Status: Idea

Overview

This proposal introduces the concept of a “shadow NFT” or sNFT: a copy of an original NFT, ownable only by owner of that NFT, which can be used to prove ownership of said original without requiring interaction with it. It introduces a way for owners of Yuga Labs NFTs (BAYC, MAYC, etc.) to safely store their original NFTs, while granting new functionality to the sNFT which can be moved around and interacted with indiscriminitely without fear of loss.

As described, sNFTs would enable legacy NFTs to be upgraded with new functionality that doesn’t existing in the original contract.

This in turn unlocks new features, and paves a safer path towards NFT-specific staking pools for $APE.

shadow | shad·ow | \ ˈsha-(ˌ)dō \

1. the dark figure cast upon a surface by a body intercepting the rays from a source of light
2. an attenuated form or a vestigial remnant
3. an inseparable companion or follower
4. a reflected image
5. shelter from danger or observation
6. a copy of something

Problem

NFTs can provide great utility, but present a security risk

There are many reasons why proving ownership over an NFT is useful. Examples include:

- Access to NFT-specific channels in Discord, Telegram, etc.
- As a key to get NFT-specific merchandise (like the Yuga Labs store)
- To enable the hexagon NFT pfp feature with Twitter
- Claiming airdrops, as with ApeCoin
- As a key to access NFT-specific staking pools, as was described in ApeCoin’sAIP-4

Keeping valuable NFTs in accessible wallets (hot wallets, even hardware wallets) opens the door to loss or theft. If you keep your valuable in an NFTs in a wallet that regularly interacts with smart contracts, is used for signatures, etc. each interaction is a potential moment for loss or theft. As Yuga Labs prepared to launch Otherside, their Instagram account was hacked and sent people to a fraudulant Otherside minting site, which then stole the NFTs in their wallet.

Author’s Note: I believe this happens partially because we are conditioned to keep our valuable in NFTs in accessible wallets as they are used as keys to other things

The best security to protect valuable NFTs is to put them in wallets that make it hard to get them out e.g. Multi-signature wallets and Hardware wallets that aren’t used for signatures or interact with smart contracts. Keeping NFTs locked away prevents their use for any other functionality or features. To use the above features, the NFTs must be kept in an easily accessible wallet or you can miss out on being able to use them.

NFTs like BAYC or MAYC are non-upgradeable

While by design, BAYC or MAYC NFTs are not upgradeable and cannot be given new features. This means that even if the community desires new functionality to be added, it’s simply not possible. e.g. if the community wants to enable soft staking (non-custodial) for an NFT that didn’t program that in ahead of time, it’s not possible.

Staking NFTs for $APE

There is a desire within the ApeCoin community to enable additional $APE staking rewards for owning a Yuga NFT (BAYC, MAYC, BAKC). However, staking the NFTs themselves would present a security risk. In Yuga Labs’ Garga’s own voice from his blog post on the subject:

First off, I don’t want to see NFTs become locked away in “staking” contracts or really any kind of contract. To me, that goes against the ethos of the APE ecosystem. Your NFT is/can be your metaverse identity. That shouldn’t be something that gets locked away in a contract. I think members should have custody of their own NFTs. Whatever happens here, I want to encourage ApeCoin DAO voters not to push forward a system where we’re forcing users to lock away their NFTs in a contract.

So-called “soft staking” or non-custodial staking has been proposed by the community as a solution for this, but as was mentioned above this isn’t possible as the NFTs aren’t already programmed with that functionality.

Background on previous NFT staking proposals:

Two AIPs (AIP-4 and AIP-5) were proposed to set up $APE staking, with the Yuga NFTs acting as a “key” to specific pools for additional rewards. For instance, if you staked $APE and used a BAYC as your “key”, you would get access to the BAYC $APE pool and its allocation.

Owners would continue to earn $APE until the end of the pool, until you unstaked, or until the “key” NFT was sold or transferred. If the NFT sold or stolen prior to unstaking the $APE, the $APE would remain locked and no longer able to be unstaked.

The “key” concept otherwise is desireable as staking the Yuga NFTs themselves would introduce additional risk. $APE is also considered a different project entirely from the Yuga NFTs.

The purpose of the “key” concept was to provide additional incentives for owners of the Yuga NFTs to participate in the $APE ecosystem. It sets up a special recognition and incentives for those with Yuga NFTs vs. those with $APE only

Author’s note: I consider this feature to be interesting, but am too concerned with the loss implications, and would prefer to not stake my NFTs directly

If $APE migrates off Ethereum, the Ape’s aren’t coming along

As has been mentioned by Yuga Labs, they are recommending that ApeCoin move off of Ethereum for greater scaleability. They describe a new L1, but there is a good amount of support and discussion around moving to an Ethereum Layer 2 instead. e.g. Polygon, StarkNet, Optimism, Arbitrum, etc.

However, if ApeCoin is indeed moved to another L1 chain or L2 solution, that means the ecosystem will be fractured, separating it from the original Yuga NFTs. This could make things difficult—as paying in $APE while proving ownership over a specific Yuga NFT would be extra challenging.

Proposed solution

Creating a new kind of NFT that could act as a proxy, or “shadow” of an original NFT could open the door to new functionality, and help safeguard valuable assets. Below we describe some prior art for this concept and explore how it could be implemented for BAYC/MAYC/BAKC NFTs and the $APE ecosystem.

Create a Shadow NFT contract, inspired by 0N1 FRAMES

I propose that we introduce a new contract able to mint NFTs that act as a shadow for original Yuga NFTs. This concept was inspired by 0N1 FRAMES by 0N1VERSE.

In their own words, from their website:

0N1 FRAMES are custom tailored for each of the 7,777 0N1. Traits such as the original 0N1’s mask and body type influence the 0N1 FRAMES and each is directly linked to it’s owner.

…

As long as you own an original 0N1, the 0N1 FRAMES are free to claim + gas.

…

0N1 FRAMES are transferable but cannot be traded via open marketplace.

This is because each one of the 0N1 FRAMES are based directly on the original token ID. This is a continuation of the IP and guarantees ownership of the specific character and its derivatives as it evolves! 0N1 FRAMES will feature matching and unique new variations on traits!

0N1 FRAMES can be moved to other wallets and through the dApp, 0N1 FORCE holders can always recall their 0N1 FRAMES!

IMPORTANT: By selling or transfer of your original 0N1 FORCE NFT you also give ownership of the respective Frame to the wallet owner.

The 0N1 FRAMES contract can be viewed here.

This approach is novel as you’re able to hold the 0N1 FRAME as a proxy for, and separate from your owned 0N1FORCE NFT. For instance, an owner can maintain the 0N1FORCE NFT securely in their cold wallet, while keeping their 0N1 FRAME in a hot wallet for:

- Social signaling
- Proof of ownership

Non-custodial NFT-keyed staking pool access

In the above described AIP-4 proposal where NFTs could be used as “keys” to gain access to NFT-specific staking pools for $APE, it left owners susceptible to loss or theft. If $APE was staked in an NFT-keyed pool, and the “key” NFT was sold, the staked $APE would be locked and lost. Further, if NFT owners are conditioned to interact with contracts with the wallet that contains their valuable NFTs, they may be susceptible to scams and hacks.

If the above described shadow / proxy / frame NFT was instead used as a key for specially incentivized staking pools, both of those risks go away. First, $APE would not be locked on transfer because the sNFT could be programmed with that case in mind. Second, since an sNFT can be kept in a separate wallet from the original NFT, one can keep the original in a cold wallet, and keep the sNFT in a hot one. If an sNFT is stolen or lost from a hot wallet, it can always be recovered by the wallet that still contains the original.

Requirements

Here we describe the basic requirements needed to make this happen. It does not describe the means by which we achieve this, but instead the test that a solution must pass to be workable.

- Owners SHOULD be able to verify their current and ongoing ownership of BAYC/MAYC/BAKC NFTs
- Verification MUST be done in a way that does not require interaction with the wallet that contains the original NFTs, or require interaction with their smart contracts
- Staked $APE MUST not be locked and made untransferrable if the “key” NFT is sold or stolen prior to unstaking
- Staked $APE MUST stop accruing in specific incentive pools if the “key” NFT is transferred to a non-user owned wallet
- Staked $APE should fall back to ApeCoin-only pool rate on such transfer
- Staked $APE should fall back to ApeCoin-only pool rate on such transfer

Specification

- Introduce a new smart contract that generates a shadow of the original NFTs
- Owners of BAYC and MAYC NFTs can interact with this contract to claim their free “Frame” (brand tbd)
- This shadow NFT could add some new art to distinguish it from the original
- This shadow NFT could add some new art to distinguish it from the original
- The Shadow NFT (sNFT):
- is directly linked to the original
- can not be sold
- owner is set to the owner of the original
- is directly linked to the original
- can not be sold
- owner is set to the owner of the original
- Once the sNFT has been minted, the owner can choose to move the original NFT to cold storage
- Owners of BAYC and MAYC NFTs can interact with this contract to claim their free “Frame” (brand tbd)
- This shadow NFT could add some new art to distinguish it from the original
- This shadow NFT could add some new art to distinguish it from the original

- The Shadow NFT (sNFT):
- is directly linked to the original
- can not be sold
- owner is set to the owner of the original
- is directly linked to the original
- can not be sold
- owner is set to the owner of the original
- Once the sNFT has been minted, the owner can choose to move the original NFT to cold storage
- Introduce a new smart contract that allows for staking-like functionality without locking up an asset

(original NFT or sNFT) * “Nesting” (brand tbd) would allow the owner to use the sNFT as a key to enter asset-specific $APE reward pools, such as a BAYC $APE staking pool

- If the original asset or sNFT is sold/lost/stolen, the staked $APE would still be accessible for unstaking
- The staked $APE rewards may reduce to the ApeCoin-only pool vs. the asset-specific reward pool
- The staked $APE rewards may reduce to the ApeCoin-only pool vs. the asset-specific reward pool
- “Nesting” (brand tbd) would allow the owner to use the sNFT as a key to enter asset-specific $APE reward pools, such as a BAYC $APE staking pool
- If the original asset or sNFT is sold/lost/stolen, the staked $APE would still be accessible for unstaking
- The staked $APE rewards may reduce to the ApeCoin-only pool vs. the asset-specific reward pool
- The staked $APE rewards may reduce to the ApeCoin-only pool vs. the asset-specific reward pool
- Allow for minting / claiming additional sNFT copies on L2’s
- Additional minting contracts could be deployed to various L2’s, so that BAYC/MAYC/BAKC ownership could be proven within

that L2

- Additional minting contracts could be deployed to various L2’s, so that BAYC/MAYC/BAKC ownership could be proven within

that L2

Benefits

- Introducing a new contract means more functionality could be added where this is not possible with the original NFTs
- “Nesting” the sNFT’s for additional staking rewards would not add risk of losing $APE if original NFT or sNFT is lost/stolen
- sNFT’s can be used as proof of ownership without risking the safety of the wallet custodying the original
- sNFT’s could exist natively within L2’s

Risks

- The owner must interact with the shadow NFT minting contract from the wallet containing the original asset
- It would be important to have Yuga Labs’ blessing on this, as they would need to promote the official URLs
- Scammers try to take advantage of the minting of a new asset
- They might set up phishing sites
- They might set up phishing sites
- The advantage of this is that the owner would only need to interact once

and could then store their original NFT securely, while moving the sNFT at will

- It would be important to have Yuga Labs’ blessing on this, as they would need to promote the official URLs
- Scammers try to take advantage of the minting of a new asset
- They might set up phishing sites

- They might set up phishing sites

- The advantage of this is that the owner would only need to interact once

and could then store their original NFT securely, while moving the sNFT at will

- Yuga Labs does not support this proposal
- This would mean the sNFTs could be considered “second class citizens” and thus not supported widely

- This would mean the sNFTs could be considered “second class citizens” and thus not supported widely

- Yuga Labs creates their own shadow contracts that “competes” with an ApeCoin DAO-supported contract
- This could create market confusion, among other things.
- Perhaps the solution here would just be to try to work directly with Yuga Labs

- This could create market confusion, among other things.
- Perhaps the solution here would just be to try to work directly with Yuga Labs

Questions

- Why not just stake the NFTs?
- The original NFT contracts weren’t built with staking in mind, and functionality remains limited.

- The original NFT contracts weren’t built with staking in mind, and functionality remains limited.

- Why is the sNFT even needed?
- Because the original NFT contracts didn’t consider future functionality beyond selling and transferring, adding features to the NFTs themselves is impossible
- Minting a shadow NFT would enable new functionality without affecting the original

- Because the original NFT contracts didn’t consider future functionality beyond selling and transferring, adding features to the NFTs themselves is impossible
- Minting a shadow NFT would enable new functionality without affecting the original

- In AIP-4 why do the original NFTs need to be used as “keys”? Why not just emit $APE for holding the NFT.
- Emitting $APE for simply holding an NFT may cause the NFTs to be considered securities under U.S. law

- Emitting $APE for simply holding an NFT may cause the NFTs to be considered securities under U.S. law

- If I have staked $APE, and both an original and sNFT, what happens when I sell the original NFT?
- The new owner who purchased the original NFT can transfer ownership of the sNFT to themselves
- Upon transfer of the sNFT, the $APE would be unstaked and returned to its owners wallet (not the new NFT owner)

- The new owner who purchased the original NFT can transfer ownership of the sNFT to themselves
- Upon transfer of the sNFT, the $APE would be unstaked and returned to its owners wallet (not the new NFT owner)

Scenarios

Claiming the sNFT and using it to prove ownership

- Scenario A:

- Alice buys BAYC #420

from Dan

- Alice owns $APE and tries to stake it in the BAYC-specific staking pool
- Alice navigates to the staking website, which alerts her that Dan still has ownership over the #420

sNFT

- Beacuse Alice owns BAYC #420

, she claims BAYC sNFT #420

and transfers to herself

- Alice can now enter the staking pool, proving ownership over sNFT #420

- Alice buys BAYC #420

from Dan

- Alice owns $APE and tries to stake it in the BAYC-specific staking pool
- Alice navigates to the staking website, which alerts her that Dan still has ownership over the #420

sNFT

- Beacuse Alice owns BAYC #420

, she claims BAYC sNFT #420

and transfers to herself

- Alice can now enter the staking pool, proving ownership over sNFT #420

Unstaking $APE on sNFT transfer

- Scenario B
- Alice has staked $APE in the BAYC-specific pool, having used her sNFT #420

to prove ownership over BAYC #420

- Alice sells BAYC #420

to Charlie

- Charlie transfers ownership of sNFT #420

to thsemlves

- Alice’s $APE is unstaked on transfer of sNFT #420

to Charlie * But notably, is not lost

- But notably, is not lost

- Alice has staked $APE in the BAYC-specific pool, having used her sNFT #420

to prove ownership over BAYC #420

- Alice sells BAYC #420

to Charlie

- Charlie transfers ownership of sNFT #420

to thsemlves

- Alice’s $APE is unstaked on transfer of sNFT #420

to Charlie * But notably, is not lost

- But notably, is not lost

Selling NFT right after staking $APE with sNFT as key

- Scenario C:

- Alice buys BAYC #420

from Dan

- Alice mints shadow NFT #420

(Dan did not mint the sNFT)

- Alice stakes $APE and uses sNFT #420

to gain access to the BAYC-specific staking pool

- Alice sells BAYC #420

to Bob

- Alice buys BAYC #420

from Dan

- Alice mints shadow NFT #420

(Dan did not mint the sNFT)

- Alice stakes $APE and uses sNFT #420

to gain access to the BAYC-specific staking pool

- Alice sells BAYC #420

to Bob

- Will Alice continue to receive $APE rewards for her staking?
- As the feature is written, yes.
- We can explore technical feasibility to limit or end rewards on transfer of the NFT, where its new owner (Bob) has not yet claimed

the sNFT, and therefore it remains behind with Alice.

- We can explore technical feasibility to limit or end rewards on transfer of the NFT, where its new owner (Bob) has not yet claimed

the sNFT, and therefore it remains behind with Alice.

- As the feature is written, yes.
- We can explore technical feasibility to limit or end rewards on transfer of the NFT, where its new owner (Bob) has not yet claimed

the sNFT, and therefore it remains behind with Alice.

- We can explore technical feasibility to limit or end rewards on transfer of the NFT, where its new owner (Bob) has not yet claimed

the sNFT, and therefore it remains behind with Alice.

- Can someone sell their BAYC NFT just after staking $APE and using their sNFT as key to the pool?

- Yes

- Yes

- What happens to the sNFT?

- The new owner of the BAYC NFT (Bob) can immediately transfer the sNFT to themselves

- The new owner of the BAYC NFT (Bob) can immediately transfer the sNFT to themselves

sNFT is stolen from hot wallet

- Scenario D:
- Alice maintains BAYC #420

in her cold wallet, and sNFT #420

in her hot wallet

- An attacker gains access to Alice’s hot wallet and transfers the sNFT #420

to themselves

- Alice re-claims sNFT #420

into her cold wallet, as that wallet is considered the owner by way of owning BAYC #420

- Alice starts a new hot wallet, and transfers sNFT #420

to it

- Alice maintains BAYC #420

in her cold wallet, and sNFT #420

in her hot wallet

- An attacker gains access to Alice’s hot wallet and transfers the sNFT #420

to themselves

- Alice re-claims sNFT #420

into her cold wallet, as that wallet is considered the owner by way of owning BAYC #420

- Alice starts a new hot wallet, and transfers sNFT #420

to it