# TBUG WHITEPAPER

V 2.1.5

# Foreword

With the rapid development of technology, artificial intelligence (AI) and blockchain technology have gradually penetrated into every field of our life. In this digital age, software has become an important part of our daily life, and the existence of vulnerabilities provides hackers and malicious attackers to take advantage of them. To address this issue, we have launched the TBUG Bounty Hunter program.

TBUG The goal of the Bounty Hunter is to create a vibrant and sustainable community where everyone can participate to find and fix software vulnerabilities together. We believe that through the power of all people, we can find and fix the vulnerabilities in the software in time, and improve the security and reliability of the software.

Over the past few years, we have witnessed the frequent occurrence of hacking attacks that have brought huge losses to businesses and individuals. Although traditional security defense methods can alleviate these problems to some extent, they often fail to detect and fix all vulnerabilities in time. Therefore, we need a more efficient and innovative solution to meet this challenge.

The TBUG bounty hunter appeared to solve this problem. Our platform will leverage AI technology to automate the vulnerability finding and reporting process, while improving transparency and efficiency in bounties through smart contracts and cryptocurrencies. In this way, we hope to help software developers find and fix vulnerabilities in time to improve the security and reliability of the software.

In the following sections, we will detail the features of TBUG bounty hunters, token issuance and distribution, technical implementation and architecture, and risk assessment. We will also explore future planning and development strategies, and our views on community building and governance.

We believe that by introducing artificial intelligence and blockchain technology, TBUG bounty hunters will create a new era where more people can participate in and contribute to software security. We look forward to working with developers, security experts, and community members around the world to create a more secure, transparent, and efficient software ecosystem.

In reading this white paper, we hope that you will feel our passion and determination for this project. We believe that, through the power of all, we can create a better future together. Thank you for your attention and support!

# Catalog

# 1. There are a lot of BUG in the Internet environment

## 1.1 Software complexity and vulnerability growth

With the wide application of software in various fields, the problem of software security has become increasingly prominent. Software is written by humans, whose complexity and scale make vulnerabilities unavoidable.

### 1.1.1 Reasons for increased software complexity

Function addition: To meet the diverse needs of users, software developers continue to add new features to their software. The increase in functionality makes the software more complex, thus increasing the possibility of vulnerabilities. Technology updates: With the popularity of the Internet and mobile devices, software technology is also constantly updated. The introduction of new technologies adds to software complexity, while new technologies can also bring new vulnerabilities.

Distributed systems: Modern software systems are increasingly being distributed, making systems more complex. Communication and data exchange links in distributed systems may be the targets of hacker attacks.

### 1.1.2 Reasons for vulnerability growth

Increased code: As the complexity of software increases, so does code. More code means more lines of code that could generate errors, thus increasing the number of vulnerabilities.

Programming errors: humans are prone to make mistakes in the programming process, such as logic errors, insufficient input verification, etc. These errors can become the breach of hacking attacks, leading to vulnerabilities.

Third party components: The use of third party components in modern software systems is increasingly common. These components may have known security vulnerabilities, and developers may not be able to track and fix them in time, thus increasing the number of vulnerabilities in the software.

## 1.2 Hacking attacks and malware

With the popularity of the Internet, the problem of network security is becoming increasingly serious. Hacking attacks and malware are important threats in the Internet security field.

### 1.2.1 Hacking attacks

Definition of hacker attack: Hacking attack refers to the process of using Internet security vulnerabilities to obtain access to the target system through illegal means, and then steal data, destroy the system or carry out other malicious behaviors. Classification of hacker attacks: According to the target and technique, hacker attacks can be divided into many types, such as phishing attacks, ransomware, DDoS attacks, etc.

Harm of hacker attacks: Hacking attacks may not only lead to data leakage, system crash and other security problems, but also may affect the normal operation and reputation of enterprises. In addition, hacking attacks may also involve criminal offenses, causing serious harm to individuals and society.

### 1.2.2 Malicious Software

Definition of malware: Malware refers to the software that is transmitted through the Internet and infects the target system. Its purpose is to carry out malicious behaviors, such as stealing data, destroying the system, monitoring users, etc. Classification of malware: According to the function and transmission mode, malware can be divided into many types, such as viruses, Trojan horses, worms, spyware, etc.

Route of malware transmission: Malware is usually spread through various channels, such as plug-ins, advertising pop-ups, download sites, social media, etc. In addition, the malware may also be transmitted through email, instant messaging tools and other channels.

## 1.3 Bounty and security defense

With the popularity of the Internet, the problem of network security is becoming increasingly serious. To address cyber security problems, many companies and organizations have launched bug bounty programs.

### 1.3.1 The bug bounty program

Definition of a vulnerability bounty plan: A vulnerability bounty plan is a reward program offered by an enterprise or organization to discover and report security vulnerabilities in its

products or systems.

Classification of the vulnerability bounty plan: According to the reward method and the participation method, the vulnerability bounty plan can be divided into many types, such as cash reward, point reward, gift reward, etc.

The meaning of the vulnerability bounty program: The vulnerability bounty program improves the security defense capabilities of enterprises and organizations, promote community participation and cooperation, increase the engagement of security experts, detect and fix security vulnerabilities, and reduce the risk of hacker attacks.

### 1.3.2 Security and defense measures

Definition of security defense: Security defense refers to the behavior of protecting the networks and systems of enterprises or organizations from attacks and destruction through various technologies and means.

Classification of security defense: according to the object of protection and defense means, security defense can be divided into many types, such as firewall, intrusion detection defense system, encryption technology, authentication, etc. The importance of security defense: Security defense can reduce or prevent hacker attacks and malicious software intrusion, protect the core assets and business operations of enterprises, and improve the competitiveness and reputation of enterprises.

### 1.3.3 Relationship between the vulnerability bounty plan and security defense

Improving security awareness: The vulnerability bounty program can motivate more people to participate in security defense and raise public awareness of cyber security issues and security awareness.

Finding and fixing vulnerabilities: The vulnerability bounty program enables security experts and developers to discover and report security vulnerabilities, which can help businesses and organizations detect and fix vulnerabilities in a timely manner.

Enhance security defense capability: Through the vulnerability bounty program, enterprises and organizations can obtain more security information and suggestions, and then strengthen security defense measures and improve security defense capability.

# 2. TBUG Project Overview

## 2.1 Project Introduction

The TBUG project is a security vulnerability bounty hunter platform based on artificial intelligence technology. The project aims to use artificial intelligence technology to automate the vulnerability finding and reporting process, while improving the transparency and efficiency of the bounties through smart contracts and cryptocurrencies. TBUG It aims to create a dynamic and sustainable community where more people can participate to find and fix software vulnerabilities and improve software security and reliability.

## 2.2 Project background

Technical support: The TBUG project is supported by Google subsidiary DeepMind, which uses its advanced AI technology, including AlphaCode systems, to automate the vulnerability finding and reporting process.

Community engagement: The TBUG project has attracted many developers, security experts, and users from around the world, creating a vibrant community. Community members can submit vulnerability reports through the platform and receive corresponding rewards.

Partner: The TBUG project has established partnerships with a number of well-known companies and organizations to jointly promote the development of security vulnerability bounty hunters. The support and recognition of these partners also guarantees the credibility and sustainability of TBUG projects.

Legal protection: The TBUG project has cooperated with legal institutions to ensure the legality and compliance of the platform. Users should also abide by relevant laws and regulations when submitting vulnerability reports on the platform to ensure their legal and compliant operation.

## 2.3 Project objectives

TBUG The goal of the project is to achieve the following goals:

Automating the bug finding and reporting process: By leveraging artificial intelligence technology, TBUG hopes to automate the vulnerability finding and reporting process, reduce

human intervention, and improve efficiency.

Improve the transparency and efficiency of bounties: With smart contracts and cryptocurrencies, TBUG hopes to improve the transparency and efficiency of bounties, making more people willing to participate and be rewarded accordingly. Creating vibrant communities: TBUG wants to create a vibrant and sustainable community that encourages more people to participate in security defense and work together to find and fix software vulnerabilities.

Improve software security and reliability: Through crowd sourcing, TBUG hopes to improve the security and reliability of software and reduce the impact of hacking and malware.

# 3.TBUG functional features

## 3.1 Definition of collaboration vulnerability finding

Collaboration vulnerability search refers to the process in which multiple security experts, developers or users participate in the vulnerability search. Through teamwork, resources, experience, and knowledge can be shared to improve the efficiency and accuracy of vulnerability finding.

### 3.1.1 Advantages of collaboration vulnerability finding

Improve efficiency: multiple people participate in vulnerability search at the same time, which can find and report vulnerabilities faster.

Increase accuracy: the perspectives and experiences of multiple people can complement each other and reduce the possibility of missing and false positives. Knowledge sharing: During teamwork, members can learn from each other and share their experience to improve their overall safety awareness and skills.

Cost reduction: Through collaboration, resources, time, and costs can be shared to improve the overall benefits.

### 3.1.2 Practical methods of collaborative vulnerability finding

Division of labor and cooperation: according to the skills and experience, reasonable division of labor and task allocation of team members.

Information sharing: establish a sharing platform or channel to timely share vulnerability information, research results and experience and lessons.

Discussion and communication: Hold regular team meetings or online discussions to exchange progress, discuss issues and share experiences.

Incentive measures: set up an incentive mechanism to encourage team members to actively participate and contribute.

## 3.2 Parameter vulnerability report

TBUG is an automated vulnerability reporting method based on artificial intelligence technology. This method detects and reports potential security vulnerabilities by analyzing the parameter input and output of the software system.

### 3.2.1 Definition of the parameter vulnerability report

The parameter vulnerability reporting refers to the process of security vulnerability detection and reporting for the parameter input and output in the software system. Parameter vulnerabilities usually involve security issues in input verification, parameter transfer and output processing, such as buffer overflow, injection attack and so on.

### 3.2.2 Principle of TBUG parameter vulnerability report

TBUG Parameter vulnerability report is based on artificial intelligence technology. By analyzing the parameter input and output of the software system, we can build a model to identify potential security vulnerabilities. The process consists of the following steps:

Data collection: collect the parameter input and output data of the software system, including data under normal and abnormal conditions.

Feature extraction: extract features from collected data, including input validation, parameter type, parameter length, output format and other on.

Model training: use the extracted features to train the machine learning model to learn the parameter input and output modes in normal and abnormal situations. Vulnerability detection: the trained model is applied to the parameter input and output data of the actual software system to detect potential security vulnerabilities.

Report generation: generate a detailed vulnerability report based on the detection results, including vulnerability type, severity, recommended repair measures and other information.

### 3.2.3 Advantages of TBUG parameter vulnerability report

High degree of automation: TBUG parameter vulnerability report uses artificial intelligence technology to automate vulnerability detection and report generation, which reduces the workload of manual intervention and audit.

High efficiency: Through automated detection, potential security vulnerabilities can be quickly found and reported, improving the efficiency of vulnerability reporting.

High accuracy: TBUG parameter vulnerability report is based on machine learning model, which can improve the accuracy and reliability of detection.

Good flexibility: TBUG parameter vulnerability report is suitable for various types of software systems, which can flexibly adapt to different systems and environments.

## 3.3 Shared cryptocurrency payments

TBUG Shared cryptocurrency payment is an innovative bounty payment method that uses cryptocurrencies to reward participants in vulnerability finding and reporting. In this way, TBUG aims to improve the transparency and efficiency of vulnerability bounties, while encouraging more people to participate in security defense.

### 3.3.1 TBUG The principle of sharing cryptocurrency payments

TBUG Shared cryptocurrency payments are based on blockchain technology and smart contracts, enabling automated, transparent, and tamper-resistant bounty payments. Specifically, TBUG uses blockchain technology as the underlying technology, allocating bounties and tasks through smart contracts, and pays using cryptocurrencies. When the participant submits a valid vulnerability report and confirms it, the smart contract automatically issues the bounty to the participant.

### 3.3.2 TBUG Share the advantages of cryptocurrency payments

Improve transparency: Cryptocurrency transactions are open and transparent, so the bounty distribution and payment process are also transparent, reducing the possibility of unfairness and fraud.

Improve efficiency: With smart contracts and automated transactions, TBUG can quickly process bounty payments and transaction confirmation, improving the efficiency and reliability of payments.

Cost reduction: Payment with cryptocurrency can reduce costs and fees for traditional payment methods, reducing the operating costs of the entire bounty program.

Globalization: Cryptocurrency is a global digital currency, free of geographical restrictions, and can attract participants from all over the world to participate in security defense.

## 3.4 Instant transaction-level security circuit breaker

TBUG Real-time transaction-level security circuit breaker is a security mechanism based on artificial intelligence technology, aiming to quickly identify and block potential security threats in a real-time trading environment. This circuit breaker combines the AI's advanced analytical capabilities and instant response features to ensure the security and stability of the trading system.

### 3.4.1 Definition of an instant transaction-level security circuit breaker

An instant trading-level security circuit breaker is a security mechanism used to monitor, identify, and block potential security threats in a real-time trading environment. The circuit breaker uses artificial intelligence technology to analyze transaction data in real time to detect abnormal patterns and suspicious behaviors, and quickly cut off transactions if necessary to prevent potential security risks.

### 3.4.2 TBUG Principle of instant transaction level security circuit breaker

Data collection: collect real-time data of the transaction system, including transaction information, user behavior, system logs, etc.

Feature extraction: The AI algorithm is used to extract security-related features from the collected data, such as abnormal transaction patterns, deviations of user behavior and so on.

Real-time analysis: The extracted features are analyzed in real time through machine learning models to identify potential security threats.

Risk score: assign a risk score to each transaction or behavior, indicating its potential safety risk level.

Decision and blocking: According to the risk score, when the predetermined threshold is exceeded, the circuit breaker will quickly cut off relevant transactions or behaviors to prevent safety risks.

Feedback mechanism: provide real-time feedback and alerts to inform relevant personnel of security incidents that have been blocked for further investigation and handling.

### 3.4.3 TBUG Advantages of instant transaction level security circuit breaker

Real-time: Through real-time monitoring and analysis of transaction data, it can respond quickly to security events and reduce potential losses.

Accuracy: Using advanced AI algorithms and machine learning models to accurately identify and distinguish between normal and suspicious transactions. Flexibility: It can be customized and optimized according to different trading systems and business requirements to accommodate various complex environments.

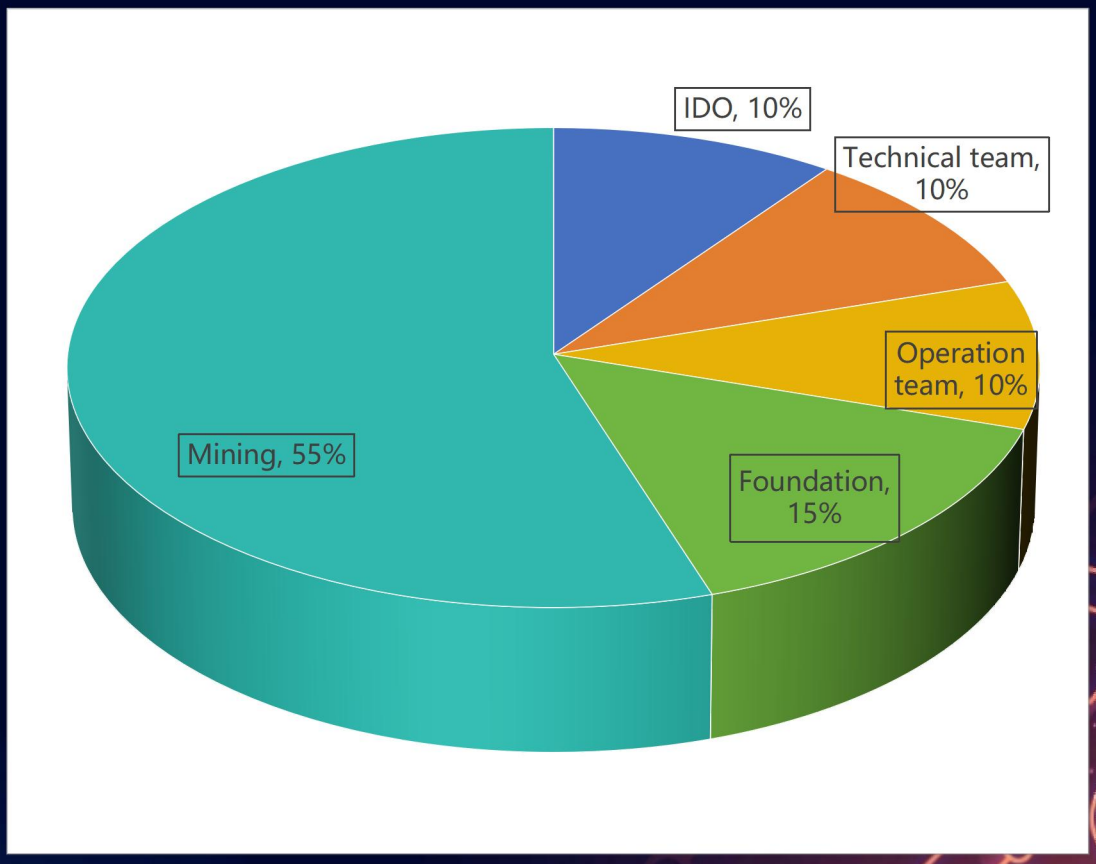
Scalability: With the growth of business volume and the emergence of new security threats, circuit breakers can be easily expanded and updated.

# 4.Token economic model

## 4.1 Token distribution mode

Token name: TBUG
Total tokens: 100 million

- **IDO: 10% ; by the market subscription output, without lock warehouse, all released before the line.**
- **Technical team: 10%;lock up for three years, and then release 1% quarterly until the release.**
- **Operation team: 10%;mainly used for project operation and daily vehicle data collection, reviewed by the foundation and released irregularly.**
- **Foundation: 15%; locked up for 6 months, and then release 10% every quarter until the release.**
- **Mining: 55%; the bug solver who** discover and report security vulnerabilities **will get TBUG reward.**



## 4.2 Main role of TBUG

Platform interaction: In order to use some functions of a specific project platform, users need to hold or buy the corresponding TBUG.

Store of value: The TBUG is designed to store value, similar to gold or other traditional assets.

Medium of exchange: The TBUG can be used as a medium of exchange for transactions in different markets or economies.

Transaction fee: TBUG can be used as a transaction fee on the TBUG network platform.

Service fee: TBUG can provide a variety of services, and charge the corresponding TBUG service fee

Mining income: Allow participants to earn TBUG rewards by participating in mining activities.

Ecosystem development: TBUG often builds a complete ecosystem, including developer communities, partners, and other stakeholders. By promoting ecosystem development and the interaction of participants, TBUG can attract more users and funds, thus facilitating ecosystem development.

# 5. Technology implementation and architecture

## 5.1 Technical architecture

**Data layer:** This layer is mainly responsible for data collection, storage and processing. Data can be obtained from multiple sources, including user input, sensor data, external APIs, etc. The data layer washes, pre-processes and transforms the data for the upper model use.

**Model layer:** This layer includes a variety of machine learning and deep learning models, such as neural networks, decision trees, support vector machines, etc. The main task of the model layer is to receive input from the data layer, make computation and inference, and then output the results.

**Control layer:** This layer is mainly responsible for controlling the process and logic of the whole system. It receives input from the user or other layers, and then controls the operation of the model layer and the data layer according on the status of these inputs and the system.

**User interface layer:** This layer is responsible for interacting with the users. It provides a visual interface allowing users to visually see the state and results of the system, while also entering instructions and data.

## 5.2 Application of artificial intelligence technology in vulnerability search

**Automated scanning:** TBUG can use automated scanning tools to conduct a comprehensive vulnerability scanning of the target system. Compared to traditional scanning tools, TBUG identifies vulnerabilities more accurately and reduces the false alarm rate. This is because TBUG is based on the deep learning algorithm, which can automatically learn and improve the model and improve the scanning accuracy.

**Threat intelligence analysis:** TBUG can analyze threat intelligence to obtain information about vulnerability exploitation and attackers. This helps to detect potential vulnerabilities and provide valuable early warning information for the defenders. By combining threat intelligence and system environment information TBUG is able to locate and fix vulnerabilities more accurately.

**Code audit:** TBUG can automatically review the source code through code audit technology and discover potential security vulnerabilities. The technology is based on machine learning algorithms and can automatically identify security defects and error patterns in the code. By working with developers, TBUG can help companies improve their code quality and security.

**Real-time monitoring:** TBUG can conduct real-time monitoring and early warning of the system in operation through real-time monitoring technology. When an abnormal behavior or potential threat is found.TBUG can timely alert to notify the administrator to take action.Real-time monitoring helps to find and repair vulnerabilities in time and reduce security risks.

**Penetration test:** TBUG can simulate the hacker attack process and conduct a Penetration test on the target System.By simulating various attacks and vulnerability/vulnerabilities, TBUG is able to identify potential security concerns and provide detailed test reports and1 recommendations for defenders. This helps to improve the security of the system and reduce the risk of an attack.

## 5.3 The application of smart contracts in vulnerability reporting and bounty payment

### 5.3.1 Application of TBUG smart contract in vulnerability reporting

**Definition and trigger conditions:** TBUG Smart contracts first define a set of rules and conditions,and when met the contract automatically triggers the vulnerability reporting process,For example,smart contracts can automatically start a vulnerability reporting process when an abnormal transaction behavior system performance degradation or a security event is detected.

**Vulnerability Report:** Once the trigger conditions are met the TBUG Smart contract will automatically package vulnerability details (including vulnerability Type,location,severity,etc.) into secure and transferable packets and send them to the organization through an encrypted channel.

**Review and repair: A**fter receiving the vulnerability report, the organizer will notify the relevant personnel to repair the vulnerability after the review and confirmation by the professionals. After the fix, the smart contract will be verified again to ensure that the vulnerability has been properly fixed.

**Bounty payment:** If the vulnerability does exist and is successfully fixed, the organizer will automatically issue the bounty to the reporter through the smart contract, depending on the severity of the vulnerability and the contribution of the reporter.

### 5.3.2 TBUG Application of smart contract in bounty payment

**Set the payment rules:** In the TBUG smart contract, a set of detailed payment rules can be defined, including the payment standard, payment method, payment time, etc. These rules will ensure the transparency and fairness of the bounty payments.

**Security Audit and Verification:** to ensure the security of bounty payments, TBUG smart contracts use multiple security audit and verification mechanisms. This includes authentication of reporters, verification of vulnerability validity, and the approval process for bounty payments.

**Automated payments:** The TBUG smart contract automatically performs the bounty payment process once it is approved and confirmed that the vulnerability has been fixed. This avoids human error and improves payment efficiency. At the same time, the transparency and imtamability of smart contracts also ensure the security and fairness of the payment process.

**Continuous optimization:** By collecting and analyzing data on bounty payments, TBUG smart contracts can continuously optimize their functionality and

performance. For example, it can learn to identify more vulnerability types, improve detection accuracy, and improve bounty payment strategies.

## 5.4 Safety circuit breaker technology and implementation

### 5.4.1 TBUG Safety circuit breaker implementation method

**Data collection and processing**: In order to realize TBUG secure circuit breaker technology, it is necessary to collect system and application traffic data and user behavior data. These data include network requests, response times, error rates, and more. By pre-processing and cleaning of these data, useful features can be extracted for subsequent analysis and detection.

**Model training and optimization:** Based on the collected data, an anomaly detection model can be trained using a machine learning algorithm. This model can be learned from the normal behavior pattern of the system and application and is able to identify suspicious activity that deviates from the normal pattern. To improve the accuracy and efficiency of the model, deep learning techniques can be used for optimization and improvement.

**Real-time monitoring and response:** deploy the trained model to the system to monitor the system and application in real time. When the model detects suspicious activity, the response mechanism triggers the safe circuit breaker. This mechanism can immediately cut the system

from external networks and notify administrators for further processing and investigation.

**Feedback and continuous improvement:** In order to continuously improve the accuracy and performance of TBUG safety circuit breakers, a feedback mechanism needs to be established. This mechanism can continuously improve and optimize the model according to the effect of practical application and user feedback. The detection accuracy and response speed can improve the model by continuously learning and adjusting the parameters.

### 5.4.2 TBUG The role of safety circuit breaker in improving system security

**Prevent malicious attacks:** TBUG Security circuit breaker can detect and identify potential malicious activities and abnormal behaviors, so as to prevent malicious attackers from attacking and destroying the system. You can reduce the risk of success by cutting the system from the external network.

**Protect sensitive data:**By monitoring the traffic and behavior patterns of the system and applications， the TBUG security circuit breaker can identify illegal access and operation to sensitive data. This helps to protect sensitive data from leakage and abuse.

**Improve system stability:** When the system is facing potential security risks, the TBUG security circuit breaker can be cut off in time to avoid system collapse or damage. This helps to maintain the system stability and availability.

**Reduce operating costs:** By automatically detecting and handling security threats TBUG security circuit breakers can reduce operating costs and improve productivity. This reduces the need to manually monitor and respond to security events， saving human resources and time costs.

# 6. Team introduction

TBUG Team is an innovative team focused on Al and machine learning， dedicated to providing advanced Hand efficient AI solutions to users around the world. The team members are composed of a group of experienced engineers, scientists and industry experts,who have a deep academic background and rich practical experience,and have outstanding performance in artificial intelligence,machine learning, network security and other fields.

**Adrian:** Is the CEO of TBUG. He was a senior researcher in a global leading artificial intelligence enterprise responsible for the development and application of machine learning algorithms. He has successfully developed a number of efficient and stable AI models that are widely used in image recognition natural language processing and other fields. He has also participated in a number of important projects， providing advanced solutions for enterprises， and has been highly evaluated by customers.

**Stanford:** Is the CTO of TBUG, with profound technical strength and rich practical experience. His research interests mainly include machine learnings deep learning, reinforcement learning and other fields, and he is committed to promoting the continuous innovation and progress of artificial intelligence technology. He also pays attention to the practical application of Al technology in natural language processing image recognition， recommendation systems and other fields and strives to apply the latest Al technology to product development and optimization

**Bradley:** Once served as the marketing director of a global leading artificial intelligence enterprise, responsible for the market development and brand promotion of the enterprise. He successfully planned and implemented a number of marketing projects, opened a new market space for the enterprise, and was highly evaluated by customers. He also participated in the strategic planning and operation management of the enterprise, providing important support for the long-term development of the enterprise.

# 7. Project development route

**Research and Development stage (completed):**

a. Establish a research and development team, including experts and software engineers in artificial intelligence and machine learning.

b. Develop the infrastructure and core functions of the AlphaCode system.

c. Implement an automated code generation algorithm for the AlphaCode system. d. Design and develop the user interface to improve the ease of use of the system.

**Test Phase(completed):**

a. Conduct ming programming testing on the Codeforces platform.

b. Analyze the test results and evaluate the performance and effect of the AlphaCode system.

c. Optimize the performance and function of the AlphaCode system based on the test results and user feedback.

**Application phase (in progress):**

a. Apply AlphaCode systems in practical scenarios, such as software development, data analysis, and prediction.

b. Cooperate with partners and customers to expand the application field and market of AlphaCode systems.

**Expansion stage (as planned):**

a. Continuously improve and expand the capabilities of the AlphaCode system according to market demand and technology trends.

b. Expand more application areas and markets, to meet the needs of different users.

C. Strengthen exchanges and cooperation with global partners, and jointly promote the progress and development of artificial intelligence technology.

# 8. Disclaimer

Nothing in this white paper constitutes legal, financial, commercial or tax advice, and you should consult your own legal, financial, business or other professional advisor prior to participating in any activity related to this. The staff of the platform, members of the project R D team, third-party R& D and development organizations, and service providers shall not be liable for any direct or indirect damages and losses that may be caused by the use of this white paper.

This white paper is for general information purposes only and does not constitute any offer for a prospectus, offer documents, an offer for securities, solicitation of investment or sale of any product, article or asset (whether digital or otherwise). The following information may not be exhaustive and does not mean any elements of the contract. The white paper cannot guarantee the accuracy or completeness of the information, and does not guarantee the accuracy and completeness of the information. In the case that this white paper contains information obtained from third parties, the platform and the team have not independently verified the accuracy and completeness of such information. In addition, you need to understand that the surrounding environment and conditions may change at any time, so this white paper may be outdated, and the platform has no obligation to update or correct the content and documents related to this.

No part of this White Paper constitutes or will not constitute any offer by the Platform, Distributors and any Sales Team (as defined herein in this Agreement), nor may it constitute the basis upon which any contractual and investment decisions are made. Nothing contained in this white paper serves as a statement, promise, or guarantee of future performance. By accessing and using the white paper or any of it, you will provide assurances to the Platform, its affiliates, and your team as follows:

You do not rely on any statements in this white paper in any decision to purchase assets (TBUG tokens);

You will voluntarily bear the costs and ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as appropriate);

You acknowledge, understand and agree that the asset may have no value, does not guarantee and does not mean any value and circulation attributes, and can not be used for speculation related investment;

Neither the Platform, its affiliates nor its team members shall be responsible or responsible for the value, transferability, liquidity of the assets or any market providing the TBUG project through third parties or other means;

You acknowledge, understand and agree that you are not qualify to purchase any assets if you

are a citizen, national, resident (tax or other relevant), residence or country of a geographical region or country that meets the following conditions:

The sale of assets may be defined or interpreted as a sale of securities (however named)or an investment product;

Countries and regions that are legally prohibited from contacting and participating in the sale of assets or in assets that are prohibited by laws, policies, regulations, treaties or administrative regulations.

The Platform and the Team will not and do not intend to make any representations, warranties or commitments to any entity or individual and hereby declare that they will assume no responsibility (including but not limited to the contents of this White Paper and the accuracy, completeness, timeliness and reliability of any other material content published by the Platform). Within the maximum extent permitted by law, the platform, relevant entities and service providers shall not be liable for any infringement, contract disputes, special, incidental, indirect, or other losses (including but not limited to any resulting breach or negligence, any loss of revenue and profit and loss of use and data). Potential purchasers should carefully consider, evaluate all risks and uncertainties related to sales, platforms and distributors and teams (including the risks of financial, legal and uncertainty).

The information provided in this white paper is intended for community discussion only and is not legally binding. No one is obliged to enter into any contract and binding legal commitments for the acquisition of TBUG, beyond which, this white paper will not accept any virtual currency or other forms of payment. The purchase and sale agreement of the assets and the long-term continued holding of the assets are subject to a set of separate terms or a purchase agreement containing relevant terms and conditions (as the case may be)that will be provided to you separately or available from the Website. If there is any inconsistency between these terms and conditions and this white papers please refer to these terms and conditions. Regulators do not review or approve any of the information listed in this white paper and they are not required or are required to be required in the laws, regulatory requirements and rules of any jurisdiction. The publication distribution or dissemination of this white paper does not mean that the requirements or rules of applicable laws or regulations have been fulfiled and complied with.

This is just a conceptual white paper to describe the vision goals of the TBUG project to be developed. This white paper may be modified or replaced from time to time. There is no obligation to update the white paper and provide additional information to audiences beyond the scope of this white paper. All statements,press releases publicly accessible statements contained in the white paper and oral statements that may be made by the platform and the TBUG project team may constitute forward-looking statements including relevant statements of intent and confidence and expectations regarding current market conditions business strategies and plans,financial position.specific provisions, and risk management decisions).

Please note that we do not rely too much on these forward-looking statements because they

involve known and unknown risks,uncertain risks,and other multiple factors, which may cause the future actual results far different from the content described by these forward-looking statements, it should be noted that there is no independent third party to review and judge the reasonableness of these statements and assumptions. These forward-looking statements are only applicable to the dates shown in this white paper and the Platform and the TBUG project team expressly assume no responsibility (whether express or implied)for the consequences or events arising from and arising from the revision of these forward-looking statements after that date.

The name or trademark of any company or platform used herein (except for content related to the platform or its affiliates) does not imply any association or endorsement to these third-party platforms and companies. The specific companies and platforms mentioned in this white paper are provided for reference and description purposes only.