

# DATS Project (\$DATS) Whitepaper

October 25<sup>th</sup>, 2021

## **ABSTRACT**

Today, technology has become a need in every single field of our lives. Despite the fact that it has become easier to access technology thanks to the emergence of the Internet revolution, it is pretty difficult to access the technology integrity that can meet the needs of several institutions and researches because of high costs. The use of the Internet, which has become a need in every field of our lives, brings along cyber risks. It should not be difficult at all to anticipate how the widespread use of metaverse projects, which constitute a current trend, and the cyber risks to be brought along by them would affect persons and institutions. States and institutions have a number of primary objectives, including ensuring that systems run smoothly in all areas where the Internet is utilized, dealing with security threats, investigating, conducting simulated exercises, and taking measures. Otherwise, cyber-attacks occurring every 11 seconds will keep on increasing. Ransomware attacks, which are among the riskiest cyber attacks, are estimated to have caused a loss amounting to 6 trillion \$ for the world economy in 2021. In order to meet all these needs, it is inevitable to possess the technology integrity, which requires hundreds of millions of dollars. Now, imagine you possess a huge technology integrity, with which you can very rapidly scan the entire Internet against a supercomputer or cyber risks without any investment or maintenance cost and take very fast actions against these risks. Are you ready to utilize DATS Project's giant technology integrity or to obtain income as a part of it? We are right behind the door opening to the future of the IT world. We are looking forward to welcoming you to the DATS Project era.

## **Problem:**

We are literally at the peak of the digital transformation that is realized in almost every area of our lives. Smartphones that we cannot give up checking, computers that we spend a long time in front of during the day for business and education processes, everyday machines, including coffee machines, that become digitalized and connected, and supercomputers that are absolute needs in several fields, such as healthcare, defense, research, etc., but hard to reach. One of the most important ones is the blockchain that has broken new ground with its principle of equality and decentralization. All these not only constitute proof that digitalization has penetrated into every area of life, but also bring along numerous cyber risks and the needs for technology integrity.

## **Problems:**

- 1) Additional cyber risks to be created by over 75 billion devices based on Internet of things that are estimated to be utilized worldwide as of 2025.
- 2) Difficulties and delays experienced in reaching the sufficient technology integrity because of the high costs of cyber security research required to be conducted frequently worldwide.
- 3) Negative impacts of the cyber risks to be brought along with the widespread use of metaverse projects, which constitute a current trend, on individuals, institutions, and developers.
- 4) The prevention by telecom operators of the traffics of services received through illegal means for DDOS attack drill.
- 5) The difficulty experienced by institutions in choosing reliable and non-certified DDOS security solutions.
- 6) Difficulties and impossibilities experienced in reaching the result and measure solutions of cyber threat intelligences.
- 7) Supercomputers, which require hundreds of millions of investments and which are difficult for academics and institutions operating in several sectors, particularly healthcare, defense, and automotive, to reach.
- 8) 51% attacks experienced by PoW-based blockchains and the periodic density of the validators of PoS-based blockchains.

## **Solution:**

Blockchain technology has been developed particularly to store and validate the complex mixtures of technical properties, charts, accounts, arrangements, protocols, standards, and property rights as well as to timestamp. This technology allows for the development of different technologies needed, in addition to the stereotyped perception of many people as storing or trading value. Ethereum blockchain has activated the tokens that allow for making instant and more complex transactions by utilizing smart contracts. It is a fact that individuals and institutions ensure the operation of this technology by spending time and mining. Now, imagine the technology integrity, which is created by millions of people by dedicating the idle system resources of the computers they currently use without making any additional investment and which does not have an investment cost of hundreds of millions of dollars. Moreover, because it will consist of the resources of currently used computers, this technology will not require extra energy consumption and will not create an additional problem for carbon emissions. If you like, you can utilize this technology integrity or start obtaining income by being a part of it. We have figured out how to investigate cyber risks, how to detect them, and have already developed the prevention mechanism. However, we are developing the technology integrity that this development and all cyber security companies need for rapidly eliminating cyber threats before they even emerge. We are inviting everyone to go through the DATS Project door into the future of IT.

# Table of Contents

Value Proposition	5
The Birth of the DATS Project	5
The Final Objective of the DATS Project	6
Cloud-based Huge Technology Integrity Solution	7
Why DATS Token? - Widely accessible, P2P, cloud-based, blockchain technology integrity solution	8
The Functioning of the DATS Project	9
Matching DATS Token Value	10
Participants' Scoring - Creating Incentives to Provide the Network with Benefits	11-12
Preventing Fraud in Services	12
DATS Token Metrics	13
Using Funds	14
Overview of the DATS Economy	15-16-17

## **Value Proposition**

The DATS Project (\$DATS) will facilitate the processes of creating high-performance and complex transactions and flow processes for all users. It will make it much easier for end-users to detect cyber threats, to scan the entire Internet for threats, to identify the risks that may be present for metaverse products, to create a node out of the huge technology integrity for blockchain risks, and to possess the technology integrity requiring a high calculation power by allowing the deployment and processing of complex CPU- and GPU-based threads (tasks) over a peer-to-peer network.

## **The Birth of the DATS Project**

ParSecure was founded in 2017 in Bilişim Vadisi (Informatics Valley), Turkey's largest theme technopark, for the purposes of preventing ransomware attacks, which are among the world's biggest 6 cyber threats, and ensuring institutions' data security. Positioned in 32 different countries, its cyber threat intelligence sensors developed within a very short period of time, ParSecure has established a live cyber threat intelligence network. It has processed in the evaluation servers the cyber threat information received from the sensors and allowed them to be hosted on a distributed network. Furthermore, the cyber threat intelligences received have allowed for fighting against ransomware developers as well. This way, it has managed to create solutions against ransomware cases even for companies that do not have customers in numerous countries of the world. With the cyber security software it developed right after that, it also ensured the integrated operation of the cyber threat network functioning live and exhibited the property of a proactive cyber security product.

However, developed technologies and artificial intelligence provide attackers with much more significant opportunities. The most effective method of fighting against that is to possess the technology integrity, to conduct the most effective cyber security researches by acting much faster than attackers, and to ensure the cyber threat intelligences' integration with security products by processing the former.

Due to all these reasons, it is essential for companies developing cyber security solutions to possess huge technology products. In order to fight against cyber risks in the most effective manner, the ParSecure team has designed the DATS Project and taken steps to realize it. At first, sensor systems positioned in 32 different countries for the DDOS Test service being developed were offered to use by the DATS Project.

## **The Final Objective of the DATS Project**

The final objective of the DATS Project is to develop the cyber security ecosystem and minimize cyber risks by developing the below-listed project legs. It is also makes it easier for end-users to reach supercomputers, which have become a need in several areas but require highly costly investments, in a controlled manner thanks to the technology integrity of the DATS Project.

- 1) DDOS Test
- 2) DDOS Certification
- 3) Cyber Security Researches
- 4) Vulnerability Search Engine
- 5) Supercomputer
- 6) Blockchain Security

In addition to these, the DATS will obtain a share in the cyber security market, whose value was 173 billion dollars in 2020 and which is expected to reach 270 billion dollars with an annual growth of 7.7 percent by 2026, and share 80% of the revenues to be obtained from the service sales to its participants who play the most important role in creating the huge technology integrity.

## **Cloud-based Huge Technology Integrity Solution:**

ParSecure will provide institutions with purchasing opportunities in a marketplace that is managed centrally and to be realized when each service leg is completed. The vision of the DATS Project is to distribute the services to be developed in the Avalanche ecosystem, thanks to its technology integrity, through a token-based system built on the DATS chain. The DATS Project aims to be a peer-to-peer ecosystem for the huge technology integrity that the customers intend to reach in the long run. We will build the DATS Project on the DATS blockchain that we will develop in the Avalanche ecosystem so that end users can achieve technology integrity, participants create technology integrity and allocate their computers' idle resources to the DATS Project.

End users make payments with \$DATS token in order to reach the DATS Project technology integrity. When the participants within the technology integrity successfully fulfill their tasks, they receive 80% of the \$DATS token paid by the user as a vested interest in proportion with the system resource they have dedicated to the participants. This will ensure that the \$DATS token system to be a much more efficient, powerful, and largely scalable huge technology integrity network. The distributed huge technology integrity model is pretty interesting. Millions of individuals who have the DATS Project application dedicate their computers' idle resources to the technology integrity, and it allows the conclusion of the research very rapidly by distributing the end users' research tasks to the participants with the DATS Project.

Nevertheless, the existing system also has some inefficient aspects. Participants can utilize a majority of the system resources for their own needs. For this reason, the participants who ensure the huge technology integrity during the testnet and mainnet will be given the titles of loyal participants and irregular participants. It will be ensured that irregular participants do not take part in critical tasks. In the tasks where they can take part, on the other hand, different reward calculations will be used. If an irregular participant leaves the service before completing the task in a task process, they will not receive a reward, and instead of the participant that left, ParSecure sensors will be commissioned and complete the task of that participant. The DATS Project will run on the basis of the principle of complete service provision.

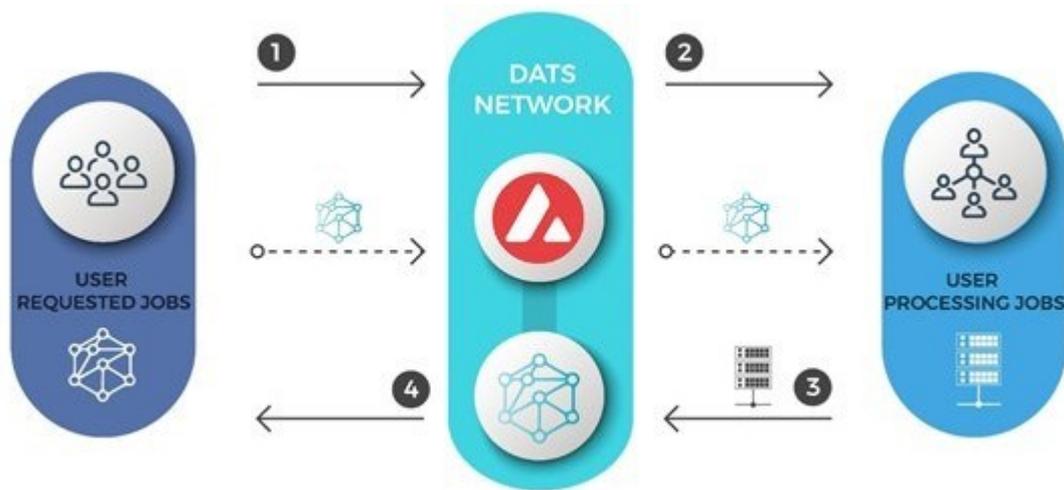
The DATS Token can utilize the potential of the already existing ecosystem between the participants and DATS Project customers and can carry it to the non-changing and distributed database of the blockchain. Such a blockchain-based huge technology integrity network can make it easier to create the creation of timestamped tasks efficiently, reliably, and profitably on a peer-to-peer basis.

**Why DATS Token? - Widely accessible, P2P, cloud-based, blockchain technology integrity solution:**

The DATS Token will be the primary unit used in the service operation exchange on the DATS Project network, which is the huge technology integrity marketplace. In its final form, the token will allow users to use a wide variety of available system resources in the peer-to-peer network and enable the reliable purchase/performance of services facilitated and tracked by the blockchain. In the DATS Project Network, users will connect to the DATS blockchain and create accounts through smart contracts and unique wallets. Users will be able to exchange DATS tokens on the network in order to purchase several services by purchasing these tokens and keeping them in their accounts. During this exchange, both parties will send a request for a DATS token smart contract in order to involve in the transaction. (Participants who dedicate their system resources to the DATS Project or individuals who request DATS Project services.) The cost of the job will be calculated and set in DATS tokens. The smart contract will transfer funds among accounts after the allocated job is completed.

After the transaction is completed, participants will be able to exchange their DATS Tokens for fiat currency in DEXes and target global cryptocurrency exchanges.

## The Functioning of the DATS Project



1. The user needs a DATS Project service, he/she enters the DATS Project portal on the web via KYC and states for which purpose he/she intends to use the service requested. He/she purchases the service he/she needs and sends the job. The DATS Project network will give the user the right to use the services whenever he/she wants.
2. After the DATS Project approves the request, the job to be given to the service is calculated, and users receive a quotation in DATS Tokens for the job - "pay", and tokens and job details are added to the smart contract. The job is sent to the participants via the DATS Project Network. Then, participants will match with the job and process the job to be given by the user.
3. The user who processes the job uses the dedicated system resources in order to process the job requested from him/her, and when it is completed, he/she sends back the completed job via the DATS Project Network.
4. After it is completed and the agreement is reached, 20% of the tokens are transferred from the user who requested to job to the DAT Project and the user who completed the job, via the smart contract.

**\* DATS will never approve the service requests made to be used for bad intentions.**

**\*\* The user will only be provided with the authorized/restricted portal access to use the requests approved.**

## **Matching DATS Token Value:**

The structure of the market, the completion of the project by the DATS Project development team within the periods specified in the roadmap, and the efforts of the sales and marketing team will directly affect the price of the DATS Token. The DATS Project team will make the maximum effort for the positive increase of the token price. In addition to all these, the participants' maximum participation in services and ensuring the technology integrity will positively affect the price. For the participants to dedicate their complete and maximum system resources to the DATS Project, a series of incentive programs will be announced.

A calculation formula has been created for each service. Furthermore, a comparison unit has been created for some services as well. The comparison unit shall be called DATS Package. In order to reflect the power of several resources in the formation of the system integrity at the beginning, the comparison unit will match with the 10-minute work of 1 DATS Package, which is a comparison unit created by the DATS Project.

- 1) DDOS TEST Pricing: 10 Mbyte / 3600 seconds / 1-month consumption type will be equal to XUSD, and the quantity of DATS Tokens will be determined with the DATS Token price on that day.
- 2) CPU Core Pricing: Each 16 Core/1 Hour will be equal to XUSD, and the quantity of DATS Tokens will be determined with the DATS Token price on that day.
- 3) GPU Pricing: Only certain display card models will be opened to use.
- 4) Vulnerability search engine: Freelancer: \$59/month, Small Business: \$299/month Corporate: \$899/month.

The users will be allowed to purchase the services with the user interface in the web environment and to send jobs to the users, and an offer will be presented for the job they requested. The offer price will be given the number of DATS Tokens over the then-current price of the DATS Token in USD. The user is obliged to purchase the DATS Tokens, the offer amount, from exchanges and to make payment. Then, the job is transferred over the network with the relevant job and service parameters added to the smart contract (for example, send traffic to 100Gbyte targets in total with the X protocol for 5 minutes). The price of a service and/or job will be taken as a basis out of the chain by analyzing the quantity of the requested available system resources and the usage period. The algorithm will analyze the quantity of the available system resources against the scale that the user needs, concurrency, and the complexity of the job. This will allow us to link the job unit dependent on the token value with the certain parameters of the job. This process also allows the allocation of the job of the service purchased in the most efficient manner at all times by ensuring that the network works at the highest capacity and that there is no system resource wasted.

**Participants' Scoring - Creating Incentives to Provide the Network with Benefits:**

Because the use of and demand for the DATS Token are scaled, it is very important to determine the way to evaluate the capability and reliability of the participants that dedicated their system resources and to rate the users who requested the jobs. The scoring will ensure that all participants on the network operate on the basis of the principle. Additionally, it will allow the users to work smoothly and efficiently as well.

**For the participants who dedicated their system resources:**

All participants who dedicated their system resources to the DATS Project will be allocated a numeric ranking ranging from 0 to 100. In the beginning, all participants will have a ranking valuing 50. The job matched with the participant is correctly and entirely completed, and if he/she earns at least 1 DATS Token in total, the score of the participant will be increased according to the values in the below-written table. Likewise, suppose the job is not completed. In that case, the participant's score will reduce by a number based on the 30-day moving average of the percentage of completed jobs and percentage of total jobs received. Both examples are given below.

**Participant Scoring Table:**

INCOME	REWARD
After earning 1 and over DATS Tokens with at least 50 points after the jobs entirely completed	
1-5 DATS Tokens	+ 1 Point
5.01-10 DATS Tokens	+2 Points
10+ DATS Tokens	+3 Points

30-DAY ACHIEVEMENT PERCENTAGE (More than 5 jobs have to be completed, and he/she has to have more than 50 points.)	PENALTY
80% or less	-3 Points
81%-90%	-2 Points
91%-99%	-1 Points

For example, the ranking of the participant X is 56, and his/her 30-day achievement percentage is 85%. He/she decides on the matching with the job for any service purchased to earn 1 point. There are two alternatives:

1. Achievement: The participant entirely completes the job matched, earns 2 points, and gets a ranking of 58 points.
2. Failure: The participant leaves the job matched half finished, leaves the job, loses two points, and gets a ranking of 54 points.

When the Participant X is given approval, he/she is obliged to complete the job entirely. The smart contract will remain open until the job is completed. If the system of the participant X is shut down for whatsoever reason and the job is not completed as specified in the smart contract, backup Participants and ParSecure sensor systems are commissioned and complete the job. In that case, the Participant X receives no repayment, and his/her ranking is reduced by -2 points.

## **Users Who Purchase the Services:**

If there is a queue for the services purchased due to density, the user's ranking will play an important role in determining the priorities following.

For example:

Usable 10,000 Core CPU resources are in usable condition, and two different users need 10,000 Core CPU resources. The User X has just participated in the DATS Project and has purchased the service for the first time. The User Y, on the other hand, regularly purchases and uses the services of the DATS Project. In that case, the User X will have priority over the User Y.

## **Preventing Fraud in Services**

In order to prevent fraud, several control and preventive measures that include in- and out-chain are available. For example; Participants are tested with respect to the system resources they dedicated. Participants who install the DATS Project Application are subjected to the speed test by the application when they want to dedicate their Internet traffic to the DDOS TEST Service. If their Internet service is below 5MByte/sec, then they cannot dedicate resources to the DDOS Test service and participate in the service. If their Internet speed is higher than 5Mbyte/sec., they can participate in the service. However, it is checked by the DATS Project application whether they sent the traffic undertaken for each job they matched with to the target determined by the user. In a contrary case, they are dismissed from the job they were matched with, and their ranking is reduced in points. Likewise, CPU and Display card models are determined and recorded by the DATS Project in the initial installation. The hardware of conforming brands/models are granted the right to participate in the services. If there is a change in the hardware dedicated to the services later on, it is identified by the DATS Project application. For hardware of non-conforming brands/models, the participation approval is canceled. If the brand/model of the hardware that the user shifted to has new technology and is not within the DATS Project database, then the user may send to the DATS Project via the application a request for the addition of his/her new hardware to the database.

The DATS Project checks whether the participant performs the job sent to him/her via smart contracts with the system resources he/she undertook. Additionally, in order to verify that the Participants entirely completed their jobs, different features were added to the network and DATS Project application. These features will not be publicly announced for not disclosing information to people with bad intentions.

Thank you for patiently reading the White Paper of the DATS Project. You can find the additional details related to the project at the address <http://www.datsproject.io>. We will publish more information in order to support the vision behind the DATS Project. In case of any question, you can contact us via our Telegram Channel, Twitter, or e-mail at the address [hello@datsproject.io](mailto:hello@datsproject.io).

THANK YOU!