Cryptocurrency Proposal: Democratizing Mining

Based on Principles from Bitcoin and b-money

Abstract

The advent of Bitcoin introduced a revolutionary decentralized digital currency system. However, its mining process has become increasingly exclusive, dominated by large mining farms due to the escalating difficulty of solving cryptographic puzzles. This project proposes a new cryptocurrency aimed at democratizing the mining process by allowing miners to choose the number of coins they wish to mine based on their processing capacity. Unlike Bitcoin, which has a fixed difficulty level, our cryptocurrency employs a dynamic mining protocol that adapts to the individual miner's capabilities, ensuring effective participation from both small-scale miners and large mining operations. By facilitating a more inclusive mining process, this cryptocurrency promotes fair opportunities for all participants, reinforcing the foundational principles of decentralized finance and enhancing network security through diversified mining activities.

1 Introduction

The concept of decentralized digital currency was first introduced by Bitcoin, which relies on a consensus mechanism for secure transaction verification and currency creation. Despite its groundbreaking nature, Bitcoin's mining process has become predominantly controlled by large mining farms due to the high computational difficulty involved. To address this issue, we propose a new cryptocurrency inspired by the same principles outlined in Wei Dai's "b-money" protocol [1]. Our project adopts an alternative approach to money creation that allows miners to select the number of coins they wish to mine based on their processing capabilities.

In "b-money," one of the significant challenges lies in the money creation protocol, which requires account keepers to agree on the computational costs. Given the rapid and sometimes opaque advancements in computing technology, this method can lead to inaccuracies and protocol inefficiencies. To mitigate these issues, our cryptocurrency implements an alternative money creation subprotocol proposed by Wei Dai. This protocol involves four phases: planning, bidding, computation, and money creation.

2 Planning

In our cryptocurrency, the planning phase is a critical component that is managed by the central server. The server is responsible for computing and negotiating an optimal increase in the money supply for the next period. This process aims to balance the network's growth with economic stability, ensuring a sustainable and fair mining environment.

Initially, the planning mechanism will function similarly to Bitcoin's halving events [2]. However, instead of simply halving the reward, our protocol will double the mining difficulty every specified number of blocks. This approach aims to maintain a steady increase in difficulty, preventing the excessive centralization of mining power.

As an alternative, the difficulty could be dynamically adjusted based on the total number of coins generated in the last set of blocks. This method involves analyzing the mining output over a fixed period and recalibrating the difficulty to ensure a consistent and manageable rate of coin creation. However, this approach could potentially lead to issues similar to those experienced by Bitcoin, where rapid technological advancements in mining hardware can disrupt the balance.

To refine and optimize the planning process, community input will be actively sought and considered. By involving the community in these crucial decisions, we aim to create a more transparent and adaptable protocol that can evolve with the needs and capabilities of its users. Alternative methods and innovative solutions will be explored to address any emerging challenges, ensuring that the planning phase remains robust and effective.

By incorporating these strategies, our cryptocurrency aims to democratize the mining process, making it accessible to a broader range of participants. This inclusive approach not only aligns with the foundational principles of decentralized finance but also enhances network security through diversified mining activities.

3 Bidding

In the bidding phase, miners play a crucial role in determining the amount of cryptocurrency they wish to create. This phase is designed to be flexible and inclusive, allowing miners to participate based on their individual processing capabilities.

Anyone who wants to create the cryptocurrency broadcasts a bid in the form of $\langle x, y \rangle$, where x represents the amount of cryptocurrency they intend to create, and y is an unsolved problem from a predetermined problem class. Each problem in this class is associated with a nominal computational cost, typically measured in MIPS-years, which is publicly agreed upon to ensure transparency and fairness.

The process for miners begins with calibrating their hashrate, which is a measure of their computational power. Once they have an accurate assessment

of their hashrate, miners can evaluate the difficulty required to mine a single coin. Based on this difficulty and their processing power, they choose a target number of coins to mine, which constitutes their bid.

To prevent abuse and attempts to overwhelm the network, an additional difficulty adjustment mechanism is implemented. If a miner chooses to mine a very low number of coins, a small extra difficulty is added to their bid. This makes the practice of submitting numerous low-value bids less profitable and discourages attempts to flood the network with such bids. Instead of achieving network saturation, these attempts would result in the creation of orphan blocks—blocks that are not accepted by the main blockchain—within the attacker's own network segment, leading to no reward.

This mechanism ensures that the network remains robust and resilient to spam attacks, while still allowing fair participation for miners of varying capabilities. By incentivizing miners to submit realistic and achievable bids based on their actual processing power, the bidding phase promotes a balanced and efficient mining ecosystem.

Through this approach, our cryptocurrency seeks to democratize the mining process, providing opportunities for small-scale miners to participate meaningfully alongside larger operations. This inclusivity reinforces the foundational principles of decentralized finance and enhances the overall security and stability of the network.

4 Computation

The computation phase is where the actual mining takes place, following the bids submitted in the previous phase. Miners who placed bids now work to solve the computational problems specified in their bids, employing the classic Proof-of-Work (PoW) consensus mechanism.

In this phase, each miner attempts to solve a cryptographic puzzle, a process that requires significant computational power. The number of coins a miner aims to create (as specified in their bid) and the hash of the transaction are included in the block template. This template serves as the blueprint for the new block the miner is attempting to add to the blockchain.

To ensure the mining process is adaptable and stays relevant with advancements in technology, the specific algorithm used for PoW will be determined by the community through an open voting process. This democratic approach allows the community to choose the algorithm that best meets the needs and goals of the network. Once a consensus is reached, the chosen algorithm will be implemented.

By adhering to the PoW model and involving the community in crucial decisions, our cryptocurrency maintains the security and integrity of the network while promoting a fair and inclusive mining process. This phase is critical in ensuring that only legitimate transactions are added to the blockchain, securing the network against fraudulent activities and maintaining trust among participants.

5 Money Creation

In the final phase, money creation, the successful completion of a block's computational challenge results in the creation and distribution of new cryptocurrency units. When a miner finds a valid solution to the problem specified in their bid, they close the block and broadcast it to the network for validation.

Upon receiving the new block, each account keeper verifies the solution. If the block is accepted as valid, the miner is rewarded with the amount of cryptocurrency specified in their bid. This reward is credited directly to the miner's account. The new block is then added to the blockchain, and the network moves on to the next block.

This phase ensures that the network continuously grows and that new currency is fairly distributed based on the computational work contributed by the miners. By accepting the highest bids in terms of nominal cost per unit of cryptocurrency created, the system ensures that the most efficient and effective miners are rewarded, maintaining a healthy balance of participation and competition within the network.

This process not only incentivizes miners to participate actively but also reinforces the security and integrity of the blockchain by ensuring that each new block added has undergone significant computational effort.

By following these structured phases—planning, bidding, computation, and money creation—our cryptocurrency aims to create a more inclusive, fair, and secure digital currency ecosystem, encouraging broader participation and reinforcing the principles of decentralized finance.

6 Conclusion

This project introduces a new cryptocurrency inspired by the foundational principles of Bitcoin and the innovative concepts outlined in Wei Dai's "b-money" protocol. By addressing the limitations of Bitcoin's mining exclusivity, our cryptocurrency aims to democratize the mining process, enabling broader participation across various levels of computational power. The implementation of a dynamic and inclusive money creation protocol, comprising planning, bidding, computation, and money creation phases, ensures a balanced and efficient mining ecosystem.

In the planning phase, the central server determines the optimal increase in money supply, adjusting difficulty levels to maintain network stability. The bidding phase allows miners to select targets based on their capabilities, with safeguards against network abuse. The computation phase employs a community-chosen Proof-of-Work algorithm, securing the network through rigorous cryptographic challenges. Finally, the money creation phase rewards successful miners and integrates new blocks into the blockchain, promoting a fair distribution of new currency units.

By fostering community involvement and maintaining a flexible approach to technological advancements, our cryptocurrency aspires to create a more equi-

table and decentralized financial system, enhancing security and trust among all participants.

References

[1] W. Dai, "b-money," `http://www.weidai.com/bmoney.txt`, 1998.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," `https://bitcoin.org/bitcoin.pdf`, 2008.