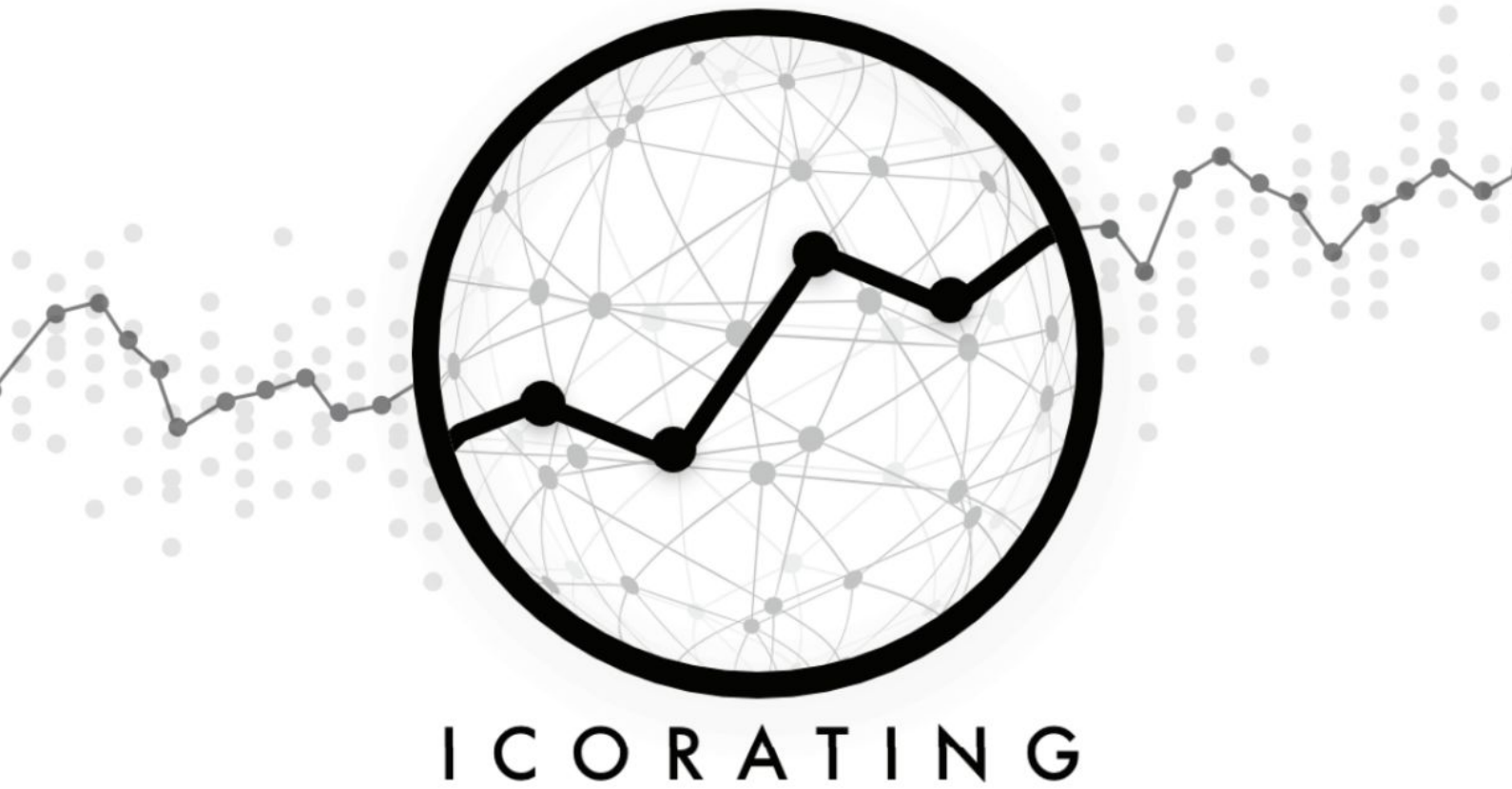
ICOrating

POLYSWARM Rating Review (https://polyswarm.io)

ICO dates (20.02.2018 - 22.03.2018)



Web: icorating.com

Email: info@icorating.com

Twitter: @IcoRating

1. Ratings

We assign the PolySwarm project a “Stable” rating.

The PolySwarm project is aimed at the cybersecurity market, and intends to solve a number of problems inherent in this market using new technologies.

The following factors could help grow the business in the long term:

1. More than half (54.51%) of funds in ETH raised during the token sale will be allocated to the development of protocols and software.
2. The team features professionals with extensive experience.
3. A number of user-friendly advantages for the platform compared to its main competitors.
4. High growth rates in the cybersecurity market.

At the same time, there are number of factors that could adversely affect the token sale and the future development of the project.

The project does not have a freely available financial model or marketing strategy, which prevents potential investors assessing a number of important parameters or drawing a conclusion about any realistic future for the project.

All of the above, together with factors indicated in the «investment risk analysis» and «analysis of factors affecting the future value of the token» chapters prevent us assigning a higher rating to the project.

2. General information about the Project and ICO

PolySwarm is a decentralized platform in the field of cybersecurity where users can create anti-virus programs, detect cyber threats and protect users for payment in tokens worldwide. The PolySwarm company solves a number of issues for modern cybersociety by implementing blockchain technology:

- Accurate and rapid identification of security threats
- Lowering of an entry threshold for community members
- Opportunity for interaction between suppliers and experts in the identification of security threats

The PolySwarm team is conducting the token sale to provide funding for platform and software development and to increase the number of platform users.

PolySwarm is a project of Swarm Technologies, which is registered in Puerto Rico.

Website
White paper
Smart contract platform: Ethereum blockchain
Contract type: ERC-20
Token: NCT
Soft cap: $5 mln
Hard cap: $50 mln

Pre-Sale: completed. $15 mln was raised at the pre-sale stage.

Token Sale:
Start date: February 20, 2018; 19:00 (UTC)
End date: March 22, 2018; 19:00 (UTC)
Token rate: 1 NCT = 0.0000319 ETH (1ETH = 31 337NTC)
Accepted payment: ETH
Minimum transaction amount: $100
Maximum transaction amount: No.

The size of the emission is not established from the start; tokens will be issued as funds are received. Issue of NCT will cease after completion of the token sale, during which the total number of tokens will be determined. The maximum number of tokens is limited. The restriction is based on the achievement of the hard cap in US

dollars, the price of NCT in ETH and the current exchange rate of ETH to the US dollar.
The project provides a bonus program for the token sale period. When certain funding amounts are achieved, the token price increases as follows (throughout the entire sale phase):

- Up to $23 mln – 37,604 NCT/ETH
- From $23 mln to $28 mln – 36,038 NCT/ ETH
- From $28 mln to $33 mln – 34,471 NCT/ ETH
- From $33 mln to 38 mln – 32,904 NCT/ ETH
- From $38 mln to 50 mln – 31,337 NCT/ ETH

The structure of token distribution is as follows:

- 70% - all stages of the token sale
- 15% - tokens to security providers and experts involved in the launch of the PolySwarm system
- 15% - development and adaptation of the ecosystem

Currently, $22.57 mln has been raised (including the pre-sale)

The distribution for funds raised during the token sale is shown in the diagram below:

New tokens will not be issued after the token sale period.

The PolySwarm team expects a decrease in legal expenses for the 2019/2020 fiscal year. The balance will be assigned to marketing costs, overheads and developer salaries.

"Know your customer" (KYC) rules will be applied to the token sale.

3. Description of the services and scope of the project

The PolySwarm project is a decentralized platform on blockchain which stimulates innovations in the anti-virus and automated cyber threat intelligence space. The platform is based on Ethereum smart contracts.

PolySwarm is creating an ecosystem for detecting security risks associated with files, network traffic and URLs (collectively known as Artifacts) in real time. This project covers enterprises, consumers, suppliers and security experts in various parts of the world. Experts develop and improve "micro-mechanisms", which carry out an autonomous exploration of the latest security threats, trying to surpass competitors' mechanisms.

A fair assessment of PolySwarm's work is the accuracy of definition of a security threat. The market rewards experts who provide the best protection for businesses and users.

In the documentation, the working principle of the PolySwarm platform is schematically represented as follows:

The following classes of participant can be distinguished:

1. End users (corporate and individual users with suspicious Artifacts) will be able to participate in the project through the Bounty program and Offer in the system.
2. Security experts (Experts). Geographically diversified experts in malicious software analyze the latest suspicious Artifacts and support mechanisms for determining cyber threats. Experts take responsibility for statements and

public declarations about the results of their analysis of the Artifact. Experts who provide correct statements are rewarded in the form of NCT tokens.

3. Ambassadors - These are companies that facilitate end-user interaction with the PolySwarm platform. Ambassadors collect traditional fiat funds (for example, a subscription fee) and suspicious Artifacts from their customers (end users). Then they place the Bounty and Offers on behalf of their clients in the market. The ambassador is responsible for parsing the statements of several Experts, creating a verdict on the malware or safety of the element examined and continuing to provide the verdict to its customers.
4. Arbiters. These are middle-level intermediaries responsible for determining the credibility of a cyber threat. PolySwarm is planning to appoint Arbiters from existing security intelligence solutions providers with a good reputation who will be willing to interact with the PolySwarm team and assist in identifying and resolving platform errors.

The specifics of the arbitral Verdict process include the following:

1. The arbiters reach consensus on reliability of the majority of votes.
2. Votes are an integral part of the complete Ethereum chain.
3. Arbiters are awarded commission fees for voting on the reliability of the security threat of Artifacts.
4. Arbiters may refrain from voting on any particular Artifact in the event that, for example, they consider themselves unqualified to determine the security threat of a particular Artifact.
5. If necessary, voting rights of an arbiter can be transferred to an additional intermediary to ensure a quorum for determining reliability.
6. If necessary, participants may challenge verdicts of arbiters on blogs or technical articles describing the threat to the Artifact.

PolySwarm offers two key tools for end-users and intermediaries - Offers and Bounty as mentioned earlier:

PolySwarm Offers.

Offers are sent directly to security experts with a good reputation to request their assesment of a security risk. PolySwarm provides well-established access to thousands of developers, thereby providing a traditional exchange of information with all participants of the platform. This interaction is ensured by Raiden-network for offers.

PolySwarm Bounty.

A "Wanted" sign is placed with corresponding contents of an Artifact with a price in NCT for resolving the issue.

Offers are the closest analogue to the current antivirus scanning market by request and they function with a millisecond delay.

In our opinion, the technology chosen is appropriate for the PolySwarm project. The proposed platform functionality and the advanced technologies involved will help attract potential participants to the system. It should also be noted that the platform will create a need for additional markets such as an intermediary market (many consumers will want to deal with the project through an intermediary), a market for publishing Artifacts (to ensure the availability of an Artifact to Experts when placing a Bounty or Offer).

4. Market Review

4.1 Market analysis

In 2004, the global cybersecurity market was estimated at $3.5 bln. It was $64 bln in 2011 and $78 bln in 2015.

According to IDC analysts, global sales of hardware, software and services related to computer security will grow by 8.2% per year. Growth will increase by 8.7% per year on average; thus the market will grow to $105 bln by 2021.

Cybersecurity Ventures predict even more rapid growth for this market. In their view, market volume will be more than $120 bln by 2021, which corresponds to annual growth of 12-15%.

The increase in computer security-related crime is causing company owners to invest more and more in defense of their businesses. Thus, JP Morgan Chase & Co. doubled its annual budget from $250 mln to $500 mln. In 2017, Bank of America published a report that it has an unlimited budget when it comes to combatting cybercrime. Microsoft has stated that it will continue to invest more than $1 bln per year in research and development for cybersecurity in the coming years. However, many corporations do not dare reveal cases of hacker attacks or sizes of increased security budgets due to a fear of causing reputational damage.

According to analysts, digital transformation is also forcing companies to actively invest in security tools. More than 30% of purchases come from companies in the banking, discrete and government sectors. The telecommunications industry is increasing its spending faster than other sectors (at 11.2% per year), thus it will become one of the top five highest-spending sectors in 2018.

More and more companies are showing interest in blockchain technology regarding matters of security since basic software does not meet key requirements such as efficiency, confidentiality, ease of management or economy of computing power. For these reasons, one of the main factors contributing to growth for the cybersecurity market is growth in the ICO and crypto markets.

In 2024, the global ICO market is forecast to be worth $20 bln. This is stated in a report by the American analytical company Transparency Market Research. The

industry will grow by 59% per year. The researchers made their assumptions based on the blockchain market in 2015, whose volume they estimated at $316 mln.

The PolySwarm project will be operating in a promising and rapidly growing market. This increases chances for its successful launch and ability to grow the business.

4.2 Competitive analysis

The cybersecurity market currently features some companies that have earned a high reputation. The main competitors for PolySwarm are the following:

Bugcrowd – an American company that positions itself as the leader in this market. Founded in 2012, headquartered in San Francisco.

HackerOne – another American company that searches for vulnerabilities. Founded in 2012 and headquartered in San Francisco. Currently, more than 700 companies have used their services.

Synack – headquartered in Redwood City, California; Synak is a global organization with regional offices in 7 countries. Founded in 2013.

Security Audit Systems – a British company for penetration testing in the IT security industry; the company was founded in 2005.

Pentestit – a Russian company, which in addition to providing penetration testing services offers courses in ethical hacking, preparing companies for compliance with PCI DSS standards, forensics, and a cloud firewall based on artificial intelligence known as Nemesida WAF.

Most companies in this field interact with small businesses, as large corporations can afford to maintain their own cybersecurity service independently.

Similar projects recently staging their ICOs include Hacken; this project is a reward system for identifying vulnerabilities on corporate websites and software. The ICO was successful; the hard cap set at $5 mln was achieved.

PolySwarm is planning to develop a number of advantages over currently operating companies providing these services. The project aims to lower the entry threshold, provide wider coverage options and create opportunities for interaction between product suppliers and security intelligence experts.

Unlike many projects, PolySwarm works with a type of threat analysis that can be automated, for example antivirus programs.

As we can see, the PolySwarm project is trying to enter a competitive market. For the most part, the above-mentioned organizations have been operating for several years, they are well known and have a large number of regular customers. According to Blockchain News, Bugcrowd for example spent the middle of last year searching for vulnerabilities in the Dash payment system.

5. Team and stakeholders

The PolySwarm team includes 9 specialists and 5 advisors. Key positions are occupied by:

Steve Bass (LinkedIn) **-** CEO, DEVELOPER, FOUNDER
Steve has more than 20 years of experience in the field of information security development, has held leading roles in various projects for government organizations and industry, is the founder of several information security companies including Narf Industries, which has worked with the Office of Defense Advanced Research Projects Agency (DARPA) and Fortune 500 companies. Conducts identity research based on Blockchain.

Education:

- Naval Postgraduate School
- Santa Clara University

Paul Makowski (Linkedin) - CTO, DEVELOPER, CO-FOUNDER

Paul has more than 10 years of experience in software development, program analysis, vulnerability research, and has developed engineering tools for malware disinfection. Paul holds a Bachelor's degree in Computer Engineering from the University of Santa Clara and a Masters in Information Technology and Management from Carnegie Mellon University. He has also worked for Narf Industries, where he was engaged in decompiling, identifying and writing tools for neutralizing malware on behalf of customers from the Fortune 100 list.

Education:

- Carnegie Mellon University
- Santa Clara University

Ben Schmidt (Linkedin) **-** DIRECTOR OF PRODUCT SECURITY, DEVELOPER, CO-FOUNDER

Ben has over 10 years of experience in the field of information security, secure software development and vulnerability analysis. At Narf Industries Ben worked on the Cyber Grand Challenge for DARPA.

Education:

- University of Tulsa**.** Bachelor's and Master's Degree in Computer Science.

Nick Davis (LinkedIn) **-** COO, DEVELOPER, CO-FOUNDER
Co-founder of Narf Industries. Has created many binary applications for vulnerability testing and program analysis. Won several DEF CON Capture The Flag competitions. Engaged in development and research in information security and malware analysis.

Education:

- Naval Postgraduate School
- University of Minnesota-Twin Cities

The project's advisory board includes the following:
Mark Tonnesen (Linkedin) - Former CIO of McAfee. Has 25 years of experience in the field of software development.

Carl Hoffman (Linkedin) - Founder & CEO of Basis Technology**.**
Entrepreneur with experience in the field of text analytics. Worked as director of business development at the Free Software Foundation.

Legal support for the project is provided by Goodwin Procter LLP.

The PolySwarm team consists of highly qualified specialists with experience in the field of computer program security, detection of threats and viruses and development of programs for their elimination. All the co-founders of PolySwarm are employees of Narf Industries, a leading information security company specializing in individual solutions for government and large enterprises. Narf is planning to develop products and services for the PolySwarm market.

Thus, given that the project management already has experience of working together and the founders have experience in business management related to cybersecurity issues, we have grounds to believe that the project has a chance of a successful launch and further development. We consider the composition of the team as one of its strengths.

6. Token analysis

NCT is an Ethereum blockchain-based ERC20 standard cryptographic token available for storage in a variety of wallets compatible with this standard. NCT is a utility token intended for use within the PolySwarm platform.

Token name - PolySwarm Nectar Token
Symbol - NCT
Decimals – 18

GitHub hosts a repository for the smart contract code: https://github.com/PolySwarm/eth-contract-metadata/commit/193ca825e52a070ca4ec588b80529b21dcdd71e7

PolySwarm Technologies, Inc. will work with Trail of Bits to conduct a professional audit using advanced EVM tools (decentralized virtual machines).

Technical development of the PolySwarm ecosystem will be provided by Swarm Technologies with funds raised from the implementation of tokens.

NCT tokens activate elements of the PolySwarm platform such as:

- Placement of the Bounty (Commission fees are paid by the intermediary):
    - Fixed commission for placement
    - Commission fees are proportional to the Bounty amount.
- Establishing, releasing or replacing the Offer channel (Commission fee paid by the intermediary)
    - The net percentage of the amount of NCT tokens is transferred through the channel.
- Registration Assertions and determination of Reliability (commission fee is paid by an expert)
    - Fixed commission for Assertion.
    - Commission fee proportional to the Assertion bid amount.

In our opinion, the use of NCT Token on the PolySwarm platform is justified and will be in demand, since all platform functions will be implemented using NCT. This in turn makes it possible to use the platform from anywhere in the world with high speed, transparent transactions.

7. Analysis of factors affecting the future value of the token

---

The documentation does not specify fees for the various transactions on the platform. We think that this could be perceived negatively by potential investors as they must clearly understand what the project offers, how pricing is structured on the platform and from which sources the future budget for the project will be drawn up. The statement that commission fees will be significantly lower than those of competitors is not backed up.

According to the founders, since NCT is intended for use on the platform, the main growth factor for its price should be an increase in number of participants in the system. The project does not provide any forecast values for this in the documentation. At the same time, we note that growth in the number of users does not lead to an increase in the cost of the services for prevention of cyber threats in the market in general and on the platform in particular, since the market mechanism for pricing works as follows: with increase in demand for tokens and a corresponding increase in prices, fewer tokens will be required to purchase services.

Holders of PolySwarm project tokens will not receive any dividends or "returns" on funds invested in NCT. The project has not provided any mechanism to reduce the number of NCT tokens in circulation.

For all the above reasons, token price will primarily be a function of the cost of services in this market.

About 70% of NCT is planned to be allocated to investors at the ICO. The remaining 30% may in the future "blur" any positive effect of growth in the cost of services in the cyber security market, for long-term token holders.

8. Investment risk analysis

First, it is worth emphasizing the risk of high competition. The market for cyber security services already features players who have earned recognition among business owners, and it will not be so easy to occupy a niche despite a general growth in demand in the market. For survival, development and implementation of the goals set, the project will require a large-scale marketing strategy.

At the same time, investors should pay attention to the fact that no future marketing strategy for the project has been published. There are qualified marketing specialists in the team, the marketing budget is also known - 13.62%, which if the hard cap is reached will amount to $6.8 mln. However, any details of the intended future promotion plans for the product are not provided. Currently, investors cannot form a clear idea of how PolySwarm will attract users to the platform nor how the marketing budget will be spent. For this reason, the project has also a risk regarding implementation of the development plans.

The lack of a financial model for the project prevents drawing any conclusion about the future results of the project or assessing its profitability and survivability after the project becomes self-supporting, which is another risk for token holders.

A similar project in the field of cybersecurity, Hacken, collected $5 mln through its ICO. In this case, the hard cap of $50 mln was not justified by the founders, and after reaching the goal of $38 mln, investors will not receive any bonuses. Therefore, there is a risk that the hard cap will not be achieved. Considering that $15 mln was collected at the Pre-Sale, which is 30% of the hard cap, and the number of tokens sold is not specified, there is a risk that there will be a large number of NCTs purchased in the Pre-Sale period featuring high bonuses. All of the above creates a market risk for NCT tokens after circulation on the open market commences.

Any other significant risks that could have a negative impact on the PolySwarm project have not been indicated.

The information contained in the document is for informational purposes only. The views expressed in this document are solely personal stance of the *ICOrating* Team, based on data from open access and information that developers provided to the team through Skype, email or other means of communication.

Our goal is to increase the transparency and reliability of the young ICO market and to minimize the risk of fraud.

We appreciate feedback with constructive comments, suggestions and ideas on how to make the analysis more comprehensive and informative.