

WhiteHub Token (WHC)

The #1 Crowdsourced Security Platform in Vietnam

Prepared by WhiteHub Team

Document version 1.1 - January 2021



CHANGELOG

Version 1.1 (30/01/2021)

Add Binance Smart Chain specs

Version 1.0 (01/01/2021)

Release the first version of the Whitepaper

Contents

1.	Introduction	3
2.	WhiteHub & Bug bounty	4
	2.1 State of cybersecurity in businesses	4
	2.2 Crowdsourced Security	5
	<i>Bug Bounty Program</i>	5
	2.3 WhiteHub security platform	6
	<i>Values of WhiteHub</i>	6
	<i>WhiteHub's achievements</i>	9
	<i>WhiteHub's valued customers</i>	9
3.	WHC Economy	10
	3.1 Uses of WHC on WhiteHub platform	10
	3.2 Technical specifications	12
4.	Roadmap	13
5.	WHC Distribution	14
6.	The Founding Team	15

1. Introduction

WhiteHub is the first crowdsourced security platform in Vietnam that connects security researchers and businesses to pre-emptively seek out security vulnerabilities in technology products through Bug Bounty programs. More than a year after launch, WhiteHub has been used by over 1,500 security experts and 50 enterprises. With the aim of expanding WhiteHub to the community of experts and businesses around the world and improving WhiteHub's application in the ecosystem of security products, we - the founders of the WhiteHub project - decided to apply blockchain technology on the reward and payment mechanism for security services and products on WhiteHub platform. This is why the WhiteHub Token (WHC) and the WHC ecosystem are developed.

WHC is a cryptocurrency built on the Ethereum Blockchain platform, with a vision of becoming the official currency in Bug Bounty programs, specifically as a bounty payment method for security researchers. Taking advantage of Blockchain technology, WHC will facilitate a more efficient payment process, reduce costs, and enhance anonymity for users. At the same time, WHC helps lower barriers for researchers and businesses worldwide to join the WhiteHub community. In the future, WHC will be integrated into the security ecosystem of WhiteHub and our partners.

Moreover, WHC can and will serve as a channel through which the founding team shares the WhiteHub platform ownership to the community; in other words, investors can own WHC to receive benefits derived from this cryptocurrency as well as from the WhiteHub Platform.

2. WhiteHub & Bug bounty

2.1 State of cybersecurity in businesses

Vulnerabilities are product security weaknesses that hackers can exploit to attack and perform malicious acts against users or issuers. Most businesses today encounter a major challenge: How to detect and fix security vulnerabilities in products BEFORE hackers exploit them.

	<u>IT team</u>	<u>Hackers</u>
Task	Find vulnerabilities	Find vulnerabilities
Purpose	Fix vulnerabilities	Exploit vulnerabilities
Number of security vulnerabilities needed	All	Only 1 critical vulnerability
Number of security personnel	1-4	Numerous

To increase product safety, businesses need to find and fix all existing security vulnerabilities in products. Meanwhile, hackers need to find only a single vulnerability that can be exploited then make all efforts of the business go in vain. This situation is the motivation behind the development of the Crowdsourced Security method.

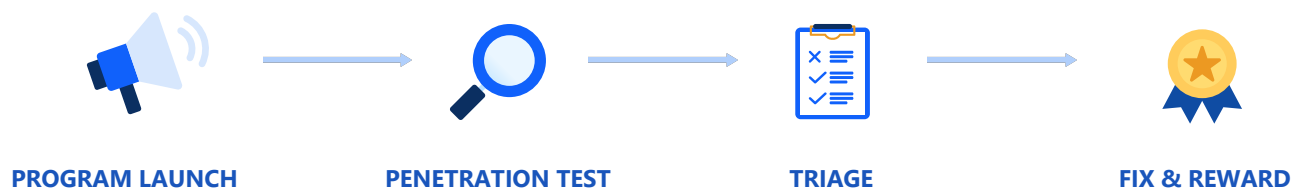
2.2 Crowdsourced Security

Crowdsourced Security is a method of enhancing the security of technology products (such as web apps, mobile apps, APIs, IoT devices, etc.) based on the contribution of the expert community (cybersecurity engineers, white-hat hackers, researchers). The experts will perform penetration tests to find out product vulnerabilities and businesses will pay rewards for valid detection.

By connecting with hundreds of independent security experts, Crowdsourced Security helps businesses find and fix security vulnerabilities as quickly as possible, reducing risks and ensuring product safety.

Bug Bounty Program

To use Crowdsourced Security, a business needs to implement a Bug Bounty program (in which the person who finds any valid security vulnerability gets paid). Here's the standard procedure for executing a Bug Bounty program:



Program launch: The business publishes a Bug Bounty program, with details of reward scope and reward amount for each severity level of vulnerabilities

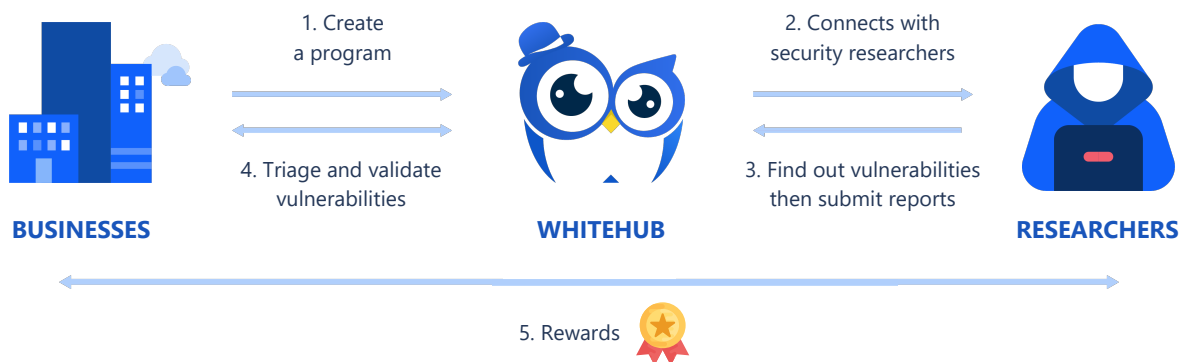
Penetration test: Experts find and report vulnerabilities to the business

Triage: The business evaluates the validity and severity of reported vulnerabilities

Fix & reward: The business fixes vulnerabilities, re-tests and rewards experts

2.3 WhiteHub security platform

Since launching in 2019, WhiteHub has been the first technology platform in Vietnam that pioneered Crowdsourced Security method. It responds to businesses' needs of security testing by connecting with experts around the world. Via WhiteHub, businesses can create and manage their own Bug Bounty programs as well as reach out to a community of more than 1,500 security experts. The programs will include details of payment policies such as payment forms and amounts for experts with valid vulnerabilities detected.



Built and designed by top cybersecurity experts and software engineers in Vietnam, WhiteHub provides a full range of features and tools to help businesses organize a complete Bug Bounty program.

Values of WhiteHub

Compared with the traditional penetration testing method, WhiteHub proves to have considerable advantages especially in terms of detection results, as summarized in the following table:

	Criteria	Traditional pentesting services	WhiteHub
Human resources	Expertise	Pentesters	Pentesters, White-hat hackers, security researchers and experts with different skillsets
	Number of participants	1 – 5	Up to hundreds of experts, depending on the need, budget and scope of the business
	Skills	Incomplete skill set	Complete pentesting skillset
	Participant selection	Not available	Participants selected based on their skills and experience on WhiteHub
Implementation	Time	Office hours	Starts immediately and operates 24/7
	Method	Based on predetermined standards and checklists	Combining standards and checklists with individual researchers' creativity and experience
	Coverage	Limited	Diverse perspectives of hundreds of researchers allow for total coverage of all vulnerable points in the product
	Developer-Pentester communication	Once every 2 - 3 weeks depending on the service provider	Continuous communication available through WhiteHub

	Criteria	Traditional pentesting services	WhiteHub
Results	Reporting	Reports provided periodically (monthly, quarterly, annually)	Reports (summarized or detailed) are continuously updated and easily exported at any time
	Quality of results	Low severity Focus on completing checklists (OWASP for instance) instead of practical issues; cannot replicate how a real life cyberattack works	Critical severity Focus on critical vulnerabilities that directly affect customers' systems and simulate the vulnerability exploitation process
	Vulnerability rating	Subjective, determined by the service provider	Compliant with VRT and CVSS Rating; customer rating also considered
Support	Fixing	Basic support	Comprehensive and quick solutions provided by researchers and WhiteHub
	Re-Testing	Additional costs potentially incurred, depending on the service provider	Free re-testing until the issues are resolved

WhiteHub's achievements

50+
programs created

1500+
researchers involved

\$200K+
awarded to experts

2,000+
vulnerabilities detected

WhiteHub's valued customers

Sendo

VinID

vntrip.vn

FINHAY

Giaohangtietkiem.vn
Chuyên nghiệp trên từng bước chân

**INSTITUTION OF
AMERICAN
EDUCATION
VIETNAM**

股

NUKEVIET.VN
SHARING SUCCESS, CONNECT PASSIONS

VND@
STABLE COIN

Olacity

Fiin

ECRM
Take Care Your Customer

MOG
Making Things Better

TomoChain

VietnamCredit
Trustworthy Insights

Getfly
SMEs perfect management solution

trustpay

IVYPREP
Success starts here

BEE
THE MOVE

watsons

LUXSTAY

HOSTVN
KẾT NỐI CÔNG NGHỆ TƯƠNG LAI

Sign up and try it out at: <https://whitehub.net>

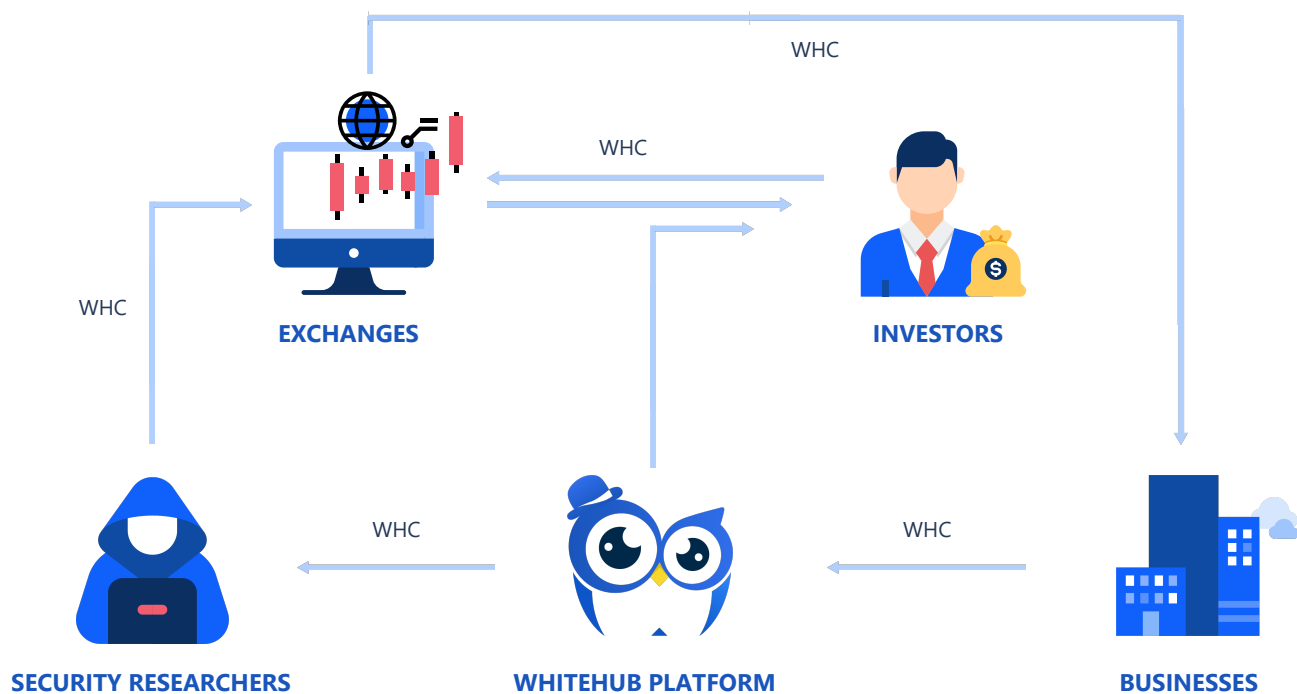
3. WHC Economy

WHC's vision is to become a payment method for security products and services.

In the first phase, WHC will be used on WhiteHub platform (whitehub.net) as a payment method based on which businesses can use to reward experts. Specifically, in Bug Bounty programs, instead of offering prizes in VND or USD, businesses will buy and use WHC to reward experts for the successful detection of valid vulnerabilities, making the payment process more convenient and transparent by removing barriers to experts' participation in the programs.

In the next phase, WHC will replace cash in payment for other security products and services, especially SaaS products and borderless services. WHC can also be used to create completely anonymous transactions.

3.1 Uses of WHC on WhiteHub platform



For Businesses

To launch Bug Bounty programs, businesses need to own a corresponding amount of WHC and deposit it on the WhiteHub platform. WHC can be purchased through the WHC-listed exchanges with a market-determined rate. In addition, businesses can also use WHC to pay for products of third-party partners.

For Security Researchers

Joining WhiteHub, researchers will have the chance to receive WHC rewards from businesses for finding security vulnerabilities in products. Then, researchers can hold WHC as an investment channel, stake in WHC pools to receive trading profits or sell directly on exchanges to earn stablecoins such as VNDC, USDT, USDC and other fiats.

For Investors

Investors are individuals and organizations that believe in the development of WHC and of WhiteHub platform. Investors can own WHC as an investment channel: they can earn trading profits when WHC's value increases corresponding to its wider application in security product ecosystems. In March 2021, we will use WHC on the CyStack platform (cystack.net), a security platform based on the SaaS model with many products for businesses.

Meanwhile, WhiteHub will also share part of WhiteHub's revenue to investors when they own a sufficient amount of WHC; this will be decided by the development team based on the actual business situation of WhiteHub and payments will be in stablecoins such as VNDC, USDT and USDC.

For Exchanges

WHC-listed exchanges' roles are to maintain WHC's value, facilitate the interaction between buyers and sellers as well as provide liquidity to this cryptocurrency. In the short term, the WhiteHub development team and early investors will be in charge of WHC's liquidity. In the long term, when WHC is widely used, market participants including experts, businesses, and investors will together maintain WHC's liquidity and stability.

For WhiteHub platform

WhiteHub is the first platform to apply WHC in paying service fees between security experts and businesses. The use of WHC will facilitate a more efficient paying process, reduce costs, and increase anonymity of security experts who normally do not want their information to be public. This will also help WhiteHub to be welcomed by even more security experts around the world.

To increase scarcity and avoid inflation of WHC, WhiteHub will burn 20% of the fees that WhiteHub collects for each transaction carried out on the platform.

For third-party applications

Besides WhiteHub, other security applications or services can also use WHC to pay and/or interact with security experts and researchers worldwide.

3.2 Technical specifications

Name	WhiteHub
Ticker symbol	WHC
Type	Utility Token
Token symbol	
Standard	ERC20 (Ethereum) BEP20 (Binance Smart Chain)
Smart contract	ERC20: 0xDDE5B33a56f3F1C22e5a6bd8429E6ad508BFF24E BEP20: 0x9246089db5f6b42502fc7da590c160bc869fab
Price	705 VNDC (\$0.03 USDT)
Max supply	100.000.000 WHC

4. Roadmap

TIME



5. WHC Distribution

WHC is built on the Ethereum (ERC20) platform, with a total supply of 100,000,000 WHC. This amount will be allocated as follows:

70% for Sale Service:

This amount will be distributed to investors and businesses that need to deploy Bug Bounty programs on WhiteHub Platform through private sales channels and cryptocurrency exchanges.

20% for the Founding Team

20 million WHC will be used as operating cost for WhiteHub platform and product development team. This amount will be locked in Smart Contract, and unlocked 2% every quarter from Q2 2021.

10% for Growth

This amount is used to implement marketing, sales, and community development programs on WhiteHub. This amount will be locked in Smart Contract, and unlocked 2% every quarter from Q1 2021.

WHC allocation in Smart contract is available at:

<https://etherscan.io/token/0xDDE5B33a56f3F1C22e5a6bd8429E6ad508BFF24E#balances>

5. The Founding Team



Chien Tran

Co-Founder & CEO

Graduating from Hanoi University of Science and Technology in 2013, Chien is a programmer, researcher in cybersecurity and blockchain technology. He is directly involved in the development of many fintech, blockchain, and security products.

Chien is now the Co-founder and Chairman of CyStack, one of 21 companies in the alliance established by the Prime Minister of Vietnam to develop cybersecurity products. Also, he is currently the Co-founder of VNDC Ventures, a fund investing in many potential projects such as VNDC Wallet, Nami Exchange, HVA Group, Livetrade, VNC Capital, SnackHouse, HanaGold,...



Trung Nguyen

Co-Founder & CTO

Trung is an experienced computer engineer and well-known cybersecurity expert in Vietnam. He has discovered many critical vulnerabilities in widely used softwares and has been acknowledged in the Hall of Fame by major firms such as Microsoft, IBM, HP, D-LINK, Deloitte,.... He also works as an active contributor to popular open-source security projects.

Trung is now the Co-founder/Chief Executive Officer and Chief Software Architect of CyStack, one of the leading companies in cybersecurity in Vietnam. At CyStack, he and colleagues apply their expertise in cybersecurity to building up solutions protecting end-users and businesses against cyber-threats from the Internet.



Yen Ha

Product Manager

Product designer with more than 4 years of experience in creating UX/UI design for Website & Mobile Application products.



Son Nguyen

Blockchain Engineer

Son Nguyen is a senior full-stack engineer. He has many years of experience in developing and building scalable systems and blockchain networks



Khai Tran

Software Engineer

Khai Tran is a senior web developer in building web applications. He is recently working with various blockchain platforms such as Bitcoin and Ethereum