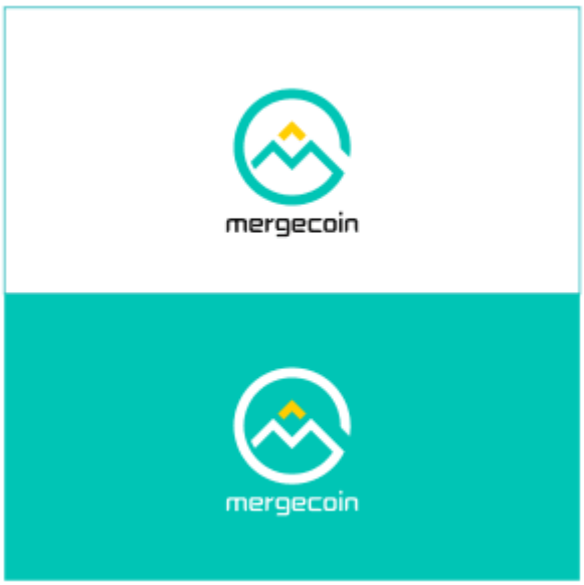
Mergecoin Technical Whitepaper

P2P cryto-currency with dash and blackcoin Hybird feature



MergeCoin

Abstract

Mergecoin is a blockchain based decentralized cryptocurrency that rewards network participation via static proof of stake. Mergecoin rewards "connectivity age" instead of “coin age,” thus eliminating abuse from exchanges and users that do not actively contribute to the network. By having a static reward system, the rewards for participation are proportional to the work every active node contributes. This discourages centralization and promotes network health. In addition to static rewards, Mergecoin implements a masternode network to incentivize large holders, and perform advanced functions such as near instant and private transactions.

This paper describes the basic coin specifications, features, and capabilities of the coin. The paper also describes coin distribution, funding purposes, future growth efforts.

Table of contents

What is Mergecoin

Mergecoin is a digital currency that enables instant payments to anyone, anywhere in the world. Mergecoin uses peer-to-peer technology over ClearNet to operate with no central authority (centralisation): managing transactions and issuing currency (MGC) are carried out collectively by the Mergecoin network. Mergecoin is the name of open source software which easy to use.

Specifications

Coin Suffix: MGC
PoW Algorithm: SHA256d
PoW Period: 1,000 Network Initiation Blocks
PoW Median Target Spacing: 64 Seconds
PoW Difficulty Retarget: 2 Blocks
Full Confirmation: 60 Blocks
PoS Target Spacing: 64 Seconds
PoS Difficulty Retarget: 2 Blocks
PoS Reward: Varied
PoS Min: 1 Day
PoS Max: Unlimited
Total Coins: 100,000,000 MGC
Block Size: 2 Mega-bytes (MB)
MainNet Parameters P2P Port = 17700 RPC Port = 17705
TestNet Parameters P2P Port = 27170 RPC Port = 27171

Masternodes

50,000 MGCs transaction with 15 block confirmations
Peer validated network uptime
Private transactions (0.01MGC fee to masternodes)
Active masternodes proportionally receive 50% of each block reward.
Masternodes validate all public transactions within about 4 seconds by communicating each transaction across all nodes on the network to prevent double spending (Duffield, Schinzel, and Gutierrez, 2014). When private transactions are initiated, masternodes also perform the work necessary to make the transactions hard to trace. The masternode network will be able to perform additional functions as new developments are commissioned and the bounties executed.

Masternode specifications

Coins required: 50,000 (minimum and maximum)
Reward: 50% of the block reward + all fees for transactions contained in the block
Peer validated network uptime

Private transactions

Masternodes facilitate private transactions through a decentralized mixing service that takes advantage of the perfect fungibility of the currency. Any unit of Mergecoin has the equivalent value to any other unit of identical size, regardless of the transaction history of any particular unit. Masternodes use this property to automatically break up private transactions into multiple identical and indistinguishable transactions, both adding complexity to the original transaction and obfuscating the provenance of any given unit.

In a block of transactions, three users submit funds in various set denominations. Users pay themselves back in the form of new outputs, which are randomly ordered.

Private Mergecoin transactions are initiated through a local wallet and received by the masternode subnetwork. Transactions are processed in groups of three. Inputs of common denominations are required – for example 0.1 MGC, 1 MGC, 10 MGC, or 100 MGC.

Upon application to the mixing pool, a receiving masternode propagates the transaction set throughout the network. If only one or two private transactions are pending, they are held in queue until three are in the mixing pool. Fees are extracted from the individual transactions, then charged collectively to further obfuscate the transaction history.

Private send is limited,thus requiring multiple sessions to thoroughly delink associated transaction history from significant amounts of money. Since each session is limited to three clients, an observer has a one in three chance of being able to follow a transaction.

Mixed transactions are chained together through multiple masternodes, making traceability exponentially more difficult with each additional chained transaction. Users have some control over the degree of mixing. More mixing takes more time, but more thoroughly obfuscates inputs. The fee for these transactions grows with each degree, as the process is more labor intensive for the masternodes (Duffield and Diaz, 2015).

This method of mixing is a trustless, integrated, on-chain, on-network service that is efficient, effective, and safe. It is initiated directly within a local wallet and completed without leaving the Mergecoin network. While some details of private transactions are obscured, the system nevertheless retains verifiable integrity of spent coins on the Mergecoin blockchain.

What is the incentive to run a masternode?

*Average daily reward (# of blocks per day * block reward * 50%) / (# of* **masternodes***)*

Masternodes receive fixed rewards (50% of the block reward) which are probabilistically distributed among peer validated masternodes. Masternodes recursively scan peer node performance, and only high performance nodes with sustained, stable, high-speed internet

connections are eligible for rewards. In addition to receiving 50% of the block reward, a masternode receives all fees for public transactions completed in a block and for all private transaction pools initiated in the block. These incentives promote continuous connectivity to maintain a high performance network.

Masternode network performance maintenance

In theory, malicious actors could also run Mergecoin masternodes, but not provide any of the quality service that is required of the rest of the network. To reduce this possibility and discourage people from using the system to their advantage, all nodes must regularly ping the rest of the Mergecoin masternode network to ensure they remain active. This work is done through a selection of 2 quorums per block. At every new block hash, Quorum A checks the service of Quorum B. Quorum A are the closest nodes to the current hash, while Quorum B are the furthest nodes from said hash.
Masternode A (1) checks Masternode B (rank 2300)
Masternode A (2) checks Masternode B (rank 2299)
Masternode A (3) checks Masternode B (rank 2298)
The masternode network is self-monitoring. Approximately 1% of the network will be checked for each block added to the blockchain. This results in the entire masternode network being checked approximately six times per day. To maintain this trustless system, nodes are selected randomly via the quorum system; the network also requires a minimum of six violations in order to deactivate a node (Duffield and Diaz, 2015).

Proof of work vs Static proof of stake

Bitcoin achieved the first distributed blockchain-based transaction ledger and an immutable digital currency. To achieve this, Bitcoin rewarded the distribution of computing equipment to maintain a decentralized blockchain and secure network. There was a short period of time when this worked well, but now Bitcoin rewards the accumulation of computing power, and only a few consolidated pools maintain the network.

The rapid growth of the Bitcoin network is also a disastrous burden on ecology. The exponential expansion of computing power has lead to a similar rise in difficulty, and power hungry mining consume a vast amount of electricity.

This concentration of power threatens the distributed model of checks and balances, and even governance over core development is at odds with how to solve the growing problems. A single transaction confirmation can take in excess of 12 minutes (blockchain.info, 2016) and the technology is vulnerable to attacks increase the delays.

Thus, we rejected mining and proof of work as the basis for security and adopted proof of stake instead.

Critics of proof of work developed proof of stake (PoS) as an alternative protocol. PoS systems depend upon a low-energy, distributed computing network to achieve the same ends of a secure, distributed blockchain. They rely on accumulation of coin instead of computing power as the basis for rewards for securing the network.

Early models of proof of stake were designed around "coin age," the length of time that the coin was held in a wallet, and “coin weight,” the total amount of coin in the wallet. These have proven to be necessary but insufficient conditions for rewards because they do not reward active facilitation of network transactions. In theory, and in practice, holders of cryptocurrencies based on the first versions of PoS could deposit large volumes of coin into a wallet, take it offline, accrue coin age for an extended period of time, then bringing the wallet online momentarily to obtain an instantaneous reward.

This first version of PoS rewards users for holding onto coins without actively contributing to the integrity of the network. In this model, exchanges and other large holders of coin maintain offline wallets, and only periodically connect them to the network to generate and sell the stake. This directly increases the coin supply while driving down the market value of the coin.

In contrast, Mergecoin uses a "static" proof of stake system, version 3 (PoS 3, or SPoS), which aligns incentives with user behaviors to actively contribute to a robust, fast, and secure network. The reward is “static” because it is always the same (50% of the block reward). Coin weight still matters, but “connectivity age,” – the duration a wallet maintains active network communication – replaces coin age as the primary probability parameter for staking. Rewards are thus contingent upon active work and the amount of Mergecoin held in wallets to maintain and secure the network.
In addition, Mergecoin implements masternodes (Duffield, 2015) to reward large holders of coin, contribute to network robustness, and perform advanced functions such as near instant and private transactions.

Block reward schedule

A total of 100,000,000 MGCs will be used for the initial coin supply. These coins are generated in the genesis block and will be held in trust by the Mergeoin team.

Year	MGCs/Block	MGCs/Year	Total
1	30	17058660	117058660
2	20	10512000	127570660
3	10	5256000	132826660
Longer…	5	2628000	135454660+…

Distribution of coin

Many alternative cryptocurrencies start with a proof of work phase. Developers reason that miners become engaged with the coin economy and earn the coin through the work of mining. The lesson the Mergeoin team has taken from the history of cryptocurrency, however, is that the PoW phase encourages "mining and dumping" which drives down the value of the asset from the start. This supposedly “engaged” user base simply uses mining as a vehicle for quick profit then leaves without contributing ongoing value to the coin or community that uses it.

Staking wallets

QT wallets have been developed for general users. Daemon wallets have been developed for advanced users. Wallets will be maintained for all major desktop platforms: Windows, Mac, and Linux. QT and daemon wallets give Mergecoin holders complete control of the security of their MGC, with controls to send and receive transactions.
Coins required: No minimum. (Wallets must contain a non-zero sum of MGCs to receive stake rewards.)
Wallet stake reward = 80% block reward for each discovered block.
Staking is probabilistic, and probability is distributed according the amount of MGC in the wallet address (coin weight) and the duration MGC is held in the continuously connected wallet (connectivity age). Valid network connectivity requires that the wallet be connected to the internet with a sufficiently high-speed, stable connection to support the blockchain.

Previous versions of Proof of Stake require what is known as checkpointing. Checkpointing is a centrally broadcasted full node that is signed by the developer and is designed to help verify coin stake before it is accepted into the block tree. In MGC, every node is a full node, and because of this no checkpoint system is needed. By removing this partial centralized dependency that existed in previous PoS versions, all nodes are fully authorized and makes a network attack far more difficult.

Blockexplorer

Blockexplorer for Mergecoin is use the insight-api which open source based on nodejs:
http://www.mergechain.com/

Conclusions

Mergecoin integrates static proof of stake (PoS v.3) system with an incentivized masternode/wallet matrix. The result is fast transaction confirmation, reliable network security, enhanced privacy through decentralized coin mixing, and reduced price volatility. This technological foundation establishes possibilities for smart contracts, colored coins, side chains and advanced security mechanisms.

This combination of Mergecoin's powerful coin technology with team creative corporate plan brings about compelling opportunities. Entrepreneurs and developers can leverage a social network of engaged customers and investors in a way that never before has been attempted in this industry.

References

Blockchain.info. (2012). *Bitcoin Median Transaction Confirmation Time (With Fee Only)*. Retrieved from https://blockchain.info/fr/charts/avg-confirmation-time

Duffield, E. (2015). *Dash: Video Series - #4 - Incentivized Infrastructure and Masternodes. *DVS15E04. Retrieved March 28, 2016, from https://www.youtube.com/watch?v=FY1mciGGhO4.

Duffield, E. and Diaz, D. (2015). *Dash: A Privacy-Centric Crypto-Currency*. Retrieved from: https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf.

Duffield, E., Schinzel, H., and Gutierrez, F. (2014). *Transaction locking and masternode consensus: A mechanism for mitigating double spending attacks*. Version 2. Retrieved from https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf

Gautham. (2016). *Blockchain Monday Blues Due to Spam Transactions on Bitcoin Network*. NEWSBTC. Retrieved from: http://www.newsbtc.com/2016/03/02/bitcoin-network-spam-attack/