BTCe

2023

BTC ERC20 WHITEPAPER

MINEABLE ERC20 TOKEN

www.btcerc20.com

TABLE OF CONTENTS

ABSTRACT

The Ethereum Network has established itself as a pioneering ecosystem for permissionless, transparent, and immutable software applications. These applications, commonly in the form of Smart Contracts, seamlessly interact with one another. To enable this seamless interaction, standard protocols such as the ERC20 standard have been developed, creating a common 'token' format. This facilitates the transfer of scarce, owned, and transferable data between Smart Contracts without the need for a centralized intermediary. Until 2018, every ERC20 token was distributed in a manner that was often considered 'securities.' They were sold to 'investors' with the expectation that the 'creator' would take actions to increase the tokens' value.

This paper introduces the first ERC20 token that aligns itself as a 'commodity' since it is distributed exclusively through 'Proof of Work Mining,' following the Bitcoin model. This token is also transferred on a blockchain in a manner very similar to Bitcoin, allowing it to interface with other software and the world in a way that is effectively identical to Bitcoin. However, this token offers several advancements, such as the ability to directly interact with Ethereum Smart Contracts and the broader Ethereum Ecosystem in a permissionless manner.

BACKGROUND

BTCe is the realization of Bitcoin on the Ethereum blockchain, making it the first decentralized ERC20 token for Ethereum. It is a community-driven open-source project without centralized leadership or an associated corporation, avoiding the capital influx typical of centralized token projects. This commitment to decentralization aligns with the fundamental principles of blockchain, providing users with open and transparent trust. Ethereum and ERC20 tokens are seen as a pivotal component of future blockchain technology.

BTCe is designed to serve as a decentralized 'bitcoin-like' token within the Ethereum ecosystem and beyond. By leveraging the Ethereum Network and globally distributed anonymous miners, it addresses issues related to centralization and security. As it adheres to the ERC20 standard, it can be stored in a traditional Ethereum wallet and transferred using standard software compatible with EIP20/ERC20 tokens. Notably, BTCERC20's decentralized distribution method means no central body controls or enforces any aspect of the token. The community operates the token with equal power among all individuals to establish it as a commodity, following the Bitcoin model.

A significant outcome of Satoshi Nakamoto's use of Proof of Work mining for Bitcoin was the anchoring and bootstrapping of the coin to computational power, eliminating centralized control. By shifting the responsibility of work to individual miners, government organizations lose jurisdiction and visibility over mined BTCe. This approach promotes relatively decentralized distribution and makes all involved parties stakeholders. BTCERC20 is groundbreaking in enabling project funding not through centralized fiat conversion but via decentralized computing power.

ETHEREUM

The Ethereum blockchain currently thrives as a permissionless ecosystem, allowing individuals to store immutable records in an open, secure, and transparent manner. Ethereum, among similar blockchains, possesses this unique capability. As blockchain applications expand in complexity and number, alternative distribution models to ICOs are needed. While the DAICO model has been introduced, relying on timed and automated value transfers via the DIACO smart contract tapping mechanism, it still classifies tokens as securities and presents potential investor risks. Allowing network users direct access to tokens by participating in proof of work mining offers a safer, controlled, and gradual token distribution process, similar to the introduction of a new commodity.

As of 2017, all Ethereum token distribution methods were susceptible to Sybil attacks, a form of computer security attack involving multiple accounts to manipulate a system maliciously. ICOs and airdrops were particularly vulnerable to Sybil attacks, as there was no way to verify the fairness of ERC20 token distribution. In contrast, BTCERC20, with its unique Proof of Work distribution method, is resistant to Sybil attacks. This makes BTCERC20 the first trustless Ethereum token globally, as its distribution relies solely on mathematical hashing rather than human intervention.

USE CASES

BTCERC20, implementing the original Bitcoin software as an Ethereum Smart Contract, combines the strengths of both Bitcoin and Ethereum. It is decentralized, permissionless, mined, and scarce, akin to Bitcoin, thus sharing Bitcoin's attributes as a transparent and permanent digital store of value. Beyond Bitcoin, BTCERC20 leverages the speed and scalability of the Ethereum network and is compatible with all ERC20 token services. This means it can be stored in any Ethereum wallet, offers Ethereum's level of security, and serves as 'the bitcoin' for the Ethereum ecosystem. Unlike Bitcoin, BTCERC20 enables the Ethereum network to interact with a commodity sharing all the properties of Bitcoin, empowering Ethereum smart contracts to hold, transfer, and trade bitcoin-like tokens in a permissionless and immutable manner, governed by their own code.

The commodity Ether, primarily used within the Ethereum network, raises questions about its ultimate usability as a decentralized store of value. Ether serves as a medium to secure the Ethereum network and is not solely intended as 'bitcoin' for Ethereum. If Ethereum implements Proof of Stake, Ether will no longer be mined through Proof of Work. In such a scenario, BTCERC20 may become the only mined asset on Ethereum, aiming to fulfill the role Ether currently plays. This allows Ether to concentrate on securing the network and maintaining Ethereum's lifeblood.

DECENTRALIZED

BTCERC20 is mined in a manner similar to Bitcoin, making it function as a commodity. Its mining difficulty automatically adjusts based on the total computational power dedicated to mining. The Ethereum ICO market's notable failure rate exposes investors to pseudo-value based on speculation. BTCERC20 addresses this issue by offering a decentralized bitcoin-like asset on the Ethereum network, capable of substituting a variety of centralized tokens in a more robust and trustless format.

This innovative approach liberates individuals from relying on third-party exchanges, vulnerable to security breaches and wallet compromises. Departing from centralization aligns with Satoshi Nakamoto's original vision for Bitcoin. BTCERC20 fosters openness, accountability, trustless, and decentralization throughout the value transfer process. Unlike Bitcoin, which relies on centralized trading, BTCERC20 can be traded permissionless within immutable smart contracts that cannot be censored or controlled by centralized entities, thus fulfilling Satoshi's full vision.

DECENTRALIZED

Account System:

As an ERC20 token, BTCERC20 employs a traditional Ethereum account system. These accounts are free from hacking or theft, as long as the private key remains secure. BTCERC20 can be stored in wallets such as Ledger Nano, Trezor, or any other that supports ERC20 tokens.

Algorithm and Methodology:

BTCERC20 employs a simple yet effective Keccak256 (Sha3) algorithm for its mining process. Miners strive to discover a nonce, a randomly generated number by mining software. When combined with their Ethereum address and a challenge number, this nonce must produce a hash smaller than the current difficulty target to be considered a valid solution to the PoW puzzle.

Dynamic Challenge Number:

To thwart retroactive mining attempts, the challenge number in the PoW algorithm continuously updates with each new Ethereum block. This dynamic feature ensures the prevention of mining works from the past and enhances network security.

DECENTRALIZED

Enhanced Security:

The inclusion of the miner's Ethereum address in the proof of work not only secures the process but also enables pool mining. This setup mitigates man-in-the-middle attacks and promotes equitable mining practices. Miners are mandated to utilize the pool's Ethereum address when generating proofs of work.

Gas Fee Optimization:

Miners who wish to avoid high gas fees can participate in pool mining. In this approach, miners submit their solutions to the pool, which manages the associated gas fees for executing the Ethereum smart contract code. The pool typically deducts a small percentage of the rewards and distributes the remainder to the miners.

Fairness and Cheating Prevention:

To ensure fairness within pools and prevent miners from submitting partial solutions to the pool while using full solutions for individual gain, pools require miners to mine using the pool's Ethereum address. This safeguards the integrity of the mining process.

Partial Solutions and Shares:

Pools often accept "partial solutions" from miners, meaning miners receive "shares" from the pool for solutions that are close to being valid but not quite. Probability theory suggests that given a sufficient number of close solutions, a full solution will eventually be found.

MINING BTCe

The BTCERC20 token was deployed to the Ethereum blockchain in February 2018 with specific attributes:

A total supply of 21,000,000 tokens.
5,750,000 pre-mine for ICO and liquidity.
Automatic difficulty adjustments based on PoW hashrate.
Rewards start at 50 BTCe tokens/block that decrease as more tokens are minted.
ERC-20 compatibility.
To acquire BTCe tokens, users can either mine them or purchase them from miners on decentralized exchanges. The mint function plays a crucial role in verifying the validity of hash solutions, updating the contract's internal state, and issuing new BTCe tokens.

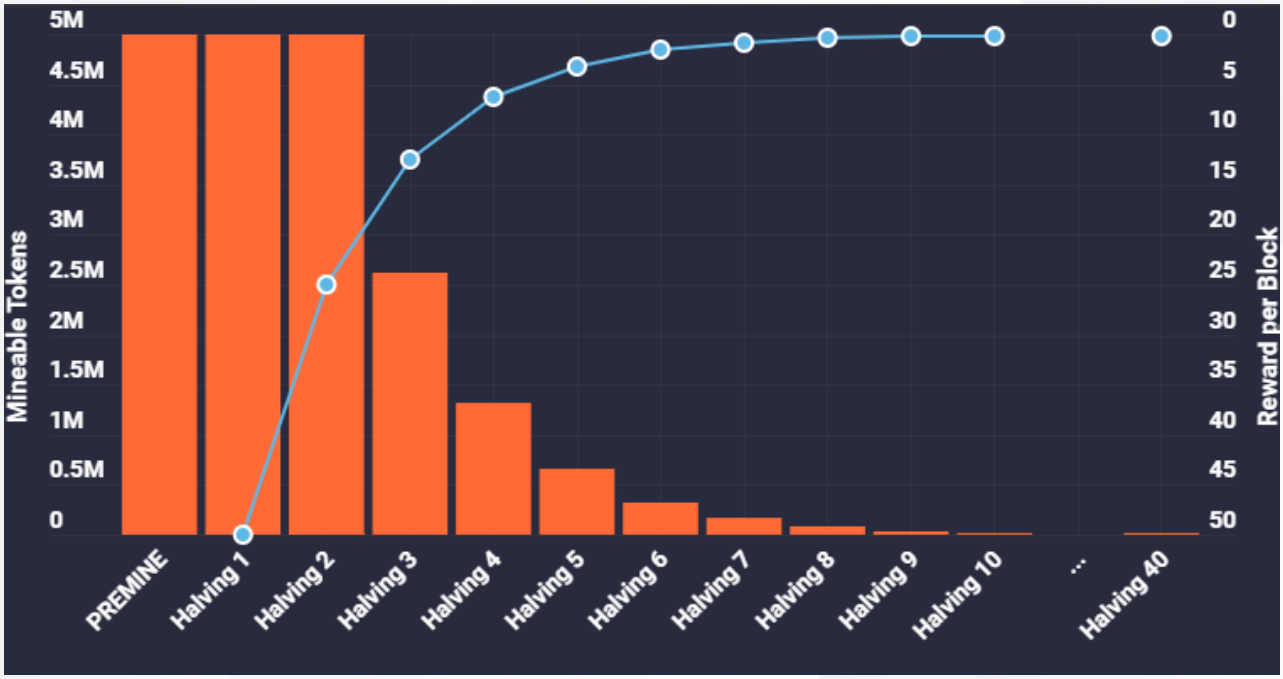
Difficulty Calculation and Adjustment:

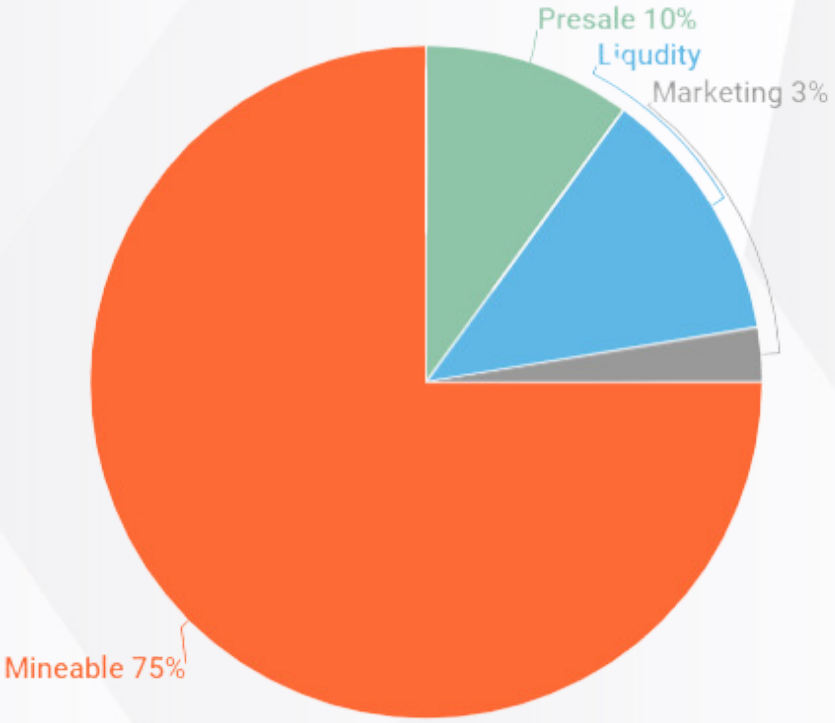
The smart contract periodically adjusts the mining difficulty after every 1024 mined blocks. Additionally, the reward era is incremented when the tokens minted count exceeds the maximum era supply, which is calculated using a halving algorithm. This algorithm reduces the block reward as more tokens are mined, ensuring that the total supply never exceeds 21 million tokens.

Calculating Mining Hashrate:

A formula is provided to estimate the time required to find a solution based on the current difficulty and hash rate, allowing miners to gauge their mining efficiency.

MINING BTCe





MINEABLE ERC20 TOKEN

www.btcerc20.com

SMART CONTRACT

Token: Provides the name of the token, which is "BTCe Token."

ERC-20 Interface: Ensures compatibility with Ethereum-based applications.
Name and Symbol: Offer information about the token's name and symbol for usability.

Total Supply: Indicates the total token supply.

BalanceOf: Enables querying the account balance of a specific address.

Mint: A critical function that verifies the validity of hash solutions, issues mining rewards to the sender, and maintains internal supply accounting.

Mint Event: Emits a "Mint" event upon successful verification and reward distribution, providing details about the reward address, amount, epoch count, and the latest challenge number.

Challenge Number and Mining Difficulty: Provide data related to the current Ethereum block's challenge number and the mining difficulty, which adjusts automatically during reward generation.

Mining Reward: Returns the current reward amount, which decreases as tokens are mined to ensure scarcity.

Mining Debug Operations: Optional methods for testing digests and sample solution verification using the same scheme as the mint method.

FAQ

1. Does BTCERC20 have its own Blockchain?
- No, BTCERC20 does not have its own blockchain. It operates as a smart contract on the Ethereum blockchain. This choice allows BTCERC20 to benefit from the speed, security, and modern features of the Ethereum ecosystem.

2. Why are there times when a lot of mints get reverted?
- Mints get reverted when there is a significant imbalance between the mining difficulty and the mining hashrate. If the mining difficulty is set too low compared to the hashrate, multiple miners may submit valid solutions in a short time frame. However, only one solution can be accepted per round, leading to the reverting of excess solutions.

3. How does pool mining work with BTCERC20?
- Pool mining with BTCERC20 is similar to traditional Bitcoin pool mining. Miners in a pool collectively work to find solutions, and when a solution is discovered, the pool submits it to the Ethereum network on behalf of its members. The pool manages gas fees for the Ethereum smart contract operations. However, it's important to note that BTCERC20 pools must cover these gas fees.

4. How often does difficulty update?
- The difficulty of BTCERC20 mining updates every 1024 blocks. This periodic adjustment ensures that the network maintains an appropriate level of challenge for miners.

FAQ

5. How does the difficulty update?
- The difficulty adjustment in BTCERC20 is dynamic. It can increase by up to 100% or decrease by 50%, with fractional changes in between. The goal is to make the mining process approximately 60 times slower than the Ethereum block rate, which translates to roughly 10 minutes per block.

6. Will there be a reward halvening event, and when will it occur?
- Yes, BTCERC20 follows a reward halving mechanism similar to Bitcoin. The first reward halving occurs at 10.5 million tokens mined. Subsequent halvings occur when half of the remaining supply has been mined, continuing for up to 40 iterations. This ensures that the total supply of BTCERC20s will never exceed 21 million.

7. Since BTCERC20 is Proof of Work, doesn't that mean it is bad for the environment?
- While Proof of Work (PoW) mining does consume energy, it serves a crucial role in providing decentralized and transparent transactional ledgers. The energy expenditure associated with PoW mining can be seen as a necessary cost for maintaining a secure and trustless financial system. Similar to how society pays for services like law enforcement and accounting, blockchain networks like BTCERC20 require energy and computation to operate and reduce financial corruption on a global scale. The environmental impact of PoW is a subject of debate, and efforts are being made to develop more energy-efficient consensus mechanisms.