

Proposal Name:

Community Based Insurance for BAYC and MAYC Holders

Proposal Category:

Ecosystem Fund Allocation

Abstract

This proposal concerns insurance and security solutions for ApeCoin holders and related NFT Holders (BAYC, MAYC and potential future projects). Holders of high value desirable NFTs are often the target of wallet drains and hacks and security researchers have shown that roughly 1.5% of Bored Ape holders have been victims of scams (See, Reference 1). We propose to develop a community based insurance solution for holders based on research (including actuarial modelling) done by our company Plural Finance (plural.fi).

Team

The team behind this proposal is from Plural Finance, which is a UK based technology company focussed on insurance in Web3.

CEO.

Dr. Viroshan Naicker

Viroshan has been consulting Web3 startups and DAOs, designing token economies and incentive mechanisms for the past seven years. At one point, he wanted to become an academic. He has peer-reviewed publications in networks, finance, and quantum mechanics and holds Ph.D. in Graph Theory, the mathematics of networks.

CTO.

Gavin Marshall

Gavin is a vastly experienced coding autodidact. He has held various senior positions in the African tech sector, including VP of Innovation at Mxit: This early mobile chat app had a sixty-million-strong user base before it was acquired. He has lectured and spoken about Bitcoin and writing smart contracts since 2015.

Product Lead.

Mathew Haswell

Mathew has been building products in the Web2 space for over ten years. He has held various C-suite product roles at established companies and has twice been a startup founder at Teachfolk and Yreeka! He is an expert in product management and behavioral design.

Community Lead.

Ben Blaine

Ben has successfully built and exited various multi-sided marketplace-style startups, including SnapScan, a payments processing app now owned by Standard Bank, and OfferZen, a developer consulting platform. He is an expert on how to help tech startups get customer traction and is usually busy with multiple startups at once. He works with Plural on community growth and strategy, particularly to help us solve the cold-start problem of building network effects from scratch.

Marketing Lead.

Laia Fernandez

Laia has over a decade of experience creating successful and creative marketing strategies. She has been the marketing lead in several NFT and Web3 projects. Her background is law and business; she has worked with large corporations in EMEA. She is passionate about new technologies, impact projects, and women's rights.

Actuarial Consultant.

Simon Warsop

Simon is the principal consultant at Bright Fathom and a Director of Insurance at Adiona. He has previously held the positions of Chief Underwriting Officer, Board Chair, and non-executive director at Aviva. He works with various Insurtech startups in the UK.

Motivation

The NFT space has a notorious reputation for scams and hacks and many major projects that have been instrumental in

bringing value and attention to the space, have also been targeted by hackers and scammers.

One way to deal with this risk is to be vigilant, and make sure that at a holder level, holders are educated and careful. However, there is only so much care that one can take, and hackers are a persistent and pervasive threat in this very global, open space. This isn't a great user experience and users are constantly looking over their shoulders.

We feel that the best place to start changing the narrative is at the top, so we are approaching the ApeCoin DAO for a grant to run a pilot project. At the end of the project, the BAYC and MAYC community will have a way to insure themselves against hacks and be protected from wallet drains. All payments for insurance/services could be done in ApeCoin.

Key Terms

NFT Insurance.

In the event that security processes fail and a digital asset is lost, NFT insurance makes a policyholder good by fulfilling the terms of a policy agreement. Eg. Replacing the lost NFT with an equivalent asset.

Community Based Insurance.

Communities create the system of insurance and governance through a mutual. Underwriters provide underlying assets, and or collateral. And, policyholders reduce their risks through the community for a fee. The community also plays a role in claims validation and blacklisting stolen/hacked assets.

Rationale

ApeDAO is at the cutting edge of the NFT space and continues to be at the forefront of innovation. There is nothing that aligns better with the mission of boldness, transparency and collective responsibility than an onchain, community driven, insurance system that helps holders remain holders should they become victims of a wallet drain or scam.

Our team at Plural Finance (Twitter: @pluralfi

) is focused on NFT insurance and Web3 risk management and has already modelled out the actuarial risk and collateral requirements for insuring BAYC/MAYC holders.

Benefits to the Ape Coin Community

In terms of benefits, having a community governed/driven insurance system, will give holders more options in terms of risk management, additional peace of mind and will be a talking point with regard to NFTs and risk. It's also quite pioneering and responsible and steps up the narrative around NFTs and Ape Coin into a more mature one: We recognise that we are the target of hacks and scams, and we're mitigating risks by investing in good systems.

If the worst should happen, the true benefit will come when a hack is prevented, or a holder is reimbursed for a loss using these tools.

Specifications

An EVM compatible smart contract system including an underwriting treasury, policy deployer and a front end system that can support it.

A EVM smart contract system for community governance system for claims validation e.g. staking + voting.

A billing system that allows holders to pay in ApeCoin for coverage from the community; and use ApeCoin for underwriting, if desired.

A custom BAYC front-end that allows users to interact

Education/instruction on how this will work for holders.

Integration into potential third party solutions for wallet drain prevention, for example, front-running solutions (See staginglabs.io).

Steps to Implement

Step 1. Adapt Plural's core technology for policy creation and underwriting; adapt the front-end for BAYC/MAYC specifically.

Step 2. Design, build and deploy a governance system for APE community insurance.

Step 3. Complete contract audits.

Step 4. Launch and educate holders on how the system works, and engage with them directly to try it out and get coverage plus security solutions.

Timeline

Step 1. November 2023

Step 2. December 2023

Step 3. January 2024.

Step 4. February 2024 (Depending on audit times,)

Estimated Overall Cost

Step 1. \$5000 (Developer and Design Costs: Front End)

Step 2. \$5000 (Developer Costs: Smart Contracts)

Step 3. \$20,000 (External Contract Auditors)

Step 4. \$15,000 Educational and Promotional Material

We expect to be able to pay back some of the grant from any fees generated if the system is well received, and successful. Our developer team is happy to subsidise some of the development costs, and we're offering our risk models/actuarial support for free.

Additional Notes

A main concern with this type of insurance system centers around fraud. Particularly, users purposefully draining themselves and then making claims from any underwriting fund intended for relief from actual hacks/scams. How does one tell the difference between a real hack or scam versus a fake one? There are a number of ways that we (and others) have been exploring around this topic. Here is a rough outline of scam and fraud prevention that may be integrated into our systems.

A. Using security tooling: There are currently several front running solutions available that help prevent drains. Plural is partnered with StagingLabs and their product Saferoot has been integrated into Metamask. Saferoot stops a significant portion of wallet drains >99.5%; and insurance would add another layer of protection on top of Saferoot.

B. Blacklists: A blacklist of stolen goods will help, but not prevent the resale of high value assets like APEs. Using technology, particularly AI, such a blacklist could be maintained via several systems (oracles), be fairly quick and flag any malicious behaviour via contract drains. Technology providers like Forta could help set this up and stop "legitimised" trading of stolen assets on major markets.

C. Community validation and verification systems. Ultimately the value of an NFT is social, and community members tend to know each other and are able to vouch for each other. How can this social credibility be used in insurance scoring and managing fraud risk? This is part of our ongoing research at Plural, where our focus is on designing credible decentralized insurance systems that can scale.

References

1. [\\$13.5 Million Worth of Bored Ape Yacht Club NFTs Stolen, Report Finds – ARTnews.com](#)
2. Plural Finance Whitepaper (plural.fi)