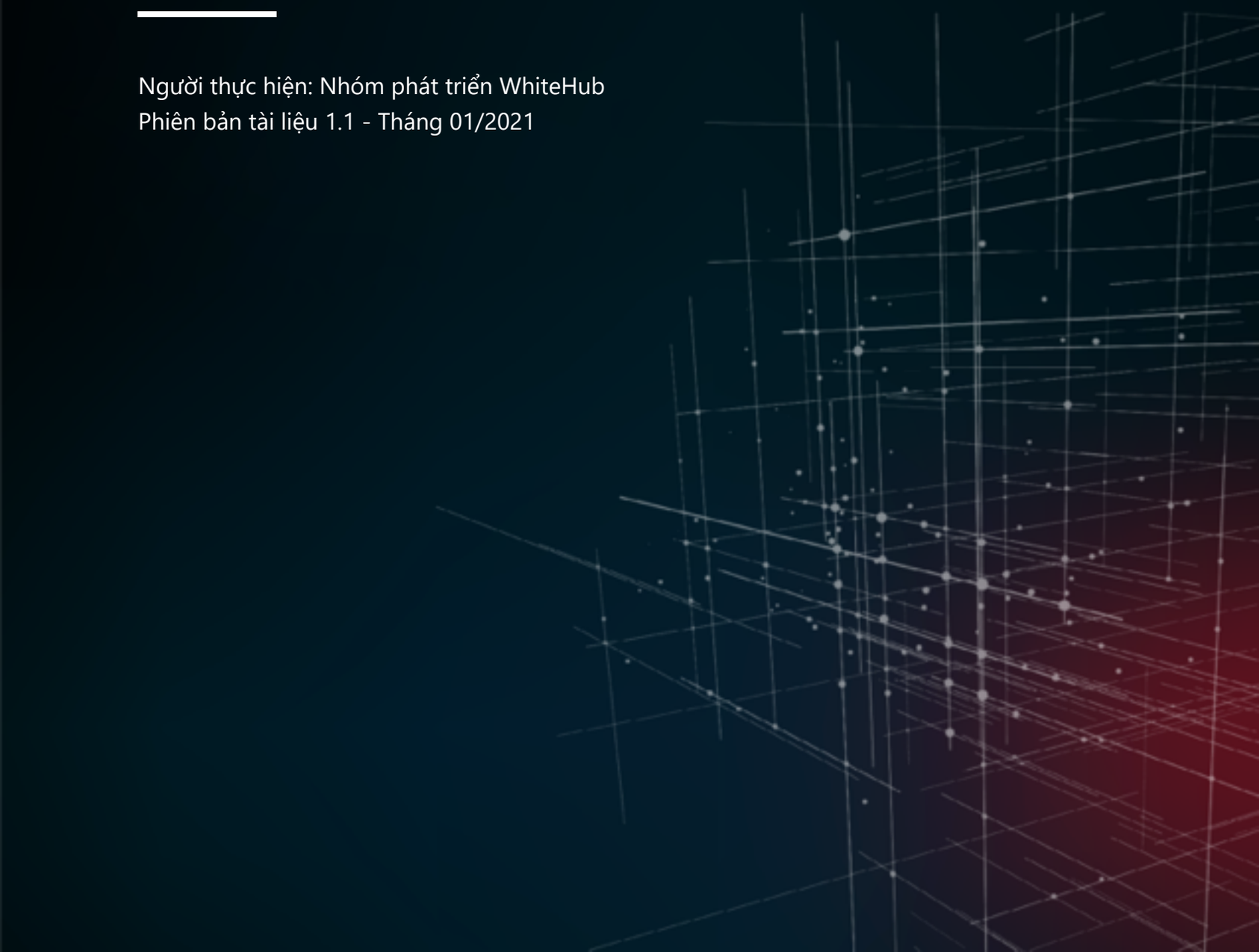
WhiteHub Token (WHC)

Nền tảng kết nối chuyên gia bảo mật và doanh nghiệp đầu tiên tại Việt Nam

Người thực hiện: Nhóm phát triển WhiteHub
Phiên bản tài liệu 1.1 - Tháng 01/2021



Phiên bản tài liệu

Phiên bản 1.1 (30/01/2021)

Bổ sung thông số kỹ thuật Binance Smart Chain

Phiên bản 1.0 (01/01/2021)

Phát hành Whitepaper chính thức

Mục lục

1. Giới thiệu

WhiteHub là nền tảng kết nối cộng đồng chuyên gia bảo mật và doanh nghiệp nhằm phát hiện sớm lỗ hổng trong các sản phẩm công nghệ thông qua một chương trình Bug Bounty. Sau hơn 01 năm ra mắt, WhiteHub đã được sử dụng bởi hơn 1,500 chuyên gia bảo mật và hơn 50 doanh nghiệp lớn tại Việt Nam. Với mục tiêu mở rộng WhiteHub đến cộng đồng chuyên gia và doanh nghiệp trên toàn thế giới, nâng cao tính ứng dụng của WhiteHub trong hệ sinh thái các sản phẩm bảo mật. Chúng tôi, những người sáng lập dự án WhiteHub đã quyết định ứng dụng công nghệ blockchain vào việc trả thưởng, trả phí cho các dịch vụ và sản phẩm mà WhiteHub cung cấp. Do đó, WhiteHub Token (viết tắt là WHC) và hệ sinh thái WHC ra đời.

WHC là tiền điện tử được xây dựng trên nền tảng Ethereum Blockchain, với tầm nhìn trở thành một tài sản trung gian trong các chương trình Bug Bounty và trả phí cho các sản phẩm bảo mật. Tận dụng điểm mạnh từ công nghệ Blockchain, WHC sẽ giúp cho quá trình trao đổi trở nên dễ dàng hơn, giảm thiểu chi phí và tăng tính ẩn danh cho người sử dụng. Đồng thời WHC cũng giúp giảm thiểu các rào cản giúp các chuyên gia và doanh nghiệp trên toàn thế giới dễ dàng tham gia cộng đồng WhiteHub.

Ngoài ra, riêng WHC cũng được coi như một kênh giúp đội ngũ sáng lập chia sẻ quyền sở hữu nền tảng WhiteHub cho cộng đồng, các nhà đầu tư có thể sở hữu WHC để nhận được những lợi ích sinh ra từ tiềm năng của WHC và nền tảng WhiteHub Platform.

2. WhiteHub & Bug bounty

2.1 Vấn đề bảo mật trong doanh nghiệp

Lỗ hổng bảo mật là những điểm yếu về bảo mật của sản phẩm mà tin tặc có thể lợi dụng để tấn công và thực hiện các hành vi gây hại cho người dùng hoặc đơn vị phát hành. Hầu hết doanh nghiệp hiện nay đều phải giải một bài toán khó: Làm sao để phát hiện và khắc phục lỗ hổng bảo mật trên các sản phẩm TRƯỚC khi tin tặc khai thác?

	IT team	Tin tặc
Công việc	Tìm lỗ hổng	Tìm lỗ hổng
Mục đích	Khắc phục lỗ hổng	Khai thác lỗ hổng
Số lượng lỗ hổng cần tìm	Tất cả	1 lỗ hổng nguy hiểm
Số lượng nhân sự bảo mật	1-4	Vô số

Để tăng tính an toàn cho sản phẩm, doanh nghiệp cần phải tìm kiếm và khắc phục tất cả các lỗ hổng bảo mật đang tồn tại trong sản phẩm. Trong khi đó, tin tặc chỉ cần tìm ra 1 lỗ hổng duy nhất là đã có thể khai thác và biến mọi nỗ lực của doanh nghiệp trở thành vô ích. Đó chính là tiền đề cho sự ra đời của phương pháp bảo mật Crowdsourced Security.

2.2 Phương pháp Crowdsourced Security

Đây là hình thức tăng cường tính bảo mật cho sản phẩm công nghệ, bao gồm: web app, mobile app, APIs, thiết bị IoT... dựa vào sức mạnh của cộng đồng chuyên gia (kỹ sư an ninh mạng, hacker mũ trắng, nhà nghiên cứu). Được triển khai dưới hình thức kiểm thử xâm nhập nhằm tìm ra các lỗ hổng bảo mật trước khi bị tin tặc khai thác. Bằng cách kết nối doanh nghiệp với hàng trăm chuyên gia bảo mật độc lập, Crowdsourced Security giúp doanh nghiệp tìm ra và khắc phục lỗ hổng bảo mật một cách nhanh nhất, giúp giảm thiểu rủi ro và đảm bảo an toàn cho sản phẩm.

Chương trình Bug Bounty

Để bắt đầu ứng dụng phương pháp Crowdsourced Security, doanh nghiệp cần triển khai một chương trình Bug bounty (trả thưởng cho người tìm ra lỗ hổng bảo mật). Dưới đây là quy trình thực hiện một chương trình Bug Bounty tiêu chuẩn thường được sử dụng rộng rãi:

Công bố: Doanh nghiệp công bố chương trình Bug bounty, bao gồm phạm vi và mức thưởng cho từng loại lỗ hổng

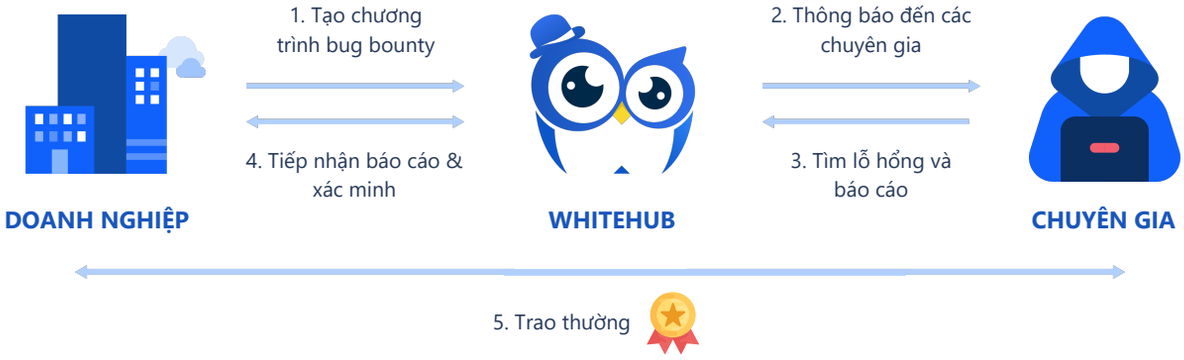
Tìm lỗ hổng: Các chuyên gia tìm kiếm lỗ hổng và báo cáo cho doanh nghiệp

Xác minh: Doanh nghiệp đánh giá tính hợp lệ, mức độ nghiêm trọng của lỗ hổng

Khắc phục & trả thưởng: Doanh nghiệp khắc phục lỗ hổng, tái kiểm tra và trả thưởng cho chuyên gia

2.3 Nền tảng bảo mật WhiteHub

WhiteHub là nền tảng công nghệ ứng dụng phương pháp Crowdsourced Security đầu tiên tại Việt Nam, đi vào vận hành từ năm 2019. WhiteHub giúp kết nối nhu cầu kiểm thử bảo mật của doanh nghiệp và cộng đồng chuyên gia tại khắp nơi trên thế giới. Thông qua WhiteHub, doanh nghiệp có thể khởi tạo và quản lý chương trình Bug Bounty, tiếp cận với cộng đồng hơn 1.500 chuyên gia. Chương trình sẽ bao gồm chính sách, hình thức và số lượng trả thưởng cho chuyên gia khi phát hiện các lỗ hổng bảo mật.



Được xây dựng và thiết kế bởi những chuyên gia an ninh mạng và kỹ sư phần mềm hàng đầu tại Việt Nam, WhiteHub cung cấp đầy đủ các tính năng và công cụ giúp doanh nghiệp tổ chức hoàn thiện một chương trình Bug Bounty.

Giá trị của WhiteHub

So với phương pháp kiểm thử xâm nhập truyền thống, WhiteHub cho thấy sự hiệu quả rõ rệt về chất lượng đầu ra như sau:

	Tiêu chí	Traditional pentesting services	WhiteHub
Nguồn lực	Chuyên môn	Pentesters	Bao gồm các Pentesters, White-hat hackers & các chuyên gia, kỹ sư bảo mật với nhiều kỹ năng đa dạng
	Số lượng	1 – 5	Lên tới hàng trăm chuyên gia tùy thuộc nhu cầu, budget và phạm vi của doanh nghiệp
	Kỹ năng	Không đầy đủ	Đầy đủ tất cả các kỹ năng về Pentest
	Lựa chọn chuyên gia phù hợp	Không có	Các chuyên gia được lựa chọn dựa trên kỹ năng và kinh nghiệm từ các chỉ số từ WhiteHub.
Cách thức triển khai	Thời gian	Thường trong giờ hành chính	Ngay lập tức & liên tục 24/7
	Phương pháp	Dựa trên các tiêu chuẩn và checklist cố định	Các tiêu chuẩn, checklist được các chuyên gia từ WhiteHub kết hợp với sự sáng tạo, năng lực và kinh nghiệm cá nhân
	Tính bao phủ	Không có	Các góc nhìn khác nhau của hàng trăm chuyên gia giúp bao phủ đầy đủ tất cả các vị trí có thể bị tấn công của sản phẩm
	Tương tác giữa đội kiểm thử và đội phát triển	2-3 tuần 1 lần tuỳ vào từng nhà cung cấp	Theo yêu cầu hoặc liên tục với nền tảng giao tiếp tại WhiteHub

	Tiêu chí	Traditional pentesting services	WhiteHub
Kết quả	Báo cáo	Một báo cáo duy nhất vào cuối các chu kỳ (tháng, quý, năm)	Nhận báo cáo liên tục và trích xuất báo cáo (tổng hợp hoặc chi tiết) tại mọi thời điểm
	Chất lượng	**Low severity** Tập trung vào các mục của checklist (ví dụ OWASP) thay vì những vấn đề cụ thể; không tái hiện được các hình thức tấn công thực tế của tin tặc để tìm kiếm lỗ hổng	**Critical severity** Tập trung vào những lỗ hổng nguy hiểm nhất, ảnh hưởng trực tiếp đến hệ thống của khách hàng dựa trên việc thử nghiệm khai thác lỗ hổng
	Đánh giá mức độ nguy hiểm	Chủ quan của nhà cung cấp	Tuân thủ tiêu chuẩn VRT và CVSS Rating và dựa trên phản hồi thực tế từ khách hàng
Hỗ trợ	Tư vấn khắc phục	Sơ bộ	Được tư vấn phương pháp khắc phục triệt để và nhanh nhất từ chuyên gia và WhiteHub
	Re-Testing	Phụ thuộc từng đối tác và có thể phát sinh chi phí	Hỗ trợ kiểm thử liên tục đến khi vấn đề được khắc phục triệt để (không phát sinh thêm chi phí)

Những con số về WhiteHub

50+
chương trình đã được tạo

1500+
nhà nghiên cứu tham gia

$200K+
đã được trao thưởng cho chuyên gia

2,000+
lỗ hổng được phát hiện

Khách hàng nổi bật đã và đang sử dụng WhiteHub

Sendo · VinID · vntrip.vn · FINHAY · Giaohangtietkiem.vn · Institution of American Education Vietnam · NUKEVIET.VN · VNDC Stablecoin · Olacity · Fiin · ECRM · MOG · TomoChain · VietnamCredit · Getfly · trustpay · IVYPREP · BEE · watsons · LUXSTAY · HOSTVN

Đăng ký và trải nghiệm tại: https://whitehub.net

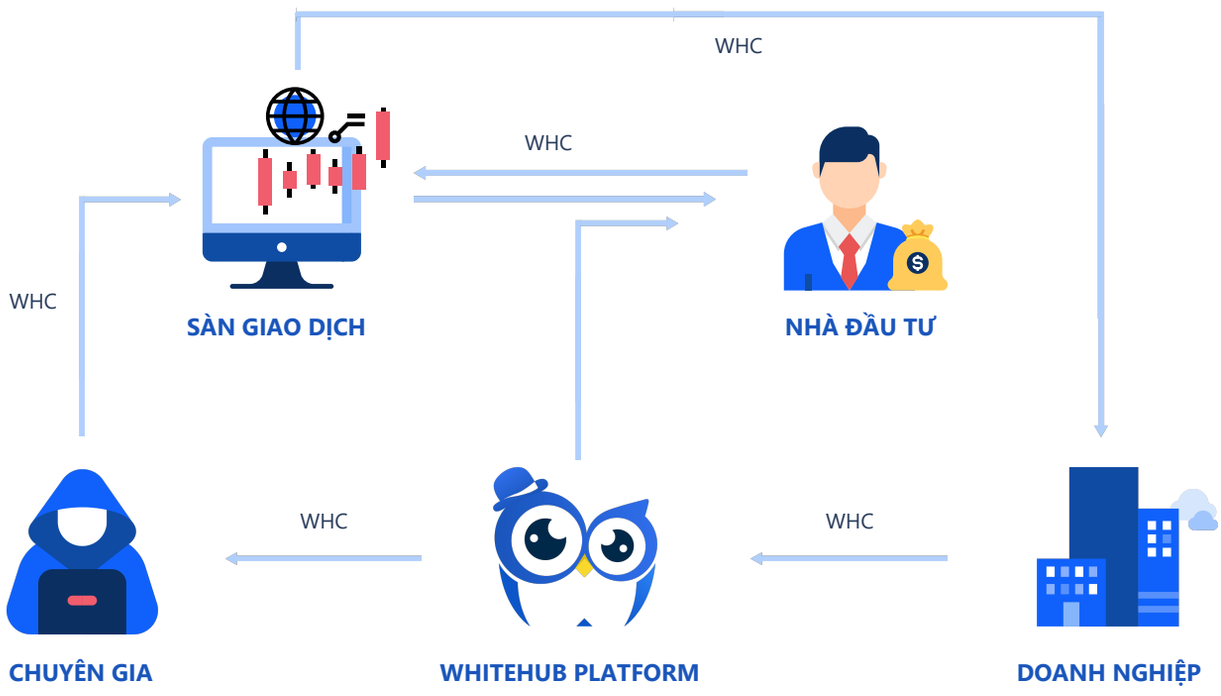
3. Hệ sinh thái WHC

WHC được sinh ra để làm phương thức trao đổi trong các sản phẩm và dịch vụ bảo mật.

Trước tiên, WHC sẽ được sử dụng trong hệ sinh thái WhiteHub Platform như một tùy chọn trả thưởng của doanh nghiệp dành cho các chuyên gia. Cụ thể, trong một chương trình Bug Bounty, thay vì đặt giải thưởng bằng VNĐ hay USD, các doanh nghiệp sẽ mua và sử dụng WHC như một phương thức trả thưởng cho chuyên gia khi phát hiện thành công các lỗ hổng bảo mật. Điều này sẽ giúp quá trình trao đổi diễn ra thuận tiện và minh bạch hơn. Xóa bỏ được các rào cản để các chuyên gia dễ dàng tham gia các chương trình Bug Bounty.

Trong giai đoạn tiếp theo, WHC sẽ được mở rộng như một phương thức trả phí cho các sản phẩm và dịch vụ bảo mật khác thay vì phải sử dụng tiền mặt. WHC có thể sử dụng để tạo ra những giao dịch hoàn toàn ẩn danh.

3.1 Ứng dụng WHC trong WhiteHub platform



Với doanh nghiệp

Để triển khai các chương trình Bug Bounty, doanh nghiệp sẽ cần sở hữu số lượng WHC tương ứng trên nền tảng WhiteHub. Doanh nghiệp sẽ cần mua qua các sàn giao dịch có niêm yết WHC, tỷ giá được quyết định bởi thị trường và nhu cầu sở hữu WHC cho mục đích đầu tư và triển khai chương trình Bug Bounty.

Ngoài ra, khi sở hữu WHC, các doanh nghiệp còn có thể sử dụng như một phương thức trả phí cho các dịch vụ bảo mật, sản phẩm bảo mật của các đối tác bên thứ 3.

Với chuyên gia

Khi tham gia WhiteHub và phát hiện được các lỗ hổng bảo mật trong các sản phẩm của doanh nghiệp, các chuyên gia sẽ nhận được những phần thưởng là WHC. Khi đó, các chuyên gia có thể giữ WHC như một kênh đầu tư, stake vào các pool của WHC để nhận được lợi nhuận giao dịch hoặc bán trực tiếp trên các sàn giao dịch để thu về các loại stablecoin như VNDC hay USDT.

Nhà đầu tư

Là những người tin tưởng vào sự phát triển của WHC và nền tảng WhiteHub. Khi sở hữu WHC nhà đầu tư có thể nhận được lợi nhuận khi nhu cầu sở hữu WHC tăng lên và giá trị WHC tăng dần. Ngoài ra, WhiteHub cũng sẽ chia sẻ doanh thu của WhiteHub cho các nhà đầu tư khi sở hữu đủ một lượng WHC, điều này sẽ được đội ngũ phát triển quyết định dựa trên thực tế tình hình kinh doanh của WhiteHub và được trả bằng các loại stablecoin.

Nền tảng WhiteHub

WhiteHub là nền tảng, sản phẩm đầu tiên ứng dụng WHC trong việc trả phí dịch vụ giữa chuyên gia bảo mật và doanh nghiệp. Việc sử dụng WHC sẽ giúp cho việc trả thưởng trên nền tảng WhiteHub trở nên thuận tiện hơn, giảm thiểu chi phí và có thể duy trì được tính ẩn danh của các chuyên gia bảo mật vốn dĩ không mong muốn thông tin mình bị công khai. Điều này cũng sẽ giúp cho WhiteHub sẽ được đón nhận bởi nhiều chuyên gia bảo mật hơn nữa.

Ngoài ra, để tăng độ khan hiếm và tránh lạm phát WHC, WhiteHub sẽ thực hiện đốt bỏ (burn token) 20% phí mà WhiteHub thu cho mỗi giao dịch phát sinh trên nền tảng.

Sản phẩm bên thứ 3 (Third-party application)

Ngoài WhiteHub, các ứng dụng hoặc dịch vụ bảo mật khác cũng có thể sử dụng WHC như một phương thức trả phí dịch vụ hoặc tương tác với các chuyên gia bảo mật, nhà nghiên cứu trên toàn thế giới.

Sàn giao dịch

Các sàn giao dịch niêm yết WHC đóng vai trò duy trì giá trị, tương tác giữa người mua/ người bán và cung cấp thanh khoản cho WHC. Trong thời gian đầu, đội ngũ phát triển WhiteHub và các nhà đầu tư ban đầu sẽ là người duy trì tính thanh khoản của WHC. Về lâu dài khi WHC được đưa vào sử dụng rộng rãi trên thị trường, các chuyên gia, doanh nghiệp, nhà đầu tư sẽ cùng nhau duy trì tính thanh khoản và sự ổn định của WHC.

3.2 Thông số kỹ thuật

Tên dự án	WhiteHub
Mã ký hiệu	WHC
Loại	Utility Token
Biểu tượng	
Tiêu chuẩn	ERC20 (Ethereum) BEP20 (Binance Smart Chain)
Smart contract	ERC20: 0xDDE5B33a56f3F1C22e5a6bd8429E6ad508BFF24E BEP20: 0x9246089db5f6b42502fcdc7da590c160bc869fab
Tỷ giá	705 VNDC ($0.03 USDT)
Nguồn cung tối đa	100.000.000 WHC

4. Lộ trình

TIME

Q1 2021: Khởi động dự án WHC & phát hành WHC trên Ethereum (ERC20)

A

01/2021

- Mở bán WHC với số lượng giới hạn (Private Sale)
- Niêm yết WHC trên VNDC Wallet
- Phân phối WHC thông qua VNDC DIPO
- Niêm yết cặp tài sản WHC/VNDC trên Nami Exchange
- Mở giao dịch WHC trên VNDC P2P Trading

02/2021

- Niêm yết cặp tài sản WHC/VNDC trên Uniswap.org
- Mở giao dịch WHC trên VNDC Exchange
- Giới thiệu dự án WHC thông qua một số nền tảng Launchpad quốc tế như: Binance launchpad, Gate.io,...
- Phát triển cộng đồng nhà đầu tư và người dùng WhiteHub

03/2021

Triển khai sử dụng WHC để trả phí cho chương trình Bug Bounty trên nền tảng WhiteHub

B

Q2 2021: Tích hợp WHC trên nền tảng CyStack

C

Q3 2021: Thu hút 5,000 chuyên gia bảo mật sử dụng nền tảng WhiteHub

D

Q4 2021: Thu hút hơn 10,000 nhà đầu tư sở hữu WHC Token tại các địa chỉ ví và sàn giao dịch tiền điện tử

E

2022

- Tăng trưởng chuyên gia, doanh nghiệp sử dụng WhiteHub, nhà đầu tư sở hữu WHC và mở rộng hệ sinh thái bảo mật có ứng dụng WHC.
- Nâng cấp nền tảng WhiteHub trở thành hệ thống tự vận hành phi tập trung (Decentralized Autonomous Organization - DAO)

5. Phân bổ

WHC được xây dựng trên nền tảng Ethereum (ERC20), với tổng nguồn cung là 100,000,000 WHC. Số lượng này sẽ được phân bổ như sau:

70% cho Sale Service:

Số lượng này sẽ được phân phối cho các nhà đầu tư, các doanh nghiệp có nhu cầu triển khai các chương trình Bug Bounty trên WhiteHub Platform thông qua các sàn giao dịch tiền điện tử. Được khóa trong Smart Contract và mở khóa 5% mỗi tháng.

20% cho Founding Team

20 triệu WHC sẽ được sử dụng làm chi phí vận hành nền tảng WhiteHub, đội ngũ phát triển sản phẩm. Số lượng này sẽ được khóa trong Smart Contract và được mở khóa 2% mỗi quý.

10% dành cho Growth

Số lượng này được sử dụng để triển khai các chương trình Marketing, Sales và phát triển cộng đồng WhiteHub. Sẽ được khóa trên Smart Contract và được mở khóa 2% mỗi quý.

Xem phân bổ WHC trên Smart contract:

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