GHOST

by McAfee

Published: May 15th, 2020

The GHOST Dev Team

Whitepaper Doc Version 1.0.2

Stay tuned for updates as development continues.

https://www.ghostbymcafee.com/

@GhostbyMcAfee

GHOST by McAfee core ideology is that your privacy is non-negotiable and is a fundamental basic human right. The operating principles utilized within our infrastructure demonstrates the capabilities to keep transactions completely anonymous and private online, hence the name “GHOST”. Behind the name is powerful technology from independent projects that has been improved upon, highly customized, and fused together by an experienced software engineering team to form a superior privacy coin “GHOST”.

The network operates on a proof-of-stake concept where any person can mine and validate block transactions. This enables each and every GHOST token holder a certain level of control to create a balanced, sustainable, and decentralized network.

This document will serve as a comprehensive resource to outline the underlying privacy technology and operating principles behind GHOST and the vision we have for the future.

Table of Contents

1 Introduction

Bitcoin is considered the preeminent cryptocurrency in the world yet the privacy of all the transactions on the network are easily traced. This is by design to prevent double-spends, the blockchain is fully public and visible to anyone. The danger of the lack of privacy became evident quickly after its 2009 release. By 2012 the cryptocurrency community began creating anonymity solutions, such as tumblers and mixers. These solutions would essentially group multiple transactions together in a way that made it difficult to associate senders with recipients. However as the digital age of online currency has progressed and independent developers have continued to revolutionize and prioritize the privacy of users and their transactions with the creation of entirely new networks with a focus on privacy. Many of these coins have incredible features that have been developed. These projects can be compared and weighed with pros and cons because they are inherently different, each with a particular vision and approach to a common goal.

Privacy is a necessity for a healthy and successful economy to thrive. Legitimate use cases for privacy are numerous: the need for businesses to protect pricing, to protect payroll information, and for consumers to freely purchase goods and services without exposing their personal information - just to name a few.

1.1 GHOST

We’ve shown that it is possible to combine aspects of new privacy innovation in the blockchain space into a unified solution. GHOST solidifies these impressive advancements that have been operating independently into a highly customized and robust network that will provide users with superior, sustainable, secure, and trusted framework for a privacy coin. With this approach we can take a giant leap forward towards building a new kind of digital infrastructure. Ongoing privacy and security protocols are currently being developed for future release.

GHOST transactions use a state of the art escrow pool to shield and erase the history of transactions.

GHOST transactions will be verified using zero-knowledge proofs.

GHOST is a decentralized proof-of-stake network controlled by GHOST coin holders. GHOST has no central company or owner. It is run and maintained by the community.

GHOST transactions are processed on chain in under 60 seconds with just a fraction of a penny paid in transaction fees.

GHOST users earn a share of the transaction fees using the staking and masternode features.

1.2 Vision and Principles

We believe every transaction and every user should have full privacy and anonymity on the GHOST network. Privacy is a right, not a privilege.

We believe that people have an inherent right to control their property, assets, and finances.

We believe that a global, private, instant, and low-cost cryptocurrency network such as GHOST will create immense economic opportunities and stimulate commerce across the world.

2 Foundation

GHOST is a cryptocurrency with a mission to provide users entirely private, secure, affordable and reliable means to transact over the network. At the foundation of the project are features pioneered by leading cryptocurrency projects such as: Bitcoin's distributed ledger consensus technology, Dash's speed and governance accessions ("InstantSend") and Masternode functionality, and ZcashSapling zk-SNARKs for additional anonymity, as well as staking. In addition to all of this is a highly sustainable "Proof of Stake consensus algorithm", the ability to stake both GHOST and zGHOST, and a dynamically calibrated coin-supply restrained by the burning of transaction fees. Thus leading to a network that is significantly better for the environment in comparison to a "Proof of Work" network. All of these extremely powerful software advancements in the industry are brought together to form a highly customized and secure platform, "GHOST".

2.1 Coin Specs

Block size: 2 MB
Block Time: 60 Seconds (Re-targeting every block)

Coin Emission Rate: Max. 6 GHOST per block (Always less due to burnt fees & unused treasury). 3 GHOST are allocated as staking/masternode rewards, 2 GHOST are split between stakers, 1 into a pool for future development.
Coin Supply Control: ALL transaction & zGHOST minting fees are burnt from coin supply.

Maximum Coin Supply

At May 25, 2020: 13,573,415 GHOST

By June 2022: 15,087,292 GHOST

By June 2040: 30,226,069 GHOST

* Calculated and will potentially be lower due to burning fees and other factors.

PoS Stake Eligibility

Minimum Input Age: 60 blocks

Reward Maturity Confirms: 101 confirms

Wallet Status: Requires wallet to be kept running & online.

Transaction Send Eligibility

Minimum Confirm: 6 confirms

SwiftX Eligibility

1 confirm for locking and 6 confirm to spend.

Collateral held for 15 blocks.

Privacy Technology: Custom zk-SNARKs ZcashSapling

Key Features: Custom accumulator check-pointing system

Accumulator Modulus: RSA-2048

zGHOST Denominators: 1, 5, 10, 50, 100, 500, 1000, 5000

Mint time: >= 0.5 seconds

Spend time: >= 2.5 seconds

Maximum single Spend limit: 35,000 GHOST

Maximum single Spend denomination count limit: 7

Fees (mint): 0.01 GHOST per minted zGHOST denomination.

Fees (spend): No fee to spend zGHOST back to GHOST.

Minimum GHOST confirmation count required to mint zGHOST: 6 confirmations

Minimum zGHOST confirmation count required before spend: 20 confirmations

Maturity requirement before zGHOST can be spent: 1 new identical denomination mint added to accumulator

Initial Masternode Coins: (now burnt & no longer exists in coin supply) [block# 000001] 120,000 GHOST for creation of 6 Masternodes for the functioning of the network.

2.2 Economics

GHOST operates on a similar philosophy of an elastic currency, where the supply is adjusted in response to economic pressure (“business volume”). This is achieved by surveying the circulating volume against the credit volume. In a working model of an elastic economy money is taken out or put into circulation. These actions occur as response to a shifting market with an ultimate outcome to nudge the economy in the desired direction.

The primary goal is to maintain the health of a dynamic coin supply. Thus GHOST burns it’s transaction fees in order to encourage liquidity whilst rewarding users for participating in the network. Block payouts will continue to be disbursed to those securing the blockchain. This will ensure transaction fees do not increase and supports liquidity, which is crucial for GHOST to operate as a currency.

At the base level there will not be a hard cap, or a defined limit of coins that will be produced. However there will be a soft cap, defined as a restriction on the number of coins produced, when a specific condition is met. This soft cap condition is met when fees charged on network actions amount to that minted within a block. Given this condition the GHOST blockchain will start burning the same amount of coins as it is generating, limiting growth and preserving the currency.

GHOST does not contract upon a single executive decision, nor does it react to calibrate circulating volume to credit volume. The only influencing factors are those based upon transaction volume and fee burning as interpreted by an algorithm. At a high rate of transactions per second, the coin supply burning will equal the same amount as it is generating, creating a neutralising effect on the coin supply.

* The Economics for GHOST will continue to be improved on to successfully compete and operate in the market. Stay updated on ghostbymcafee.com

2.3 Coin Supply

Total Supply: 55,000,000

* reference 2.2 Economics for soft cap explanation

Initial Supply: 13,573,415

* reference 2.3.1 ESH Token Holders

The remaining supply of **GHOST** coins will be allocated towards masternodes, proof of stake rewards, and future development over time. See 4.5 Reward Breakdown for specifics.

2.3.1 ESH Token Holders

25% (13,573,415 GHOST) of the GHOST supply will be distributed to ESH token holders upon launch on May 25th. The exact amount that will be awarded to each token holder will be a percentage of their ESH holdings against the total ESH supply (since the initial supply is equal to the total supply of ESH this will essentially be a 1:1 ratio).

A global "snapshot", a total count of all the wallets holding ESH will be taken before GHOST launch. It is highly recommended, a requirement to an extent, that your ESH tokens are held, and stored in a wallet fully under your control. If your ESH tokens are in an exchange it's highly likely that you will not receive GHOST.

If on May 25th your ESH tokens are held in an exchange wallet it is almost a guarantee you will lose your **GHOST**. Below are a few examples of recommended wallets:

Trust Wallet

MyEtherWallet

MetaMask

Atomic Wallet

MyCrypto

Parity

Mist

Eidoo

Enjin Wallet

imToken Wallet

Exodus

Jaxx

KeepKey

… etc

IMPORTANT

To receive GHOST on May 25th make sure you have ESH tokens in an Ethereum ERC-20 supported wallet under your control, where you have either the private key or backup phrase secured, and you’re good.

3 GHOST Technology

At the very core of blockchain ledger technology is Bitcoin, a true pioneer in the cryptocurrency space. The basis for operations was a peer-to-peer currency exchange without the need for any intermediary over the internet. This system was to run on the network of nodes that can verify transactions happening over the course of time. These nodes were not composed of a single authority but rather a pool of computers, thus creating a decentralized network. These nodes essentially are the processing power behind Bitcoin and maintain the integrity of the ledger. Transactions are recorded into data chunks, or a “block”. The ledger, a collection of these blocks, counts on the processing power of the mining computers to solve a cryptographic puzzle by identifying an arbitrary number (nonce) to hash with. This reliance on mining is known as a Proof of Work (PoW) system. As the network grows, these cryptographic puzzles increase in difficulty, becoming harder to solve and drawing more processing power.

These fundamental properties of Bitcoin have been carried over into the foundation of GHOST. However similar, the operations behind **GHOST** are vastly improved.

Unlike Bitcoin, **GHOST** does not rely on a Proof of Work (*PoW*) system. One of the largest issues with a Proof of Work system is that they are mostly compromised, and highly incentivised, as mining pools. These pools are groups of computers working together to solve the cryptographic block hashes and divide the reward among all the users in the pool. In this way they are able to circumvent the need for increasing processing requirements to remain competitive. As this sounds like a great solution it leads to the supreme processing power of the pools to push out individual miners that are unable to compete. Unfortunately this method fundamentally will slow the network down over time, especially as it grows. Additionally it consumes a great deal of energy and negatively impacts the environment.

Read more about Proof of Stake in 3.5 Proof of Stake Consensus Algorithm below.

3.1 Masternodes

Within GHOST are the roots of an altcoin Dash and the **Masternode concept** behind it. Behind this is the ability to instantly send transactions, giving speed to the network powered by masternodes. These masternodes are crucial for the operation of the network. They are by necessity nodes in the network that provide maximum uptime and service. For example, on the Dash network running a masternode requires the node stakes at least 1000 Dash and is ultimately rewarded with dividends from block rewards. Additionally, Dash uses a two-tiered approach, where miners contribute to the overall processing of transactions on the network as well. The tasks are split where miners create new blocks while masternodes process other internal services.

3.2 PrivateSend

PrivateSend is a trustless method of running a sequence of transactions (*known as "mixing"*) such that an external observer is unable to determine the source of funding when a PrivateSend transaction is created. This gives your transaction enhanced privacy. The mixing and denomination process is seamless, automatic, and requires no intervention on the part of the user. The exact method behind PrivateSend includes obscuring transactions by dividing funds to protect their source. In the case of a simple transaction from Bob to Alice the funds will be divided into mixed transactions, making it extremely difficult to track any one mixed transaction. This mixing process is allocated to the masternodes, rather than a single node on the network, removing a potential vulnerability and further increasing the privacy for a single transaction.

GHOST utilizes this methodology and further improves upon the privacy aspect while incorporating zk-SNARKs privacy protocol and additional measures.

3.3 InstantSend

As with Dash's near instantaneous transactions **GHOST** has improved upon this technology to offer a more secure and private transaction to take place on masternodes in a single second. The transaction time can compete with the speed of a credit or bank card transaction.

This process happens on a quorum between masternodes. When a transaction is initiated, the inputs of this transaction are secured by a random delegate masternode, making these funds spendable only through a specific transaction. Ultimately any conflicting blocks or incoming transactions would therefore be rejected. Once the delgrate masternode completes the hash of the locked transaction it's then broadcasted via ZeroMQ (*a high-performance asynchronous messaging library*) over the Masternode network. The result is a near instantaneous consensus, eliminating the need to await confirmations, and preventing double-spend exploits.

- *A basic demonstration of an InstantSend transaction.*

Key: Black: standard node. Fuchsia: masternode
Fuchsia with D: delegate masternode. !: InstantSend transaction.

1. A standard node makes an InstantSend transaction.
2. The InstantSend transaction is broadcast to the Masternode network.
3. A random masternode becomes InstantSend delegate and locks the transaction.
4. The delegate masternode broadcasts the locked transaction to the network, wherein all non-abiding block discrepancies will be denied.

3.4 Sapling, zk-SNARKs

The future of GHOST is with Sapling, a zk-SNARKs based privacy protocol, originally developed by Zcash. This will greatly improve privacy of the entire network and secure transactions. Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKS) is a non-interactive zero-knowledge proof (ZKP) that can be verified without any interaction with the prover.

The primary reason this protocol was selected is due to the vast amount of research and development behind the protocol. In addition to that is the fast verification time and increased level of anonymity.

3.5 Proof of Stake Consensus Algorithm

The GHOST network operates on a Proof of Stake consensus algorithm. This technology was first introduced via a paper by Sunny King and Scott Nadal in 2012. The innovative concept was based around the notion of “coin age”, essentially how long an Unspent Transaction Output has not been spent on the blockchain. Given this focal point it differs greatly from a Proof of Work system. Instead of simply rewarding miners anyone willing to participate in the network is rewarded. This protocol has been greatly improved and refined since then, with security fixes such as double spend exploits, or honest nodes abusing the system. The most recent addition to this protocol was contributed by ZcashSapling, zk-SNARKs privacy protocol.

To further go into detail about the notion of “staking”, it’s really just a matter of making computing resources available to the network. Depending on the delimited competition this staked computing power may or may not be selected to generate the latest block on the blockchain. In the case of GHOST, these limits are considered by the balance (*UTXOs*) staked by the wallet. Every staking node is competing to create a valid block. Nodes, however, are technically limited in the number of trials in a given time (eliminating the need for higher computing power) and the difficulty to get a valid block is inversely proportional to the amount being staked. A higher balance means a higher chance of satisfying the difficulty criteria, validating the block, and being rewarded.

Compared to PoW mining, such as with Bitcoin, staking is significantly less demanding on resources. The need to push towards ever increasing difficulty and computing power to solve more and more advanced cryptographic problems is not required. This being the case a PoS, Proof of Stake, network is an environmentally friendly alternative to existing Proof of Work used by many.

By reducing the power needed to operate nodes the true vision to have an entirely decentralized network is held together. Currently mining pools can easily outperform any independent miners. Even with an expensive setup with the highest quality hardware it is very difficult to compete. This is not a fair market, instead it will continue to be a controlled monopoly where only the most exclusive network of miners reep the rewards.

3.6 zGHOST

zGHOST is a more private version of GHOST. To be phased out and combined into simply GHOST in future releases, while taking on all the privacy improvements of zGHOST. For all simplicity zGHOST is NOT a unique currency from GHOST and has the exact same currency value as GHOST. It is simply a form GHOST coin can take on, one being more transparent than the other.

Developments and specifications to come.

4 Masternode Network Cont.

The outlined GHOST protocol operates as a two-tier network. First it comprises the staking tier, which is available for all users to participate in through staking their GHOST coins. Followed by the more exclusive masternode tier.

The final masternode tier mentioned above are a set of incentivised nodes within the GHOST network that are responsible for processing specific operations. This two-tier approach has been carried over from Dash, with significant restructuring to fit GHOST’s Proof of Stake consensus algorithm.

4.1 Proposal Voting

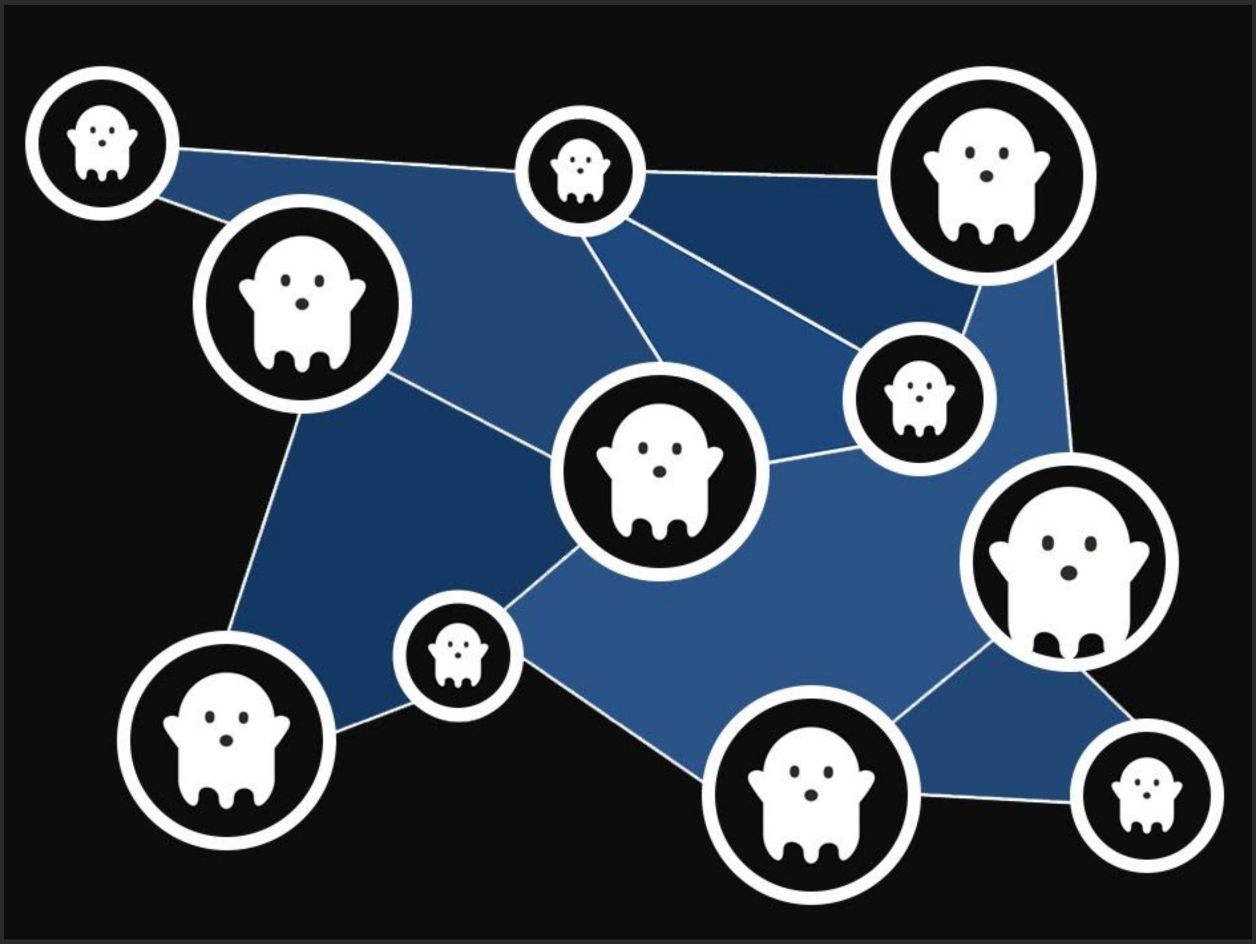
To ensure a decentralized but collaborative system the Masternode network is able to vote on proposals and collectively determine the future of the GHOST project. Each Masternode is able to vote once on any given proposal. The majority votes decision will determine whether the proposal is passed or rejected.

For example, this could allow the GHOST coin to hire a core developer, and pay them directly from the development pool, once the approval of the work from the Masternode network goes through.

The specific means to vote for a proposal will be available using commands inside the GHOST wallet or even using third party tools outside of it. This vote is then broadcasted to the network, validated, recorded and stored as a blockchain object.

4.2 Masternode Acquisition

For those that are interested in operating a masternode on the GHOST network here is all the information you need to know.



20,000 GHOST must be stored on the masternode's wallet. The 20,000 GHOST coins must remain in the wallet operating the masternode at all times. Sending these coins to another wallet will remove the status of a masternode for your wallet, in which case you will not be eligible for masternode rewards from that point on (until 20,000 GHOST coins are resupplied).

The reason behind the requirement for the 20,000 GHOST coins ensures that a high enough percentage of nodes remain staking. In addition, this allows the masternode to reliably provide a masternode service for the network over a long duration of time, rather than quickly leaving and rejoining. However the most important reason is the **20,000 GHOST** requirement strongly inhibits a single entity to host enough masternodes to achieve a 51% stake.

A static, unique IP (remains constant) is also required to operate a masternode. To reliably broadcast information between nodes the IP address of a single masternode must remain constant throughout. In addition to a static IP a reliable internet connection is also required to remain online dependably to process information.

Hosting more than one masternode per IP is not possible. If you wish to host multiple masternodes you must have unique, static IP addresses for each masternode. If this is not possible it is suggested that you instead stake your GHOST, which comes with rewards as well.
See below 4.6 Masternode Staking.

Quickly Explained a Masternode operator:

– Requires 20,000 GHOST be left unusable by the holder to remain functioning as a masternode.

– It must be left connected at all times.

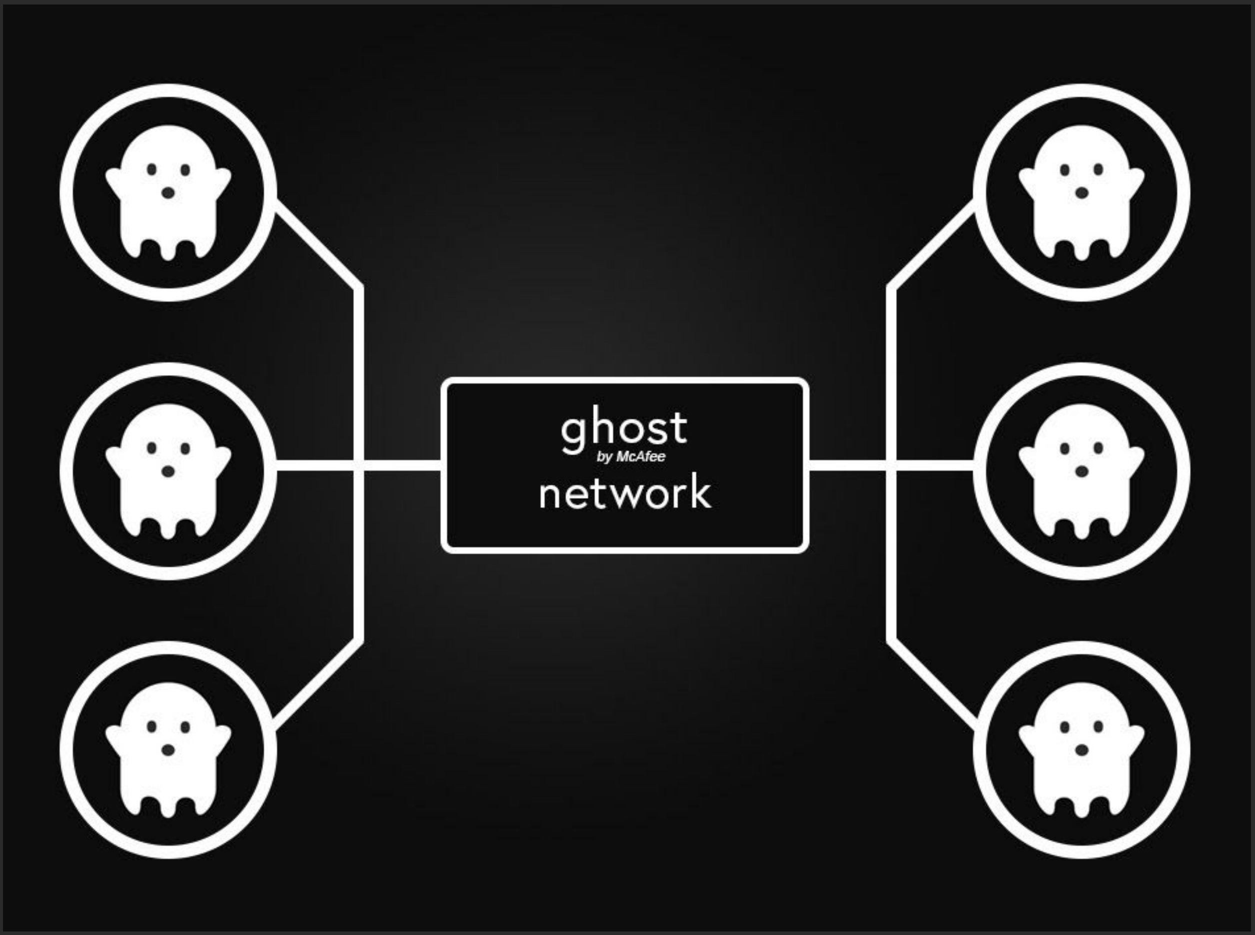
– It requires a separate, stable IP address to the user’s wallet intended for use.

- The masternode service can be ran on a Linux machine.

- Tech savvy operators that are familiar with basic security measures.

4.3 Masternode Staking

GHOST is a two-tiered network, relying on both participants of staking and Masternode tiers to maintain the health of the network. While both of these means of accruing rewards over time the exact amount, stability, and means differ.



The difference in rewards from masternodes and staking wallet is overall not that different. That being said, masternode will pay out reliably, where as staking involves more variance.

A user staking can assume the following:

– The ability to opt in and out of staking as the user pleases.

– Can be done regardless of GHOST amount.

– The option to divide up holdings between addresses.

– No requirements on specific amounts (masternode 20,000 requirement).

4.4 Zero Knowledge Proofs

Unlike many other Proof of Stake currencies GHOST allows users to remain anonymous while doing so.

To provide complete privacy and allow stakers to remain anonymous GHOST incorporates the zk-SNARKs privacy protocol. In this process it uses zero knowledge proofs while establishing pools for zGHOST in accumulators which are drawn from to pay out transactions with zGHOST coins (which carry no data pertinent to their past history). zGHOST can consequently be minted from GHOST at will for a fee, in turn destroying the GHOST converted to zGHOST.

GHOST protocol Technical Specs (v1.0)

Key Features: Custom accumulator checkpointing system
Accumulator Modulus: RSA-2048
zGHOST Denominators: 1, 5, 10, 50, 100, 500, 1000, 5000

Mint time: >= 0.5 seconds
Spend time: >= 2.5 seconds

Maximum single Spend limit: 35,000 GHOST
Maximum single Spend denomination count limit: 7

Block size: 2 MB
Fees (mint): 0.01 GHOST per minted zGHOST denomination.
Fees (spend): No fee to spend zGHOST back to GHOST.

Minimum GHOST confirmation count required to mint zGHOST: 6
Minimum zGHOST confirmation count required before spend: 20

Maturity requirement before zGHOST can be spent: 1 new identical denomination mint added to the accumulator after yours is added.

Confirms before zGHOST can be staked again: 200.

4.5 Reward Breakdown

Year	Reward	Masternodes & Stakers	Future Dev
2020	6 GHOST	5 GHOST	1 GHOST
2021	6 GHOST	5 GHOST	1 GHOST
2022	5.7 GHOST	4.75 GHOST	0.95 GHOST
2023	5.415 GHOST	4.5125 GHOST	0.9025 GHOST
2024	5.14425 GHOST	4.286875 GHOST	0.857375 GHOST
2025	4.88703 GHOST	4.072531 GHOST	0.814506 GHOST
2026	4.64267 GHOST	3.868904 GHOST	0.77378 GHOST
2027	4.41053 GHOST	3.67545 GHOST	0.735091 GHOST
2028	4.19 GHOST	3.49167 GHOST	0.698336 GHOST
2029	3.9805 GHOST	3.31708 GHOST	0.66341 GHOST
2030	3.781475 GHOST	3.151226 GHOST	0.63023 GHOST

... continued

GHOST

by McAfee

Whitepaper Doc Version 1.0.2

Stay tuned for updates as development continues.

https://www.ghostbymcafee.com/

@GhostbyMcAfee