ICOrating

GLADIUS Rating Review (https://gladius.io/)

ICO dates (01.11.2017 — 30.11.2017)

Web: icorating.com

Email: info@icorating.com

Twitter: @IcoRating

1. Ratings

We assign the Gladius project a "Stable +" rating and recommend participating in the project's ICO to investors who are aware of the risks identified in our review.

Gladius is a project for the creation of a decentralized peer-to-peer serverless network to protect against DDoS attacks and improve access to web content using blockchain technologies.

Payment for the platform's services is implemented in GLA tokens; users can act as nodes and earn rewards in the form of GLA tokens. The future dynamics of GLA tokens will largely depend on the popularity of the platform; there is investment potential for the growth of token price.

It is also notable that the hard cap of Gladius looks very adequate against the background of the other ICO projects that are staging their own crowdsales simultaneously. Given the quality of ICO marketing, reasonable collection targets, and an interesting "blockchain" idea we think that Gladius will be able to collect the hard cap, and demand will exceed supply due to which the token may grow in value in the secondary market after the ICO.

The risks of the project include possible technical difficulties that the team may encounter in the development process.

2. General information about the Project and ICO

Gladius is a project for creating a decentralized peer-to-peer (p2p) and serverless network to protect against DDoS attacks and improve access to web content using blockchain technologies. Using free network capacity and Ethereum smart contracts, Gladius is going to create a system of protection and easier access to internet resources, which is intended to be the most effective and safe one, and accessible to any user.

Against the backdrop of the active development of ideas on uses for the free (i.e. not currently involved in activities) resources of an individual, Gladius has developed the idea of monetizing free high-speed data transmission channels and computer capacity, which postulates a win-win scheme for both consumer and supplier of these resources. Everyone who has processing power and access to the internet can connect to the Gladius network and provide data processing during DDoS attacks, storage and transmission of information within a Content Distribution Network (CDN) [1].

The project stands out primarily as an idea, as it uses the existing, effective technology of anti DDoS systems and CDN networks, while applying a completely new approach to their implementation. In addition, the scheme for the interaction of people involved in the Gladius platform and its business model are notable for their simplicity and potential.

The Gladius platform's architecture connects two sides – a power supplier and their consumer within a p2p network. An infrastructure is built between them on the basis of blockchain technologies, which involves the use of smart contracts and GLA tokens. In this scenario, both consumer and supplier pay only for services actually rendered, which offers huge potential for reducing the cost of these services in comparison with the centralized counterparts on the market.

The tokens issued for the ICO are a component of the developed Gladius network - they involve settlements with both power suppliers and consumers. Commissions for the use of network services, through which it is intended to finance activities of the platform, are also nominated in GLA.

The Gladius smart contract code is publicly available on GitHub. The smart contract is audited by Hosho (https://github.com/DecentralizedIT/gladius/blob/master/docs/reviews/Hosho.pdf) and SmartDec (https://github.com/DecentralizedIT/gladius/blob/master/docs/ reviews / SmartDec.pdf); the conclusions are generally positive; minor errors were corrected in a timely manner.

Gladius Website: https://gladius.io/
Whitepaper: https://gladius.io/pdf/gladius-whitepaper.pdf \
Medium: https://medium.com/@gladiusio
Twitter: https://twitter.com/gladiusio
Facebook: https://www.facebook.com/gladiusio
Bitcoin talk: https://bitcointalk.org/index.php?topic=2217711
Telegram: https://t.me/gladiusio
GitHub: https://github.com/DecentralizedIT

ICO start date: 1 November 2017, 11:00 BST (UTC+1)
ICO end date: 30 November 2017, 10:00 BST (UTC+1)
Hard cap: 25,000,000 USD (presale+public sale)
Soft cap: 2,000,000 USD
Token: GLA, standard ERC-20
ICO price: 1 GLA = 0.002 ETH
Accepted payment: ETH
Total emission: 96,320,000 GLA

- 60% - Public Release
- 15% - Advisory, community, and marketing teams
- 15% - Operational costs, which includes bounty programs, day-to-day costs, etc.
- 10% - Founders

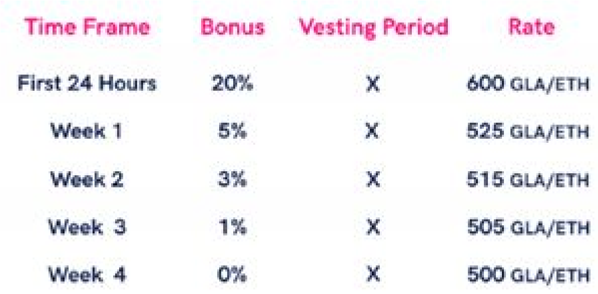
On sale: 68,000,000 GLA
Distribution:
40% - Core development
20% - Security
20% - Operations
10% - Legal
10% - Marketing

- The private pre-sale was announced; its parameters are not disclosed, except the amount attracted in fiat (min $2 mln - max $12.5 mln).
- After the ICO, tokens will be frozen for 18 months.
- The other coins will be available through various vesting periods and will be given out to members of bounty programs, advisors, and early

node operators. Pre-sale bonuses will be locked for a certain period to vest.

- Part of the GLA supply will be kept for potential future funding. These funds will come out of the budget allocated to operational costs.
- Some of the GLA tokens will be used to promote platform adoption, developer interest, and community growth.

Bonuses on the ICO were announced depending on the time of participation, from 20% in the first 24 hours to 1% within 3 weeks.



Time Frame	Bonus	Vesting Period	Rate
First 24 Hours	20%	X	600 GLA/ETH
Week 1	5%	X	525 GLA/ETH
Week 2	3%	X	515 GLA/ETH
Week 3	1%	X	505 GLA/ETH
Week 4	0%	X	500 GLA/ETH

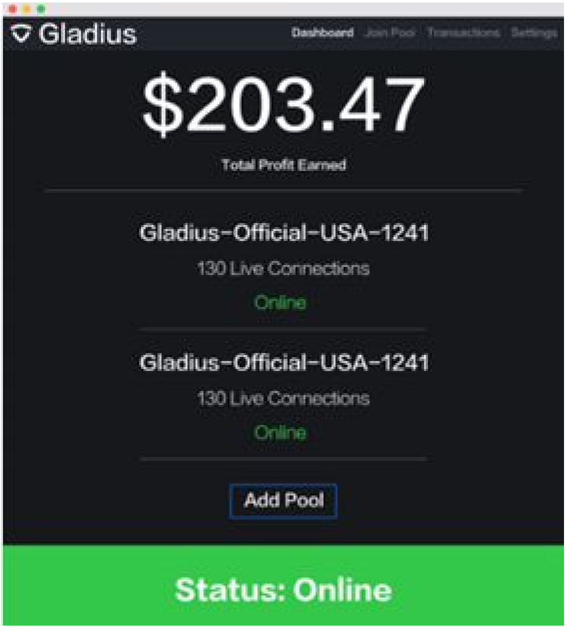
[1] https://en.wikipedia.org/wiki/Content_delivery_network

3. Project services and their usage

Gladius services should be considered from two points of view – for buyers of CDN services and DDoS protection (in fact, buyers of power and virtual storages); for capacity vendors and owners of network nodes. The Gladius platform itself connects these two parties and regulates their relations and work through the desktop client and web portal.

A desktop client is a cross-platform application that can run in the background, which the Gladius network node creates from the user's computer. Nodes form the decentralized Gladius network and use available computer power to process incoming requests. Nodes are combined into pools by demographic criteria in order to simplify interaction with incoming traffic, while a separate node can be a member of several pools at the same time, which maximizes the demand for all provided capacity.

Gladius provides screenshots of the desktop client interface in its white paper:

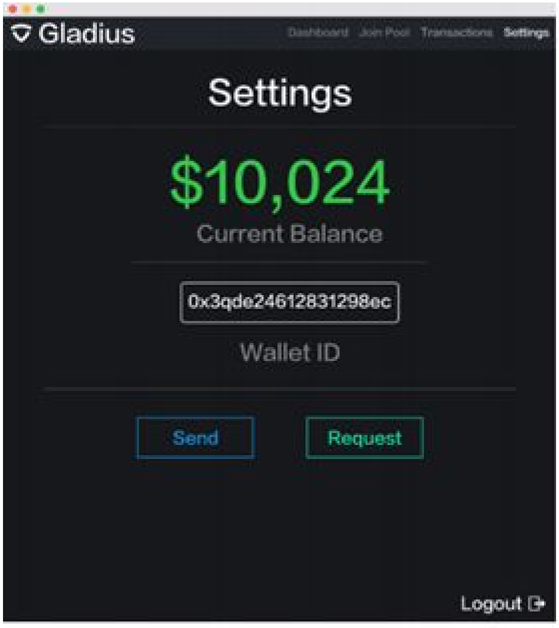


$203.47
Total Profit Earned

Gladius-Official-USA-1241
130 Live Connections
Online

Gladius-Official-USA-1241
130 Live Connections
Online

Status: Online



Settings

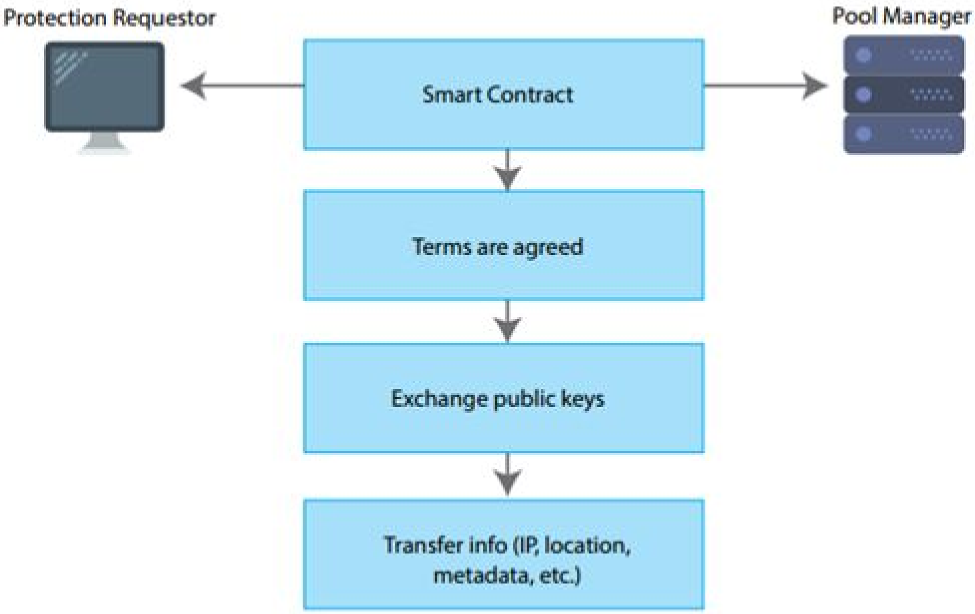
$10,024
Current Balance

0x3qde24612831298ec
Wallet ID

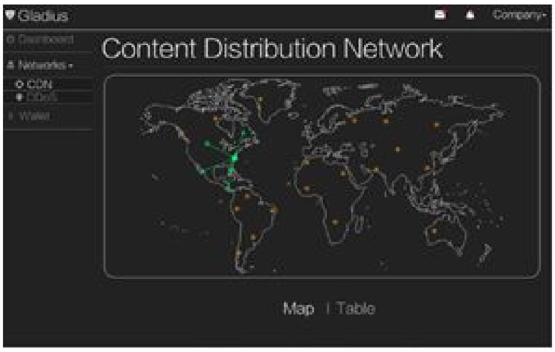
The online web portal serves as a communication tool for Gladius with consumers of DDoS protection services and CDN. An individual or company registers and sends a request for the provision of services to its website. In this case, based on the available information, the client himself chooses by means of the capacity for which pool services will be provided (rating, geographic location, price, etc.).

After selecting the pool and sending the request, there is an exchange of public keys, private data (IP, location, metadata, etc.) and the creation of a smart contract.

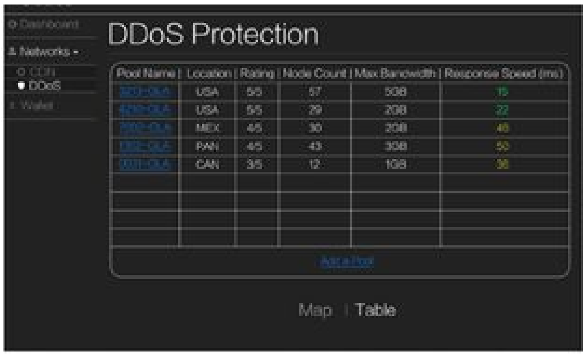
After the agreement is concluded, the website owner only needs to change the DNS settings to the required ones. Payment for the provision of services is sent after the successful completion of the smart contract.



Since the MVP for the web portal is not yet published, Gladius gives screenshots of ongoing work:



Content Distribution Network



DDoS Protection

Pool Name	Location	Rating	Node Count	Max Bandwidth	Response Speed (ms)
[illegible]	USA	5/5	57	5GB	15
[illegible]	USA	5/5	29	2GB	22
[illegible]	MEX	4/5	30	2GB	46
[illegible]	PAN	4/5	43	3GB	50
[illegible]	CAN	3/5	12	1GB	36

Add a Pool

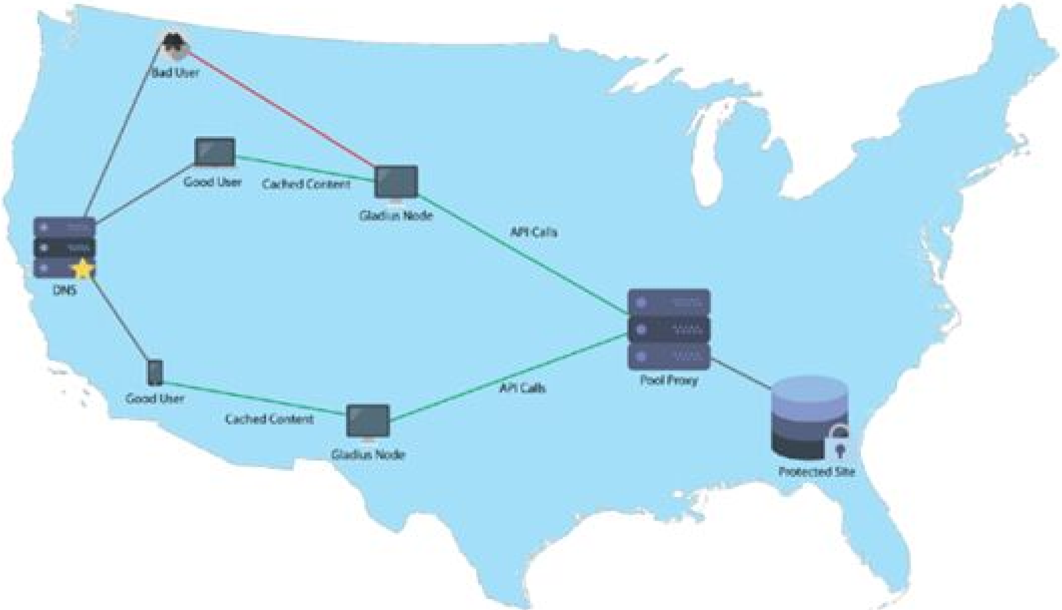
Pools are designed to facilitate the interaction between the network and incoming traffic, as they combine many nodes on a demographic basis. A pool can also consist of one node and not approve other applications; thus, a user can form a separate traffic processing point.

When working with Gladius, a client can see a list of available Pools and their parameters - geolocation, size (bandwidth), reputation, cost of services, and select the ones most suitable for the request.

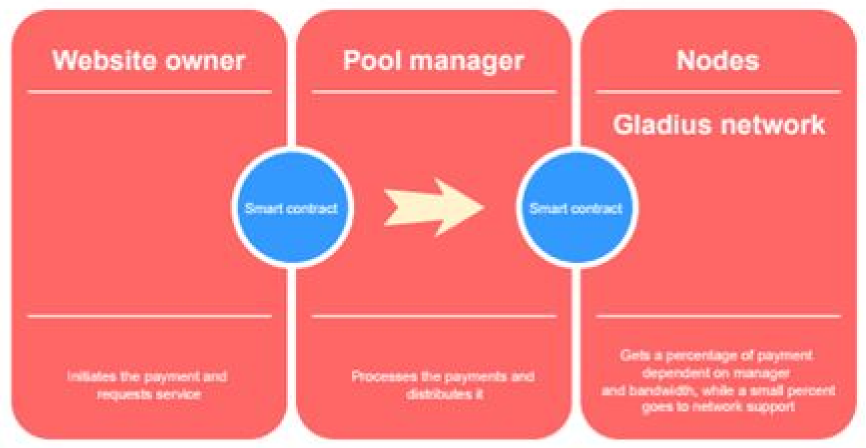
The database of all pools is stored in blockchain; the request for connection to the pool from the node is also initiated through an Ethereum smart contract. Commissions within the framework of the Ethereum blockchain will encourage participants to be honest and serious. Information about reputation, bandwidth, maximum cache size and geolocation will be available within the pools database. Reputation will consist of the following components: user reports and subsequent investigations, protection provided over time, total pool age and total pool size. Pools with a specified number of outdated clients will also be noted in their reputation, meaning pools will always be pushing their nodes to update their clients.

The process of joining a node to a pool is technically the same as the process of interaction between a client and a pool manager: since the information transferred from the pool to the node can be used by an attacker, after the approval of the application they exchange public keys; then exchange of private data (IP, location, etc.) takes place; information about the node ID is added to the smart contract.

Each pool will have a DNS service, through which incoming traffic will be sent to the nodes for verification. Gladius indicates that this will create a potentially protected system via the self-protection of each node of the network. Also, a pools manager will have a final proxy server (one or more) to mask the true IP of the destination from any potentially malicious node.



The calculation scheme provided by Gladius involves the movement of funds from a client (the owner of a served website) to each node that processes incoming traffic or provides its virtual storage. The whole scheme of calculation is built on the basis of Ethereum smart contracts in GLA tokens. Payment for services, minus the commission for Gladius (the amount of which is not disclosed in the documentation) is sent to the pool manager, after which he distributes it proportionally between the nodes, taking into account the load balancer (this is determined by the pool provider).


Website owner
Pool manager
Nodes
Gladius network
Smart contract
Smart contract
Initiates the payment and requests service
Processes the payments and distributes it
Gets a percentage of payment dependent on manager and bandwidth, while a small percent goes to network support

Methods of DDoS protection and CDN services:

To combat DDoS attacks, Gladius nodes within pools will use proven traditional methods to detect and filter out malicious requests:

- Rate-limiting: malicious IP addresses are detected and blocked by defining thresholds for persistent queries.
- IP Address Matching: grouping of IP queries through their matching and analysis, and blocking of group data.
- Intelligent geo-matching: Analysis of incoming data by geographical criterion for detection and blocking of malicious addresses.
- Browsing behavior: analysis of the content of a request to determine its profitability.

The team promises to develop new methods of mitigating negative traffic, and points to the possibility of self-learning pools for preventive blocking of "standard" intruders.
Within the CDN network, Gladius will provide quick access to supported websites (their content) by redirecting a client's request for this website to the geographically closest node (less in the volume of virtual storage in comparison with a traditional server.) Due to the wide potential geography of nodes, network efficiency can be greater than with traditional CDN providers, since in their case requests are directed to the closest server with a large capacity.

To exclude malicious websites, there is a mechanism for checking information for obsolete (will be reflected in a website's reputation) or maliciousness (the node will be excluded from the pool.) Each pool will be able to send verification requests from the final proxy through another node to the node being tested. This ensures that each node has no knowledge of the other nodes in the network, ensuring that they would treat a verification request like any other.

The reputation of nodes will be calculated based on random uptime requests initiated by the pool as well. The reputation of the node will directly affect the amount of reward received, since the pool manager will distribute received cryptocurrency on this basis.

4. Development strategy and Roadmap

The implementation of the project's functionality is divided into three phases:

1. By March 2018 work on phase 1 is expected to be completed, including:

- Smart Contract V2.0
- Gladius Client V2.0 - Full pool integration, headless client mode, and improved blockchain integration
- Gladius Node Pools V2.0 - Improved blockchain integration, and the start of a vetting process for new nodes
- Fully Encrypted communications.

2. By August 2018, phase 2 is expected to be complete:

- Removal of centralized server
- Smart contracts for discovery and identification services
- Interface implementation for add-on modules
- Gladius Node Pools V3.0 - full vetting and rating process
- Completion of auto-payment and bid/ask system for the marketplace

3. Work on the project will be completed together with phase 3 by December 2018:

- Release of open source network builder for closed-systems
- Completion of multi-pool support for protection purchasers
- Addition of novel CDN techniques to further increase load speeds
- Stretch Goals

The project will be ready for commercial use after phase 2 is completed. There is relatively little time by the standards of start-ups from the current moment to phase 2 - less than 10 months. This is positive for investors in the project.

In addition to three iterations, Gladius reserves the right to change the functionality, depending on the amount of funds raised during the ICO:

- ○ $4 million - Basic DDoS, CDN, and Load Balancing
- ○ $8 million - CDN File Upload
- ○ $12 million - 5 Layer DDoS Protection
- ○ $16 million - CDN Static Content Caching
- ○ $18 million - CDN Dynamic Content Caching
- ○ $20 million - Gladius App Store
- ○ $22 million - Layer 7 DDoS Protection

- $24 million - Advanced CDN optimizations
- $25 million - Advanced DDoS optimizations

5. Market Review

In its documentation, Gladius provides a worthy analysis of the CDN market and protection against DDoS attacks, citing such authoritative sources as NexusGuard, Forbes, United States Department of Homeland Security and Dyn. In the relevant section of the white paper, the team gives a description of the current state of the industry and describes key problems for customers and service providers. Unfortunately, there is not so much quantitative data in this section, which is explained by the closed nature of most analytical studies.

According to Marketsandmarkets research[1], the volume of the Distributed Denial of Service (DDoS) protection and mitigation market was $824 million for 2016. The authors predict an increase in market volume to $2,163m by 2021, with the expected CAGR of 21.3%. Growth drivers will be: The need to mitigate the impact of increased DDoS attacks for private companies, the growing penetration of IoT and enterprise mobility trends across organizations.

At the same time, the activity of intruders in DDoS attacks continues to grow against the backdrop of the evolution and continued penetration of digital networks into mass use. According to a Nexusguard report, for Q1 2017 the frequency of harmful effects for the reporting period increased by 380% compared to the same period the previous year.

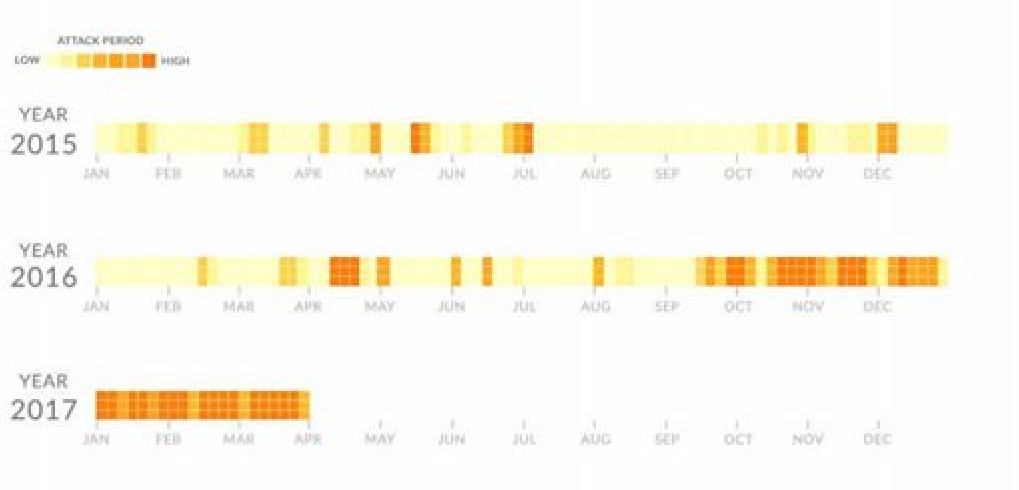
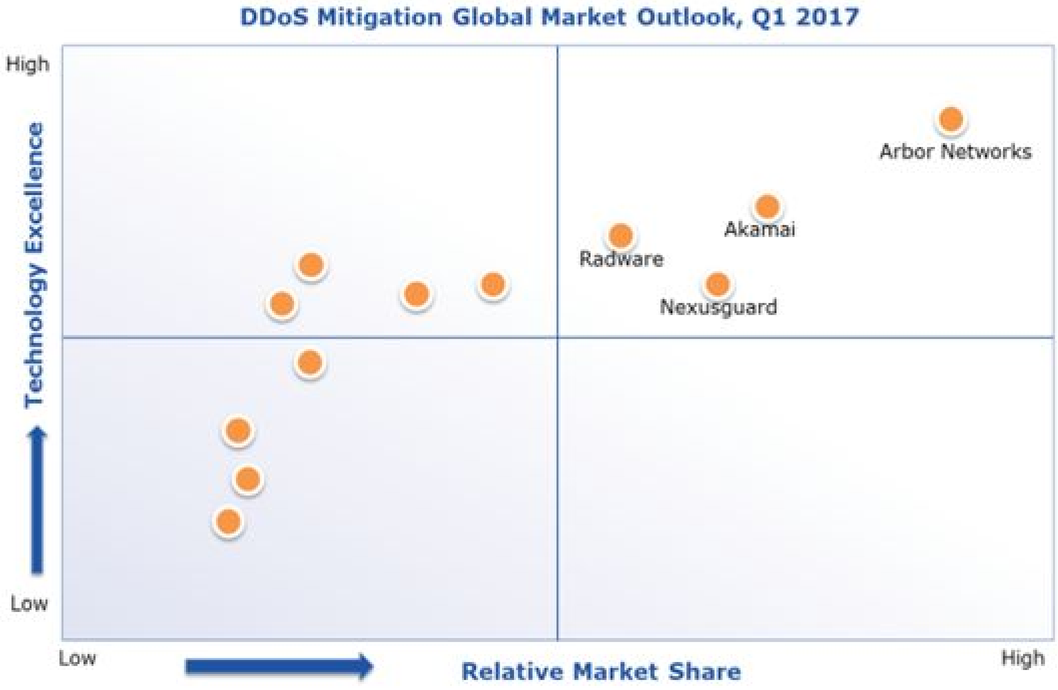


Figure 1. Attack Frequency in Q1 — 2015 through 2017

October 21, 2016 was the date of the largest attack in the history of DDoS on the leader among DNS providers - Dyn. As a result, many large internet companies suffered - their web resources using Dyn's services were completely or partially inaccessible. Among the victims were Twitter, Reddit, AirBnB, Heroku, Github, Netflix, PayPal, Spotify and even Amazon.

In fact the market for protection against DDoS is shared among such major players as Redware, Akamai, Nexusguard, Arbor, Cloudflare and Imperva[2]. Other participants occupy an insignificant share, since the majority of clients of this market are large companies and corporations for whom the advantages of small and medium business are not a decisive factor.



According to Marketsandmarkets[3], the CDN market can be estimated at $6.05 billion in 2016. According to forecasts, this figure will reach $23.22 billion with the expected CAGR of 30.9% in 2021. The high growth rates researchers attributed to an increase in the volume of traffic consumption in the network and the distribution of video and multimedia content. The leading players in this market are: Akamai Technologies, Inc. (Cambridge, U.S.), Google, Inc. (California, U.S.), Level 3 Communications (Colorado, U.S.), Limelight Networks, Inc. (Arizona, U.S.), Amazon Web Services, Inc. (Washington, U.S.), and Verizon Communications, Inc.

[1] "DDoS Protection Market by Component (Solution, and Service), Application Area (Network, Application, Database, and Endpoint), Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2021"

[2] http://quadrant-solutions.com, https://pages.arbornetworks.com/rs/082-KNA-087/images/Knowledge%20Brief_Arbor%20Networks_Market%20Technology%20Leader_DDoS%20Mitigation%20FINAL.pdf

[3] "Content Delivery Network (CDN) Market by Type (Standard/Non-video and Video), Core Solution (Web Performance Optimization, Media Delivery, and Cloud Security), Adjacent Services, Service Providers, and Region - Global Forecast to 2021"

6. Team

The project is presented by a team of 3 founders; all of them are students of the University of Maryland College Park specializing in Computer Science. Given their age, the founders have no experience in the field of cybersecurity and fintech start-ups; this can be flagged as a main risk of the project.

Max Niebylski - Founder
The founder of Gladius. Trained as a Software Engineer in Bloomberg and National Institutes of Health, and has also worked for Rotunda[1].
https://www.linkedin.com/in/maxniebylski/

Alexander Godwin – Co-founder
Alexander plays a key role in the creation of smart contracts and the architecture of the main platform. According to LinkedIn data real experience, in addition to that as software developer at the University of Maryland, is missing.
https://www.linkedin.com/in/alexander-godwin/

Marcelo Mcandrew – Co-founder and developer
Marcelo is engaged in the development of the desktop client platform and web portal. He has experience working as an intern at Dogotal Infuzion, and has also worked as a developer in the exchange sharing start-up Karavan Carpool.
https://www.linkedin.com/in/marcelo-mcandrew-7a2a68126/

The project has a strong advisory board, represented by high-class professionals in the areas of PR, Cybersecurity and Cryptocurrency, including media personalities.

Joseph Steinberg
A recognized and well-known expert in cybersecurity; columnist, CEO and founder of SecureMySocials, a real-time security monitoring system for social media. Sufficient information on Joseph can be found in the press and media; he also runs his own website josephsteinberg.com.
https://www.linkedin.com/in/josephsteinberg/

Jeremy Epstein
Well-known marketer, with more than 20 years of international experience. Has extensive experience working with venture projects and fintech start-ups. Jeremy is also marketing faculty member for the Blockchain Research Institute, and co-Founder of Crypto Explorers, a leading community for passionate individuals

seeking to understand the decentralized future, that hosts quarterly gatherings called "Crypto Valley Trips" in Switzerland.
https://www.linkedin.com/in/jer979/

Michael Terpin
Michael Terpin is a serial entrepreneur in marketing and cryptocurrency. His bitcoin endeavors include BitAngels, Bitcoin Syndicate, and CoinAgenda. His PR firm, Transform, has worked with more than 30 cryptocurrency companies, as well as other tech companies. He also runs SocialRadius, one of the nation's first social media marketing firms, and he founded and sold Marketwire, one of the world's top three company newswires.
https://www.linkedin.com/in/michaelterpin/\

Frank Bonnet
Founder and Developer of Dcorp, having advised several other successful ICOS, Frank Bonnet comes with nine years of experience designing, as well as building a countless enterprise .NET applications. Within the framework of the project it is engaged in advising the process of platform and smart contract development.
https://www.linkedin.com/in/frank-bonnet-3b890865/

The professional experience and competence of the consultants partly compensates for the youth and inexperience of the team; however this aspect of the project cannot be called a strong point. For investors' detachments, professional and media backgrounds are often an important factor in the consideration of the project, so community questions about the composition of the team inevitably arise. At the same time, promising young people often find new solutions for established business models; history records many cases of the creation of the largest companies by university students.

[1] http://www.rotundastore.com/

7. Marketing strategy

Gladius spends a lot of resources on ICO marketing - this can be seen from the volume of published marketing materials. Nevertheless, the interest of the community is still low. It is also difficult to talk about real interest among professional investors, since the announced pre-sale is not public.

The team leads the project blog on Medium (at the time of writing this review it has 157 followers and 4 postings); the main social media for communication are Facebook (1945 followers) and Telegram (1269 members). There is also Twitter (1370) and a thread on Bitcointalk (6 pages of comments). There is an announced bounty campaign for early October (Medium, Twitter, Facebook and Telegram).

Gladius has approached announcements on information cryptoportals seriously. Marketing materials are placed on Coin Telegraph, Coinspeaker, Crypto Insider, SteemIT, BitNewsBot, Bitcoinist, Investopedia, Zero Hedge, etc. In total, there are more than 30 announcements in various news publications.

The marketing plan for product promotion is not presented in the documentation. This is an important component for the project, as there is no understanding of the methods of penetrating the current market with the product – a market where customers prefer large reputable providers to small ones.

Gladius note that current market has a specific request for small companies - local entertainment or gaming platforms are often attacked by order of dishonest customers or competitors, while the cost of the services of large providers is unaffordable. The architecture of Gladius can solve this problem. After the release of the product, the team is likely to focus on this segment, since the available capacity (number of nodes) in the Gladius network will initially be low.

8. Competitive Advantages of the Project

Gladius differs from many ICO start-ups in its competitive advantages. Thus, there are no competitive start-ups for DDoS protection and CDN in the market - Gladius will have to win its share only from current players; at the same time, most of the market is claimed by large service providers.

This is connected with the nature of the market - consumers prefer to use the services of large providers, justified by the availability of their infrastructure and experience of mitigating intruders. In addition, access to the market is complicated by the fact that it is necessary to create sufficient capacity; so many providers have begun to develop DDoS and CDN directions based on existing IT business. In these conditions, it is not surprising that there is no enthusiasm for young projects.

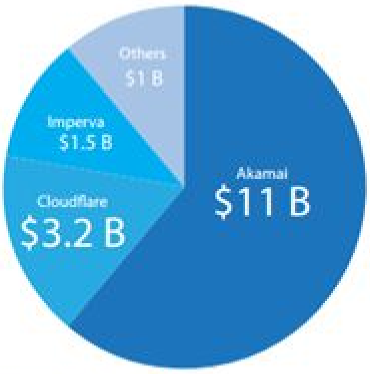
Thus, the review of competitors and advantages is aimed strictly at existing market participants and their solutions. Gladius also gives an analysis of the competitive environment in the white paper; their conclusions are more than logical:

1) Non-competitive business model

A large amount of power and virtual storage (server hardware) is required to build an infrastructure for DDoS protection and CDN creation within the framework for standard solutions. A service provider is forced to maintain this equipment even if there is no request from a client. In addition, a large-scale attack of intruders is a rarity and their scale is constantly growing. Thus, the company needs large investments to provide sufficient protection against potential attacks, and for financing of equipment maintenance costs.

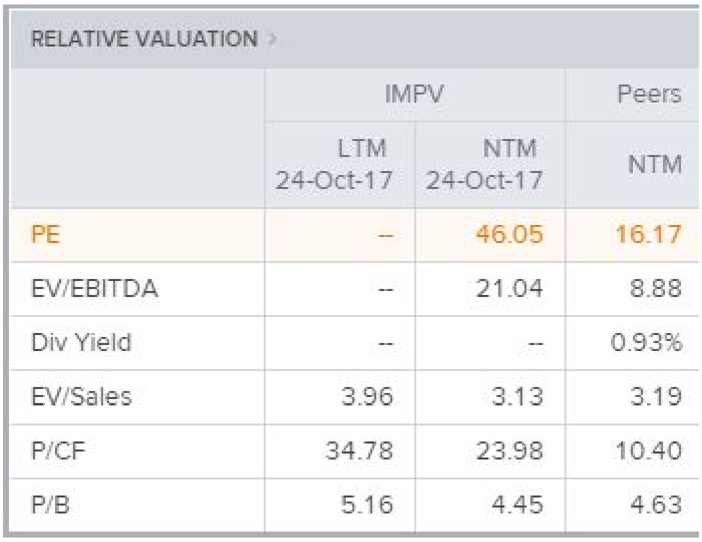
The situation regarding CDN is better - the equipment is not idle, but ensuring a maximum response for the website worldwide is often very expensive and logistically problematic (for example, a small number of users use the connection in a remote region hence servers will be economically unprofitable in such a region.)

This weakness of working providers is partly traced when considering the cost of such companies. It may often not correspond to the volume of services provided, justified by a high proportion of companies' own funds in the form of computer equipment. In particular, Gladius cites the following data on the capitalization of some large market participants, noting their disproportion to real business:



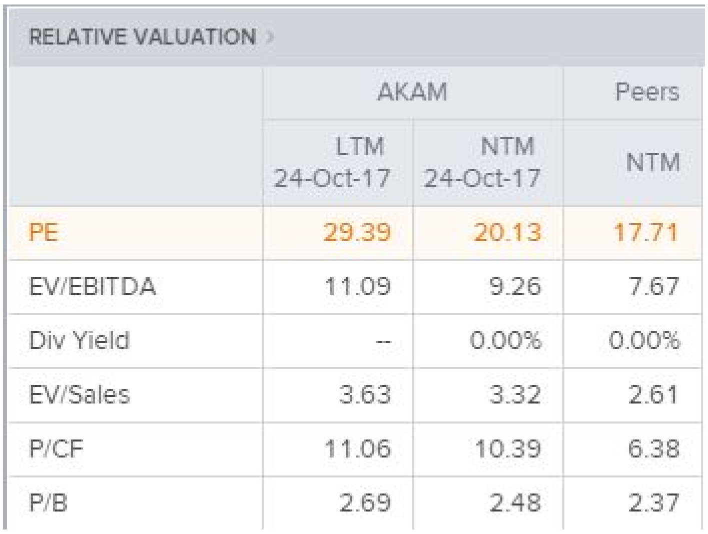
(Stratusly and Yahoo Finance and Fortune)

We can agree with this analysis. Cloudfare is a non-public company, but for Imperva and Akamai there is an opportunity to calculate market multipliers. So, Reuters estimates P / E NTM = 46 for Imperva, and 20 for Akamai:



RELATIVE VALUATION ›

	IMPV		Peers
	LTM 24-Oct-17	NTM 24-Oct-17	NTM
PE	--	46.05	16.17
EV/EBITDA	--	21.04	8.88
Div Yield	--	--	0.93%
EV/Sales	3.96	3.13	3.19
P/CF	34.78	23.98	10.40
P/B	5.16	4.45	4.63



RELATIVE VALUATION ›

	AKAM		Peers
	LTM 24-Oct-17	NTM 24-Oct-17	NTM
PE	29.39	20.13	17.71
EV/EBITDA	11.09	9.26	7.67
Div Yield	--	0.00%	0.00%
EV/Sales	3.63	3.32	2.61
P/CF	11.06	10.39	6.38
P/B	2.69	2.48	2.37

The use of a decentralized network, where each user (node) is actually a provider for these services, as well as a principle of payment for used capacity, solves these problems. The Gladius business model is much more flexible and cost-effective.

2) The existence of a single point of failure

The centralized nature of existing providers carries potential risks when an attack can be made directly at them. Theoretically, an attacker can get into a provider's system and make its protection useless. In this case, Gladius has the standard advantage of any business based on a decentralized system - security.

3) Cost of services and pricing

This problem follows from the first case (business model.) Given the low cost-effectiveness of periodic DDoS protection and irregular distribution of CDN nodes, providers set unreasonably high prices for their services.

4) Power limits

Since the installed capacity of a provider is proportional to its inefficiency in time, any provider will be limited in its ability to process incoming traffic. The capacity potential of Gladius is theoretically equal to all free and available power worldwide, and in fact, with the proper development of the platform, it can allow for deflecting the strongest attacks. The same with the efficiency in a CND system - due to the absolute geography of activity Gladius can potentially provide any user quality access to content.

All the competitive advantages, as well as the project as a whole, contain one nuance - without properly penetrating the platform into the network and having sufficient free and ready-to-use capacity, the client may not receive adequate protection or a quick response at all. Thus, the risks of inefficient platform development partly offset its prospects compared to competitors.

9. Risks of the Project

Gladius is a complex high-tech project. The key risk of such projects is technical implementation. Currently we cannot know whether the young team will be able to realize all the plans.

We hope that all key elements of the code will be available for audit by the community. This, on the one hand, reduces the risk of critical platform vulnerabilities, but on the other hand, can lead to a prolongation and increase in the cost of development.

Other risks, in our understanding, pale beside the above-mentioned ones. We will follow the progress of product development.

10. Economy of the Project

Gladius services' will be paid for in GLA tokens. Most of the revenues for the project will go on payments to nodes. A smaller share of revenue will remain in the company to finance protocol development and support. The white paper does not disclose what proportion of the income this will be. We have posed this question to representatives of Gladius and received a response - 1-2%. We think that 1-2% is very small.

At the same time, the economic risk will be reduced by the fact that 15% of the total GLA token issue will be used to finance operating expenses.

Also, part of the funds raised during the ICO will be reserved for potential future funding. The team expects that the launch of phase 2 of the roadmap may require additional funding. These funds will come out of the budget allocated to operational costs.

Thus, we note that the importance of economic risk will be strongly correlated with the volume of funds raised during the crowdsale. We still have a few questions about the financial model of the project, and we do not know whether the level of elaboration of the business model is really low, or instead that the team intentionally does not disclose information to a wide range of investors. This uncertainty should be borne in mind when deciding whether to invest in GLA tokens.

11. Investment highlights of the token

Gladius makes use of the computing power of its users and pays them a reward in the form of GLA tokens. Users - node owners - will form mining pools. Owners will be paid for their individual work in these official mining pools.

The more the demand for Gladius' services, the more the demand for the GLA token. It is assumed that all proceeds in GLA tokens will be transferred to node owners, minus Gladius' commission; this was described in the "Project Economics" section. Accordingly, the proportion of GLA tokens that will be sold to the market after reaching node owners will depend on the profitability of node owners. Node owners are not likely to sell more GLA tokens on the market than they need to finance their own costs. A significant portion of the costs are constant costs; together with the growth in demand for Gladius services, the demand for GLA tokens will grow, and along with the growing demand for GLA tokens, node owners' margins will grow. This is a positive endless circle for token value.

However, it is important to keep in mind that within the next 10 months, until phase 2 work is completed, cash flow for node owners will be zero.

Nevertheless, we do not recommend postponing purchase of GLA tokens. We emphasize that the project's hard cap looks very adequate against the background of most other ICO projects that conduct their own crowdsales simultaneously. Given the quality of ICO marketing, reasonable collection targets, and an interesting "blockchain" idea, we assume that Gladius will be able to collect a hard cap, and demand will exceed supply, due to which the token may grow in value on the secondary market after the ICO.

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.