MalwareChain
Cyber Security Lab

WHITEPAPER

MalwareChain
(MALW coin)

A distributed anti-malware solution featuring a mixed Proof-of-Stake/Masternode architecture, a governance token, and a wrapped ERC20 token

White Paper
V.2.0
September 2020

Contents

Abstract

MalwareChain offers a novel approach to malware detection and removal. It's a distributed antivirus system, in which any user can run a special client to scan files and links uploaded by others – and earn a share of the fees in return. The platform implements a network of masternodes to ensure the integrity of the threat database. The next step is introducing a strong DeFi element, with a decentralized governance system, liquidity pools, and a wrapped token on the Ethereum blockchain.

Annual global losses from malware and viruses are close to half a trillion dollars. The antivirus market makes over $20 billion a year in revenue, with such popular programs as Norton and McAfee taking the lead. While they are good at repelling well-known threats, but extremely inefficient when dealing with unknown threats. Besides, all antiviruses use the same method to scan the same areas of the web and devices, and their databases largely overlap. This leads to a constant waste of resources.

On MalwareChain, resources are pooled and used in the most efficient way thanks to a system of several types of nodes. Scan nodes perform anti-malware checks; PoS mining nodes confirm transactions and add new blocks to the chain; Discovery nodes crawl the web and update the threat library; and masternodes ensure the overarching stability of the system.

The key feature of the platform are investments in masternode shares. Masternodes (MNs) are the most profitable type of nodes, but setting up and running a node on one's own is costly and complex. Instead, users can buy shares in a masternode, pooling their resources. . MalwareChain already has a fully functional web-based antivirus client and a network of masternodes, with 98% of all block rewards allocated to MN shareholders.

In the near future, MalwareChain will introduce an Ethereum-based governance token, MalwareChain DAO (MDAO), and a wrapped asset that will represent the MALW token on the Ethereum blockchain, wMALW. Users will be able to get MDAO as a reward for contributing liquidity to trading pools, as well as for wrapping MALW into ERC20 tokens wMALW. In addition, masternode owners will receive additional rewards in MDAO for keeping their MNs online.

The White Paper provides a detailed overview of the architecture, tokenomics, features, rewards, and project timeline. With its complex yet elegant architecture and vast monetization possibilities, MalwareChain will provide a worthy alternative to traditional antivirus programs.

1. The antivirus software industry: overview and issues

1.1. Anti-malware market: size and trends

Computer viruses and malware cost the global economy more than $450 billion every year. WannaCry virus alone caused over $4 billion in damages in 2017. Therefore, it's not surprising that antivirus software is a very large business: the total annual revenue of companies that make anti-malware exceeds $23 billion. The most popular products for Windows are Norton by Avast (17%), Malwarebytes, McAfee, and ESET.

Market Share of Major Antivirus Programs for Windows

Company	Market share
AVAST Software a.s.	17.04%
Malwarebytes Corporation	13.34%
McAfee Inc	11.73%
ESET	11.52%
Bitdefender	8.52%
Webroot Inc	6.99%
Kaspersky Lab	6.25%
Safer–Networking Ltd	5.96%
Avira GmbH	5.1%
Sophos Limited	3.83%
Others	
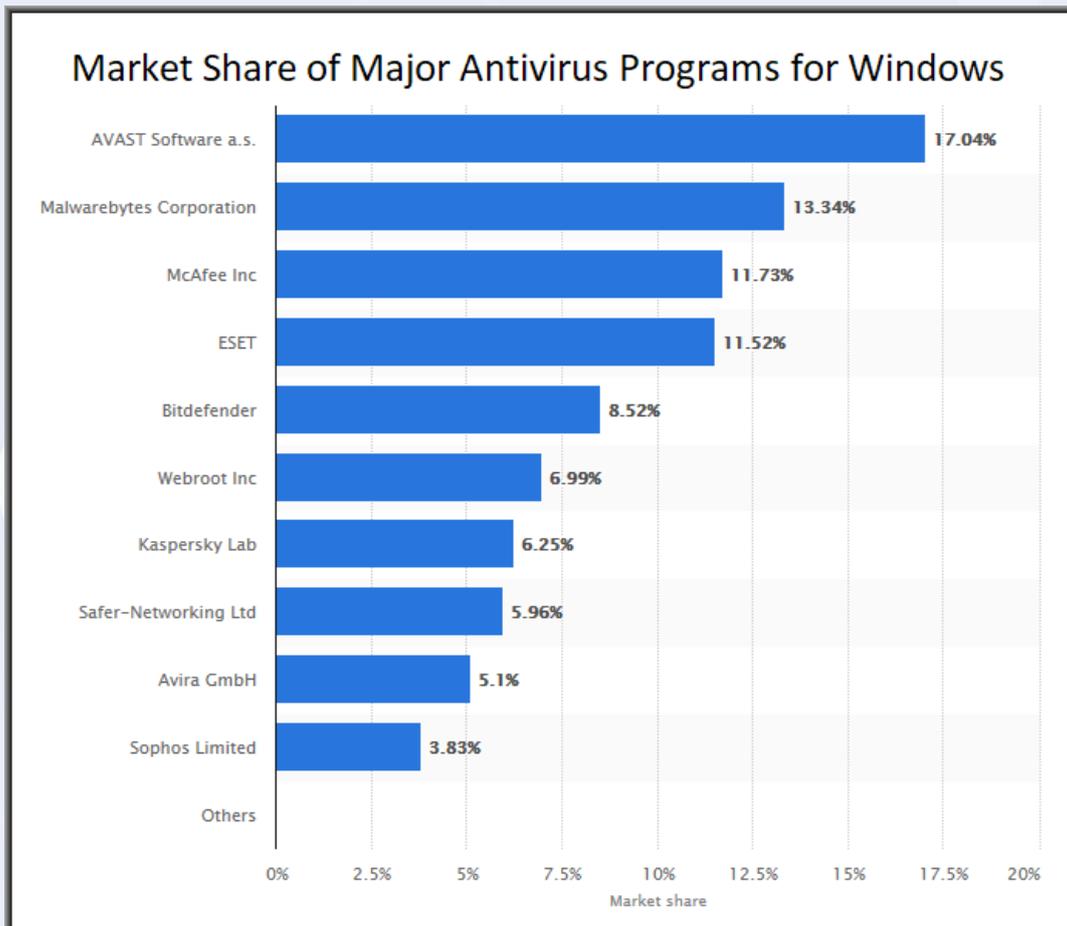
Source: safetydetectives.com

(Note: the antivirus market for Apple computers remains small. This is because Mac computers are much less susceptible to viruses; plus, MacOS includes a very good pre-installed antivirus).

The most commonly exploited attack vector is Microsoft Office (47% of all attacks on Windows). Almost 40% of malware is disguised as .doc files. They have replaced .exe files as the number one threat, since users have learned from experience not to open unknown programs.

The price of most popular antivirus programs ranges from low to medium. The basic version of Norton Antivirus costs $50 a year; for McAfee, it's $20; Malwarebytes, $40 for one device.

There are also free antivirus software, such as AVG Free, though they come with a lot of unwanted ads or additional programs that have to be installed.

The main problem of all major antiviruses is not their price, however, but rather their lack of efficacy. According to some studies, less than 5% of anti-malware programs can quickly detect and identify new viruses as threats. This is one of the key issues that MalwareChain aims to solve.

1.2. The problem: traditional antivirus products are inefficient

As we have seen, major antivirus developers, including Kaspersky, Norton, etc. thoroughly dominate the cybersecurity market. The products they offer are largely interchangeable – though not interoperable. All these companies utilize the same algorithm to identify and remove threats – and roughly the same monetization model. Here are its main principles and issues related to each:

1) The antivirus company's computer systems continuously scan the Internet in search of new threats.

Inefficiency: all antivirus developers scan the same space, and the threats they find are also the same. They don't divide the Internet among themselves to make speed up the process and don't share their findings with each other, either. This can be compared to several independent surveyors mapping the same area of the forest. They find and add to their maps the same ditches and cabins, ending up with roughly the same result. Needless to say, a tremendous amount of resources is wasted this way.

2) Once a previously unknown threat is found, it's analyzed and given a unique identifier. (hash) The identifier is added to the database.

Inefficiency: A lot of human labour goes into analyzing threats and updating the program. Since it's all done on site and in developed countries, the companies have to pay relatively high salaries to their staff. They have no way of using independent specialists who could charge a lower rate. These costs are later transferred onto the final consumer.

3) Recently identified threats are integrated into the next software update.

Inefficiency: updating is not real-time. There is a lag between the moment when a new virus is discovered and when an end user installs the update that contains a fix. Since new viruses emerge every day and every hour, actual protection will never be up to date. Antivirus companies are constrained by their own rigid system of updates.

4) At any given moment, different antivirus databases (and, therefore, software versions) aren't identical. They largely overlap, but which viruses are included depends on what each detection system found and how quickly the company managed to introduce new elements into the next update.

Inefficiency: to achieve maximum protection, end users have to pay for several antiviruses and run them simultaneously. They mostly duplicate each other and can't collaborate (lack of interoperability).

5) Antivirus software is resource-hungry.

Inefficiency: This places an unnecessary strain on the device, causing it to slow down and freeze. To solve the issue, the user has to turn off the anti-malware program, leaving the computer unprotected.

6) Detection systems sometimes give false positives – they flag files and pieces of code that aren't actually viruses.

Inefficiency: users find their files and programs blocked for no reason. Sometimes it takes a long time to google the issue and discover that an antivirus is the culprit. However, often the only way to unblock a file is to disable the antivirus.

7) Threat databases and updates are stored on centralized servers.

Inefficiency: a hacker can gain access to the server and wreak havoc with the list of viruses.

2. MalwareChain: a distributed cybersecurity database, detection engine, and scanner

2.1. Ecosystem structure

MalwareChain is an advanced decentralized system for identifying and removing viruses. It comprises a complex ecosystem:

1) Malware hunters (Discovery nodes) – users who work on detecting new threats;

2) Threat library and the hashing algorithm. The complete database of threats and their hashes is stored in a decentralized fashion. Each threat and each scanned file have its own hash that serves as a proof that a check has been completed;

3) Engine developers – users who design highly specialized detection engines for specific virus families and work on improving the basic client;

4) Anti-malware nodes (Scan nodes) and the P2P scanning/matching algorithm. Users run the antivirus client (proprietary software for distributed threat analysis) to scan files uploaded by other members;

5) Proof-of-Stake mining nodes: users who confirm transactions and add them to the blockchain every time a file is scanned for viruses and a reward is paid;

6) Masternodes – higher-level blockchain nodes storing a full copy of the blockchain; they also carry out overall control of the system;

7) MALW coin: the system's own cryptocurrency, used as collateral for masternodes and PoS nodes, as well as to pay out rewards.

2.2. Malware search and identification

The threat discovery system of MalwareChain will be distributed – as opposed to centralized systems employed by Norton and others. Specialized network members (Discovery nodes) will crawl the web, applications, files, and devices connected to the network to discover new threats and match them to the database. The whole process is completely automated. Any newly identified threat will be automatically assigned a unique cryptographic hash and added to the MalwareChain threat library. The information about it will be recorded on the blockchain, and all the nodes running the P2P antivirus client will receive an automatic update.

Threat discovery is a relatively resource-intensive process, since it requires a node to crawl large volumes of data. As a means of compensation, Discovery nodes will receive a reward for each new threat added to the library. 30% of the fees charged for scanning user files (see below) will be allocated for the purpose.

Note: the current MVP of Malware Chain is already running an advanced system for detecting new threats. For now, it's merged with the scanning algorithm and the malware library. The

major difference between the MVP and the upcoming beta release is the introduction of a decentralized system for discovering vulnerabilities.

2.3. Threat library and system updates

All threat-related data in MalwareChain will be crowdsourced and instantly shared with all network members. Each virus will be identified using a unique hash stored in the library. Every node involved in file scanning will have an up-to-date version of the library, automatically updated whenever a new threat is added by someone in the network. This gives us reason to call MalwareChain a self-updating decentralized antivirus program.

Adding a virus to the database will be treated as a blockchain transaction with a zero value, subject to the standard network fee. (However, as mentioned before, malware hunters will be rewarded for their effort, and the fee itself will be negligible.) Consequently, every change to the library will in itself receive a hash – a crucial feature for ensuring correct behavior of all network nodes (see "Masternodes").

2.4. Engine design

The basic antivirus client for MalwareChain (https://scan.malwarechain.com) will already be up and running at the moment of the network launch. The source code for the client will be made open to the public two or three years later. This way, any developers who join the network can make their own modifications and improvements and present new versions of the MalwareChain client to the community. Moreover, there's nothing stopping developers from designing new virus detection engines – as long as they satisfy to the list of requirements, which will be published soon after launch.

All proposed modifications and new engines will be voted on by the users who own masternode shares (see below). A client can be approved for official use within the network as long as it satisfies the following requirements:

- Full compatibility with the MalwareChain blockchain, library, and cryptographic hashing system;

- Open-source;

- The client must have a GitHub page with regular commits;

- Compatible with the specified types of devices run by Scan nodes (see below).

All approved clients will be available in the Downloads section on the platform. Every time a node starts running a certain client, a record will be made on the blockchain. The client's creator will receive a reward in MALW coins.

2.5. Interaction with the platform: file uploading and scanning; Scan nodes

In MalwareChain, end users don't have to install special software to find threats on their own computers. Instead, they can upload a suspicious file, app or email to the network and have it analyzed for them. The reason is simple: any antivirus program that is powerful enough to quickly match a piece of code to a vast list of known threats is bound to slow down one's computer. This deters many users from buying an antivirus.

By contrast, MalwareChain allows to check any file remotely and almost instantly for a tiny fee. All that a user needs to do is access the interface via web or a native mobile app, choose a file, and click on Scan. The file will be automatically sent via a P2P channel to the first available Scan node.

A Scan node means any user who has one of the approved MalwareChain antivirus clients running on their device. The job of a Scan node is to process files sent by users for scanning and detect threats. Some Scan nodes will run on enterprise-grade servers and will be able to process hundreds of requests per minute. Others will be hosted on retail-grade laptops and even mobile devices. Users will also be able to decide when to run the client – the device doesn't need to be online 24/7.

However, those nodes that show the highest speed over time(that is, the lowest average time per request) will have a higher rating and thus get a precedence. A Scan node earns 50% of the scanning fee, so the more requests it processes, the higher the reward. This will motivate owners of powerful server hardware to join MalwareChain and make it an attractive alternative to data storage, fog computing, etc.

After a file has been scanned, the results are sent to the user who had requested the scan, a detailed report is generated, and a new record is added to the blockchain. This record contains data on the user who requested the scan (and paid the fee), the Scan node that performed the check, the size of the fee, and the hash for the report in the Input Data field.

If a user tries to upload the same file for a second time, an error message will appear, saying that the hash matches that of a previously scanned file.

Apart from files stored locally on the computer, it's also possible to enter a link to a file stored on a cloud or the URL of a website.

It's worth pointing out that the same device can do both scanning and vulnerability search – that is, act as a Scan and Discovery node at the same time. This requires good hardware, but it also allows to maximize the fee revenue.

2.6. Proof-of-Stake mining

1% of the maximum supply of MALW coins will be pre-mined and some of them will be sold at the pre-sale, form a development fund and establish the first industry partnerships. The rest will be generated via a mechanism of Proof-of-Stake mining.

In order to join the mining, a user needs to purchase a certain amount of MALW and create a stake – that is, freeze the coins. Everyone who has a stake is eligible for confirming new blocks, but the reward frequency is determined by the size of the stake.

We note that the minimum stake size is 500 coins. For example, a user whose stake constitutes 2% of all the issued MALW will have the right to validate 2% of all blocks – as long as their device is constantly running. In addition, miners will receive a share of the transaction fees.

For those users who can't leave the laptop on 24/7, it can be more profitable to invest in MalwareChain masternode shares (see below).

Note that the PoS mining client is different from the antivirus scanning client. Depending on the available hardware, a user may decide to operate both a PoS node and a Scan node.

2.7. The role of masternodes

MalwareChain masternodes are very different from all others. They don't confirm transactions or add new blocks to the blockchain. They don't perform antivirus checks, either. The main purpose of a masternode is to store a complete version of the blockchain. It has to be updated constantly, 24/7 – therefore, a masternode must be up and operational around the clock.

For a platform like MalwareChain, having multiple up-to-date copies of the blockchain is crucial, because it contains data on cybersecurity threats and hashes of scan reports. Any antivirus system is dependent on its past records – perhaps more so than a simple system for sending money to others. As a consequence, MalwareChain makes its masternodes a keystone element of the ecosystem, allocating 98% of all block rewards to the users who operate them.

Apart from safeguarding the integrity of the blockchain, masternodes have a few other functions:

- Network governance: masternodes can vote on various decisions in the community. This includes approving or rejecting new antivirus clients, changing the reward allocation structure, switching to a different system of decentralized data storage, or penalizing users who abuse the system;

- Instant transactions: users can choose to get their antivirus scan performed instantly ahead of the queue thanks to the Instant Scan feature. In this case, the transaction is confirmed by a masternode quorum and executed without delay (a blockchain record is still made, only somewhat later). The transaction fee is higher for instant scans. Nonetheless, the feature will be useful to those who work on mission-critical tasks and can't wait to find out if a site or file is dangerous or not;

- Refusing blocks presented by PoS miners who violate the rules.

An important clarification: proof-of-stake nodes and masternodes are not the same thing. Running one's own MalwareChain PoS node is easy: one needs to install a mining software client, stake the necessary amount of coins, and keep the client open when the device is in

use. If the device is offline for some periods of time, nothing happens – the user will simply confirm fewer transactions and earn less rewards.

A masternode is a very different matter. Since it's so important for the whole network, it must always be online, updating the blockchain every time a new block is added. If it goes offline, its operator will be fined. This means that a regular device like a laptop won't do – the node must run on its own server that ensures at least 99.99% uptime. Consequently, masternode operators usually rent a virtual private server from a hosting company. It can be quite expensive but the reward from the work of the masternode will repeatedly cover these costs. Masternodes also require a lot of technical expertise to set up, as well as a very large stake (known as collateral). The initial investment can reach thousands of dollars.

MalwareChain provides an alternative: buying masternode investment shares. For details on this solution, see below.

3. Tokenomics and timeline

3.1. Investing in masternode shares

Masternodes represent one of the most attractive investment opportunities in the crypto market. They are much more profitable than PoS mining – and with the current market slowdown and growing electricity prices, masternodes also yield more profits than traditional hardware mining or cloud mining.

The disadvantages are the large collateral, technical complexity, and server requirements. Only a minority users have the money and the expertise to run a full masternode. A solution to this problem is presented by shared (pooled) investments.

In MalwareChain, users can purchase small shares of a masternode and receive a corresponding share of the reward. Since every masternode requires a predefined amount of collateral, it can take some time before sufficient investments are collected to launch a new node. Normally this waiting period doesn't exceed one week.

The investment mechanism is very simple and intuitive. A user chooses the amount they are willing to invest and makes the collateral deposit in MALW. Once there is enough funds to launch a node, the user receives a notification. After that, rewards automatically start accruing. There is a special formula for calculating each investor's daily reward. It depends on the total number of minted blocks during a period, reward per block, and number of masternodes in operation.

Owners of masternode shares can instantly withdraw their rewards to their blockchain wallet. The same goes for the collateral itself. Thanks to a special advanced algorithm employed by MalwareChain, there is no need to disassemble a node when one of its shareholders decides to withdraw.

How this will be technically implemented? MalwareChain will be added to the most popular shared masternode service which will guarantee complete protection of customer funds. In addition, will be realized the opportunity to invest in "instant" shared maternodes within our own ecosystem.

3.2. Role of the MALW coin

MALW is the fuel that powers the whole MalwareChain ecosystem, from threat discovery to mining. Pre-mined coins (which constitute only a small portion of the maximum total supply) will be available for purchase during the pre-sale. After the completion of the pre-sale, new coins will be minted in the process of PoS mining. New coins will be distributed among different groups of beneficiaries: miners, masternode investors, Scan nodes, Discovery nodes, and developers.

Here are the main functions of MALW:

- Paying for antivirus scans and other services (threat detection, development of antivirus

clients. It will also be possible to pay in BTC, ETH and other cryptocurrency, but users who choose to pay for scanning in MALW will enjoy lower fees;

- Staking for PoS mining; the stake can be unfrozen and withdrawn at any moment without any penalty. Naturally, the user won't receive any mining rewards anymore;

- Collateral when buying masternode shares. Users can withdraw their collateral deposit at any moment instantly;

- Blockchain transaction fees;

- Block rewards for PoS miners;

- Reward payouts for owners of masternode shares;

- Rewards for Discovery nodes that identify new threats and add them to the library;

- Rewards for developers who improve on the official antivirus client or develop new ones (awarded whenever a client is approved by the community); apart from this reward, a developer receives a small payout every time a Scan node downloads and runs a client they developed);

- Voting (only for users who own masternode shares); a minimal amount has to be sent to cast a vote, which is written into the Input Data field;

- Money transfers – users can treat MALW as any other cryptocurrency: trade it at a crypto exchange, send it to each other's blockchain wallets, etc.

3.3. Types of user rewards

Every member of the ecosystem will have ways to earn MALW. This will ensure an uninterrupted and ever-growing circulation of the coin within the ecosystem. Below is a list of the key sources of income for project participants:

1) Investing in masternodes. 98% of block rewards will be allocated to the owners of masternode shares and divided according to each investor's share in the total pool and the amount of time that has passed since they joined. Accumulated masternode rewards can be withdrawn instantly at any moment. The setup and maintenance of the nodes will be carried out by the platform. Therefore, of all the ways of earning with MalwareChain, this one is best-suited for users who don't own a powerful device.

2) Running a Scan node (analyzing files and links uploaded by users) – 50% of the fee charged for each scanning operation. The final price for the scan of each file or website depends on the amount of data processed. Owners of enterprise-grade hardware will naturally have an advantage, running dozens of requests per minute and generating a substantial income. Though scanning fees can also be paid in BTC (and, in the future, other cryptocurrencies), all rewards will be paid in MALW. The platform will automatically convert BTC into MALW using the best available exchange rate.

3) Proof-of-Stake mining: 2% of the block reward. Requires a stake in MALW (min 500) and a mining client, which can be installed on any device connected to the Internet (including a smartphone in the future). Users with larger stakes have a better chance to add a new block, so on average their income will be higher.

4) Operating a Discovery node - crawling the web and devices for new, previously unknown viruses and malware, and adding them to the library. 30% of the scanning fees are distributed among all nodes that added new threats to the database in a given period in proportion with each node's input. Example: suppose that 2000 MALW are to be distributed. Node 1 discovered 10 threats, Node 2 added 20, Node 3 detected 30, and Node discovered 40 threats (a total of 100 threats). Therefore, Node 1 will receive 10% of the total reward (200 MALW); Node 2, 20% (400 MALW); Node 3, 30% (600 MALW); and Node 4, 40% (800 MALW).

5) Developing new versions of the antivirus client. Each new client needs to be approved by the users who have a vote (masternode investors). After approval, the client can be used by any Scan node. Whenever a Scan node installs a specific client, the developer gets a small reward. Further, 10% of all scanning fees are allocated to those developers who built the respective clients. Example: Scan nodes running the client Snowflake generated $500 in scanning fees in a given month. 10% of this sum, or $50, will be awarded to Developer Bob who created Snowflake.

6) Bounty program: MalwareChain will run a bounty campaign where any participant can receive free MALW for completing easy tasks. They include sharing the official news posted by the project, publishing original posts about MalwareChain, creating video reviews and articles, posting on blockchain forums, etc. The reward can reach $100, as long as the content is unique and engaging.

For rewards in MalwareChain DAO (MDAO) governance tokens, see the next section.

4. MDAO – the governance token of MalwareChain

4.1. What is MalwareChain DAO (MDAO)?

MDAO is an ERC20 token that will play several important roles within the MalwareChain ecosystem:

1) Governance token: MDAO holders will be able to participate in decentralized decision-making on the platform. Governance tokens are used by many DeFi projects. In order to vote on various changes to the protocol, token holders will need to send their MDAO to a specified smart contract address.

2) Incentive for masternode owners. Our goal is to have a large and stable network of masternodes that will support the security and stability of MalwareChain. For an ecosystem based on masternodes, it's very important that they stay online all the time or at least most of the time. Therefore, we will offer an additional reward to those masternode owners whose MNs remain continuously online for at least a month.

3) Incentives for regular users to interact with MalwareChain through the DeFi ecosystem on the Ethereum blockchain. This means providing liquidity to decentralized pools, using wrapped MALW tokens for borrowing and lending, etc.

4.2. Three ways to get hold of MDAO: Uniswap pools and wMALW wrapped tokens

MalwareChain DAO (MDAO) will not be pre-mined or distributed through any sort of an ICO or IEO procedure. Instead, it fill be minted as needed. There are three ways to obtain MDAO: the first two are available to all users, while the third is reserved for masternode owners.

4.2.1. MDAO Uniswap pools

Uniswap is an automated market-making protocol – a new type of decentralized exchange that guarantees ready liquidity for any token.

In the past, decentralized exchanges suffered from a constant lack of liquidity. For tokens with a small-to-medium market capitalization, there often wasn't a way to fill exchange orders, because there were no matching offers on the order book. For example, a user who wanted to sell token A couldn't find a buyer, so the trading volume remained at zero.

Uniswap changed all that by introducing self-balancing swapping pools where the price of an asset depends on how much liquidity is deposited in the pool, not on supply and demand. Each currency pair has its own pool: in our case it will be MDAO/ETH and MDAO/USDT. When joining one of these pools, a user will need to deposit some MDAO tokens plus an equivalent amount in ETH. So, for example, if the price of MDAO is 0.01 ETH, a user can deposit 100 MDAO and 1 ETH, or 150 MDAO and 1.5 ETH, and so forth.

This liquidity is used to execute token swaps (trades). The relative price of the two assets will constantly change depending on the size of the order relative to the size of the pool. Thanks to this system, liquidity is always available for any trade.

When users deposit liquidity in the pool, they get special Uniswap tokens in return, known and MDAO/ETH (or MDAO/USDT) UNI-v2 LP. These tokens act as a proof that the user owns a part of the pool. LP tokens aren't personal: they are just ERC20 tokens, so one can transfer them freely to any Ethereum address. Whoever holds these UNI-v2 LP tokens can always redeem them for the corresponding share of the liquidity in MDAO and ETH.

The benefit of participating in liquidity pools for users is that they will earn a percentage of the trading fees AND an additional reward in MDAO tokens.

Trading fees. By default, Uniswap charges a 0.30% fee on every trade. The fees are distributed among the pool's owners according to the number of UNI-v2 LP tokens they hold. We will do our best to promote trading in MDAO, in order to ensure that a good amount of fees are generated.

Uniswap staking rewards. LP token staking became one of the strongest crypto trends of 2020. It's a great mechanism for DeFi project to award their users who contribute liquidity to the network. It's known as liquidity mining or yield farming.

In essence, liquidity providers will be invited to stake their MDAO UNI-v2 LP tokens by sending them to a dedicated smart contract deployed by MalwareChain. Each of the two Uniswap pools will have its own contract. With every tenth Ethereum block, we will issue 400 MDAO to be distributed among the stakers, masternode owners and project development fund. This is to incentivize MalwareChain users to contribute liquidity to Uniswap and to promote the trading of MDAO.

Expected APR. We forecast that Uniswap trading fees will generate an annualized yield of at least 60% for each liquidity provider. In addition, the liquidity mining program will yield no less than 50%. Thus, the total APR (annualized percentage rate) for Uniswap pool members will be at least 110%. This isn't as high as it seems: it's not uncommon for Uniswap pools to yield over 100%, and for liquidity mining programs to pay up to 1000%.

However, we prefer to stick to more conservative estimates. Some DeFi projects make the mistake of paying excessively high rewards. Users seek to sell the tokens they have farmed and the market becomes oversaturated with these tokens. The result is that the price of the farming token collapses. We don't want this to happen to MalwareChain DAO (MDAO), so we'll employ a tokenomics model to support the price and reward stakers at the same time.

4.2.2. wMALW wrapped token

Together with MalwareChain DAO (MDAO), we will launch another token – a wrapped version of MALW on the Ethereum blockchain, or wMALW.

A wrapped token is an asset that has the same value as the original token and is backed by that token, but 'lives' on a different blockchain. Most wrapped tokens are issued on the Ethereum blockchain.

Every wMALW will be backed by 1 MALW and worth exactly 1 MALW. We'll use a smart contract algorithm to fetch the up-to-date pice of the underlying MALW token and reproduce it on Ethereum.

The purpose of wMALW is to allow MalwareChain holders to participate in the DeFi ecosystem – for example, borrow and lend funds on the blockchain or trade their assets on decentralized exchanges like Uniswap and Kyber. Until there is an operational cross-chain solution that could connect Ethereum and MalwareChain blockchains, a wrapped token is the best option. But the main purpose of wMALW is to use them for MalwareChain DAO (MDAO) staking.

Any MALW holder who wishes to get some wMALW will be able to do it through the Malware Chain platform. The steps are as follows:

1) The user sends MALW to the custodian (the platform) and provides an ERC20 address where the wrapped tokens should be sent.

2) An equivalent number of wMALW are minted and sent to the said ERC20 address.

3) At the same time, some MDAO tokens are minted and sent to the same address (this requires additional actions from the user).

Thus, users will get a reward in MalwareChain DAO (MDAO) every time they wrap MALW and stake them. The platform as a custodian will store their tokens in a special multisig wallet until the user wishes to swap them to original MALW. The reverse procedure works this way:

1) The user sends wMALW to the smart contract address to be redeemed.

2) The wMALW transferred by the user are burned.

3) MALW coins are returned to the user's address.

Even though this type of scheme is not allowed, there is a way to increase one's gains through minting wMALW. The MDAO received as a reward can be immediately deposited in one of the two Uniswap liquidity pools to earn additional rewards through yield farming.

Of course, since wMALW is a derivative asset created and managed by an organization (the MalwareChain project), it cannot be as trustless as the original MALW. Therefore, we will make all the information about wMALW emission and transactions available on-chain. For example, users will be able to see how much MALW was transferred into the wMALW address to mint new wMALW, and compare this to the actual number of wMALW created. Likewise, it will be possible to monitor how the wMALW are burned when users redeem their MALW coins. We'll also subject both new smart contracts (wMALW and MDAO) to an obligatory comprehensive audit.

4.2.3. Rewards for masternode owners

We've already mentioned that those masternode operators whose MNs stay online for at least a month will get a reward in MalwareChain DAO (MDAO). By a month we mean 24 hours a day for 30 or 31 consecutive days. The reward for each additional 30 days of uptime will be increased by 10% if the masternode holder didn't withdraw his MDAO tokens. The reward will be paid immediately every 10 Ethereum blocks, starting from the next day after the first month of consecutive uptime is completed.

Example: Suppose a new masternode joins the network on March 1 and then remains online at least 99.8% of the time (making a provision for hosting server downtime, which isn't the node's fault) until March 31. Let's assume that the reward for 1 month of consecutive uptime is 10 MDAO per day, so for a month of 31 days that makes 310 MDAO. Starting from April 1, the MN owner will start receiving 10 MDAO per day. At the same time, each consecutive day of uptime after March 31 will also result in a reward of 10 tokens. But if the operator goes offline at some point, their 'reward streak' will be broken off.

The allowed downtime within a month (or rather, a rolling period of 30 days) is 0.02%, which makes 1 hour 30 minutes. So, if the masternode goes offline for one hour on April 5, for example, it will keep receiving rewards every day. But if it stays offline for 2 hours, it will only receive the MDAO due to it for the period from March 1-31, and then the payouts will stop. The MN will need to stay online from April 5 (the moment it went down) until May 5 to start getting rewards again.

If a masternode remains online for 2 consecutive months (99.8% of the time), its daily reward will increase by 10%. Instead of 10 MDAO per day it will get 11 MDAO. After 3 consecutive months of uptime, the reward will be increased by an additional 10%, so the owner will get 12 MalwareChain DAO (MDAO) every day, and so forth with every new month spent online.

To benefit from the rewards, the owner will first need to register the masternode in a special section on the MalwareChain platform. Any resulting blockchain fees can be paid in MalwareChain DAO (MDAO) (when transacting through the platform) or in ETH (when interacting directly with the smart contract).

4.3. MDAO development fund

5% of the MalwareChain DAO (MDAO) emission will be transferred to a special development fund – a reserve to be used for further improvement of MalwareChain. The fund will be organized as an open blockchain wallet, and it will be up to the MalwareChain DAO (MDAO) holders to decide how the tokens in it should be spent.

The development fund is a crucial element of the decentralized governance ecosystem. MalwareChain DAO (MDAO) holders will vote on various protocol improvement proposals – some of them entered by the project's developers, others by users themselves. For most of the proposals, there will be just two options to choose from: 'approve' or 'not approve'. Each voter will need to send MalwareChain DAO (MDAO) to one of the two smart contracts, each

corresponding to one of the options: a 'Yes' contract and a 'No' contract. After the vote, users will be able to recover their governance tokens by paying a standard Ethereum transaction fee.

5. Key information on MALW and MalwareChain DAO (MDAO) and roadmap

5.1. MALW and MalwareChain DAO (MDAO): key facts

MALW

Ticker:	MALW
Number of decimals:	8
Algorithm:	Proof of stake + masternodes
Maximum total supply:	315 000 000 MALW
Pre-mine:	3 150 000 (1%)
Block reward:	4.0 MALW
Masternode reward:	98%
PoS validator reward:	2%
Average block time:	60 seconds
Coin maturity period:	180 minutes
Blockchain:	Proprietary blockchain based on PIVX
Masternode collateral:	5000 MALW
Minimum Input Age for Staking:	12 hours

MDAO

Ticker:	MDAO
Number of decimals:	8
Blockchain:	Ethereum
Standard:	ERC20
Pre-mine:	no

5.2. Project roadmap

Completed: Q2 2019 - Q3 2020

- Researching the antivirus market, analyzing other blockchain antivirus projects, formation of the idea, hiring key team members;

- Analysis of the masternode investment market; planning of the project tokenomics;

- Development of the alpha release of the antivirus app;

- Work on the proprietary blockchain;

- Publication of the White Paper and launch of the official website;

- Wallet release;

- Antivirus web version MVP launch;

- MALW coin pre-sale;

- MALW is listed on 2 exchanges;

- Company's legal registration;

- Finalizing the threat hashing algorithm;

- Work on the distributed threat library;

- Social Media Marketing campaign.

Q4 2020

- Release of MDAO governance token;

- Enabling DAO (Network governance);

- Launch of MDAO pools on Uniswap;

- Work on the wMALW wrapped ERC20 token;

- Staff expansion;

- Launch of the beta version of the app;

- Online scanner: attracting more users;

- Masternodes start earning DAO tokens.

Q1-Q3 2021

- Release of the apps for Android and iOS;

- First votes on project governance by MDAO holders;

- Attracting developers to join the network and design new antivirus clients;

- First alternative antivirus clients are released;

- Developers of alternative clients receive first rewards;

- Work on the native apps for iOS and Android;

- First 20+ Discovery nodes join the network;

- Launch of the distributed threat library;

- Work on a decentralized storage solution for scan reports based on IPFS.

Q4 2021 - Q1 2022

- Listing on more exchanges;

- Target number of Scan nodes: 2500;

- Target number of Discovery nodes: 250;

- Target number of alternative antivirus clients: 5;

- Target monthly number of scanned files/links: 100 000;

- Development of reward distribution subsystem for Discovery/Scan nodes;

- Using blockchain for complete data storage.