Decentralized
Cyber Security

ACESO
WHITE PAPER REVIEW

15.08.2018

Table of Contents

1. Disclaimer

Please read the following notification properly before taking part in Aceso ASO token sale. This notice applies to all persons who read this document. Please note this notification may be changed or updated.

ASO token sale is carried out by ACESO LT, UAB, a company incorporated and existing under the laws of Lithuania (hereinafter – the «Seller»). We also draw your attention, that the ACESO Whitepaper (hereinafter – «WP») does not constitute any relations between you (hereinafter – «you» or the «Buyer») and the Seller. Purchasing of ASO tokens is available only after accepting the Terms and Conditions (hereinafter – «T&C») and Privacy Policy.

Purchasing of ASO tokens does not present an exchange of cryptocurrencies or conventional currencies for any form of ordinary shares of the Seller and the Buyer of ASO tokens is not entitled to any guaranteed form of dividend. The Buyer is only entitled to certain rights within the T&C. ASO tokens are not intended to constitute securities in any jurisdiction.

WP does not constitute a prospectus or offer document of any sort, and is not intended to constitute an offer of securities or a solicitation for investments in securities in any jurisdiction. WP is posted for information purposes only. The content of WP is not a financial promotion. Therefore, none of the content parts of WP should be considered an invitation or inducement to engage in any sort of investment activity. The Buyer should carefully consider and evaluate all risks associated with cryptocurrencies, operations with them, ICO and respective business activities. Before purchase ASO tokens read carefully all the information set out in this Disclaimer, WP, T&C and Privacy Policy and ensure that you are aware of all potential risks. The section «Risk Statement» (in T&C) details all potential risks that you should consider. We strongly recommend you to seek out independent financial and legal advice before engaging in any sort of business endeavor.

2. Executive Summary

Around 400 new threats are created globally every minute, and 70% of those threats go undetected. Cybercrime damage will cost the world around $6 trillion by 2021, and according to Cybersecurity Ventures, cybersecurity costs will exceed $1 trillion cumulatively by the same year.

ACESO is decreasing the costs of protecting a computer from malware to a minimum (1$), where users will no longer have to pay for the software, but for the real Malware Threat removal instead. We introduce Pay-per-Fix model.

Users commonly turn to anti-malware programs when their computers become infected with malware already. Anti-malware software costs $30 on average and paying this amount for the removal of just one malware seems illogical. We minimize the expenses of anti-malware protection to $1 per fix, replacing traditional software packages with customizable solutions, where the user pays only if there is a real threat. There is no such solution in the market yet.

Based on the data from our 1 million users, we know that an average user encounters 5 real malware threats per year. This means that by using ACESO, the user could decrease expenses to $5 per year. Compared to $30 per software on average that is 83% less.

This becomes possible due to the active cybersecurity community. Community is helping users to solve their PC problems already, but we will empower them by giving away 90% of the fee end-user is paying for the fix. Analyst for fixing the issue gets 60% of the price user is paying. Researcher for providing malware sample gets 30% of the price user is paying. All together community will earn more than $50 million in the first 5 years.

ACESO's success lies not only in the innovative anti-malware protection model, but in the experienced team as well. Founders bring a great deal of experience to the cybersecurity market from both development and marketing sides. Romualdas Cukuras, CTO with over 10 years of experience in cybersecurity, has created 4 malware/spyware removal programs already. Mindaugas Sinkevičius, CEO with over 8 years of experience in cybersecurity, has a proven track record in growing cybersecurity businesses with data-driven marketing solutions.

ACESO founders own the anti-malware software WiperSoft, which has more than 1 million users across more than 100 countries. Since its launch in 2015, WiperSoft has removed more than 200 million infected items (files, registries, browser extensions, etc.) already.

Under the Intellectual Property agreement, ACESO is using WiperSoft's engine to create a more innovative business model based on blockchain technology. Freemium WiperSoft users have already expressed interest in our low-cost solutions. This should secure $1,9 million in revenue immediately after the product's launch.

ACESO offers both B2C and B2B solutions. Initial launch will be made to the B2C market, where innovative solutions will secure a fast user base and malware sample growth. This will allow us to establish brand awareness and help create a sufficient malware database, necessary to become competitive in the B2B market. In the second year of commercial activity, ACESO will enter the B2B market and will primarily target the SMB market, which will become the main revenue stream in the long run.

3. Introduction

Getting rid of a computer infection has proven to be a complicated task for uninformed administrator and PC users, which is why the willingness-to-pay for cybersecurity products is rather high.

Many anti-malware security programs charge $30 dollars, which gives access to superficial detection and which sometimes does not even include an active solution for malware removal. The average infected user does not know which malware solutions exist. Their purchase decision is highly impacted by the Brand awareness or the pricing levels.

Common behavior of average user is to turn towards antimalware protection once computer is infected already. Anti-malware on average costs around $30. So if a malware infected user buys the program to fix one infection and never gets infected again (or at least during the subscription period), he/she would be paying $30 for that one fix, which seems illogical. What if a pay-per-fix solution was available?

ACESO introduce an innovative antimalware protection model, where users will no longer have to pay for software, but for a service instead. We minimize the expenses of anti-malware protection, replacing traditional limited software packages by an all-round tough customizable solution within the framework of a service-based business model. At the same time, we create new revenue stream capturing unserved market segment.

4. Cyber Security: Market Overview

The cybersecurity market offers huge potential on a global scale. Cybersecurity Ventures predict that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. Global spending on cybersecurity products and services will exceed $1 trillion cumulatively from 2017 to 2021. This is 12% - 15% year-over-year growth through 2021.[1]

Study published by Bank of America Merrill Lynch suggests that there are close to 400 new threats created per minute, with an estimated 80-90 million threats per year. Additionally, the study suggests that over 70% of these threats go undetected.[2]

State of Malware Report 2017 highlights the increase in Ransomware threats, in both, the corporate and consumer environments.[3] While traditional malware such as banking Trojans, spyware, and keyloggers requires cybercriminals to oversee multiple steps before revenue is delivered to their bank account, ransomware makes it a seamless, automated process.

Research of the March & McLellan[4] states Asia-Pacific (APAC) is the ideal environment for cyber criminals to thrive in because of high digital connectivity in contrast to low cybersecurity awareness, growing cross-border data transfers, and weak regulations. Beyond legislations, governments can further mitigate cyber risks through public/private information sharing, development of cybersecurity knowledge hubs, and growing the talent pool.

According to IBM X-Force researchers[5], malware facilitates the most prolific type of cybercrime attacks in Brazil. Because Brazilian malware tends to be less sophisticated than malware made in Eastern Europe, cybercriminals in Brazil compensate with attack volume. Brazil's large population includes many internet users with relatively low security awareness, along with large amounts of enterprising cybercriminals.

In regards to the B2C segment, due to internet connectivity and services becoming available in more parts of emerging markets, many people are accessing online services for the first time. Security is often an afterthought to new internet users, increasing their chances of becoming victims of cybercrime. Besides low cybersecurity awareness, another big concern is the lack of low cost anti-malware protection solutions.

The B2B Cybersecurity Market will be worth $22.79 Billion by 2023[6]. The major factors driving the growth of the industrial cybersecurity market include: increasing government funding to improve the cybersecurity of the industrial environment, and the growing incidents of data security breaches due to the rising number of connected devices in industrial control systems.

5. Pain Points and Opportunities

Expensive anti-virus software programs do not guarantee fool proof protection. Because large anti-virus companies focus mostly on widespread infections, smaller malware threats may be overlooked. Furthermore, using only smaller anti-virus software solutions will also be insufficient and unpractical. Therefore, choosing one right security solution for a specific malware problem tends to be tough and time-consuming for non-experts. For this selection process, users heavily rely on online forums for help, describing their problem to cybersecurity experts. These experts then provide detailed instructions for the specific situation, often without charging any fees. In some cases, those instructions are provided by vendors to promote their own products.

Following pain points characterise the current cybersecurity market:

1. Growing malware threat

a. High security costs

Aware of these risks, users incur huge expenses to protect their computers against cyber threats. Despite the high costs, users are often left behind with different types of malware infecting their systems, due to improper or insufficient software solutions. Moreover, government institutions cope with high malware threats, spending millions of dollars on protection.

b. Lack of IT Experts

New malware threats appear every single second, boosting the demand for quick solutions and for research. However, existing anti-virus software packages are too slow. Also, the existing databases are too poor to properly react to the new emerging threats. Anti-malware can only cope with the most significant threats, leaving the minor threats unsolved. The high demand for fast and efficient solutions is unmet due to a shortage of IT Experts. Moreover, these Experts charge also high service fees.

c. Limited coverage

Antivirus and antimalware software providers often separate low-priority and high-priority malware issues based on the impact it has on the usability of the infected computer and based on the number of computers that are infected by high-impact malware.

The existing products and solutions for malware detection and removal only focus on the high-priority issues, leaving a large amount of less intrusive malware problems undetected and unsolved. The limited coverage often contradicts the price charged by the provider.

d. No Real-Time Analysis

Users that facing cyber threats need a quick real-time analysis of the malware problems and potential solutions. Due to a lack of IT Experts, on-demand problem analyzers are hard to obtain.

To conclude, ACESO meets the demand for an alternative to the overstated price, the underperformance and the impracticality of current software solutions. The solution proposed by ACESO also creates new opportunities for cybersecurity experts to create revenue streams while continuing to help infected users.

2. The Aceso Solution

ACESO offers an innovative model changing the user behavior since it enables every user to independently control cyber threats. In contrast to existing providers who only offer a software product, ACESO developed a model that combines these products with security services.

ACESO allows users to save money on improper and unnecessary security software. In case of an malware attack, ACESO software will quickly act upon it, protecting the user. In contrast to existing anti-virus software, real-time and quick research for new and effective solutions is provided, since malicious software is determined as soon as it starts to spread.

Per attack, the user pays a small compensation – 1 USD in ASO tokens. This fee will be distributed using the ACESO distribution key between all the stakeholders that actively and effectively contributed to finding a proper solution for the infected user.

The ACESO solution is built upon two main pillars: malware detection & prevention and malware identification & removal. Both pillars of the solution feature innovating and progressive qualities compared to the existing cybersecurity market.

a. Malware detection & prevention

ACESO offers a security program that acts as an anti-virus detection mechanism. This software continuously monitors the computer for malware of any nature or size.

The scope and coverage of the detection by ACESO is therefore not limited to high-priority malware issues. Additional anti-virus programs will not become redundant. Whether the computer is infected with adware, spyware, joke programs, data-stealing Trojan, or any other unwanted programs that harm the performance of the computer or that cause inconvenience, the ACESO software will notify the user about it. Moreover, whenever a suspicious activity or file is detected, the user will automatically be helped to reach a solution.

Furthermore, ACESO also offers ransomware prevention using artificial intelligence. This function will be offered to all users for free. Users will be protected from ransomware infections, such as the famous WannaCry, which locked more than 1 million computers worldwide.

We also use the ant colony optimization algorithm (ACO). We were able to adapt this algorithm to our back-end servers for several purposes, primarily of which is to speed up the lookup functionality, as we need to detect and identify millions of files quickly. We were able to categorize files and put them in a particular graph like structure. By only using ACO, we achieved outstanding results for the lookup function in this structure.

For the purpose of empowering the simplest AI model to detect and remove generic, behavior based malware, we have also written a custom scripting language. By further developing the

scripting language and AI combination, we believe we will be able to reduce the necessity to check every decision made by a malware researcher. This is currently in the research stage.

b. Malware identification & removal

On top of detection, the ACESO service offers malware identification and removal. At this stage, the further development of the process depends on whether a customized solution is required.

ACESO has in-field experience within the anti-spyware industry since the ACESO team already founded WiperSoft, a spyware detection and removal program. Therefore, ACESO has prior knowledge about well-known malware and access to existing and ready-made solutions, which will be usable for ACESO users.

However, for customized solutions ACESO is developing an innovative service, featuring a community or network that is reunited on one anti-malware peer-to-peer platform. The platform will help infected users to decreases expenses of anti-malware while enabling others to provide customized solutions. The ACESO platform employs outside malware researchers, analysts and companies. Thanks to ACESO, the parties who contribute to finding a solution can further monetize their advice on malware problems.

If a customized solution is necessary, the acquired information will be stripped of any personal data and then sent to the Malware Analyst. This ensures the privacy of all infected users and the protection of their personal information.

There are four main players in the platform: 1) the End User, 2) the Researcher, 3) the Malware Analyst and 4) ACESO.

- End user – a user with an infected computer who requests a solution to the malware problem;
- Researcher – a user who provides samples of the malware;
- Malware Analyst – a user who analyses the samples and provides the user with a solution for the malware;
- ACESO – the mediator between end user and malware researchers and analysts.

The platform's accuracy, workability and trustworthiness are aided by the usage of a blockchain. A decentralized database is used to gather the anti-malware information and build extensive knowledge over time. The spread of malicious software is stopped as soon as researchers put samples about the malware on the ACESO blockchain, and as soon as the analysts can identify the malicious malware.

To smoothen and securitize the payment process, a token model is used. Tokens will be the main fuel for users to solve their malware issues through the ACESO network. The researchers and analysts will receive tokens as a compensation for their contribution. The fees paid by users will be distributed among the contributing researcher and analyst. ACESO will collect a part of the earnings to assure a well-managed and secure ecosystem.

Following predefined distribution key will be used:

- 30% to researcher
- 60% to analyst
- 10% to ACESO

ACESO enables synergies between all parties involved:

- Clients get higher value for money, saving them having to spend on endless software solutions;
- Researchers earn tokens by providing general blocks of information;
- Malware analysts earn tokens by identifying malicious blocks.

3. Pain-solution analysis

Our solution answers to all the problems and opportunities mentioned in the first section of this paper.

High security costs – Our solution enables to cut cybersecurity costs for our users using network effects. Cyber infections usually spread within the same geographic area and through the same security gap. These infections can be solved easily if all the infected users work together to find a solution for their common problem. In case one hundred users with the same problem pay $1 via the ACESO platform, $100 can be shared between the Researcher, the Analyst and ACESO.

Lack of IT Experts – Cybersecurity Ventures predicts that the cybercrime epidemic is expected to triple the number of open cybersecurity positions to 3.5 million over the next five years.

ACESO has proof of concept guidelines on how to spot and identify malware. ACESO will present step-by-step guidelines and video lessons to help new contributors obtain knowledge required for this field, training our own experts. There are also a lot of users who already have a good grasp in this field. They contribute in various forums for free and help people fix their computers. Via ACESO, they will start earning significant money on this activity.

Limited Coverage (70% of threats go undetected) – Big security software vendors are only quick and interested in fixing malware infections that are quite widespread, with at least a thousand infected users. ACESO, on the other hand, is able to solve the bigger and the smaller malware infections in a quick, effective and rewarding way.

No Real Time Analysis – Our general information blocks will hold necessary information to detect and distinguish malicious software. The blocks will be held in a decentralized network location. The stored information will be frequently updated due to the ACESO market. General information blocks will be constructed on users' machines, and placed on a decentralized network. Without the need of expensive anti-malware labs, the blocks will be categorized and activated for all users. In addition, Malware Analysts are incentivized to solve the issues as fast as possible because the first person with a solution will earn the most tokens.

6. The Aceso Framework

ACESO disposes of a proof of concept framework that confirms the expected viability and real-life success of the proposed solution. The framework counts four main components.

1. Distributed Malicious detection

ACESO provides a network of professionals who can distinguish malicious and non-malicious software by accessing prepared (depersonalized) information blocks. Furthermore, ACESO provides a service to minimize false positives in detection while merging professionals' judgments and input.

2. The market

Malware detection and distinguished information is stored in a separate decentralized blockchain supervised by ACESO or an independent company. Markets ensure that payments are made when a service has been correctly and completely provided. Supervision ensures that malicious software is not ignored, no personal information is leaked in the network and no false positive actions are made upon service requester.

3. The method

ACESO developed its own method from the ground up. The method enables people to share their worries about computer infections they incur with people who had similar symptoms. These informed or experienced people can share their knowledge on how to fix the problem. This method does not require powerful computers for wasteful computation to mine blocks. The main requirement is sufficient time to create and store general information in the network.

4. General information

Each block of the Blockchain contains general information about software installed on user's computer. The information helps to detect and destroy malicious software. Furthermore, it helps to prevent false positive situations. This information is stored in a decentralized way so that it is accessible at any time. ACESO supervises the information flow.

7. Business Model

The model of ACESO is mainly built upon network effects and peer-to-peer contributions. Each category of participant in the network is essential. Managing a good communication and workflow between them is essential for the viability of the platform.

End User – downloads the ACESO malware detection software and for each malware detected, the end user can choose to remove it from the computer by paying a small fee. The end user always has the option to leave the malware untouched and to not pay for the removal. The single threat management process in combination with full autonomy for the end user makes the ACESO solution stand out from its competition.

ACESO offers end users to pay an average of $1 fee per malware prevention or fix for their computer. Often the same infection spreads from the same security holes in the same geographical area. If hundred of users have the same problem, they can use the network effects ACESO offers by collectively submitting the problem to the ACESO platform and paying each a small fee of about one EUR/USD. The aggregate fee will then make it worthwhile for researchers and analysts to join the workflow for this fix.

Researcher – The Researchers are the first active component in the network. They make sure necessary information is gathered on the topics. Their job is to surf through the internet to collect new and relevant information. ACESO then provides a platform where people can just submit various files, system screenshots, schemes or drawings. No prior experience or knowledge is required to fulfil the function of Researcher. A Researcher profile is every person who is looking for an accessible online source of additional income.

Malware analyst – Malware analysts are the second active component in the network. Their job is to analyse the malware samples and provide the user with a solution for the malware in question. The profile of a malware analyst is every person that is already active in cybersecurity field or wants to become active in helping end users with their malware issues. An analyst usually has prior knowledge in the field. Moreover, ACESO disposes of proof of concept guidelines on how to spot and identify malware. With this knowledge, ACESO will provide step-by-step guidelines and video lessons to help new contributors obtain practical knowledge in the field to become a high-quality ACESO analyst.

Malware analysts will work with encrypted information. No personal data of the end users will be exposed to the analysts or to anyone else in the network.

ACESO – This ecosystem will be enabled, maintained and continuously improved by ACESO. To guarantee reliability, security and high quality for our clients, researchers and analysts, ACESO will make use of its fast-growing database of information on how to treat malware issues. To sustain this community, network and database, a fee of 10% per malware fix will be collected.

The peer-to-peer structure of the ACESO network is more efficient, effective and reliable than the current anti-virus and anti-malware software solutions that dominate the cybersecurity market. Furthermore, the knowledge stored in the ACESO database can be packaged and sold to other anti-virus companies and vendors. Research information on malware can be shared as last week's or last month's malware updates.

8. Token Model

The ecosystem will be fuelled by ACESO tokens for the payments between the participants of the platform. To enable an integrated and well-oiled ACESO token payment system, a tokens market will be created for clients to exchange tokens against knowledge and all-round malware solutions. The token model critically improves the protection of all our clients, researchers and analysts for payment and privacy purposes.

The use of a token model offers many advantages:

- A token model ensures a secure and integrated way for our users to pay for a malware solution. This model also secures an efficient and safe reception of the payment for our Researchers and Analysts.

- A token model does not only enable us to safeguard a smooth and ongoing payment process, but also solid protection of our End Users' privacy and personal data. The safety of token-based payments is structurally reinforced by the blockchain technology. The anonymity of the payment account of our End Users is an essential characteristic. This is especially interesting when a user's computer is struck by a malware infection. The identity of the End Users remains totally safe and unknown. No bank account or credit information is revealed for ACESO token-based payments.

- Another benefit to the ACESO token model is that it allows active management of the payment process and continuous supervision by the ACESO team. This is the only way to guarantee a fast completion of the process without banking restriction.

An essential benefit to a token model is the creation of a community. Counting on the fact that early participants in our ICO will become our first big pool of active members, it is always possible to continue issuing new tokens enlarging the ACESO community.

The operations behind the token model – To have access to real-time protection via ACESO or to immediate help and interference from the ACESO community, the clients need to first dispose of a number of tokens. The purchased tokens will be reserved and will only be consumed when the malware is successfully removed or help received. Purchasing them will also provide certain computer protection features, such as real-time file guard, network traffic control, parental control and ad blocker.

Whenever users purchase tokens and put them on the ACESO platform, they automatically get additional features, which include:

- File guard;
- Network traffic control;
- Parental control;
- Ad blocker.

These additional features will be active as long as the users hold the tokens.

Once the malware solution has been delivered to the user, the token-based compensation paid by the user will be distributed to the three parties involved, the researcher, the analyst and ACESO.

Researchers earn tokens only when they provide useful samples for a malware of which the solution has been requested. Analysts earn tokens when they provide a correct and effective solution to a malware problem. After earning ACESO tokens through these activities researchers and analysts will be able to exchange them on exchange services.

9. Blockchain Technology

ACESO uses blockchain technology to ensure two main things:

1. **Traceability and audit:** A blockchain is an append-only database where every change is publicly visible and traceable. This allows Aceso to trace every virology request as well as its funding from the users. People will be able to have a clear understand of what they are paying for and how their contribution empowers the development of the Aceso network.

2. **Democratic decision-making mechanism:** Traditional antivirus companies have all the power to choose which infection should be investigated over another. This is very opaque and undemocratic. We propose a vision where the people decide what are the priorities of such a company. We propose Aceso.

The ACESO is an ERC20 compatible token on the Ethereum Blockchain. However, ACESO will use a sidechain in order to guarantee speed and flexibility that a public ledger can't provide. The sidechain will store all ACESO specific information and will provide a state channel mechanism that will allow instant ACESO token transfers between the public blockchain and the ACESO sidechain.

In its essence, a sidechain is a secondary blockchain using a specific consensus algorithm that works in tandem with the main Blockchain. Its primary goal is to off-load complex and costly logic to a secondary chain, the side-chain, and only keeping the financial logic on the main chain. Aceso aims to use a sidechain in order to develop a scalable and responsive ecosystem.

Sidechains solve two main problems that decentralised Blockchains like Ethereum often have. Those problems are a low transaction speed and a high transaction cost.

- ***Low Transaction speed:*** Due to its parallelized architecture, Ethereum does not scale very well. Since the execution logic is distributed throughout the network, the network total transaction speed is bottlenecked by the slowest machine.

Additionally, there is a bottleneck cap of approximately 25tx/sec due to the nature of the Ethereum Virtual Machine (EVM) that cannot process blockchain transactions quicker. In a sidechain that does not use Proof of Work, block producers are known in advance such as the transaction speed can be linearly scaled with load balanced block producer nodes.

- ***High Transaction fees***: Ethereum is an append-only distributed database. Every modification is appended to the database as a transaction which cost needs to be paid by the transaction sender. This cost does not scale with the price of Ether such as complex smart contract logic can become very costly, up to 30$ per transaction.

Moreover, a secondary market with the price of gas, determined by the miners, can amplify the transaction cost. As matter of example, Ethereum gas cost went up to 200-250 Gwei per gas in mid-July. A sidechain does not have a cryptocurrency, or even if it does this cryptocurrency is not used financially. Which makes the transaction virtually costless.

Distributed malware detection is built on top of the ACESO sidechain. Clients spend tokens for malware detection; researchers and malware analysts earn tokens by growing the blockchain data and distinguishing malicious blocks from benign ones.

- ACESO supervises malicious files detection and filters requests using supervised markets. Clients and malware analysts set the prices for the services requested and offered and submit their order to the markets.

- The markets are operated by ACESO which supervises the information flow with its proof of concept method. It ensures that researchers have correctly stored general information, that malware analysts have correctly identified malicious software and that clients have received proper service.

- Researchers can participate in the creation of new blocks in the ACESO sidechain. They will be able to submit files to ACESO and earn tokens by doing so.

Decentralization. Decentralisation is very important for ACESO. Users decide where the funding should go and what the virology research should accomplish. Every user can submit a malware for inspection thanks to the ACESO decentralised software.

Independent malware analysts will be able to verify the information and ACESO will help to filter spam with their top-notch research team. The whole process is decentralised since it is initiated and verified by the community. The role of ACESO consists in purely ensuring the quality of the software.

10. The Ecosystem

This section explains the main players and operations active within the ACESO ecosystem. Anybody can join the network as a client, researcher or malware analyst.

1. Clients

Clients can at any time download the free ACESO detection software. This software checks for matching general information between computer and blockchain. Suspicious activities can be either matching information, either the software will suggest placing an order on the ACESO platform. The client retains at all times the option to respond to this suggestion or to not engage the ACESO market.

Clients can access an order via a 'Find' requests. After sending such a request, the client can opt for a continuous or single-use service. As 'client' can also be considered the joint networks that want to file a 'Find' request to identify their own generated general information blocks by our rules.

When an order is created on the platform, the participants in the market are notified about the existence of this potential malware problem. To identify general information blocks, the client can use the general information received from a Malware Analyst about general information blocks, or the client can sign an order with a Malware Analyst for a customized malware fix. At any stage before engaging with an external party in the market, the client has the option to close the order.

2. Researchers

Researchers generate general information blocks via the ACESO software. They provide new information streams towards the ACESO network via the 'Put' method. They can create new general information blocks or extend general information block by specifying more details. They set a price for this general information within specific limits.

This operation is the first step required to be able to earn tokens as a researcher. To guarantee high quality content for the clients, the general information must contain full descriptive information about malicious software. This information is approved by malware analysts or by the ACESO Company.

To receive research rewards, there must be a 'Find' request for this particular block by geographically different clients. The client willing to pay for this general information block is key to reward the malware analyst.

3. Malware analysts

The malware analyst identifies and distinguishes new general information by confirming the general information contents earlier provided by a researcher.

Malware analysts can ‘accept’ requests and get rewarded if this information provided by researchers is correct. Likewise, if the information proves to be incorrect, a penalty will follow.

Analysts can also earn tokens by accepting an order and a price from the client. Their job is to distinguish general information provided by the client on the platform. For transparency reasons and to incentivize the analysts, ACESO acknowledges and distributes trust points to analysts depending on their performance. Trust points and pricing for a certain service will help the clients to choose certain analysts on the market.

4. Workflow process

One malware fix workflow could have the following outlook:

1. An end user places a bid on the ACESO MARKET.

2. A researcher provides samples and detailed information to the ACESO market.

3. A malware analyst finds the provided samples and determines whether they are malware or non-malware samples. If necessary, the analyst provides more detailed information.

4. The malware analyst makes a deal with a user for further malware investigation if necessary. The user determines which compensation she/he wants to pay.

5. ACESO compares the bid from the user with the market. If the users’ problem is marked as malware, ACESO will communicate the possible solution and eventual fee as agreed upon towards the end user. This fee is divided between the Researcher (30% of the fee), Malware analyst (60% of the fee) and ACESO (10% of the fee). After each solution is executed successfully, the information gathered on the market will be stored on the ACESO Malware chain.

6. An anti-virus company wants to buy information about a certain malware. The company offers a price in return for the required information. This income is divided between the Researcher (30% of the price) and the Malware Analyst (60% of the price). Tokens are given as soon as the full information is provided. Also, the information in the ACESO database could be sold to anti-virus vendors as packages containing research information and the ‘latest malware updates’ from last week/month.

5. Marketplace

Movements on the market are fully influenced by participants placing:

- ‘Find’ requests for general information blocks;
- ‘Put’ requests for new general information block with a pre-calculated price;
- ‘Accepts’ a general information block and pushes it to the ACESO blockchain;

The market is actively used to create orders and to monitor the state of these orders.

6. Blockchain

The blockchain has multiple uses within the ecosystem, since for each new block, it:

- checks if the block is in a valid format;
- checks if the block contains all the necessary general information;
- checks if the block contains unique information;
- checks if the block is supervised;
- checks if all transactions are valid;
- checks if all orders are valid;
- discards a block if any of the above fail.

The ACESO system works with 3 target groups: client cycle: put – get, researcher cycle: put – get, malware analyst cycle: put – get (see Figure 1).

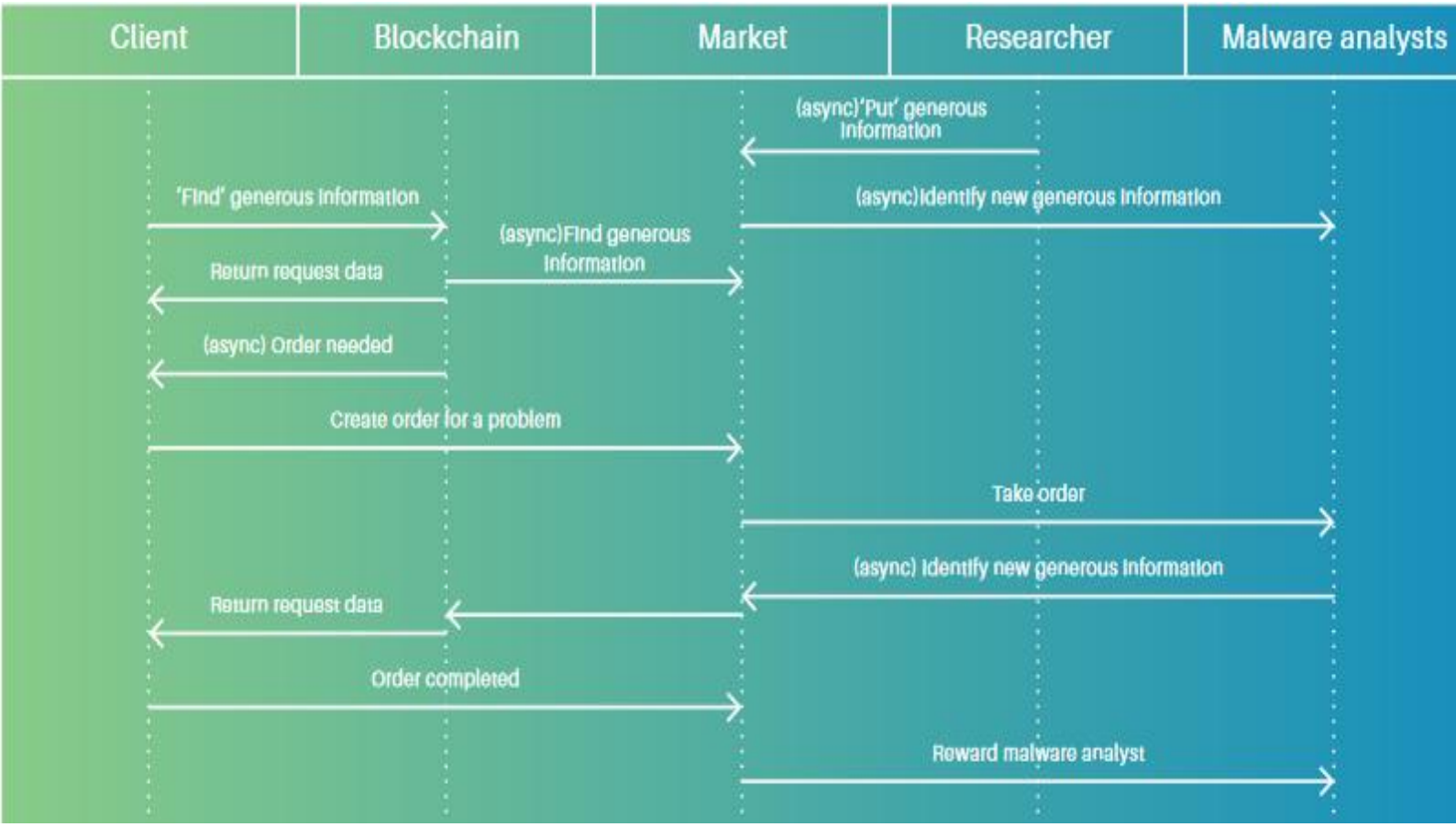

Figure 1. The sketch of ACESO system

11. Distributed Malicious Detection

ACESO proudly presents the notion of distributed malicious detection (DMD). The DMD scheme aggregates detection offered by multiple independent cyber security professionals and companies. DMD employs a decentralized structure while ensuring active supervision by an experienced institution, ACESO Company.

Several strategies are possible for detection, reaching from a simple hash algorithm to even intuition. (see Figure 2):

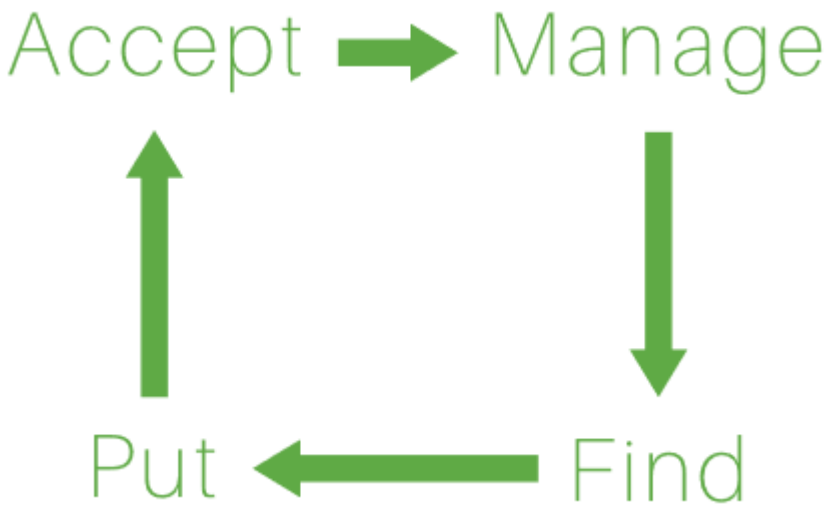

Figure 2. Summary of DMD scheme for clients, Malware analyst and ACESO

- Find (data) → Client executes a 'find general information' request to receive information about the existence of malicious software;
- Put (data) → Researcher executes a 'put general information' request to put information about software and earn coins;
- Accept (data) → Malware analyst confirms general information being good/bad;
- Manage → ACESO manages the network of participants via the Manage protocol. The Manage protocol helps to audit and supervise participants' actions and data integrity.

This scheme must guarantee general information integrity, confidentiality of personal information, early false positive prevention and equitable reward.

1. Early Detection and Real-time Analysis

The ACESO solution provides early detection and real-time analysis. Both are a result of the structural framework used by the ACESO solution: a pragmatic combination between market-based decentralized detection sources and decentralized information storage.

To fully understand the current demand on the cybersecurity, it is essential to distinguish two types of malicious software: 0-day (zero-day) and forgotten clone. A zero-day exploit is a cybersecurity attack that uses a security vulnerability the same day that vulnerability becomes known to the public or to the vendor or software provider.

In case a zero-day malicious software has just started spreading, millions of computers have been infected. The main anti-virus companies, however, have just started investigating where this software malware came from, what it does and how to stop it. Moreover, if the zero-day appears to be not aggressive, it will be classified as a low-priority research object, called forgotten clone. Only when there is considerable interest on the internet, the main anti-virus companies will start to classify the problem as a malicious software worthy of their time and attention. This, however, often does not happen earlier than a few days or weeks after the attack. Currently, forgotten clones are plentiful, receiving very low to no attention from anti-malware providers. Forgotten clones are just as dangerous as 0-day malicious software.

The ACESO solution meets these demands effectively. Both types of malicious software can be resolved, as the DMD architecture guarantees early detection and real-time analysis.

ACESO makes sure that any emergency is detected as soon as possibly, irrespective of its size, impact or type and that this problem gets notified to the user of the infected computer. That way ACESO enables proactive malware prevention, e.g. preventing zero-day malicious software to become operational. ACESO will even be able to geo-localise the potential emergency, allowing to alert the targeted region well up front.

2. How does it work?

Thousands of researchers will generate and submit information blocks to the ACESO monitoring systems. When there is a new block or a group of blocks with similar characteristics, ACESO is able to detect possible suspicious or malicious software which is capable of causing cyber threats.

In addition, thousands of professional cyber experts will get a chance to earn tokens by analyzing new information, stored and accessible on the decentralised ACESO database. By the time users are informed about the threat of a cyber-attack on their systems, ACESO will be able to simultaneously offer a practical solution. The user receives thorough information, a report: where the cyber threat came from, when it started and what damage it has done.

This way, other users are protected as well, and simultaneously help is provided to those users who have suffered damage. All this is possible due to our innovative User-To-User system.

Regarding the forgotten clone, ACESO offers an efficient and effective solution to the current thousands of other malicious software versions emerge every day. Some of these successfully carry out destructive actions, infecting millions of computers. Some of forgotten clones

"hibernate" and wait for the time to start activity. Using blockchain technologies, no single malicious software will become forgotten any longer. Its general information block is in the ACESO memory and when it restarts, ACESO can detect it again. A forgotten clone can revive with new details but even a modified version retains its nucleus and principles of activity. In essence, ACESO identifies it through rediscovery. Also for this activity, ACESO will reward researchers and malware analysts.

3. False positives

ACESO maximally reduces error probability. If the Put-Accept method is used by just one single user, the probability that the solution is wrong is 50-50 as only one expert has delivered a judgment. However, if the judgment of 1,000 professionals regarding a single general information block, the probability of an error, a false positive, gets highly reduced.

The market-approach, allows ACESO to rate professionals. Malware analysts with multiple errors on their name virtually damage their reputation on the market. Those with a high number of correct decisions and judgments increase their market value and reputation. This rating systems creates a variation between the analysts' level of experience, enabling the clients to decrease the possibility to error to a minimum.

General information contains very important data that helps to automate the process of distinguishing malicious software. Using the Naive Bayes algorithm in combination with data from general information blocks, ACESO can determine the character of information placed in the blockchain in real-time. However, if case of any doubts, ACESO uses the help of malware analysts. ACESO classifies the information contained in general information block (see Table 1).

Class	Malicious?	Safe?		
Network	3	1	=4/12	0,33
Hash	5	0	=5/12	0,42
Substrings	2	1	=3/12	0,25
Total	10	2		
	=10/12	=2/12		
	0,83	0,17		

Table 1. Likelihood table

This table does not reflect how many malware analysts voted for a particular general information block. It shows that not all analysts agreed with the given data pointing to malicious software. This is an acceptable situation. In a later stage, ACESO can calculate the probability of an error and decide upon rewards and penalties.

With the table above, it is possible to predict a 0.72 probability that this general block contains malicious software information. ACESO's partners use this formula to avoid false positives as much as possible. However, in the future, when a voting right is granted to a large number of malware analysts, the formula will be changed accordingly.

12. The Market

Market plays a significant role for the user who wants to access the service and also for users who want to earn. For the sake of simplicity, we can split the market into four segments: Client market, Put market, Pro market, and Supervisor market. All regular users, depending on what they are trying to achieve, can simply join/use the first three market segments. The last segment of market is for closed networks that want to get access to information, approve it and use it in their own services. (See Figure 3)

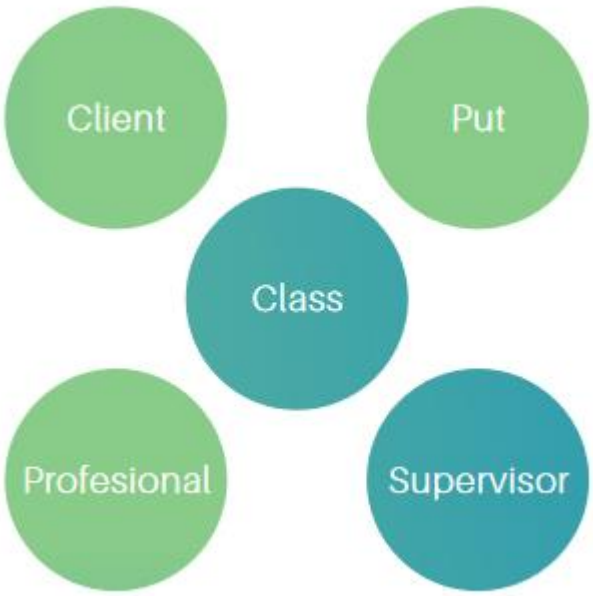

Figure 3. Users' roles in the market system

1. Client Market

The program we present is 'pay for the service, not for the software'. A user who suspects that his/her computer could have been a victim of cyber-attack can acquire a short-term service that eliminates malicious software. Even if there is 0-day malicious software in his/her computer, the service we provide will help him/her by using the support of malware analysts' community. But we recommend our users to purchase service tokens before a cyber-attack takes place. In addition, our client has a possibility to purchase tokens from the devices she/he uses (cell phones, tablets, and other computers).

There are situations when a user gets infected with malicious software that has not spread widely yet. In such cases, it is more difficult to get help. Thus, we offer a bid on the market, which would help solve the problem faster than usual. A client pays with a ACESO token, which can be bought on our sales, or on the market.

Ps is the price that the client pays for a service. There are two types of services: one-time service, just to find and fix problems, and continuous protection service.

Pm is the price that the client is willing to pay to a malware analyst to identify his/her computer problem.

The formula how to determine a price is the following:

M min<=Pm<=M max

M defines market price, meaning, a user cannot underpay and overpay for a service.

2. Put market

Certain users could be assigned to a higher risk malicious software group (aka those who are more prone to getting infected). These users can make use of that increased risk. They can easily put general information blocks generated by our market after having browsed unsafely, or after having installed unknown software. As soon as those blocks are identified on demand, rewards are paid to clients who placed them. However, ACESO does not want to encourage users to infect their computers on purpose.

There are two periods: – 30 days. ΔT7- 7 days and ΔT30 – 30 days. This means that if the general information block is used within the first 7 days, a researcher will receive 30 % of income, if in 30 days – 20 %.

The formula how to calculate income:

$PM_{put} = \sum$

ACESO equally divides the income between all researchers $PM_{put} / \sum M$. Each researcher receives 30% or 20% depending on their block put time. This market does not require good knowledge about computer processes or the cyber security industry at all. All a researcher has to do is run a program that monitors the computer state and generates general information blocks for the ACESO network. For this action and contribution, a researcher can get rewarded in tokens.

3. Pro market

This is a higher level of users group. It includes users knowledgeable about the cyber security market and who can earn tokens from how they can recognize information in a general information block. One does not need to infect computers on purpose, it is suicient to identify and find similarities.

Cyber security professionals will earn rates for their work. The higher the rate, the higher the trust. Additionally, professionals will earn tokens for their work: they will get 60% for general information block identification and 90% for a service paid by a user.

We calculate the 60% of income based on this formula:

$PP_{accept}=\sum$ Ps/Gb

It is very similar to the Put marker formula, except that we define the number, how much identifications we need for a general information block. We model this number by calculating prediction, described in 4.2 False positives section. We also define that this is always true:

$PM_{put} < PP_{accept} * 1.6$

This means, that the pro market will always receive the same quantity of income as the put market.

4. Supervisor Market

The last but not the most important market segment is ‘supervisor market’. It funds ACESO subsistence and development of activities: improvement and purchase of equipment. This segment of the market solves emerging problems and rates malware analysts. Thus, we create a small market on the market. Users buy services there; market supervisors, who take small shares for maintaining the order, work there; a blockchain, which takes its share for data storage and processing is also there.

13. The Method

We have developed and expanded a method of malicious software detection and prevention that has been successfully used for several years. In general, ‘The method’ includes distributed malicious software detection, the Market and General information blocks. The innovation of the method we have developed is that it is easily scalable. But it is reduced in such a way that one company can successfully manage it with the resources it has. In addition, there are no clear limits where market participants are and what has to be rated and rewarded. We seek to expand the method to such an extent that we could become just observers, and all the power is focused on technology (general information blockchain) and the user-to-user intellectual capital.

This is how we would scale the method we worked out:

- A client who has a valid token has the option to use the service. It does not matter if s/he needs the service now or will need it in the future; s/he can use the service as long as s/he has a valid token. Depending on the type of selected service, s/he either needs to have the software to access the service or does not. The system works in a simplified way: there is no need to pay for software, it is provided as an addition. The payment is for a service, just like for electricity or telephone connection.

- A client can supply his/her service program. We will scale this method until independent cyber security providers have a possibility to check/find the general information block and determine which category it belongs to. · We offer an external market, i.e. User-to-User will identify a general information block. We, as observers, will make the final decision about the inclusion of information into a blockchain. While moving this segment we will try to speed up identification, to prevent situations when unknown malicious software is spreading, and one has to wait for many days until the main AVs include it into identification systems.

- The algorithm we have developed has no limits to generate general information blocks. It means that in the future, it will easily integrate or expand to more complex ones, which will be able to accumulate more information, but at the same time, it will outstandingly implement backward compatibility.

14. General information blocks

General information blocks containing precious pieces of data are stored on the blockchain. These blocks are uploaded by researchers. Their integrity and correctness are confirmed by malware analysts. ACESO carries out only the actions of monitoring to make sure that a blockchain is not damaged while making a decision about the type of general information block.

For the sake of simplicity, two types of general information can be considered: static and dynamic. Static general information can be a hash string for a program or program group, substrings of a file or even a URL address. A dynamic information block holds behavior description. It is captured in time, monitoring particular program behavior.

It possible to imagine a computer infected by malicious software that activates itself only when the computer is in the idle state for quite some time, like many office computer overnight. The malicious software continuously checks for URL addresses generated by a specific algorithm. While the requests might not seem suspicious for regular office administrators or antivirus software programs, ACESO will perceive also this activity as suspicious. This detailed detection mechanism is crucial to make general information blocks. ACESO creates behavior information blocks and asks for identification from a malware analyst. Since this block of information came from a user who paid for the service, there is a countable budget for identification. The sooner a professional identifies this behavior as malicious, the sooner a reward can be received. This also increases the received rating.

ACESO uses blockchain technology since the high expansion rate and increasing complexity of the cybersecurity market. ACESO believes such amounts of vital information cannot be placed in one centralized location, as it does not offer sufficient protection in case of an unforeseen cyber-attack.

15. Smart Contracts

ACESO provides three basic functions to the end users: Find, Put, and Accept. These functions allow clients to find (merge, compare), put and accept general information to the markets at their preferred price. While the functions cover the default use cases for ACESO, more complex operations can also occur using smart contracts.

Smart Contracts allow ACESO users to expand the functionality of the market. In these contracts, the use of tokens can be (re)defined and the possibilities of data use can be expanded, while ensuring integrity. Users can interact with each other via smart contracts. They can send transactions to the ledger that trigger function calls in the contract.

ACESO employs a smart contract system to support specific operations: from accessing support contracts specific to a general information block, as well as more generic smart contracts.

For general contracts, ACESO allows users to program the conditions for which they are offering general information. Several examples are worth mentioning:

- contracting malware analysts: clients can specify in advance the professionals offering the service without participating in the market;
- payment strategies: clients can design different reward strategies for the malware analysts, for example, a contract can pay the malware analyst increasingly more through time, another contract can set the price of service informed by a trusted oracle;
- ticketing services: a contract could allow a client to deposit tokens and to pay for service on behalf of their users;
- more complex operations: clients can create contracts that allow for general information update.

16. System integration

ACESO is developing tools that will smoothen the integration of the ACESO blockchain with other systems, in both directions.

- ACESO on other platforms: although there are not many other blockchain systems with cyber security functionality, ACESO is developing an interim interface to integrate ACESO functionality and to expand limits. Offering custom solutions for practical integration of the ACESO system on other platforms, is a strategic move to increase competitiveness and availability of ACESO services. It also provides a higher degree of freedom to the users.

- Other platforms in ACESO: ACESO is developing an interface for other systems offering their services and working with blockchain technology.

17. Business Strategy

Complete Business Plan and 5-year cash flow are available upon request. Below are the main points only.

1. Market Overview

The cybersecurity market offers huge potential on a global scale. Cybersecurity Ventures predict that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. Global spending on cybersecurity products and services will exceed $1 trillion cumulatively from 2017 to 2021. This is 12% - 15% year-over-year growth through 2021.[1]

Study published by Bank of America Merrill Lynch suggests that there are close to 400 new threats created per minute, with an estimated 80-90 million threats per year. Additionally, the study suggests that over 70% of these threats go undetected.[2]

State of Malware Report 2017 highlights the increase in Ransomware threats, in both, the corporate and consumer environments.[3] While traditional malware such as banking Trojans, spyware, and keyloggers requires cybercriminals to oversee multiple steps before revenue is delivered to their bank account, ransomware makes it a seamless, automated process.

Research of the March & McLellan[4] states Asia-Pacific (APAC) is the ideal environment for cyber criminals to thrive in because of high digital connectivity in contrast to low cybersecurity awareness, growing cross-border data transfers, and weak regulations. Beyond legislations, governments can further mitigate cyber risks through public/private information sharing, development of cybersecurity knowledge hubs, and growing the talent pool.

According to IBM X-Force researchers[5], malware facilitates the most prolific type of cybercrime attacks in Brazil. Because Brazilian malware tends to be less sophisticated than malware made in Eastern Europe, cybercriminals in Brazil compensate with attack volume. Brazil's large population includes many internet users with relatively low security awareness, along with large amounts of enterprising cybercriminals.

In regards to the B2C segment, due to internet connectivity and services becoming available in more parts of emerging markets, many people are accessing online services for the first time. Security is often an afterthought to new internet users, increasing their chances of becoming victims of cybercrime. Besides low cybersecurity awareness, another big concern is the lack of low cost anti-malware protection solutions. Most anti-malware programs cost around $40, with the cheapest high-quality protection just below $20.

The B2B Cybersecurity Market will be worth $22.79 Billion by 2023[6]. The major factors driving the growth of the industrial cybersecurity market include:

- Increasing government funding to improve the cybersecurity of the industrial environment;
- The growing incidents of data security breaches due to the rising number of connected devices in industrial control systems.

2. Competition

Global market share held by Windows anti-malware vendors in 2018 is led by AVAST with 19% market share. The other 2 big players with more than 10% market share are ESET and Malwarebytes.

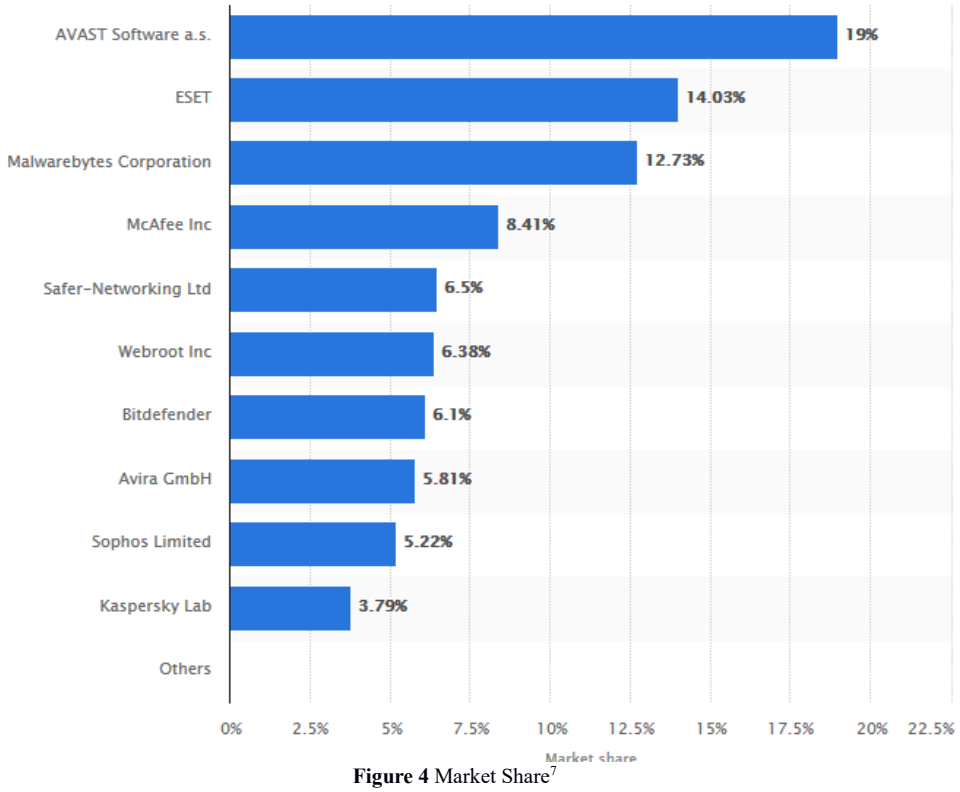

Figure 4 Market Share[7]

B2C. Looking at the product composition and marketing strategy, ACESO's main competitor is Malwarebytes.

For a few years, Malwarebytes offered its product for free to capture the market share. In recent years, they started to monetize it. Now, their premium product with the same functionality as ACESO costs $39.99 per year.

ACESO has 2 advantages compared to Malwarebytes and other anti-malware market players:

1. It focuses on a different market segment;
2. It offers low price solutions.

Different market segment. The nature of a threat is that it infects multiple computers. Due to the enormous malware amounts, major AV companies are only quick and interested in fixing malware infections that are quite widespread, with a thousand infected users at the very least. Dealing with less widespread infections is not profitable due to the limited number of in-house researchers and analysts.

By focusing on infections that affect less than 1000 computers, we will avoid competition from major anti-virus companies. Due to the innovative business model, it is beneficial for us to consider infections that have affected as little as 100 users.

Low price solution. Based on the same anti-malware protection features (real-time protection, on-demand malware scan, behaviour-based detection, ransomware protection), the main ACESO competitors are listed below.

Bitdefender	$44.99
McAfee	$44.99
Symantec	$49.49
Webroot	$18.99
Kaspersky	$39.99
Malwarebytes	$39.99

Figure 5. The Best Malware Removal and Protection Software of 2018[8]

The cheapest anti-malware solution starts from $20 per year, and costs around $40 for premium brands. Considering all possible discounts, we can say it cost around $30 per year. None of the competitors can offer a pay-per-fix model.

Even more, comparing the average threat number per year (which, based on our 1 million user data, is 5), we can see that the yearly protection cost using ACESO would be $5 on average. That is 83% less than the average and 73% less compared to the cheapest solution.

We also ensure that the end user will not pay more than $10 per year, no matter how many threats will infect the PC. From our 1 million+ users, we see 10+ threats per year is a rare case. This will help increase trustworthiness among users and ensure low cost protection.

Due to the focus on low spread threats and low-cost solutions, ACESO does not have any true competition, making this an innovative business model twinned with a **blue ocean** strategy.

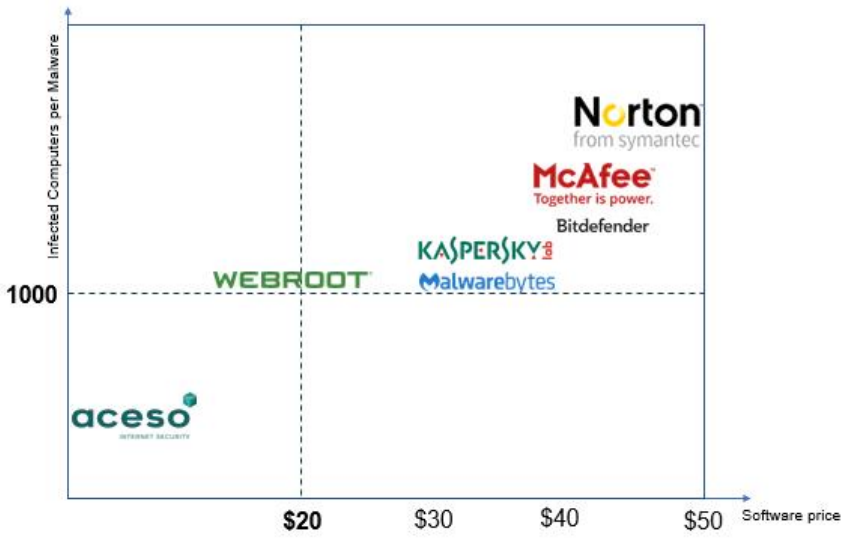

Figure 6. Competition landscape

B2B. Sophos is a leader in security and data protection with 300,000 B2B customers. It will be ACESO's direct competitor.

In 5 years, ACESO aims to capture 13% of current Sophos B2B market share. Last year Sophos grew its customer base by 40,000 and improved sales by 22 per cent to $769m[9]. ACESO aims to acquire 35 000 SMB customers in the 5th year of activity.

This is a safe approach, because due to the growth of the cybersecurity market and planned government activities in emerging markets, optimistic outlook is much greater. Our B2C presence in emerging markets will help to establish our brand awareness and allow us to enter the B2B segment easier.

3. Target Audience

ACESO offers both B2C and B2B solutions. Initial launch will be made to the B2C market, where innovative solutions will secure a fast user base and malware sample growth. This will allow to establish brand awareness and help create a sufficient malware database, which is necessary to become competitive in B2B market. In the second year of commercial activity, ACESO will enter the B2B market and will primarily target the SMB market, which will become the main revenue stream in the long run.

a. B2C Audience and Monetisation

By doing multiple pricing tests for 1 million+ freemium WiperSoft users, we have found that the most price sensitive users live in Brazil, India, Thailand and other emerging markets. That fits our innovative business model well, as our price will be $1 per fix. Freemium WiperSoft users have already expressed interest in low cost solutions. Based on the data from price modelling and testing, existing user base should secure $1,9 million in revenue immediately after the product is launched.

New users will be acquired using marketing funds. Our CEO has 8 years of experience in cybersecurity marketing, managing as big as $2 million marketing yearly budgets. This knowledge allows us to state that the first year Cost Per Acquisition (CPA) will be up to $3 per new user.

Based on the Growth Hacking methodology, in the following years, we will focus on the most efficient marketing channels to rapidly decrease CAC costs, until we reach the optimum $1 CPA. This is projected for the 3rd year of activity.

User base	Year 1	Year 2	Year 3	Year 4	Year 5
Existing End Users	300,000	443,333	800,333	1,728,942	3,415,397
New End Users	333,333	700,000	1,669,583	3,150,197	4,396,263
Total B2C users:	633,333	1,143,333	2,469,917	4,879,139	7,811,660

Figure 7. B2C Users

There are 2 monetisation streams:

1. **Initial scan**. Every new user upon joining our network will have to scan their computer to ensure that a clean user is entering the market. Based on data from our 1 million users, we know that there usually are more than 3 malware threats after the first scan. Our USP (Unique Selling Proposition) is $1 per fix, but in order to not scare off new users, we vow to not charge more than $3, even if more than 3 threats are identified.

    - *Scenario 1*: a new user joins the network, and during the initial scan we detect 15 threats. We will remove all 15 threats but will charge only $3.

    - *Scenario 2*: a new user joins the network and during the initial scan we detect 2 threats. We will remove both threats and charge only $2.

WiperSoft's malware database will be integrated into ACESO, so when a new user joins ACESO and his/her computer is scanned for malware, all funds will go to the Aceso company.

2. **On-demand fix**. All existing users in the market will be charged $1 per fix. Based on data from our 1 million users, we can judge that a user is affected by 5 threats per year on average. It's $5 per user. ACESO will get 10% of that amount (90% will go back to the community), which means ACESO will get $0.50 per one user.

Revenue per User	Year 1	Year 2	Year 3	Year 4	Year 5
Initial Scan&Fix, $3	$1,900,000	$2,100,000	$5,008,750	$9,450,591	$13,188,790
On-Demand Fix, $0,5	$158,333	$239,167	$441,906	$943,226	$1,817,605
Total B2C revenue:	$2,058,333	$2,339,167	$5,450,656	$10,393,816	$15,006,395

Figure 8. B2C revenue

We are looking at a 30% yearly churn rate. This is our pessimistic scenario, but we want to be sure our cash-flow numbers are on the safe side.

b. B2B Audience and Monetisation

ACESO solution is being developed to fit two different B2B market segments:

- **Closed Enterprise Solution (1000 + computers).** This solution is offered to military, government or big corporations, where strict rules for privacy and data breaches are highly important. This type of solution has a one-way connection to our backend services and only requests for product/malware database updates. This solution requires additional technical staff to work with our product because he/she needs to monitor inside computer status, read incident reports and act when unknown malware is found.

We are already in discussions with potential clients and are negotiating their needs (https://www.etic.lt/en).

- **Open Solution for Small/Medium business (5 – 999 computers)**. This solution is more relaxed. There is no need to have an additional person because we cover that. This solution is not strict, so the communication to our backend services is done in

tuple way: we capture incidents of unknown malware, we update program/malware databases.

When entering the B2B market, good connections within target markets are necessary. ACESO will introduce its B2B solutions to the emerging markets with the strongest B2C presence first. In the first year of operation in the B2B market, we will allocate $500 CPA from our marketing budget. The allocated CPA will decrease in the following year by 30% and will eventually reach an optimum $250 CPA.

We see major expansion into the B2B markets in year 3 due to high B2C product penetration, brand awareness and optimum CPA.

User base	Year 1	Year 2	Year 3	Year 4	Year 5
SMB	Development	1200	4900	15675	35756
Enterprise Solutions	Development	4	15	29	46

Figure 9. B2B client base

- Enterprise Solution revenue potential: $350.000 per company (15-20 EUR per computer).
- SMB Revenue potential: ~$2.000 per company per year (~25 EUR per computer a year).

Revenue per User	Year 1	Year 2	Year 3	Year 4	Year 5
SMB, $2k	$0	$2,400,000	$9,800,000	$31,350,000	$71,512,500
Enterprise Solutions, $350k	$0	$1,400,000	$5,250,000	$10,237,500	$16,078,125
Total B2B revenue:	$0	$3,800,000	$15,050,000	$41,587,500	$87,590,625

Figure 10. B2B revenue streams

We receive a lot of interest from **Internet of Things (IOT)** related businesses**.** Considering the big scope we already have, Aceso IOT protection is not included into the roadmap, and might be developed only based on a separate contract and additional funds to our ICO.

Once our roadmap obligations to the ICO investors are met, Aceso IOT protection development might start, which would include a host firewall, device and configuration control, file integrity monitoring, intrusion detection, operating system hardening, application whitelisting, automatic sandboxing, and many more features.

18. History and Team

ACESO founders own the anti-malware software WiperSoft and under the Intellectual Property agreement, ACESO is using WiperSoft's engine.

WiperSoft. When it was first launched in November 2015, WiperSoft was free for home users. In the same year, it was downloaded more than five thousand times, with one thousand users registered on our system, who were able to use WiperSoft to its full functionality. Over the next year, the program's detection and removal functionalities were improved, the scan engine was re-created, and it was launched with a new design. Coming back with a modern look and an improved user interface in 2016 October, WiperSoft became a paid a version for home users.

In 2016, WiperSoft saw a considerable increase in downloads. Compared to 2015, the program's download rate increased by 4600%, with more than 230 thousand downloads. 850 users worldwide purchased the license in that year. In 2017, the numbers continued to go up, with over 1.1 million downloads and 8 thousand sold licenses. While the program was used in more than 100 countries in 2017, the majority of downloads, 60%, were made by users residing in Europe, 9% were made in the US, and 20% in Brazil. We are expecting a similar growth in users in 2018.

We have more than 20 thousand active users on a daily basis, 4,5 thousands of which are scanning their computers. Since WiperSoft was launched in 2015, its threat database has grown very quickly, and users are now protected from 16 thousands threats. Every month, WiperSoft detects more than 18 million infected items (files, registries, browsers extensions, etc.) on users' personal computers. Overall, since its launch, WiperSoft has removed more than 200 million infected items from users' computers.

In 2018, ACESO, along with technical documents and the whole structure started being developed. In 2019, when ACESO is released, WiperSoft will become the part of it.

The ACESO team. The team that is developing ACESO is the same team behind the WiperSoft. ACESO's malware track engine has already been developed. In addition, ACESO has created the proof of concept method, which will help to identify and track malware as soon as it starts spreading. Our goal is to expand it to the extent that it will become a blockchain principle service and will be accessible to every user, every day. We want to remove the limit, where malware identification and removal is defined with a profit margin by major companies.

Romualdas Cukuras

Co-Founder / CTO

Co-Founder of ACESO, already created 4 malware/spyware removal software. 10+ years of experience in software development and apps. CEO and Core Developer of WiperSoft antispyware. Co-developer on cellular network GSM/3G, network inspection, embeddable scripting language and other projects.

Mindaugas Sinkevičius

CEO

Having worked and consulted for LionBridge and Fortune 50 companies, professional services firms and startups across diverse industries, Mindaugas can boast 8 years of experience in data driven Marketing, Product Management and Market Research.

Giedrius Morkūnas

Head of Growth and Marketing

Co-Founder of Riard. With 13 years of experience working in both start-ups and Fortune 500 companies, he is also involved in the Lithuanian Marketing Association. Board member in Lithuanian Marketing Asociation (LiMA) and member of LiMA Blockchain Marketing group. SEO and Growth Hacking trainer.

Povilas Jurna

Lead Blockchain Developer

As a specialist in blockchain, Povilas has successfully started ICOs like SpectroCoin, an all-in-one solution for Bitcoin, and Bankera. As a developer, he has strong technical, analytical, architectural and communication skills, and is willing to help the team, as well as share his knowledge.

Jonas Krikštopaitis

Cloud Specialist

Over 10 years of professional IT expierience in local and international companies including Barclays. Jonas took part in major project developing and supporting secure scalable and resiliant platforms for self-service consumption. Provided hosting integration for AWS cloud, VMware, Nutanix, Red Hat Openstack and other internal service hosting solutions. Skilled in IT service management and big-scale projects technical delivery.

Milda Morkūnienė

CFO

With the extensive experience on treasury management as well as cash-flow and investments management for international companies, Milda will look after business and financial planning, cash-flow planning and forecast, financial reporting and treasury management.

Marius Sinkevičius

Lead Database Developer

With experience as division team lead in Technologiju ir inovaciju centras, Marius will serve as the technical lead in database-centric software development projects of moderating-to-high complexity. As team lead, he will also be responsible for hands-on software development and design, as well as creating and updating ACESO project plans and/or task checklists for assigned projects.

Gintarė Edintaitė

Head of Human Resources

Gintare is currently a PHD Lecturer at Kaunas University of Technology. Gintare believes that the team is the most important component of a successful business, and she will ensure this success in ACESO as Head of Human Resources.

Marius Vizbaras

Lead of Technical Support

Marius is currently involved in projects for Evo-soft Ltd, a leading UK Microsoft Gold Enterprise Resource Planning Partner. As Lead of Technical Support in ACESO, Marius brings experience in secure software engineering, vulnerability analysis, digital forensics, and reverse engineering. He is experienced in developing software for a wide range of platforms, from embedded microcontrollers to large distributed systems, as well as in reverse engineering a variety of targets, and performing threat analysis on malware samples.

Tomas Zuklys

Lead Software Engineer

Tomas is Full Stack Java Team Lead at CUJO AI, which offers Internet Security Firewall for home users and a modular package of services for Network Operators. He can boast more than 10 years of experience in developing software for local and international companies, as well as 5+ years on technical leadership with architecture responsibilities. As lead software engineer in ACESO, he will help deliver cutting-edge research using partial homomorphic encryption applied to network signatures, and audit thousands of lines of code for security vulnerabilities. He will also create a variety of custom-designed binary applications, each possessing deliberate vulnerabilities, which will be used to test the efficacy of automated programs analysis tools.

Vaida Kardokaitė

VP of Community Management

While working for a wide range of organizations, both small start-ups and worldwide brands, Vaida has gained valuable experience in working and consulting in digital marketing, community management and content creation.

João Leite

Community manager

Working with several blockchain projects for half a year. Founder and manager of a crypto community. Cybersecurity degree with Cisco CCNA certificate.

ADVISORS

Fabio Cardoni

Blockchain & ICO advisor

Serial entrepreneur, business development strategist. Trading and investing in cryptocurrencies since 2012. Member of the Jur network, advisor for lympo, carVertical and BIT. Previous experiences: Founder & CEO of The Black Douglas Motorcycle Co., Tessier (Founder & CEO), Chilworth Technology.

Shahar Namer

ICO Advisor

Shahar is an early Bitcoin investor and the founder of The ICO Rocket. He co-founded a London based Venture Capital Fund together with the former CEO & Chairman of Warner Music International (sushivp.com). Shahar also built from scratch 3 international startup accelerators in London and in Israel, the "Start-up Nation" including StartupBootcamp.org which currently has 17 startup accelerator programmes across 11 countries.

Paul Cliffe

ICO Strategy Consultant

CEO of Block Venture Project, a company with the primary aim of creating a bridge for traditional investors to gain exposure to crypto-assets through risk managed, diversified funds which help to expand efficient frontiers for their portfolios. Paul's musings on bitcoin and other such crypto-assets have been featured in Yahoo finance and he is a regular contributor to such sites as cryptotelegraph.co.uk and cryptocurrencyhub.io

Lora Yessenova

Head of Investor Relations

Senior Partner at the world's first Underwriter for Initial Coin Offerings at The ICO Rocket The ICO Rocket brings a global wealth of knowledge, experience, and expertise in cryptocurrency issuance, ICO marketing and token presale capital raising.

Vadim Toptunov

Cybersecurity Advisor

A cyber security professional, possess 18+ years of experience in information and cyber security planning, servicing, management and consulting. Advocating crypto economy since 2011, contributing, investing, advising and securing various blockchain related projects.

David Lofts

ICO Strategy Consultant

David is a Brand Architect with a solid background in global consumer marketing with organisations like BAT, Mars, Chrysler JEEP, Lloyds Group, Saudi American Bank & AXA. David now works exclusively in the field of ethical start-up funding for blockchain businesses. He is a founder of crypto & blockchain start-ups Chainstarter and the 21 Million Project.

19. Roadmap

Here we present preliminary development milestones (see Figure 11):

2018	Q4 Scaling Process
2019	Q2 ACESO prototype
2019	Q3 Initial market for researchers
2019	Q4 Market for malware analyst
2020	Q1 ACESO market
2020	Q2 Monitoring

Figure 11. ACESO project development milestones

2018 Q4 – **Scaling Process**. Technical specification adoption, WiperSoft components integration into Aceso Network.

2019 Q2 – **ACESO prototype.** This program will be key for using the ACESO service. This initial release will allow us to begin capturing general information blocks and putting them onto the market. This initial release will be accessible only for selected test users and test researchers.

2019 Q3 – **Initial market for researchers.** We open the initial market model. Temporarily, there will be no possibility to do the planned actions, but it will be possible to monitor the status of blocks and demand for general information blocks.

2019 Q4 – **Market for malware analysts.** Professional cyber experts market is opened. Malware specialist can already emerge there, start collecting tokens and carry out ratings for the work done. We will start testing their methods of monitoring and we will look for the right algorithm identifying errors.

2020 Q1 – **ACESO market.** We will transform the prototype into a fully functional program, connect it to the market and start testing.

2020 Q2 – **Monitoring.** It will be Monitoring of the whole system integrity and correcting errors. We will also provide a possibility for other companies to buy parts of the general information block from our network.

Future Work. Our project milestones reveal plans and pursuits on how we intend to expand the distributed malicious software detection method. At present, the technology has been successfully tested for a few years. Therefore, we want to share it with the world and expand to a safe user-to-user system. And this is only a starting point for our future research on malicious software detection and prevention methods.

20. Open questions and risks

There are a number of open questions accompanied by risks to which the answers have the potential to substantially improve the project as a whole, despite the fact that none of them have to be solved before the launch.

- New algorithms for detection and prevention of the evolving malicious software world.
- To develop user cooperation on the market, to grant reward points that will increase the trust in user actions.
- To fully automatize the company's monitoring mechanisms by employing AI methods.
- To increase transparency and data availability that allows to check the system integrity and efficiency.
- A possibility to involve already existing cyber security companies and jointly develop data network.
- Not to limit ourselves to the range of serviced devices (cell phones, personal computers), to attract IoT devices.
- To develop the algorithm of network monitoring, able to detect "hot" sources of malicious software spread and to prevent future spread.

21. ICO bonuses and discounts

BONUSES AND DISCOUNTS FOR ICO STAGE

ICO discounts will be issued in 5 stages. There will be a fixed amount of ETH for each stage. When a certain ETH amount is reached, another stage will start. The earlier the funding starts, the higher the discount will be received. (See Figure 10).

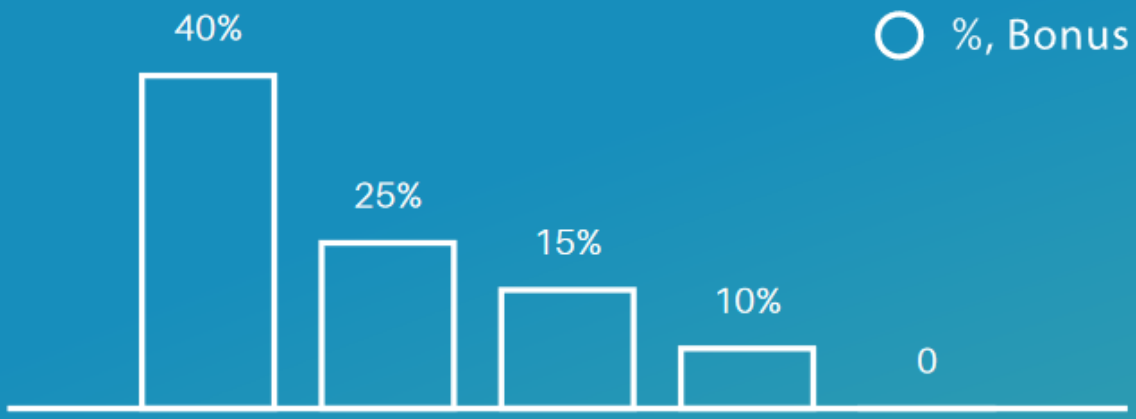

Figure 9. Discounts for ICO stage

Public ASO tokens Sale				
Bonus, %	ETH count	ETH interval	1ETH=xxx ASO tokens	ASO tokens count
40,00 %	2048	0-2048	14000	28672000
25,00 %	8192	2049-10240	12500	102400000
15,00 %	12288	10241-22528	11500	141312000
10,00 %	7168	22529-29696	11000	78848000
0	3072	29697-32768	10000	30720000
Total, ETH:	32768		Total public, ASO:	381952000

Figure 10. Public ASO tokens Sale

Token allocation is as follows:

60% - Token Holders (not locked);
15% - Team (2 year lockup);
10% - Private sale;
6% - Advisors, Legal Counsel, third – party services;
5% - Future developments;
4% - Strategic partnerships & mergers.

22. References

1. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
2. https://www.grandviewresearch.com/industry-analysis/internet-security-market
3. https://www.malwarebytes.com/pdf/white-papers/stateofmalware.pdf
4. http://www.mmc.com/content/dam/mmc-web/Files/APRC/aprc-cyber-risk-in-asia-pacific.pdf
5. https://securityintelligence.com/the-brazilian-malware-landscape-a-dime-a-dozen-and-going-strong/
6. https://markets.businessinsider.com/news/stocks/industrial-cybersecurity-market-worth-22-79-billion-usd-by-2023-1002282496
7. https://www.pcmag.com/roundup/354226/the-best-malware-removal-and-protection-tools
8. https://www.statista.com/statistics/271048/market-share-held-by-antivirus-vendors-for-windows-systems/
9. https://polaris.brighterir.com/public/sophos/news/rns/story/r7gl6zr