Black Gold Coin (BGCO): A Peer-to-Peer Digital Asset

Abstract

Black Gold Coin (BGCO) is a decentralized digital currency inspired by the Bitcoin protocol, with modifications to block timing and reward structure to enhance scalability and value preservation. Like Bitcoin, BGCO employs a peer-to-peer network to timestamp transactions and uses a proof-of-work system to achieve consensus without a central authority. BGCO distinguishes itself by producing a block every 2 minutes and reducing the block reward by 10% annually, ensuring a stable supply rate and improved transaction throughput.

1. Introduction

Traditional online transactions depend on centralized financial institutions, which introduce fees, delays, and restrictions. Bitcoin presented a revolutionary model for decentralized, trustless transactions using cryptographic proof. Black Gold Coin seeks to build upon this foundation with a system optimized for faster transactions and controlled reward distribution, while maintaining robust security through proof-of-work. By introducing a 2-minute block time and an annual 10% decrease in mining rewards, BGCO aligns the network's growth with a sustainable asset distribution model.

2. Transactions

BGCO, like Bitcoin, represents each coin as a chain of digital signatures. Owners transfer BGCO by digitally signing a hash of the previous transaction and the public key of the next owner, thus creating a verifiable chain of ownership. To avoid double-spending, transactions are publicly broadcast, allowing all nodes to validate each block and ensuring that only the longest chain of proof-of-work is considered valid.

Each BGCO transaction consists of multiple inputs and outputs, allowing users to combine or split amounts as necessary. This design facilitates efficient transfers without the need for managing each unit of currency individually.

3. Timestamp Server

To maintain the chronological order of transactions without a centralized timestamp authority, BGCO employs a distributed timestamp server. Each block contains a timestamped hash, which is linked to the previous block, forming an immutable chain. The timestamp server verifies that transactions have occurred at a specific point in time, providing cryptographic proof of the chronological order in the blockchain.

4. Block Generation and Proof-of-Work

The BGCO system uses a proof-of-work algorithm that assigns a new block every two minutes. This is the time required to find a hash value that meets the required difficulty specifications, which automatically adjusts to maintain this constant rate.

Key Parameters of Black Gold Coin:

- **Block Time**: every 2 minutes.
- **Difficulty adjustment**: 1 hour.
- **Total supply**: 10.5 millions.
- **Initial coin reward**: 4 BGCO.
- **Reward Reduction**: 10% annually.
- **Consensus Algorithm**: proof-of-work
- **Algorithm**: SHA256D

Black Gold Coin uses a proof-of-work system based on SHA-256, like Bitcoin, requiring miners to solve complex computations to add blocks to the chain. For BGCO, this proof-of-work is adjusted to maintain a 2-minute average block time. Each node must find a hash value below a specific target, and this target difficulty is periodically adjusted to account for the collective processing power of the network. This protocol ensures that no single entity can control the network unless it possesses most of the computational power.

The proof-of-work also prevents Sybil attacks, where attackers might use multiple identities to subvert the system. Since proof-of-work relies on computational resources rather than identities, Black Gold Coin’s consensus mechanism is robust against such threats.

5. Network

The BGCO network operates as a decentralized peer-to-peer system with the following steps for transaction processing:

1. **Broadcast**: New transactions are broadcast to all nodes.

2. **Block Creation**: Each node collects pending transactions into a block.

3. **Proof-of-Work Computation**: Nodes compete to find the proof-of-work, which meets the required difficulty.

4. **Block Broadcasting**: When a valid proof-of-work is found, the block is broadcast to all nodes.

5. **Validation and Chain Extension**: Nodes validate the block, and, if it meets all criteria, it is appended to the chain. Nodes always prioritize the longest valid chain, following the “longest chain rule.”

This decentralized approach ensures network resilience. Nodes can join and leave the network at will, and as long as most of the the network’s computational power is controlled by honest nodes, the chain remains secure.

6. Incentive Structure

In BGCO, mining incentives align with the structure introduced in Bitcoin, where miners are rewarded with new coins for validating blocks and helping maintain the network. However, Black Gold Coin introduces an annual 10% reduction in mining rewards. This reduction rate balances initial issuance with long-term scarcity, progressively transitioning from block rewards to transaction fees as a source of miner revenue, ultimately preventing inflation and maintaining value over time.

By convention, the first transaction in each BGCO block is a “coinbase” transaction that assigns the block reward to the miner. This reward is the primary incentive for nodes to remain honest, as deviating from the network rules undermines the security of their own holdings.

7. Privacy

To maintain user privacy, BGCO transactions are publicly announced but anonymized. Public keys serve as pseudonyms, and new keys are used for each transaction to prevent linkage of transactions to specific users. While nodes track transactions in the network, they do not require personal information, preserving user anonymity.

8. Calculations and Security Against Attacks

Black Gold Coin inherits Bitcoin's security model against double-spending and malicious forks. The network's proof-of-work ensures that rewriting history to alter a transaction is computationally prohibitive. To accomplish this, an attacker would need to outpace the cumulative computational power of the network, which becomes exponentially harder as more blocks are confirmed.

Given that BGCO's block time is 2 minutes, the probability of an attacker successfully creating an alternate chain diminishes significantly with each confirmed block, following a Poisson distribution as demonstrated in the Bitcoin protocol. If the network remains secure under majority-honest conditions, malicious blocks are consistently rejected.

9. Conclusion

Black Gold Coin builds on Bitcoin's pioneering framework by introducing a faster block generation time and a sustainable reward reduction, offering a secure and efficient decentralized transaction network. BGCO's modifications address both scalability and value retention, making it a viable digital currency for a broader range of transactions. Its reliance on proof-of-work, combined with a self-adjusting difficulty mechanism, ensures long-term integrity and incentivizes miners to support the network honestly.