

# Gladius Network Project

Whitepaper Version 0.9 - Working Draft (Subject to Change)



**Gladius**

# Decentralized CDN and DDoS Protection on the Blockchain

---

An automated marketplace where you can rent out your spare bandwidth and storage as well as purchase content delivery and DDoS protection services.

# Table of Contents

<b>1   Our Motivation</b> . . . . .	
1.1 The Gladius Solution . . . . .	4
1.2 Gladius' Mission . . . . .	5
1.3 Primary Objectives . . . . .	6
1.4 The Gladius Platform . . . . .	7
1.5 DDoS Protection Market . . . . .	8
1.6 Content Delivery Market . . . . .	10
<b>2   Gladius Token</b> . . . . .	
2.1 Token System . . . . .	14
<b>3   General Architecture</b> . . . . .	
3.1 Platform Overview . . . . .	15
<b>4   Roadmap</b> . . . . .	
4.1 Competitive Analysis . . . . .	16
4.2 Funding Breakdown . . . . .	17
4.3 Development Roadmap . . . . .	18
<b>5   Token Creation Breakdown</b> . . . . .	
5.1 Funding Details . . . . .	21
5.2 GLA Creation Ratios . . . . .	21
5.3 Additional GLA . . . . .	22
<b>6   Gladius Architecture</b> . . . . .	
6.1 High-Level Overview . . . . .	24
6.2 Databases and Network Joining . . . . .	25
6.3 Pools and Load Balancing . . . . .	26
6.4 Desktop Node Client . . . . .	27
6.5 Payment Services . . . . .	30
6.6 Online Web Portal . . . . .	31
6.7 DDoS Mitigation . . . . .	34
6.8 Content Distribution . . . . .	36
<b>7   Our Team</b> . . . . .	
7.1 Team Overview . . . . .	37

# 1.1 | The Gladius Solution

How Gladius is changing the cybersecurity landscape.

DDoS attacks are becoming an increasing reality of operating a business with an internet presence. These attacks can cost an incredible amount of money, not just in lost uptime, but also a loss of consumer trust and crisis PR. Last year alone DDoS attacks amounted to a \$150 billion loss, while on average corporations can spend over \$5000 a month on protection from other DDoS protection services, even if they never suffer an attack. This happens while a majority of computing power and bandwidth in the world goes unused. Gladius envisions a future where these vast resources can be utilized to mitigate attacks. ([Incapsula](#) and [SecureList](#))

By leveraging the blockchain to allow communication between computers, and a pay as you go marketplace, Gladius can facilitate the creation of the extremely fault tolerant and inexpensive pools tailored to a client's specific needs. Asside from just filtering traffic, these pools will be able to accelerate content as well.

By decentralizing and removing the middleman, the whole nature of protecting a website will change. Buisness that previously couldn't afford adequate protection can purchase services that perfectly fit their budget. Those paying hundreds of thousands of dollars for a service they never fully utilize can start paying for only exactly what they use - and for much less. In addition, customers who are tired of paying for a high speed internet connection (that is only used for a few hours a day) can finally put that connection to good use.

## 1.2 | Gladius' Mission

Our motivations, directions, and goals as a company.

Since the dawn of the internet, the technology surrounding websites has been constantly evolving. With this new technology comes the power to enhance a business' online presence but also harm it. Technology is truly the greatest double edged sword, however. Gladius' mission is to negate the harm brought by new vulnerabilities and take advantage of the same style of decentralized network that attackers have long used. Gladius is concerned primarily with protection from DDoS attackers and the implementation of a high quality CDN.

While there are many who believe DDoS protection is only needed in very few circumstances, DDoS protection is important for any entity that has a presence on the internet. DDoS attacks have cost millions for household names like Blizzard Entertainment, the BBC, and GitHub. The average DDoS attack costs a company 2.5 million dollars.

Any business should want to increase their site speeds as well as their response times. A well done CDN can do not only that but also greatly expand a site's reach offering unparalleled access in any corner of the globe. The massive advantage that a CDN grants to businesses is easily noticeable by the fact that the CDN market in 2015 was worth \$4.95 billion dollars but is expected to more than triple by 2020 to a value of \$15.73 billion dollars.

The ability to greatly, if not completely, negate DDoS attacks and the ability to create an effective and secure CDN puts the Gladius team in a unique position. The team's goal to fully utilize blockchain technology to fight against DDoS attacks and provide a competitive CDN service. However, above all else, the Gladius team is constantly striving towards a highly competitive marketplace in order to bring any consumer the best possible service. This goal is always at the forefront of Gladius' mission to make businesses safer and more effective.

## 1.3 | Primary Objectives

The primary milestones we are aiming for with our core product.

### **Phase I: Building an Initial Content Distribution and DDoS Protection Network**

The Gladius team is aiming to create a CDN and DDoS mitigation service by using blockchain technology, distributed mining pools and smart contracts.

This goal will be met and these technologies will be incorporated throughout the entire course of Phase I which is made up of 3 stages (see Roadmap). Once Phase I is complete, there will be a complete and comprehensive network that is capable of handling several Gbs of connections per second and drastically improving site load times. This will include multi-level protection and a private rollout to select partnered websites.

### **Phase II: Develop Network to a Commercial Scale**

The aim of Phase II is to finalize the network from Phase I and making it commercially viable on a large scale. This means greatly increasing the amount of data throughput to cope with a far greater demand. Additionally, Gladius node pools will be greatly improved with full vetting and rating processes and smart contracts will be expanded for discovery and identification services.

Once Phase II is complete, there will be a polished network that is ready to take on the demands of hundreds, if not thousands, of websites. Phase II also allows for the possibility of expanding pools. Each pool will be rated and validated to ensure proper performance. Additional CDN features such as static content caching will be added depending on levels of funding reached.

## 1.4 | The Gladius Platform

How our entire system comes together.

Gladius' goal is to create a fully decentralized, peer to peer, serverless node network to connect bandwidth and storage pools to websites looking for DDoS protection and expedited content delivery. Anyone with a computer can download and run the Gladius peer client in the background to rent out their unused bandwidth and storage space and earn Gladius Tokens (GLA). Large pools with hundreds, if not thousands, of nodes will then be able to handle a continuous stream of requests to validate website connections and block malicious activity.

Client nodes can be started up on any Linux, Windows, or MacOS machine and will automatically run in the background when you choose. Users will be part of localized verification pools. Every website request a user validates will earn them Gladius Tokens. In turn, users can sell these tokens back to websites to create an economic cycle that promotes the growth of the Gladius Network.

Websites looking for protection will simply be able to create an account on Gladius' website, acquire Gladius Tokens, and then request services in a matter of clicks. Once a website is part of the Gladius network, a live request graph will be available to monitor connections, protection, and speed deltas.

The entire platform will progress in 3 steps which can be seen in Section 4. First we have the proof of concept stage that will showcase all of the basic functions of the network while not actually going into official production mode. Then, after our token sale, we will have a closed production period where anyone can download and run the client node. However, only approved websites can purchase protection since the network and pools will still be in early growth stages. Once the Gladius Network can support a large attack and the core tech is improved, we will enter the next stage. The Gladius Network will then allow anyone to purchase services from the various pools.

The process will be streamlined for both the clients and the requesters. People who want to purchase web services will simply be able to create an account with Gladius, purchase Gladius Tokens through us, choose a website they wish to synchronize, set a base and max price for how much they are willing to spend, and then request and monitor all connections to their website.

Nodes will easily be able to create a local account and wallet, configure the network settings to open any necessary ports, join any pools that they are best suited for, and start earning GLA. Users will be able to toggle when they are renting their spare bandwidth and space in a matter of seconds. There will also be additional configuration settings to automatically toggle the service based upon time of day, other programs running, and even more in-depth user configurable parameters.

## 1.5 | DDoS Protection Market

What is pushing the DDoS protection market forward.

It has become increasingly obvious that any business today looking to compete requires a strong internet presence. This unfortunately creates more opportunity for attacks and thus protection, like that offered from Gladius, is required.

Research has shown that the increased vulnerability to DDoS attacks is one of the main forces that push the growing market for internet security solutions:

### 1) Growing risk of cyber attacks

As the world becomes more connected by the internet, valuable information and services also come under greater risk of attack. DDoS attacks have become more and more common in recent years and the stakes have greatly increased. This increased threat results in the quick expansion of security solutions to deal with and prevent DDoS attacks.



## 2) Unfavorable market conditions

While the need for DDoS protection as a concept is excellent, the solutions available are not. DDoS protection is often very expensive and has varying degrees of success. The lack of a reliable and cheap solution creates a need for new players in the DDoS protection business.

## 3) Government interest

Numerous attacks to private industries and government databases in past years has brought more attention to defending government information. This has increased the demand for proper protection from DDoS attacks.

DDoS attacks are unfortunately becoming increasingly common and are en route to becoming an expected occurrence for any company on the internet.

According to [Nexusguard's Q1 2017 "Threat Report"](#), DDoS attack frequency has increased by a staggering 380 percent in the first quarter of 2017. Nexusguard is currently a huge player in the business of DDoS mitigation and thus their word is not to be taken lightly.

Nexusguard comes to the conclusion in its most recent threat report that DDoS attacks are unpredictable. Additionally the "Internet of Things" has created many openings for potential attackers to abuse, these new and exploitable devices can easily give valuable information and create new targets for attacks from hackers.

This new level of threat is evident in one of the largest DDoS attacks in history, this attack took place on October 21st, 2016 and managed to affect a myriad of services. These services, like Airbnb and Amazon, were crippled and effectively brought to their knees by this attack. Some may view this attack as an extremely well coordinated and a difficult maneuver to pull off.

However, according to [Forbes](#), a single “angry gamer” was to blame for such a devastating blow to numerous companies. The fact that a single person can bring down corporate giants is an extremely worrisome concept and must be addressed.

In response to this attack, the United States department of Homeland Security has taken measures to prevent future DDoS attacks. However, even Homeland Security admits in their article, [Snapshot: Turning Back DDoS Attacks](#), “CSD’s DDoSD project is beginning to tilt the playing field toward defenders. Much work still needs to be completed, especially in the area of developing proactive defenses against new types of attacks. Cyberspace is always changing, and the work to prevent DDoS attacks and other threats from malicious actors will never stop.”

With all of this information in mind, it is evident to any observer that there is much work to be done in the field of DDoS protection. It is the hope of the Gladius team that our product can address the needs of an ever changing internet landscape and meet the requirements set forth by these market driving forces.

## 1.6 | Content Delivery Market

What is pushing the CDN market forward.

The value of CDN services is apparent to any latent observer purely based on the extremely fast growth of the industry as well as the widespread use, and success, of such services. With more and more options to choose from in the CDN market, it is the role of Gladius to offer superior and unparalleled service at a cutthroat rate.

Research points to one of the main forces for growth in the CDN industry is the need for speed from users on all platforms:

### 1) User demand

Today, users demand higher quality connections to sites and in addition, there are significantly more devices connected to the internet than ever before. In 2017, 8.4 billion devices will be in use. This demand requires more means to deliver content quickly and effectively.

### 2) Raising the bar

While a CDN used to be something that is optional or perhaps something that businesses would use to “go the extra mile”, CDN’s have become an expected feature of nearly every major site. Today, there are 14,620,983 live websites using a CDN. A CDN is no longer optional, it is an expectation of the consumer.

### 3) Monetary implications

A CDN provides significant improvements in speed, and in an age where the consumer expects instantaneous responses it is vital to appease the consumer in this regard. This appeasement is not only beneficial so the consumer is pleased, but more importantly, so the consumer actually consumes what is available. In fact, this need for information quickly is so pronounced that over half of consumers will leave a retail or e-commerce site if it’s slow.

CDN’s are an exciting new way to greatly increase the speed of information. The speed at which information travels around our interconnected globe is the greatest factor in determining the growth of businesses everywhere and CDN services, like those offered by Gladius, are at the forefront of connecting consumers to businesses and consumers to consumers everywhere.

According to Dyn’s Global Consumer Online Shopping Expectations 2015 report, 2015 saw sales figures upwards to \$1.592 trillion, this e-commerce accounted for 6.7% of retail sales globally. These figures are only going to grow as e-commerce continues to show its numerous benefits over physical sales.

It is only logical to improve the quality of CDN's since it is obvious that e-commerce will continue to grow, and with it, the need for effective CDN services.

Dyn comes to the conclusion in their report that a major barrier keeping even more people from shopping online is the fear of insecure sites as well as slow speeds. Long loading times on sites makes the site seem untrustworthy to most consumers and insecure. Having an established CDN makes sites seem significantly more trustworthy and safe. This impression of trustworthiness and security is not lost with the consumer and is will increase the likelihood of a purchase from the consumer, as is evident by Dyn's findings.

Dyn also finds, in page 6 of their 2015 report, that "over 60% of consumers plan to make an upcoming purchase from their mobile device". If any device at all in the arsenal of the modern consumer is expected to be fast, it is the mobile device. The mobile device is the epitome of the inherent consumer need for things to be quick. Everything about a mobile device is designed to be fast, its design, interface, layout and now it is only reasonable for the sites on a mobile device, like any device, to be as fast as possible for the average consumer.

However, the most compelling argument for a CDN has little to do with consumers preferring speed. In fact, there are presumably few that would "prefer" the speed that a CDN has to offer. Instead, consumers require the speed of a CDN, they require the immediacy of intimacy to their information. They require the next page to load to search for what's next and what to click on. They require the prompt just around the corner, just around the loading screen to see the great yellow button that almost seems to command them to buy. Everything about a mobile device is designed to be fast with its layout and its interface. It is therefore reasonable to assume that all sites need to make their websites as fast as possible for the average consumer.

The human attention span is eight seconds. Just eight seconds. It is these seconds that must be utilized to the fullest and not ignored.

For it is these eight seconds that bring them to rubble. It is these eight seconds that bring them to their knees. It is these eight seconds, which if taken advantage of, can build corporate empires, or if ignored, leave them in the wind.

A CDN is more than just a way to speed up a business's site, this speed is the very lifeblood of nearly all e-commerce transactions, it is the foundation and pinnacle, it is alpha and omega. More importantly, as the ecommerce market grows, the demand that a company has a good CDN to compete and satisfy consumers with consistency, effectiveness and efficiency, will dramatically increase

## 2.1 | Token System

The role of tokens in the Gladius Network Ecosystem

For our platform we will be releasing the Gladius Token, or GLA. A fixed supply of tokens will be issued during the Token Creation and no more tokens will ever be created. The tokens will immediately be available to be used on our network system we are launching prior to the public sale.

GLA will be a key component to the Gladius Network in that the token will be used by websites to buy DDoS protection and CDN services. The majority of the fees will go to the node owner (the individual renting out their spare bandwidth and storage space) with a small portion going back to protocol development and support. All fees will be denominated in GLA, which is subject to change based on supply and demand.

The previously mentioned node owners who are part of protection pools will essentially act as miners and be incentivized with GLA for their network support. Owners will be paid for their individual work in these official mining pools. As opposed to typical blockchains, mining will be rewarded for sharing bandwidth and storage space rather than computing power (proof of work), and ownership of the currency (proof of stake).

The token is designed so that it will likely reflect the growth of the Gladius Network. Additionally Gladius will look into commissions for node owners in currencies other than GLA.

Max Sale Issuance: 34,000,000 GLA

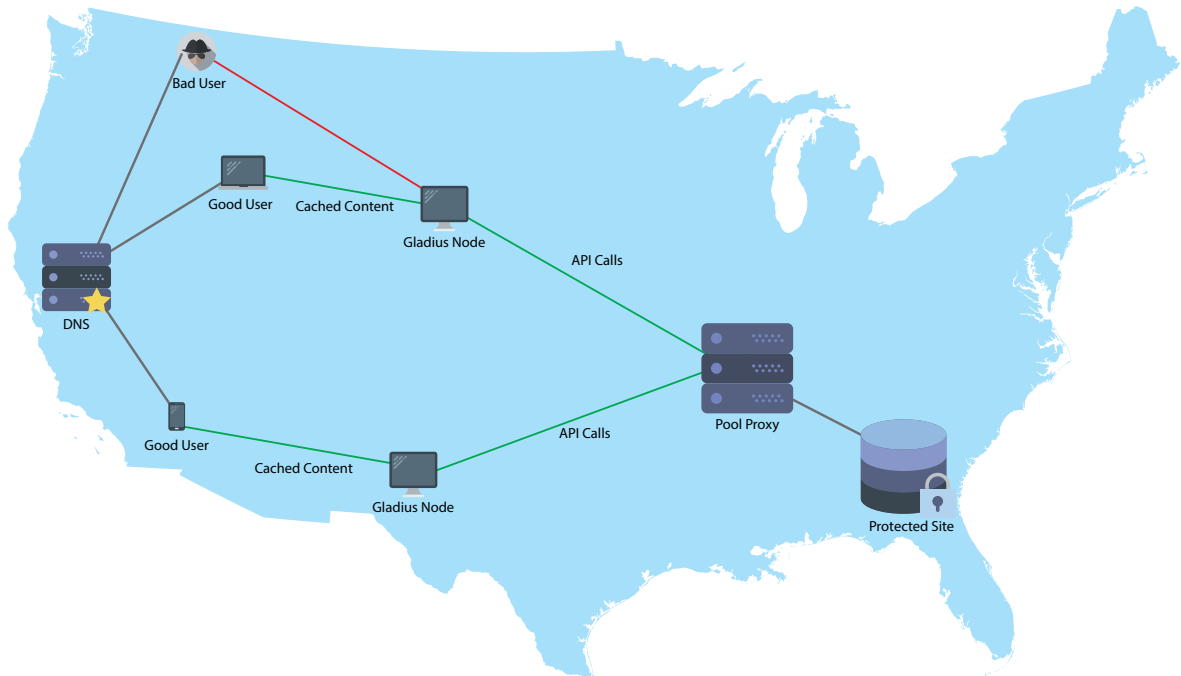
Max Token Issuance: 48,200,000 GLA

Max Token Market Cap: \$12,500,000

Max Market Cap: \$20,500,000

## 3.1 | Platform Overview

The general architecture of the Gladius Network.



The Gladius Network architecture, comprised of several distinct sections.

### 3.1.1 ETHEREUM BLOCKCHAIN

Acts as a centralized database for storing the proxies and their associated service providers. There is a cost associated with being added to the database.

### 3.1.2 CUSTOM PROXY

A series of clients act as a distributed traffic validator while keeping the protected service hidden from the exterior. These nodes will also be able to cache site content and be part of the Gladius CDN as points of presence.

### 3.1.3 PROTECTED & ENHANCED SERVICE

Simply changes their nameservers to the ones associated with the custom proxy to enable protection. These services are negotiated with a smart contract.

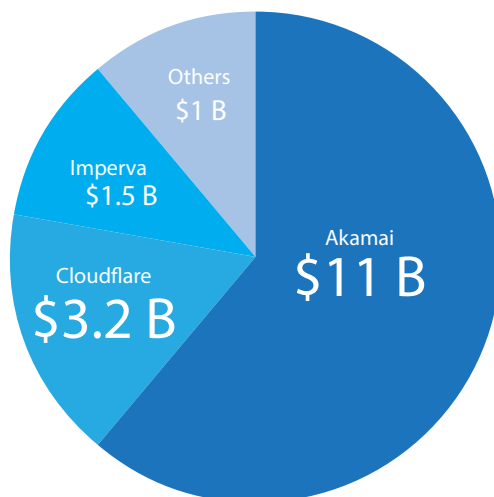
## 4.1 | Competitive Analysis

Our differentiation with the competition.

On October 21st 2016 Dyn, a company that controls an enormous part of the internet's DNS infrastructure, was hit by largest DDoS attack the world had ever seen. Over 1.2 Tb/s of malicious connections brought down this cornerstone of the internet. Sites including Twitter, Netflix, Reddit, CNN were all completely shut down for an entire day. Billions of dollars were lost because of that attack. ([The Guardian](#))

Moreover, it is becoming cheaper to actually launch DDoS attacks. For as low as \$5, anyone can purchase access to a botnet and start causing mayhem. For \$400 you can practically take down any site- even ones protected by industry standards such as Cloudflare. This entire network for rent is capable of hitting sites with 125 Gbps. This means that the actual cost of an organized DDoS attacks "using a botnet of 1000 workstations can amount to \$7 per hour." ([Security Affairs](#))

Cloudflare has a market cap over \$3.2 billion. Imperva/Incapsula's cap is over \$1.5 billion. Akamai's is over \$11 billion. Every one of these DDoS protection industry standards charge websites an absurd amount of money for protection that may or may not even be needed. Cloudflare's lowest enterprise tier starts at \$5000/month, but the actual prices charged to each client is larger than this depending on the size of the website. ([Cloudflare](#))



([Stratusly](#) and [Yahoo Finance](#) and [Fortune](#))



Gladius takes the middleman out of the picture by decentralizing the entire network. Our pay-as-you-go service enables websites to custom tailor protection to their exact specifications also. If you don't get DDoS'd you don't have to pay as much. It's that simple. Our marketplace of protection pools means that individuals will compete to provide protection at the lowest price possible. So as the platform matures the price per Gb will be on a continuous downward trend.

In the past Cloudflare has been put under backbreaking loads. These attacks have left rippling effects for all websites under Cloudflare's guard. Cloudflare is centralized. There's no going around that for them. This means there is a single point of failure in their network. If an attacker can take down their main servers, all the underlying websites fall to pieces also.

The Gladius network is designed so that this will never happen. Websites will be under the protection of thousands of different pools. An attacker would have to hit every single pool to have the same effect as DDoSing Cloudflare. Never before has DDoS protection been done this way using a blockchain facilitator.

## 4.2 | Funding Breakdown

The specifics of where all money will go.

Funds from our token sale will help the development of the Gladius Network. The following is a tentative breakdown of how we are planning to use funds for development.

### **Core Development | 40%**

The largest portion of funds will go to completing the development of the Gladius Network as described in this paper. This includes the Gladius node network, intelligent DDoS protection, smart node pools, smart contract systems, supporting protocols and systems, end user applications, etc.

### Security | 20%

The next major portion of the funds will be going towards developing extremely tight security for our network. In specific this will be encapsulate encryption between nodes, DNS obfuscations, and more.

### Operations | 20%

This covers the day-to-day costs incurred for a functional system. This includes hosting, infrastructure, staffing, outsourcing, management, and other related expenses.

### Legal | 10%

To comply with the industry's numerous regulations, we will need legal advice and consultation to navigate these sometimes precarious waters.

### Marketing | 10%

The marketing budget will be used for strategic partnerships and directly marketing to consumers. This will lead to a larger network with more nodes, and more websites using the services. Overall more money will be running through the system and going to the node owners.

## 4.3 | Development Roadmap

The stages of our network development.

### PRE TOKEN SALE

The goal of this stage is to complete a minimum viable product to showcase the core system architecture of the Gladius Network. We will have a functional CDN that users can participate in and earn tokens for their bandwidth and storage space. DDoS protection will be done through firewall rules.

Note - This stage will be immediately usable by purchased tokens. This is our core product for the Gladius Token. Additional features are scheduled to be added to this version.

#### Development Goals | Pre Token Sale (Released on GitHub: [github.com/gladiusio](https://github.com/gladiusio))

- Smart Contracts V1.0 - Payment flow from websites to pools to nodes
- Gladius Client V1.0 - Ability to earn GLA renting bandwidth and storage space
- Gladius Web Portal - Ability to pay pools for website CDN service
- Gladius Pool - Ability to create pools

#### PHASE 1 - ETA MARCH 2018

The goal of this stage is to complete a working first iteration of a complete CDN and DDoS protection network capable of handling several Gbs of connections per second. This will include multi-level protection and a private rollout to select partnered websites.

#### Development Goals | Phase 1 (ETA: March 2018)

- 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

#### PHASE 2 - ETA AUGUST 2018

The goal of this stage is to completely finalize the network so that it will be commercially viable on a large scale. This means that we will have a network large enough to take on hundreds, if not thousands, of websites. Additionally we will potentially allow for more pools to be created, each being rated and validated to ensure they are performing up to standards.

### Development Goals | Phase 2 (ETA: August. 2018)

- Remove 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
- Complete auto-payment and bid/ask system for the marketplace

### PHASE 3 - ETA DECEMBER 2018

The goal of this stage is to add several additional features to the Gladius Network.

### Development Goals | Phase 3 (ETA: December 2018)

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

### FUNDING GOALS

\$4 million - Basic DDoS, CDN, and Load Balancing

\$5 million - CDN File Upload

\$6 million - 5 Layer DDoS Protection

\$7 million - Advanced WAF

\$8 million - CDN Dynamic Content Caching

\$9 million - Gladius App Store

\$10 million - Layer 7 DDoS Protection

\$11 million - Advanced CDN optimizations

\$12.5 million - Advanced DDoS optimizations

## 5.1 | Funding Details

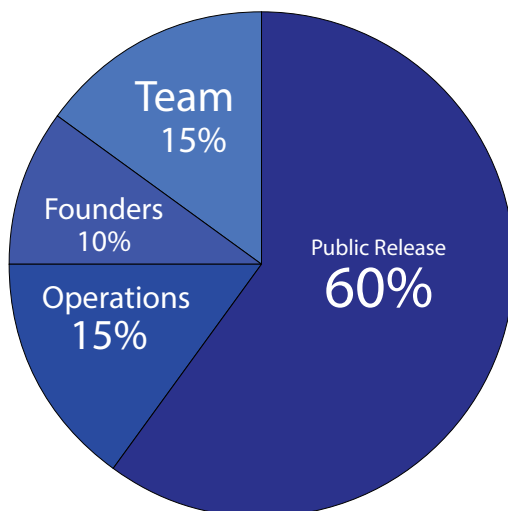
The specifics of our Token Sale.

Gladius Token Public Presale will commence November 24th

- ETH will be accepted for acquiring GLA.
- Presale will take place before the public sale to accredited investors only.
- Public Presale and Public Sale will be open to everyone
- Token Sale Minimum: \$4 million
- Token Sale Hard Cap: \$12.5 million
- Max Coin Distribution: 48.3 million GLA
- Address for the sale will be on our website: [gladius.io](http://gladius.io). Do not send ETH to any other address you see!
- Tokens will be readily usable in our network to improve websites.

## 5.2 | GLA Creation Ratios

How the fixed supply of Gladius Tokens will be allocated.



Tokens will adhere to this distribution. After the funding period is complete, the Partnership and Core Dev tokens will be allocated based on the amount of public coins sold.

## 5.3 | Additional GLA

How the rest of the coins will be put to use.

The additional GLA generated will be for both the core development team and for future stakeholders and strategic partnerships. Additionally coins will be given out to members of our bounty programs.

### 5.3.1 TOKEN SPLIT

-10% of all GLA will go to the core founders. 15% will go to the advisory, community, and marketing teams. 15% will go to operational costs, which includes bounty programs, day-to-day costs, etc.

-The coins for the founding team will be locked for 18 months.

-The other coins will be available through various vesting periods and will be given out to the members of our bounty programs, advisors, and early node operators. Pre-sale bonuses will be locked for a certain period to vest.

### 5.3.2 FUTURE SPENDING

Part of the GLA supply will be kept for potential future funding. The Gladius Network Phase 2 may require additional funding and we see this as a way to accomplish just that. These funds will come out of the budget allocated to operational costs.

### 5.3.3 COMMUNITY CATALYZATION

We will use a portion of our Gladius token supply to promote platform adoption, developer interest, and community growth.

## 5.4 | GLA Pricing

The change of pricing for Gladius tokens over the sale period.

### Public Sale

No Lockups

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

### Public Presale

ONLY bonuses are vested!

Contribution	Bonus	Vesting Period	Rate
1ETH - 17ETH	20%	1 Month	600 GLA/ETH
17ETH - 34ETH	25%	1 Month	625 GLA/ETH
34ETH - 103ETH	30%	1 Month	650 GLA/ETH
103ETH - 334ETH	35%	1.5 Months	675 GLA/ETH
334ETH - 689ETH	40%	2 Months	700 GLA/ETH
689ETH - 1724ETH	45%	2.5 Months	725 GLA/ETH
1724ETH+	50%	3 Months	750 GLA/ETH

### Gladius Token Distribution

Total Supply	<b>48.2M GLA</b>
Sale Supply	<b>34M GLA</b>
Total Market Cap	<b>\$20.5M</b>
Sale Market Cap	<b>\$12.5M</b>

## 6.1 | Gladius Architecture

The overarching technical solution.

Gladius works similarly to traditional CDN and DDoS protection companies by creating a custom proxy which sits between a website's server and the open internet. However, unlike traditional networks the layer that sits between the website and the internet is made up of small clients that split up the traffic verification and cached files/content into thousands of tiny parts that are able to communicate with each other in fractions of seconds.

Pools of nodes exist to group people into demographic groupings to provide a better and faster network experience. These pools can be seen and accessed through a marketplace where their information on geographical location, pool size, and reputation can be viewed. Pools can additionally consist of only one individual's or organization's resources, allowing them to run their own instance of a Gladius pool by not approving outside nodes. Using our contracts, anyone can distribute their content and combat DDoS attacks.

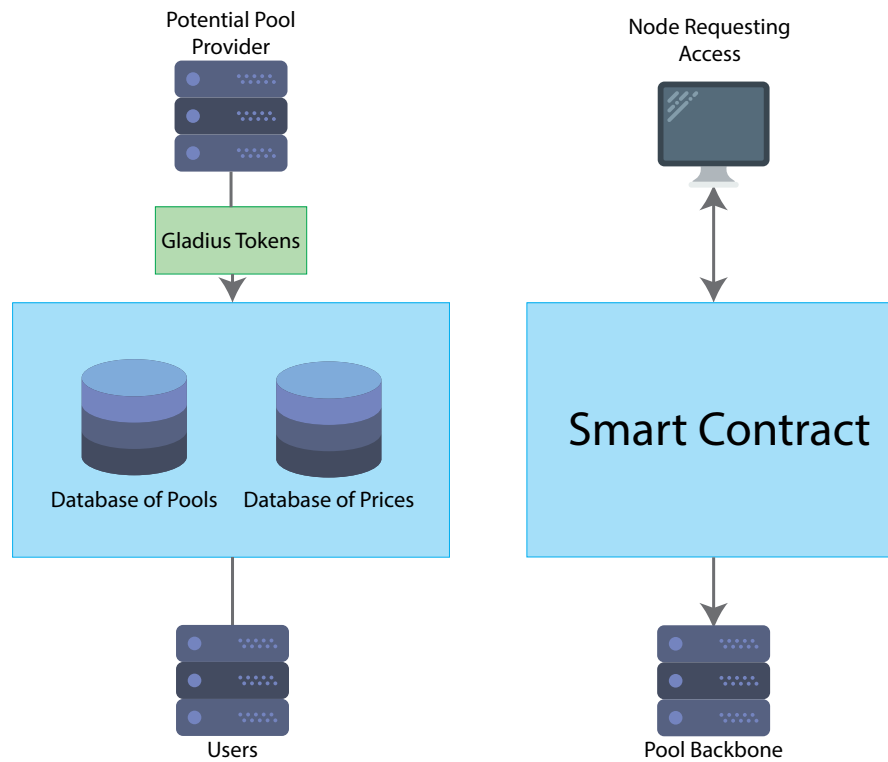
A critical component of any DDoS protection system is keeping the IP address of the server hidden which the Gladius network accomplishes by having a final proxy mask the IP from the nodes in the pool. The network will also have a built in reputation system to prevent malicious pools. Pools also have the ability to approve individual nodes entering the pool, allowing for a secure experience.

To create a fully functioning CDN, each node will be capable of caching key content, and then delivering that content to nearby clients. A client will be directed to closest node to them by using a location based DNS server, guaranteeing they will always be sent to the nearest available node.

## 6.2 | Databases & Joining the Network

The key features of the databases, and joining.



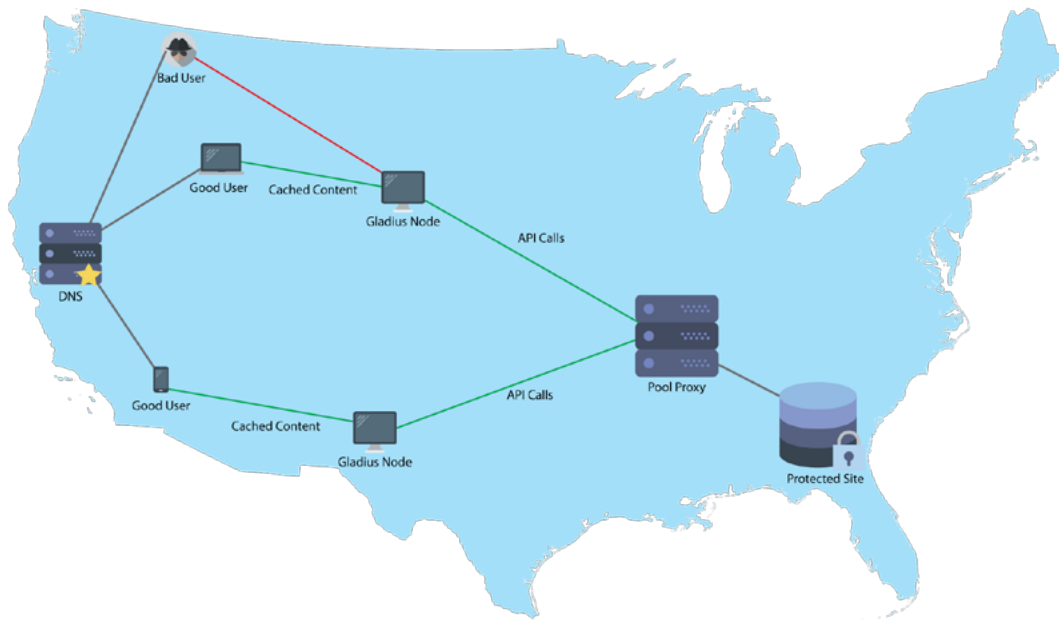


The database of pools will be maintained on the blockchain and appended to by miners. This has an inherent cost associated with it, along with a fixed cost, which incentivizes nodes to be serious as well as honest. Joining a pool is initiated by a node with an Ethereum smart contract. The pool can deny this request if it believes the node would not be beneficial based on the user's general demographic information such as location and available bandwidth and storage space.

The database of pools will contain information about reputation, bandwidth, maximum cache size, and location. Reputation will be based on key information such as user reports and subsequent investigations, protection provided over time, total pool age, and total pools size. Bandwidth will be based on the aggregate of the nodes available bandwidth as well as the maximum bandwidth the pool receives. Location will be viewable on a per node basis. Maximum cache size is based on the aggregate of storage space made available by nodes. Having all of this information allows for websites to choose pools that would be best suited for their needs. For instance, websites could pay more for a very trusted pool that has many nodes close to their target audience.

## 6.3 | Pool Manager

The key features of the load balancing, and pools.



Every pool would have a DNS service that would distribute the traffic to the nodes for verification. Because of the nature of DNS, it is easy to distribute the load over multiple nameservers creating a very fault tolerant system. This coupled with the fact that these nameservers could be protected from most attacks with firewall rules because they are only serving very simple content. Pools would then have the ability to decide how they want to distribute their resources to best fit the needs of their customers.

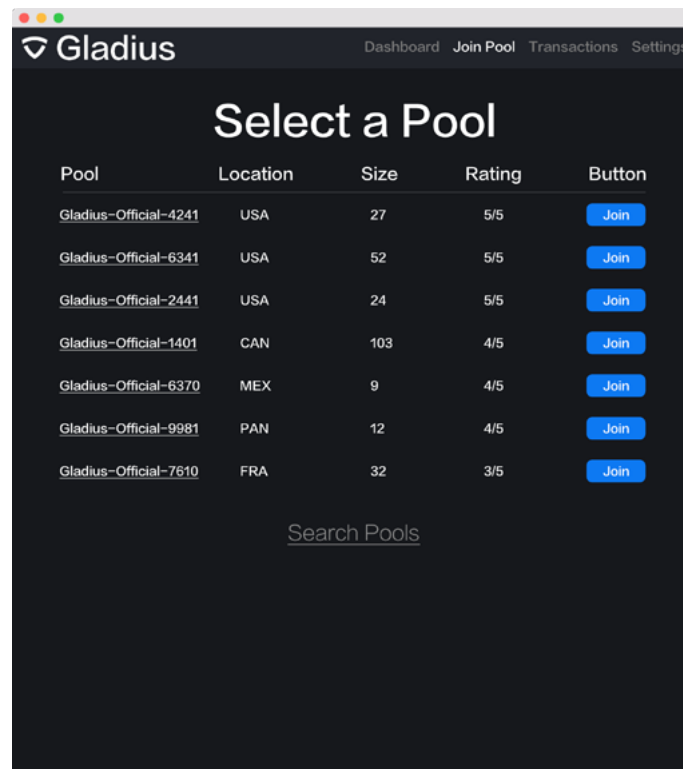
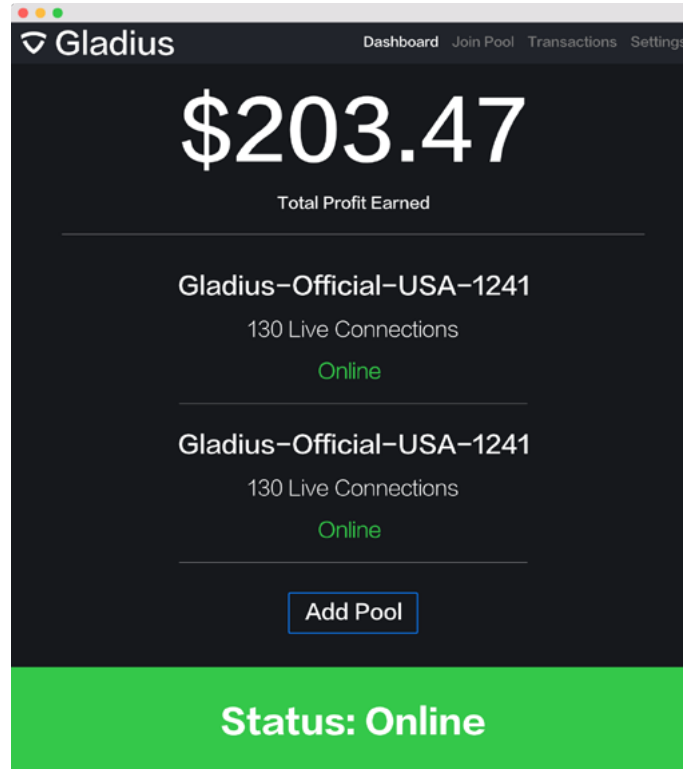
There will also be a final proxy server (or servers) run by the pool manager to mask the true IP of the destination from any potentially malicious node.

This model allows for highly scalable and efficient traffic verification, as well as geographically based acceleration. The protection layer of nodes is hidden from potential bad actors with DNS, making the pool very tolerant to attack on nodes.

This architecture results in only a small point of failure to the system which is key to a successful DDoS mitigation service. Because of the hidden nature of the majority of the network it is easy to see where an attacker would target, allowing the pool to fortify the single point of entry.

## 6.4 | Desktop Node Client

The key features of the software client for nodes.



Gladius Dashboard Join Pool Transactions **Settings**

# Settings

**\$10,024**  
Current Balance

0x3qde24612831298ec  
Wallet ID

[Send](#) [Request](#)

[Logout](#)

Gladius Dashboard Join Pool **Transactions** Settings

# Transactions

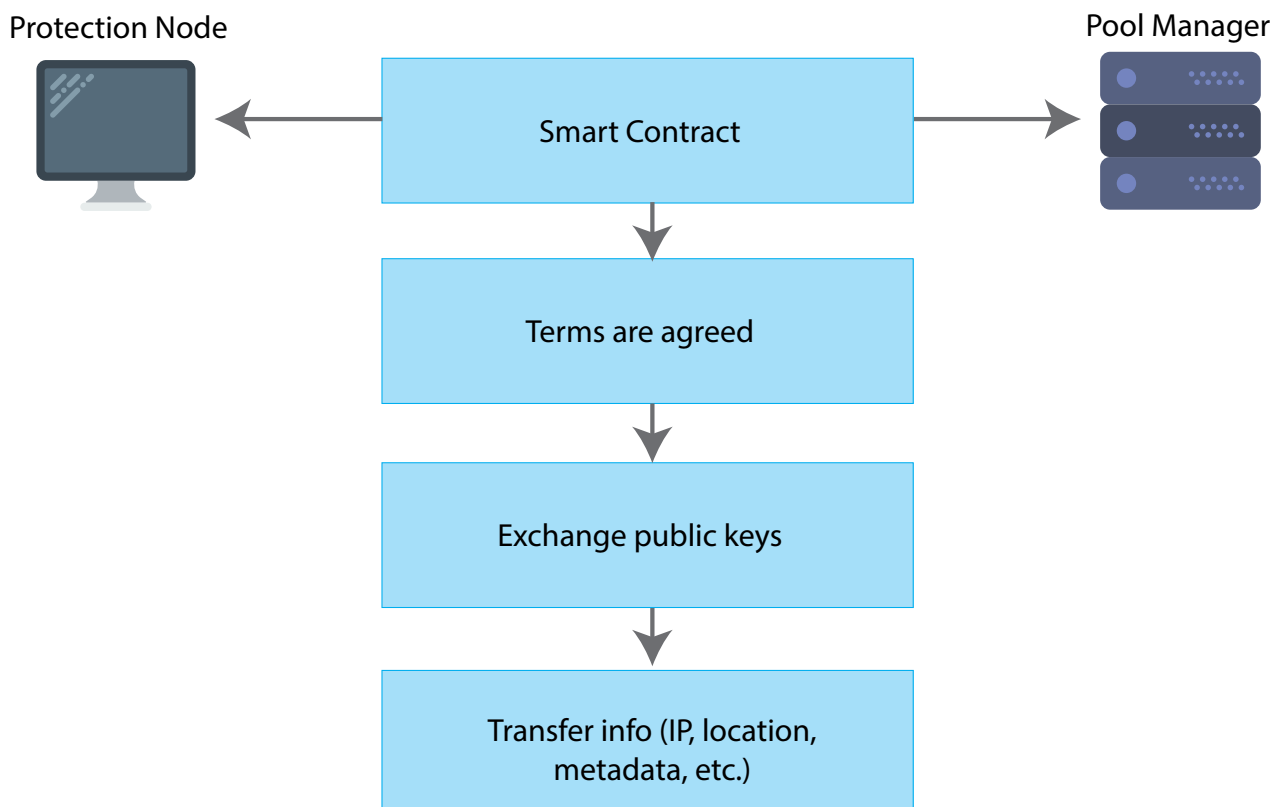
Transaction ID	Earned	Date
<a href="#">0x07bf874625273481</a>	\$0.27	2017-02-05 13:05:45
<a href="#">0x924fvef625273481</a>	\$0.43	2017-02-05 13:05:45
<a href="#">0x8826412bdu3d2011</a>	\$0.11	2017-02-05 13:05:45
<a href="#">0x05234grg25273481</a>	\$0.92	2017-02-05 13:05:45
<a href="#">0x028r1481dw1412331</a>	\$0.10	2017-02-05 13:05:45

[See Older Transactions](#)

The software node client is a cross-platform desktop application that runs a lightweight service in the background to communicate with associated pools and verify forwarded traffic requests in real-time. Each node makes up an integral part of the entire system, but having one go down results in little to no protection loss.

In a fraction of a second the client will verify the requests and send a response back to the pool if the request is valid, otherwise nothing will happen and the malicious request will never be routed to the destination. All of this work takes place on the user's computer and is securely encrypted. Once the cycle is completed then the contract is completed and the node is awarded a portion of the Gladius Tokens.

The nodes can be part of multiple pools so long as they fit the demographic requirements. This means that you can accumulate more GLA so long as your bandwidth, storage, and computation power can handle it.

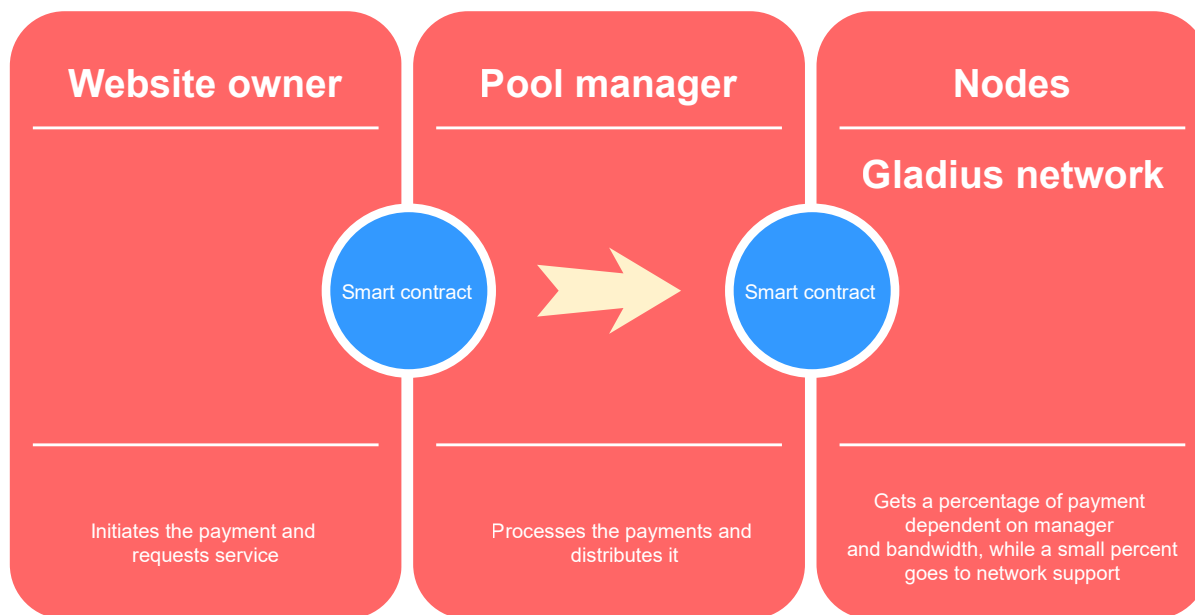


When a node has been approved it will exchange public keys with the pool manager allowing it to securely transfer information such as IP address and location. Once this is complete the node ID will be appended to the blockchain as a member of the pool. This allows verification of the number of members of the pool.

Each node can communicate with other nodes to exchange information about which IP addresses are currently flooding the network, or what type of traffic one node believes is malicious. This strategy can quickly enable a pool wide block of traffic before the attack even if only one node identifies it.

## 6.5 | Payment Services

How payments travel through the system



Cost is determined by the pool provider and split proportionally among the nodes in the pool with the possibility of a certain percentage being maintained by the load balancer (as determined by the pool provider). This is to incentivise the upkeep and maintenance of high quality pools while discouraging anyone from creating low effort pools with weaker hardware.

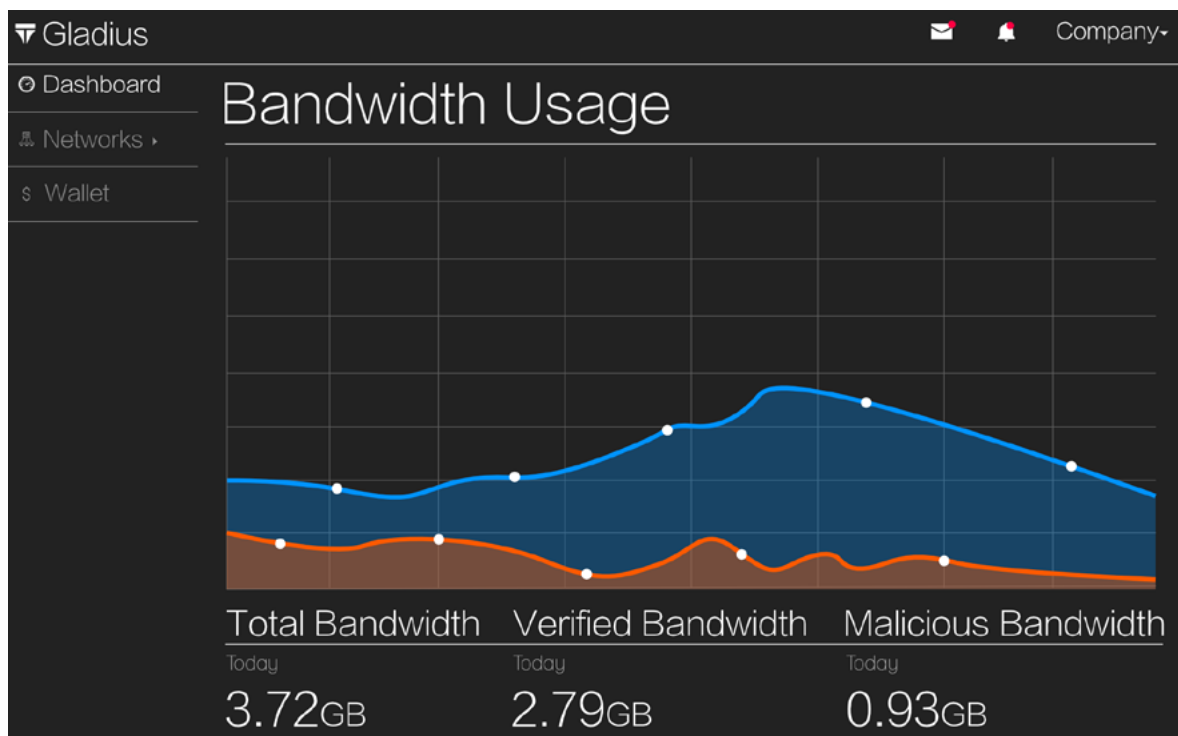
High quality pools will have better ratings and will subsequently be selected more often by services and sites looking for DDoS protection.

This architecture means there will be extreme competitiveness while also keeping margins for the pool fairly good due to there being no middle man. Pools can adjust prices on a need basis (usually to adjust for Gladius Token value). This will shift prices around occasionally, but pools can have the option to select a USD value which will change the amount of GLA charged in real-time.

A small percentage of every transaction in the Gladius Marketplace will go back to the company for purposes of incentivizing open source development and bug bounties. This will be a negligible amount so as to not discourage pools from

## 6.6 | Online Web Portal

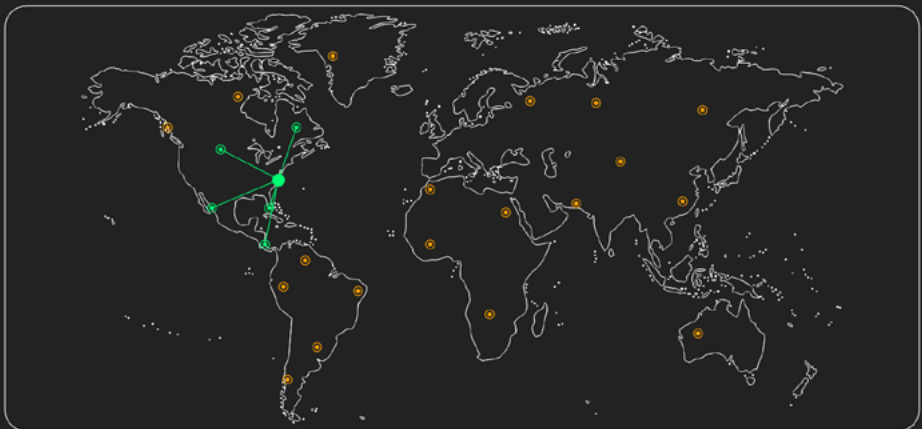
How users can request DDoS protection for their services.



Gladius
Company

- Dashboard
- Networks
- CDN
- DDoS
- Wallet

## Content Distribution Network



Map | Table

Gladius
Company

- Dashboard
- Networks
- CDN
- DDoS
- Wallet

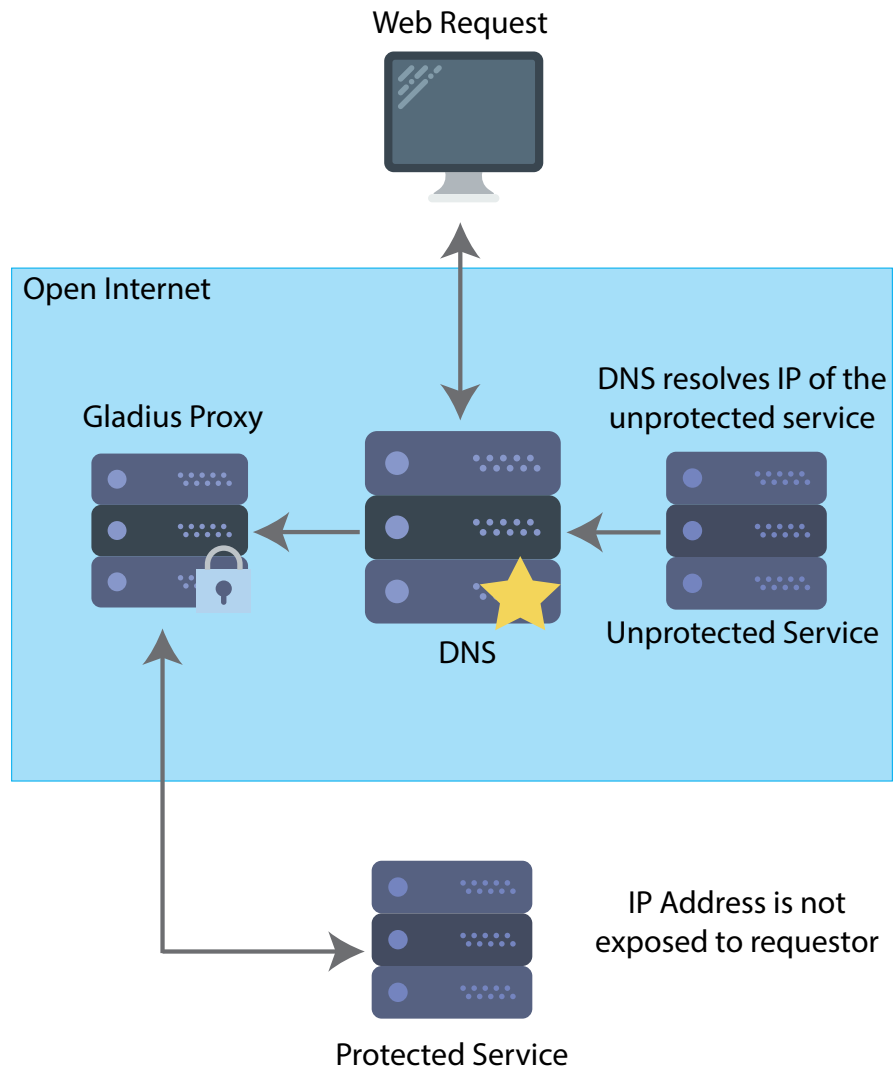
## DDoS Protection

Pool Name	Location	Rating	Node Count	Max Bandwidth	Response Speed (ms)
<a href="#">3213-GLA</a>	USA	5/5	57	5GB	15
<a href="#">4210-GLA</a>	USA	5/5	29	2GB	22
<a href="#">7002-GLA</a>	MEX	4/5	30	2GB	46
<a href="#">1302-GLA</a>	PAN	4/5	43	3GB	50
<a href="#">0031-GLA</a>	CAN	3/5	12	1GB	36
<a href="#">Add a Pool</a>					

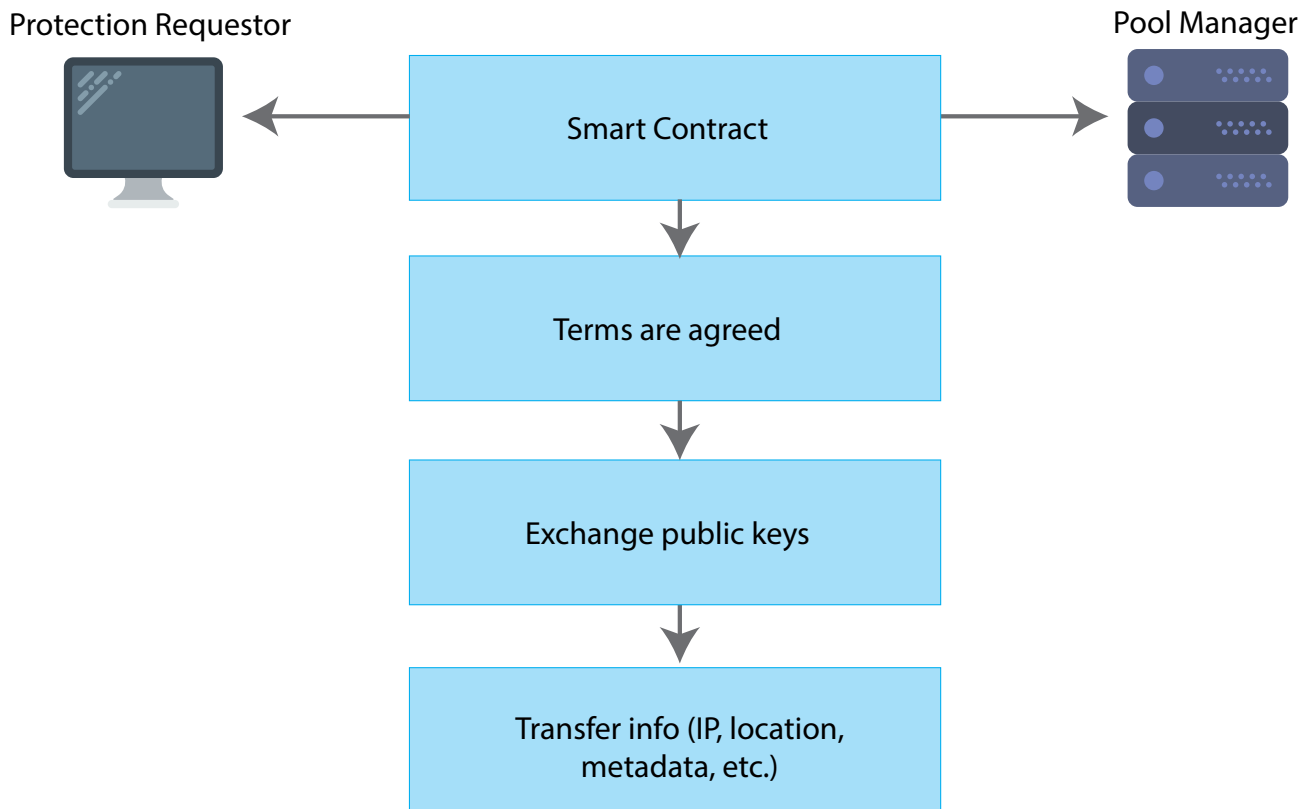
Map | Table



To request DDoS protection, individuals and companies can go onto our web portal and add a new request for either a website or some other service they want to protect. This is then communicated with selected pools and activated in seconds through Ethereum smart contracts. Then all the user needs to do is change their DNS settings to the ones we generate for them.



The client simply adds the provided domains to their primary nameservers and the site is protected behind the pool. These domains can expire if the contract is not renewed, effectively ending service. Additionally the payment is sent only when the successful completion of a contract occurs. This means every transaction is provably fair and open.



The web client performs a database lookup to find a pool with your required bandwidth and space as well as price and allows you to initiate a smart contract with them. The pool agrees to provide the client services and the client agrees to pay them in exchange.

## 6.7 | DDoS Mitigation

The techniques used to combat malicious requests.

To combat DDoS attacks Gladius nodes inside the pool will perform a number of services and computations to ensure requests are not malicious. These are all common techniques used by current DDoS mitigation services and have proven to be extremely effective in combating attacks (including Layer 7 and beyond).

**Rate-Limiting.** By identifying IP addresses that are constantly making website requests, Gladius can block these requests from getting access to the website. Once the threshold of requests is hit (which is set by the service requestor) the IP will no longer be able to access the site.

**IP Address Matching.** Similar to rate-limiting but smarter, IP address matching will be able to group similar IP address together that have known associations with each other. This will take shared information from the pool to block threats ahead of time.

**Intelligent Geo Matching.** Additionally Gladius can analyze requests and find geographic anomalies to detect and block attacks.

**Browsing Behavior.** By using information gathered from the request (whether it be from a web browser on a headless request), Gladius can pick out obvious dangers and block the requests in their tracks.

Overall a large amount of the protection utilizes anomaly detection to stop malicious attacks in their tracks. A key feature of the Gladius Network is that pools over time will learn about common attackers and block them preemptively for all other sites and services that are being protected.

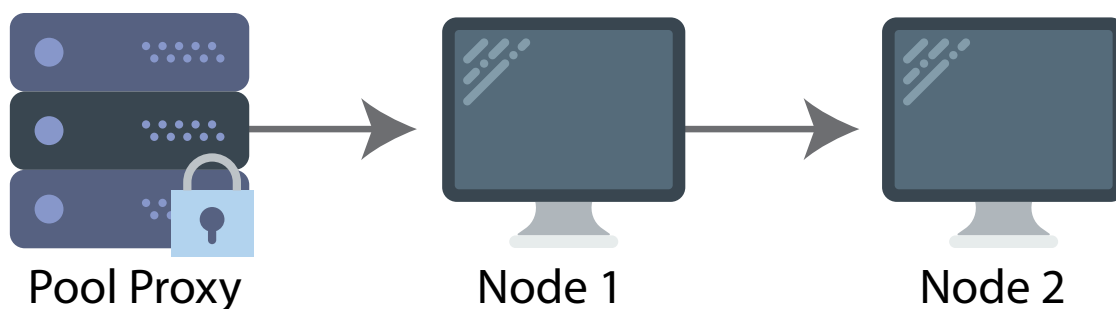
Over time there will be new client updates that introduce novel methods of protection. Gladius will always be looking for new types of attacks and will quickly respond to them with new prevention software. Pools with a specified number of outdated clients will also be noted in their reputation, meaning pools will always be pushing their nodes to update their clients.

## 6.8 | Content Delivery Network

The techniques used to speed up website load times.

The Gladius network can more effectively deliver fast content than any existing architecture because of the decentralized nature of it. By having many relatively low bandwidth nodes spread over a large area, a potential client will be connected to a node that is extremely close to them. Instead of having a datacenter far away but with high capacity, a client will connect to someone with less capacity but very close. Every node will have static file caching so that the bulk of the data that a client requests will come from a nearby node, while API calls and other dynamic data will still be passed through to the end server.

To verify that files have not been tampered with by a malicious node, 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. If the files do not match, the pool will have the option to immediately remove the node, or damage its reputation if it simply has out of date files.



Reputation of nodes will also be calculated based on random uptime requests initiated by the pool as well. Reputation will be treated as a multiplier on top of the profit earned from the number of requests, so that the total amount the pool pays out never changes, but shifts from poorly performing nodes to better performing ones. Additionally content delivery optimizations can and will be added as the platform matures. From dynamic sampling of website metadata in order to intelligently update caches, to better and more custom-tailorable load-balancing techniques, there are dozens of additional features to be added after the initial release of the Gladius Network.

## 7.1 | Team Overview

The history of the Gladius team.

The Gladius Team started in early 2017 as a University of Maryland College Park student team with a specialty in computer science, blockchain technology, and cybersecurity. Gladius' founding members set off to research just how effective blockchain technology could be in the world of cyber security. After looking into the devastating power and sheer frequency of DDoS attacks along with the unsatisfactory market conditions, it was clear that the Ethereum blockchain could be the solution to these problems. Over the course of weeks and months, the team developed the core architecture that soon became the Gladius Network. Along with the technology growing, the team has grown in size since then. The additional talent has enabled the team to quickly create a working prototype for the upcoming token sale.



MAX NIEBYLSKI

Max is the original founder of Gladius. Max is an enormous proponent of decentralization and blockchain technology. With over 8 years of experience in programming and entrepreneurship, he is the perfect person to lead Gladius where it needs to go for it to become a mainstay in the DDoS protection industry.



ALEXANDER GODWIN

Alex is a co founder at Gladius. He has been interested in programming since a young age and wanted to be involved in a decentralized project as he believes it is the future of the Internet. Alex plays a key role in developing smart contracts and general system architecture.



### MARCELO MCANDREW

Marcelo is a co-founder and developer for Gladius. With a passion for web development and creating new technology he is determined to make Gladius a leader in the DDoS protection and CDN industries. Marcelo plays a crucial role in the development of the Gladius Desktop Client and Web Portal.



### JEREMY EPSTEIN

Jeremy has 20 years of international marketing experience in helping to bring innovative technologies into the mainstream. He was VP Marketing at Sprinklr which grew from a \$20 million valuation and 30 people to \$1.8 billion valuation and 1400 people in 4 years. Jeremy is also the marketing faculty member for the prestigious Blockchain Research Institute, and the 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.



### RUBEN STRANDERS

Dr. Ruben Strandens studied Computer Science at Delft University of Technology in The Netherlands and holds a PhD in Artificial Intelligence from the University of Southampton, UK. He is a co-founder of FireServiceRota, a company specialized in planning and dispatching software for emergency services. Ruben lives in Mexico (and enjoys the food!), where he teaches AI at Tecnológico de Monterrey in Querétaro. In addition to his role as consultant and tester for the DCORP DAO, he also builds trading bots for cryptocurrencies using AI.



### 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 countless enterprise .NET applications. With a deep understanding of solidity and smart contract development, he is an essential advisor to our team. Frank has a business view with a developer's expertise.



#### MIKE BALAGNA

Insightful and multi-talented, Mike has been phenomenal in giving shape to many innovative marketing ideas. A PR professional who has served as Marketing and Communications Manager for Dcorp, he brings value to Gladius from multiple angles. He's advised and managed in several projects in the Blockchain space, playing a strong role in many successful ICOS.



#### HANSCO LEEK

Early Bitcoin adopter and investor, currently investing in Ether among others. Successful stockbroker, entrepreneur and business owner. Has had great success trading and speculating on many markets. A co-founder of Dcorp, and a valued advisor of several successful Fintech projects and ICOS, he is a strong supporter of Gladius and advises our team from multiple directions.



#### ORI LEVI

Digital marketer with over 10 years of experience in PR, SEO, and content marketing. He is a cryptocurrency enthusiast who has been trading altcoins for several years. Ori has been involved behind the scenes in a countless number of successful marketing and business development ventures, and has advised many ICOS and blockchain startups in 2017.



#### NADAV DAKNER

Nadav is a veteran online marketer and a serial Entrepreneur. He is the Founder and CEO of InboundJunction, an established digital marketing firm that helps well-known brands and startups boost their online visibility and reputation through PR, SEO, reputation management and influencer marketing. As a digital influencer and a crypto expert, he also advises blockchain startups and ICOs on marketing, operations and business development. He also holds investments in many different cryptocurrencies.

## Acknowledgements

A big thanks to Frank Bonnet for helping us with some of the general system architecture, as well as some technical specifics for how pools will interact with each other.

Also a big thanks to both DCORP and InboundJunction for the support and work building things from the ground up together with us.

## Disclaimers

All claims in this whitepaper are not final or binding. Everything is subject to change before the official release of the Gladius platform and the various token sales.

Do not send ETH to any address besides the one that can be found on our website: [gladius.io](http://gladius.io).