

eBTC: la versione Ethereum di Bitcoin con Smart Contracts,  
Bassi costi di transazione e alta velocità

eBTC's Community Foundation

Abstract

eBTC, eBitcoin o Ethereum's Bitcoin è una versione di Bitcoin in ERC20, basata su Blockchain Ethereum. Propone di risolvere il costo delle transazioni, la velocità e la scalabilità, oltre che tutto ciò che concerne l'inefficienza dell'originale blockchain Bitcoin, utilizzando un livello di blockchain basato su Ethereum molto più efficace e scalabile. Supportata da una vasta e dinamica community globale, eBTC intende diventare più affidabile, veloce e flessibile sistema di pagamento elettronico peer-to-peer.

Intende farlo mantenendo gli ideali fondamentali di Bitcoin integrandoli con l'ecosistema di Ethereum.

L'anno 2017 ha visto l'emergere di molteplici fork di Bitcoin che tentavano di risolvere una o più delle sue preoccupazioni esistenti: bassa velocità di transazione, costi di transazione elevati e attività di mining centralizzate.

Tuttavia, nessuno dei fork ha attualmente la capacità di risolvere efficacemente tutti questi problemi. Al contrario, il design apparente e stranamente semplice di eBTC consente di affrontare queste sfide in modo efficiente, aggiungendo anche funzionalità di smart contract agli ideali fondamentali di Bitcoin.

Con la crescente consapevolezza e accettazione, eBTC intende diventare un meccanismo di elaborazione dei pagamenti globale, veloce, economico e completamente decentralizzato, pur continuando a integrare tutti i futuri sviluppi nella rete Ethereum. In questo modo, l'eBTC rappresenta i valori fondamentali originali di Bitcoin, come un mezzo sostenibile di pagamento

elaborazione dei pagamenti globale, veloce, economico e completamente decentralizzato, pur continuando a integrare tutti i futuri sviluppi nella rete Ethereum. In questo modo, l' eBTC rappresenta i valori fondamentali originali di Bitcoin, come un mezzo sostenibile di pagamento elettronico e di conservazione del valore, portando allo stesso tempo la necessaria modernizzazione di Bitcoin utilizzando l' ecosistema eterogeneo di Ethereum e consentendo l' implementazione in eBTC di tutti i casi d' uso disponibili di un sistema di pagamento accettato a livello globale.

*Parole chiave: eBTC, Bitcoin, Ethereum, eBitcoin, ERC20, strato fondazionale astratto, blockchain, moneta digitale, contante elettronico.*

## Sommario

Contesto: introduzione all' evoluzione di Blockchain e alla creazione di eBTC	3
I problemi attuali	4
La soluzione proposta	6
eBTC: l' errore nella solidità del token e lo swap	8
eBTC: i fondamenti sostenuti dalla semplicità e da una globale diversificata e dinamica community	9
eBTC: Caratteristiche tecniche	10
eBTC vs. Ether	10
L' offerta totale, la distribuzione e il mining	10
Deflationary eBTC e Inflationary Ether	11
La Smart Contract Capability di eBTC e gli sviluppi futuri di Ethereum	11
Conclusioni	12
Riferimenti	13

### **Contesto: introduzione all' evoluzione di Blockchain e alla creazione di eBTC**

Bitcoin è stato il pioniere del sistema monetario elettronico peer-to-peer decentralizzato quando il mondo ha assistito alla comparsa di un articolo dal titolo: A Peer-to-Peer Electronic Cash System (Nakamoto, 2008). Questa ingegnosa invenzione ha portato al mondo due cose: una moneta digitale e un meccanismo di consenso distribuito. Il mondo delle cryptovalute è molto cambiato da allora e sempre più nuove tecnologie sono apparse nell' ecosistema blockchain.

Il cuore è la scalabilità di Ethereum, a un livello funzionale astratto standardizzato e interoperabile: la blockchain Ethereum.

Il consenso distribuito di Bitcoin si è evoluto e ha fornito al mondo una tecnologia più efficiente e flessibile quando Ethereum è stato proposto per la prima volta da Buterin nel suo articolo intitolato A Next Generation Smart Contract & Decentralized Application Platform (2013).

Grazie ad una maggiore efficienza, velocità e flessibilità, è stato possibile creare soluzioni innovative e decentralizzate per applicazioni diverse e di ampia portata.

Il suo linguaggio di codifica, ha permesso la creazione di smart contracts, applicazioni decentrate (DApps) e organizzazioni autonome decentralizzate (DAOs). I punti di forza dinamici di Ethereum risiedono nei suoi elementi fondamentali: scalabilità, standardizzazione, completezza delle caratteristiche, facilità di sviluppo e interoperabilità (Buterin, 2013, p. 13). Gli smart contracts godono di tutti questi attributi di qualità dell' ecosistema Ethereum.

L' eBTC è stato introdotto come conseguenza diretta della graduale evoluzione di entrambe queste blockchain: ovvero una versione ERC20 di Bitcoin in possesso delle vaste capacità della piattaforma Ethereum.

## I problemi attuali

Uno degli aspetti più critici dell' implementazione di Bitcoin è stato quello di eliminare la necessità della fiducia dei terzi e quindi i costi di transazione inevitabili associati a tali accordi intermedi.

Nakamoto ha documentato che tali costi di transazione limitavano al minimo i costi pratici dimensione delle transazioni e la possibilità di piccoli pagamenti occasionali (2008). Durante l' elaborazione dell' implementazione di Bitcoin sulla Fondazione P2P per la prima volta, Nakamoto ha osservato che tali intermediari rendevano impossibili i micropagamenti (2009).

Ironicamente, lo stesso fenomeno limita attualmente la dimensione minima pratica delle transazioni su Bitcoin e impedisce agli utenti di effettuare transazioni di piccole dimensioni a causa del suo valore di mercato sempre crescente e altamente volatile.

I crescenti costi di transazione di Bitcoin hanno cominciato ad assomigliare a quegli stessi accordi che si supponeva fossero inizialmente compensati. Attualmente, una transazione Bitcoin costa in media da 2 a 5\$ o più di circa 30.000 satoshis.

La velocità delle transazioni Bitcoin rappresenta un' altra sfida. Il tempo medio di blocco Bitcoin è di circa 10 minuti e attualmente ci vogliono 6 conferme o circa 60 minuti per raggiungere la finalizzazione della transazione.

Entrambi questi fattori limitano l' adozione di Bitcoin come mezzo sostenibile di scambio digitale, compromettendo l' anima ingegnosa dell' ecosistema Bitcoin originariamente proposto. L' utilizzo di Bitcoin come efficiente sistema elettronico di cassa per l' uso quotidiano è sempre più impegnativo.

Immagina di transare virtualmente beni o servizi sotto \$2 o quando i tempi di transazione sono di importanza critica.

Sembra che la filosofia originaria di Bitcoin, che presentava al mondo un' alternativa rivoluzionaria rispetto ai sistemi bancari e fiat tradizionali, si stia diluendo con i suoi costi di transazione in continua crescita, tempi di blocco lenti e dibattiti incessanti.

Di recente sono emerse più forcelle Bitcoin che hanno cercato di risolvere una o più delle sue preoccupazioni prevalenti:

scalabilità, dimensioni del blocco e l'attività di mining sempre più antidemocratica. Ma nessuno di essi ha attualmente la capacità di risolvere in modo efficiente tutti i problemi sottostanti che coinvolgono l'ecosistema Bitcoin.

Una modernizzazione più fondamentale di Bitcoin è quindi necessaria per realizzare la sua visione originale. Attualmente esistono due fork documentate di Bitcoin, ovvero Bitcoin Cash e Bitcoin Gold, mentre un terzo, SegWit 2X, è stato proposto. La questione dei tempi di blocco lenti non è ancora stata affrontata da ciascuna di questi fork.

Nel complesso, l' attuale ecosistema Bitcoin può essere meglio descritto come una vera e propria genesi del meccanismo cripto-universo e un meccanismo digitale altamente volatile di memorizzazione del valore. La tabella documenta le preoccupazioni di Bitcoin per il lento blocco temporale e i suoi fork più recenti e imminenti.

COMPARAZIONE BTC/BTG/BCH/B2X	BITCOIN BTC	BITCOIN CASH BCH	BITCOIN GOLD BTG	SEGWIT 2X B2X
Supply	21 milioni	21 milioni	21 milioni	21 milioni
Block Time	10 minuti	10 minuti	10 minuti	10 minuti

Block Time	10 minuti	10 minuti	10 minuti	10 minuti
Block Size	1M (2-4M)	8M (8M)	1M (2-4M)	2M (4-8M)

Figura 1: differenze degli intervalli di blocco tra Bitcoin e i recenti e imminenti fork (Bitcoin Gold, 2017)

### La soluzione proposta

L'evoluzione di Bitcoin in un'infrastruttura Ethereum più efficiente e flessibile ha permesso agli sviluppatori di creare applicazioni innovative e decentralizzate oltre al suo livello astratto di fondazione.

Lo strato di fondazione ha permesso la possibilità di creare cripto-culture veramente decentralizzate e senza fiducia.

Questa capacità ci ha permesso di creare un sistema elettronico peer-to-peer di pagamento e contante sotto forma di eBTC.

L'eBTC, come versione Ethereum degli ideali fondamentali di Bitcoin, risolve le suddette preoccupazioni offrendo velocità di transazione più rapide, costi di transazione inferiori e la possibilità di lavorare con smart contract.

Come sistema di pagamento elettronico in contanti e denaro, l'eBTC aspira a rappresentare in modo sostenibile gli attributi chiave di Bitcoin su blockchain Ethereum senza dover affrontare i fastidiosi tempi di blocco lenti, i costi di transazione più elevati, l'attività di mining centralizzata e fork continui, fornendo anche il supporto per i smart contracts. Grazie alle capacità di Ethereum per gli smart contract, eBTC cerca di implementare tutte le possibilità di utilizzo offerte da tali contratti per promuovere l'adozione di eBTC come moneta digitale e meccanismo di pagamento realmente globale e utilizzabile quotidianamente.

Poiché l'eBTC esiste oltre lo strato costitutivo dell'Ethereum, le caratteristiche del suo ecosistema - costi di transazione, velocità di transazione e capacità contrattuale intelligente - rispecchiano gli attributi sistematici di Ethereum. Una transazione eBTC costa all'incirca da 0,15 a 0,5 dollari e il suo tempo di blocco è almeno 10 volte più veloce di Bitcoin e di tutti i suoi fork recenti e imminenti.

La tabella sottostante riassume in modo completo il meccanismo di transazione veloce ed efficiente e varie altre caratteristiche di eBTC rispetto a Bitcoin e a tutti i suoi fork recenti e imminenti. L'eBTC si propone di risolvere in modo efficace le preoccupazioni e i problemi che continuano a causare la continua crescita dei fork nell'ecosistema Bitcoin.

"Bitcoins"	BTC (Bitcoin)	BCH (Bitcoin Cash)	BTG (Bitcoin Gold)	B2X (SegWit2X)	eBTC (eBitcoin)
<b>Total Supply</b>	21 Million	21 Million	21 Million	21 Million	<b>21 Million</b>
<b>Platform</b>	Original Bitcoin "1MB"	Bitcoin Fork "8 MB"	Bitcoin Fork "Equihash"	Bitcoin Fork "2MB"	<b>ERC20 Token on Ethereum</b>
<b>Mining</b>	Yes (ASIC & Cent.)	Yes (ASIC)	Yes (GPU)	Yes (ASIC)	<b>No (T. in Circulation)</b>
<b>Launch</b>	2009-Jan.	2017-Aug.	2017-Oct.	2017-Nov.	<b>2017-Oct.</b>
<b>Block Time</b>	~ 10 Minutes	~ 10 Minutes	~ 10 Minutes	~ 10 Minutes	<b>~ 15 Seconds</b>

<b>Launch</b>	2009-Jan.	2017-Aug.	2017-Oct.	2017-Nov.	<b>2017-Oct.</b>
<b>Block Time</b>	~ 10 Minutes	~ 10 Minutes	~ 10 Minutes	~ 10 Minutes	~ <b>15 Seconds</b>
<b>Finality</b>	6 Confirmations (~ 60 min.)	6 Confirmations (~ 60 min.)	NA	NA	<b>12 Confirmations (~ 3 min.)</b>
<b>Avg. Tx. Cost Range</b>	~ (\$2 – \$5)	~ (\$0.06 – \$0.3)	NA	NA	~ <b>(\$0.15 – \$0.5)</b>
<b>Consensus</b>	PoW	PoW	PoW	PoW	<b>PoW (soon PoS)</b>
<b>Scaling</b>	Lightening Network (not launched)	Larger Block Size No layer on top	Lightening Network (not launched)	Lightening Network (not launched)	<b>Lightening + Sharding + Plasma</b>
<b>Privacy</b>	Dandelion (not live)	NA	NA	NA	<b>zkSNARKs (on testnet)</b>
<b>Smart Contracts</b>	No	No	No	No	<b>Yes</b>
<b>Capabilities</b>	Payments (Rootstock soon)	Payments	Payments	Payments	<b>Payments + Smart contracts</b>
<b>Payment Acceptance</b>	High	Medium	Minimal (In Progress)	NA	<b>Minimal (In Progress)</b>
<b>GitHub Stars</b>	18,707	239	296	326	<b>97</b>
<b>Market Cap.</b>	~ \$120 Billion	~ \$10 Billion	~ \$3 Billion	NA	~ <b>\$2 Million</b>

Figura 2: Confronto tra Bitcoin, i suoi Forks e eBTC (Larsson, 2017)

Con gli sviluppi sostenibili e futuristici di Ethereum, eBTC continuerebbe a godere e sfruttare al meglio le capacità di Ethereum offrendo alla comunità globale gli ideali fondamentali di Bitcoin su una piattaforma più diversificata, scalabile e innovativa.

L'adozione di eBTC, rafforzerebbe anche il riconoscimento di Ethereum nell'universo cripto come moneta digitale abilitata e come meccanismo di accumulazione del valore e potrebbe rivelarsi un asset strategico per l'ecosistema complessivo di Ethereum.

### **eBTC: l'errore nella solidità del token e lo swap**

L'implementazione originale dell'eBTC conteneva un errore critico nel suo codice di solidità ERC20, che poteva consentire al creatore del contratto di creare erroneamente più token rispetto alla fornitura massima di 21 milioni.

Mentre il difetto non è mai stato sfruttato e apparentemente involontariamente, ha fatto precipitare la fiducia nel progetto.

Dopo aver rilevato diligentemente i diritti al progetto eBTC dal creatore originale, eBTC Foundation ha deciso di eseguire uno swap contrattuale dove tutti i detentori con i token esistenti hanno ricevuto i propri token eBTC privi di errori in un rapporto 1:1.

Dopo aver debitamente annunciato in anticipo i prerequisiti per lo swap, eBTC Foundation ha quindi implementato la nuova architettura di smart contract ERC20, dove tutti i detentori di token privati esistenti hanno ricevuto token nuovi e privi di bug in un rapporto di 1:1 secondo il nuovo contratto accuratamente revisionato.

Il contratto in corso è pubblicato come open source su GitHub, libero per chiunque a recensioni. Nonostante i solleciti dovuti di eBTC di spostare e trattenere i token in portafogli che consentono la

contratto accuratamente revisionato.

Il contratto in corso è pubblicato come open source su GitHub, libero per chiunque a recensioni. Nonostante i solleciti dovuti di eBTC di spostare e trattenere i token in portafogli che consentono la proprietà privata della chiave, una parte dell' offerta circolante dei token è stata purtroppo tenuta in exchange basati su Ethereum durante l' attuazione della swap. Dato che i smart contract forniscono l' energia a tali exchange e che non vi è alcun controllo umano su di esse, circa 2,1 milioni dei nuovi token eBTC sono permanentemente detenuti all' esterno e non faranno mai parte della nuova fornitura circolante. La nuova offerta totale e circolante di eBTC ammonta rispettivamente a circa 18,9 milioni.

## **eBTC: i fondamenti sostenuti dalla semplicità e da una globale diversificata e dinamica community**

eBTC è una crypto valuta cripto basata su community e a catena a blocchi che funziona come un token ERC20 sfruttando i migliori attributi di Bitcoin ed Ethereum.

Si tratta di una versione token di Bitcoin sulla catena a blocchi Ethereum e quindi completa in modo unico entrambi.

Mira a rappresentare e sostenere gli attributi fondamentali di Bitcoin, come mezzo elettronico di scambio e riserva di valore sostenibile, sulla catena Blockchain di Ethereum, ma con una prospettiva più intelligente e veloce.

La creazione di un rappresentante ERC20 di Bitcoin sulla catena incatenata di Ethereum può sembrare troppo semplice, ma scoprire la possibilità di implementare gli ideali di Bitcoin su una tecnologia blockchain esistente e più evoluta, veloce, flessibile e più scalabile non è altro che un processo di pensiero innovativo e dirompente.

eBTC è questo processo di pensiero e cerca di implementare la visione idealistica di Bitcoin su blockchain Ethereum permettendo velocità di transazione più elevata, costi di transazione inferiori e capacità di smart contract senza sperimentare i problemi contestuali di fork e mining centralizzato.

eBTC è fermamente convinta che una comunità globale, solida e dinamica di appassionati di crittografia sia fondamentale per un' evoluzione sostenibile dell' intero ecosistema

La Fondazione eBTC è composta da un corpo globale diversificato e vibrante di individui ispirati, tutti fermamente impegnati a promuovere la causa semplice ma dirompente dell' eBTC.

Inoltre, il ruolo della comunità allargata di eBTC è fondamentale per diffondere la parola sul potere dei libri contabili distribuiti e sul modo in cui eBTC può cambiare il tessuto stesso di come sviluppiamo la conduzione delle transazioni finanziarie online.

## **eBTC: Caratteristiche tecniche**

### **eBTC vs. Ether**

eBTC è un sistema di pagamento in contanti ed elettronico e abilitato su sistema Ethereum, -il criptocarburante per la rete Ethereum (-What is Ether?, 2017) serve a convalidare le transazioni eBTC attraverso la catena a blocchi Ethereum.

Come carburante, Ether supporta l' intero ecosistema Ethereum.

Per chiarire, Ethereum non era mai stato pensato per essere una moneta, ma con lo scopo di servire come carburante per il funzionamento della piattaforma distribuita di applicazione su Ethereum (-What is Ether?, 2017). È una forma di pagamento da parte dei clienti della piattaforma alle macchine che eseguono le operazioni richieste (-Che cos' è Ether?, 2017)? D' altro canto, l' eBTC, nel suo senso più puro, è solo una moneta digitale utilizzabile quotidianamente e un sistema di pagamento ottimizzato, cioè un mezzo di scambio e di conservazione del valore più veloce ed economico.

pagamento ottimizzato, cioè un mezzo di scambio e di conservazione del valore più veloce ed economico.

## **L' offerta totale, la distribuzione e il mining**

La totale e massima offerta di eBTC è pari a 21 milioni di euro, divisibili per 8 cifre decimali. Alla genesi, tutti i token eBTC sono stati distribuiti in modo trasparente e senza ICO alla comunità globale diversificata e impegnata degli appassionati. Fin dall' inizio, eBTC è una moneta digitale resistente al mining e orientata alla circolazione, in quanto la sua offerta totale è stata interamente distribuita alla comunità e la fondazione eBTC con un rapporto percentuale di 97,92:2,08 rispettivamente.

## **Deflationary eBTC e Inflationary Ether**

Poiché l' offerta totale di eBTC è limitata a 21 milioni, riflette gli attributi deflazionistici di Bitcoin su una catena a blocchi Ether più flessibile e intelligente.

In altre parole, con l' aumento sostenibile del valore dell' eBTC, il suo potere d' acquisto apprezzerrebbe anche il fatto di essere l' unico rappresentante Bitcoin sulla catena a blocchi Ether con caratteristiche deflazionistiche.

La natura deflazionistica dell' eBTC significa inoltre che potrebbe fungere da meccanismo di stoccaggio del valore sostenibile e adeguato sull' ecosistema Ether. Ironia della sorte, l' offerta totale di Ether è attualmente non coperta.

Ciò significa un fenomeno interessante: l' eBTC, una moneta digitale deflazionistica, funzionerebbe sulla catena di blocchi decentralizzata con l' assistenza ottimizzata di un cripto-carburante inflazionistico, cioè l' Ether. Considerando la qualità inflazionistica dell' Ether e la sua relativa stabilità dei prezzi, l' eBTC continuerebbe a sostenere i minori costi di transazione della rete Ethereum.

## **La Smart Contract Capability di eBTC e gli sviluppi futuri di Ethereum**

Essere una versione ERC20 di Bitcoin sulla piattaforma Ethereum offre all' eBTC il vantaggio innovativo di lavorare con una varietà diversificata di smart contract, DApp e DAO abilitati per Ethereum. L' eBTC progetta strategicamente di coordinarsi e integrare questi innovativi casi d' uso che contribuirebbero a farne un sistema elettronico di contanti e pagamenti veramente globale e altamente accessibile. Con l' adozione e la graduale evoluzione, l' eBTC può anche diventare un asset strategico per l' ecosistema Ethereum.

## **Conclusioni**

Abbiamo discusso il design di base, il concetto e le caratteristiche di implementazione di eBTC come una versione token di Bitcoin sulla catena a blocchi Ethereum che serve come un efficiente, robusto e più flessibile contante elettronico peer-to-peer e un sistema di pagamento.

Iniziammo con l' evoluzione dei meccanismi di consenso senza fiducia e stabilimmo il progresso del consenso distribuito di Bitcoin nel più flessibile, diversificato e interoperabile strato di Ethereum.

Abbiamo poi discusso di come eBTC sarebbe nato, ovvero come conseguenza diretta dell' evoluzione di Bitcoin in quello che più tardi è diventato per essere conosciuto come catena a blocchi di Ethereum.

Abbiamo evidenziato le preoccupazioni prevalenti di tempi di blocco lenti, costi di transazione più elevati, mining centralizzato e fork in continua crescita dell' ecosistema di Bitcoin - che attualmente non hanno un supporto per smart contract, e come eBTC può risolvere tutti questi problemi visto che funziona come una versione ERC20 degli ideali fondamentali di Bitcoin sull' ecosistema di Ethereum ampiamente capace e continuamente ottimizzante.

Abbiamo anche documentato i fondamenti dell' eBTC, i suoi aspetti tecnici e il modo in cui la

Abbiamo anche documentato i fondamenti dell' eBTC, i suoi aspetti tecnici e il modo in cui la comunità globale impegnata e diversificata è fondamentale per la consapevolezza generale e l'adozione di eBTC.

Crediamo che, con l'adozione e la consapevolezza, eBTC possa permettere a tali comunità globali di sperimentare ancora una volta Bitcoin su una catena a blocchi più flessibile ed efficiente senza dover passare attraverso i dibattiti ideologici e politicamente carichi sui sempre crescenti fork Bitcoin.

## Referimenti

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. Theblockchain.com. Retrieved from [http://www.theblockchain.com/docs/Ethereum\\_white\\_paper\\_a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalikbuterin.pdf](http://www.theblockchain.com/docs/Ethereum_white_paper_a_next_generation_smart_contract_and_decentralized_application_platform-vitalikbuterin.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>