin documentés, à savoir Bitcoin Cash et Bitcoin Gold, tandis qu'un troisième, Segwit 2X, a également été proposé. La question liée à la lenteur de validation des blocs n' a pas encore été abordée par chacun de ces forks. Dans l'ensemble, l'écosystème actuel de Bitcoin peut être décrit comme une véritable genèse du crypto-univers et un mécanisme de stockage de valeur numérique hautement volatil. Le tableau ci-dessous documente les préoccupations de Bitcoin en matière de durée de validation de bloc, ainsi que ses forks plus récents et à venir.

Comparaison BTC/BTG/BCH/B2X	**BITCOIN BTC**	**BITCOIN CASH BCH**	**BITCOIN GOLD BTG**	**SEGWIT 2X B2X**
Quantité max	21 millions	21 millions	21 millions	21 millions
Durée de validation d'un bloc	10 minutes	10 minutes	10 minutes	10 minutes
Taille d'un bloc	1M (2–4M)	8M (8M)	1M (2–4M)	2M (4–8M)

Schéma 1 : Comparaison des intervalles de blocs entre Bitcoin et ses forks récents et à venir (Bitcoin Gold, 2017)

Solution proposée

L'évolution de la blockchain Bitcoin en une infrastructure Ethereum plus efficace et plus flexible a permis aux développeurs de créer des applications innovantes et décentralisées en plus de sa couche d'abstraction de base. Cette couche fondatrice a permis de créer des devises cryptographiques véritablement décentralisées et sans besoin de faire confiance. Cette capacité nous a permis de créer un système de paiement et d'encaissement électronique peer-to-peer sous la forme d'eBTC. eBTC, en tant que version tokenisée des idéaux fondamentaux de Bitcoin, résout les problèmes susmentionnés en offrant des vitesses de transaction plus rapides, des coûts de transaction réduits et la possibilité de travailler avec des smart contracts à la communauté mondiale des crypto-enthousiastes et au-delà.

En tant que système de paiement électronique, eBTC aspire à représenter durablement les attributs fondamentaux de Bitcoin sur la chaîne de bloc Ethereum sans avoir à subir les inconvénients des long délais de validation des blocs, des coûts de transaction plus élevés, du minage centralisé et des forks continues tout en fournissant également le support pour les smart contracts. Grâce aux capacités d'Ethereum en matière de smart contrats, eBTC s'efforce de mettre en œuvre tous les cas d'utilisation disponibles que ces programmes autonomes offrent en vue de promouvoir l'adoption d'eBTC en tant que véritable monnaie numérique et mécanisme de paiement véritablement mondial et utilisable au quotidien.

Comme eBTC existe au-dessus de la couche fondatrice d'Ethereum, les caractéristiques de son écosystème - coûts de transaction, rapidité des transactions et capacité contractuelle intelligente - reflètent les attributs systématiques d'Ethereum. Une transaction eBTC coûte approximativement entre 0,15 $ et 0,5 $ et la durée de validation d'un bloc est au moins 10 fois plus courte que celle Bitcoin et tous ses forks récents et à venir. Le tableau ci-après résume globalement le mécanisme de transaction rapide et efficace et les diverses autres caractéristiques d'eBTC par rapport à Bitcoin et tous ses forks récents et à venir.

eBTC propose de résoudre efficacement les préoccupations et les problèmes qui continuent d'être à l'origine de la croissance constante des forks dans l'écosystème Bitcoin. Avec les développements futuristes et durables d'Ethereum, eBTC continuerait à profiter du meilleur des capacités d'Ethereum tout en offrant à la communauté mondiale les idéaux fondamentaux

« Bitcoins »	BTC (Bitcoin)	BCH (Bitcoin Cash)	BTG (Bitcoin Gold)	B2X (SegWit2X)	eBTC (eBitcoin)
Quantité totale	21 millions	21 millions	21 millions	21 millions	**21 millions**
Plateforme	Bitcoin original « 1MB »	Fork Bitcoin « 8 MB »	Fork Bitcoin « Equihash »	Fork Bitcoin « 2 MB »	**Token ERC20 sur Ethereum**
Minage	Oui (ASIC & Cent.)	Oui (ASIC)	Oui (GPU)	Oui (ASIC)	**Non (Tokens en circulation)**
Lancement	Janvier 2009	Août 2017	Octobre 2017	Novembre 2017	**Octobre 2017**
Durée de validation d'un bloc	~10 minutes	~10 minutes	~10 minutes	~10 minutes	**~15 secondes**
Irrévocabilité	6 confirmations (~60 min.)	6 confirmations (~60 min.)	NA	NA	**12 confirmations (~3 min.)**
Coûts moyens de transaction	~(2$ – 5$)	~(0,06$ – 0,30$)	NA	NA	**~(0,15$ – 0,50$)**
Consensus	PoW	PoW	PoW	PoW	**PoW (bientôt PoS)**
Scalabilité	Lightening Network (non lancé)	Blocs plus grands Pas de surcouche	Lightening Network (non lancé)	Lightening Network (non lancé)	**Lightening + Sharding + Plasma**
Confidentialité	Dandelion (non actif)	NA	NA	NA	**zkSNARKs (sur testnet)**
Smart Contracts	Non	Non	Non	Non	**Oui**
Capacités	Paiements (rootstock bientôt)	Paiements	Paiements	Paiements	**Paiements + Smart contracts**
Reconnaissance en moyen de paiement	Haute	Moyenne	Minimale (en cours)	NA	**Minimale (en cours)**
GitHub Stars	18 707	239	296	326	**97**
Capitalisation du marché	~120 milliards $	~10 milliards $	~3 milliards $	NA	~2 millions $

Schéma 2 : Comparaison entre Bitcoin, ses forks et eBTC (tel qu'adopté par Larsson, 2017)

de Bitcoin sur une plateforme plus diversifiée, évolutive et innovante. Avec l'adoption d'eBTC, Ethereum serait également reconnu dans l'univers cryptographique comme une monnaie numérique et un mécanisme de stockage de valeur compatible et pourrait s'avérer un atout stratégique pour l'écosystème global d'Ethereum.

eBTC : L'erreur sur le contrat du token et le Swap

La mise en œuvre initiale du eBTC comportait une erreur critique dans le code solidity du ERC20. Cette dernière pourrait permettre au créateur du contrat de créer indûment plus de tokens que la limite maximale de 21 millions. Bien que la faille, en apparence involontaire, n'ait jamais été exploitée, elle a naturellement fait chuter la confiance dans le projet. Après avoir pris en charge avec diligence les droits du projet eBTC auprès du créateur initial, la Fondation eBTC a décidé d'exécuter un swap, c'est-à-dire un échange, sur le principe de « détention et réception » des tokens, où tous les détenteurs de clés privées de portefeuilles contenant les tokens existants recevraient de nouveaux tokens créés par le contrat corrigé, selon une parité de 1 pour 1 et après un bloc prédéfini sur Ethereum. Après avoir dûment annoncé les conditions préalables à l'échange, la Fondation eBTC a mis en œuvre la nouvelle architecture de smart contract ERC20, dans lequelle tous les détenteurs de clés privées des tokens existants ont reçu de nouveaux tokens exempts de bugs selon la parité de 1 pour 1, conformément au nouveau contrat soumis à un examen minutieux et à un audit approfondi. Le présent contrat est publié en open source sur GitHub, en libre accès.

Malgré les appels répétés d'eBTC de déplacer les tokens afin de ne les conserver que dans des portefeuilles permettant la détention de clés privées, une partie des tokens en circulation étaient malheureusement toujours détenue dans des bourses décentralisées basées sur Ethereum pendant la mise en œuvre du swap. Etant donné que ce sont des smart contracts qui organisent de tels échanges et qu'il n'y a aucun contrôle humain sur ces marchés de change, environ 2,1 millions des nouveaux tokens eBTC sont détenus en permanence par ces échanges et ne devraient donc jamais pouvoir être mis en circulation. 21 millions d'eBTC ont donc été créés et environ 18,9 millions sont en circulation.

eBTC : Des fondamentaux soutenus par la simplicité et une communauté mondiale diversifiée et dynamique

eBTC est une monnaie cryptographique basée sur une communauté qui fonctionne en token ERC20 en tirant parti des meilleurs attributs de Bitcoin et d'Ethereum. C'est une version tokenisée de Bitcoin sur la blockchain Ethereum et qui complète donc de manière unique les deux. Elle vise à représenter et à soutenir les attributs de base de Bitcoin, en tant que moyen électronique d'échange et de stockage durable de valeur sur la Blockchain Ethereum, mais avec une perspective plus judicieuse et plus rapide.

La création d'un ERC20 représentant Bitcoin sur la blockchain Ethereum peut paraître un peu « trop simple », mais découvrir la possibilité de mettre en œuvre les idéaux de Bitcoin sur une technologie de blockchain existante, plus développée, rapide, flexible et plus évolutive n'est rien de moins qu'un raisonnement innovant et disruptif. eBTC est ce processus de réflexion qui cherche à mettre en œuvre la vision idéaliste de Bitcoin sur la blockchain Ethereum permettant des vitesses de transaction plus rapides, des coûts de transaction plus bas et des capacités contractuelles intelligentes sans avoir à faire face aux problèmes de forks et de minage centralisé.

eBTC croit fermement qu'une communauté mondiale, robuste et dynamique, de passionnés de cryptographie est essentielle pour une évolution durable de l'écosystème tout entier. La Fondation eBTC est composée d'un corps mondial diversifié et dynamique d'individus inspirants qui sont tous fermement engagés à promouvoir la cause simple, mais disruptive de l'eBTC. De plus, le rôle de la communauté élargie de l'eBTC est crucial pour faire connaître le pouvoir des ledgers distribués et la façon dont l'eBTC peut modifier le tissu même de la façon que nous faisons évoluer la conduite des transactions financières en ligne.

eBTC : Caractéristiques techniques

eBTC vs. ether

eBTC est un système de paiement électronique et de paiement en espèces et électronique basé sur Ethereum et l'ether, « le crypto-carburant du réseau Ethereum » (« What is Ether », 2017), sert à valider les transactions eBTC sur la blockchain Ethereum. En tant que combustible, l'ether soutient l'écosystème global d'Ethereum.

Pour être clair, l'ether n'a jamais été conçu pour être une devise sur Ethereum. Son but est plutôt de servir de carburant pour faire fonctionner la plate-forme d'applications distribuées sur Ethereum : « Il est une forme de paiement effectué par les clients de la plate-forme aux machines exécutant les opérations demandées » (« What is Ether », 2017). D'autre part, eBTC, dans son sens le plus pur, n'est qu'une monnaie numérique utilisable au quotidien et un système de paiement optimisé, c'est-à-dire un moyen d'échange et de stockage de valeur plus rapide et moins coûteux.

Création, distribution et minage

Le nombre total et maximal d'eBTC créés ne sera jamais supérieur à 21 millions et l'eBTC sera divisible jusqu'à 8 décimales. A l'origine, tous les tokens eBTC ont été fournis de manière transparente et gratuite, sans ICO, vers la communauté mondiale diversifiée et engagée de crypto-enthousiastes. Dès le début, eBTC est une monnaie numérique résistante au minage et orientée vers la distribution, car son offre totale a été entièrement distribuée à la communauté et à la fondation eBTC à un ratio de respectivement 97,92:2,08.

L'eBTC déflationniste et l'ether inflationniste

Comme l'offre totale d'eBTC est limitée à 21 millions, elle reflète les attributs déflationnistes de Bitcoin sur une blockchain Ethereum plus flexible et plus adaptée. En d'autres termes, avec une augmentation durable de la valeur de l'eBTC, son pouvoir d'achat apprécierait également qu'il devienne le seul représentant bitcoin de la blockchain Ethereum ayant des caractéristiques déflationnistes. La nature déflationniste de l'eBTC signifie en outre qu'elle pourrait servir de mécanisme durable et approprié de stockage de valeur sur l'écosystème Ethereum.

De façon ironique, l'offre totale d'ether est actuellement non plafonnée. Cela signifie un phénomène intéressant: eBTC, une monnaie numérique déflationniste, fonctionnerait sur la blockchain décentralisée avec l'aide optimisée d'un cryptocarburant inflationniste, c'est-à-dire l'Ether. Compte tenu de la qualité inflationniste de l'ether et de ses prix relativement stables, eBTC continuerait à connaître durablement les coûts de transaction moins élevés du réseau Ethereum.

La possibilité de réalisation de contrats intelligents d'eBTC et les développements prospectifs d'Ethereum

Le fait d'être une version ERC20 de Bitcoin sur la plate-forme Ethereum offre à l'eBTC un avantage novateur en termes de collaboration avec une grande variété de smart contracts, DApps et DAO basés sur Ethereum. eBTC prévoit stratégiquement de coordonner et d'intégrer ces cas d'utilisation novateurs, ce qui contribuerait à en faire un système de paiement électronique véritablement mondial et hautement accessible. Avec son adoption et son évolution progressive, eBTC peut également devenir un atout stratégique pour l'écosystème Ethereum.

Conclusion

Nous avons présenté la conception, le concept et les caractéristiques fondamentales de l'eBTC en tant que version tokenisé de Bitcoin sur la blockchain Ethereum. eBTC sert de système de paiement électronique pair-à-pair efficace, robuste et plus flexible. Nous avons commencé avec l'évolution de mécanismes consensuels sans besoin de confiance et avons établi le progrès du consensus distribué de Bitcoin dans la couche fondatrice abstraite plus flexible, diversifiée et interopérable d'Ethereum. Nous avons ensuite discuté de la façon dont eBTC a vu le jour comme conséquence directe de l'évolution de Bitcoin vers ce que l'on a par la suite connu sous le nom de blockchain d'Ethereum. Nous avons mis en lumière les préoccupations dominantes liées à la lenteur de validation des blocs, aux coûts de transaction plus élevés, au minage centralisé et aux forks de l'écosystème de Bitcoin qui ne bénéficie pas actuellement d'un protocole de smart contracts, et à la façon dont eBTC peut résoudre tous ces problèmes tout en fonctionnant comme une version ERC20 de Bitcoin sur l'écosystème d'Ethereum, qui est extrêmement performant et optimisé en permanence. Nous avons également documenté les principes fondamentaux de l'eBTC, ses aspects techniques et la manière dont la communauté mondiale engagée et diversifiée est essentielle à la prise de conscience générale de l'eBTC et à son adoption généralisée. Nous pensons qu'avec l'adoption et la prise de conscience, eBTC pourrait permettre à de telles communautés mondiales de revivre le bitcoin une fois de plus sur une blockchain plus flexible et plus efficace sans avoir à passer par les débats idéologiques et politiquement chargés sur les forks de Bitcoin en croissance constante.

Bibliographie

Bitcoin Gold. (2017). Bitcoin Gold and other forks of Bitcoin – Source : 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 . Source : 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 – Source : https://allcoinwiki.com/bitcoin/

Nakamoto, S. (2008). Bitcoin: A peer - to - peer electronic cash system. Bitcoin.org – Source : https://bitcoin.org/bitcoin.pdf

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

What is Ether. (2017). In Ethereum.org – Source : https://ethereum.org/ether