

4K Protocol Whitepaper

Stephen Gu

Richard Li

Tyler Sullberg

June 4, 2022

v1.2

1 Abstract

The blockchain has transformed how we can own and interact with digital assets - ownership records are decentralized and composable in the larger blockchain ecosystem. However, these innovations have applied exclusively to purely digital assets, and the blockchain does not have an interface for the physical world. The blockchain does not yet have a sense of touch.

4K is a decentralized protocol that enables anyone to bring physical assets on-chain as a physically-backed token. Assets are securely held by a guardian who guarantees that the asset owner's physically-backed token can be burned in exchange for the physical asset at any time. Guardians are held accountable through on-chain audits and staking pools. At its core, the protocol is a coordination layer between the digital and physical worlds.

By creating physically-backed tokens, we are introducing a new composable primitive to the Web3 ecosystem and enabling humanity to use physical assets in unprecedented ways. With an on-chain representation of a physical asset, owners of physically-backed tokens can transfer physical assets at a fraction of the cost and friction of a traditional transaction. Anyone can use physically-backed tokens as collateral in a loan, a means of fractionalization, and even as the basis of a stablecoin. One will no longer need to be in the same physical proximity of a physical asset to use it. Idle physical assets will be brought into the metaverse, become the basis for membership into social clubs, and enable other use cases we can't yet imagine.

2 Introduction

The key problem of bringing physical assets on-chain is that the physical world is fundamentally uncertain. Whereas we can have near certainty about the validity of a purely digital on-chain asset by replaying the blockchain's transactions since the genesis block, there is no such certainty with physical assets. In the real world, there are bad actors, geopolitical instability, and physical decay. Rather than pretend this uncertainty does not exist, the 4K Protocol embraces it.

The scope of this white paper is focused on the *physical guardian protocol*, which is designed to ensure that a physically-backed token is truly backed by a physical asset. However, the broader vision of the 4K Protocol is to be the coordination layer for every way in which the on-chain users may want to interact with a physical asset. This will include the *authentication protocol* to maximize certainty that a physically-backed token is exactly what it represents itself to be and a

valuation protocol to maximize certainty of an asset’s market price. These protocols will be detailed in subsequent papers.

The 4K Protocol is a novel approach for bridging physical and digital worlds; previous attempts to create the physical-digital bridge have been centralized, ad-hoc, and rife with misaligned incentives. In comparison, the 4K Protocol is built to be:

- **Decentralized:** Assets are brought on-chain through a decentralized network of guardians, authenticators, and appraisers. The network comes to a consensus on whether a physical asset is truly backing a physically-backed token, whether that asset is what it represents itself to be, and how much that asset is worth.
- **Universal:** The 4K Protocol is a universal protocol for bringing *any* physical asset on-chain (e.g., watches, wine, art, real estate).
- **Incentive aligned:** Nodes in the network have a financial stake in the network and are incentivized to act in the best interest of protocol.
- **Composable:** The 4K Protocol is built with compatibility in mind and is creating a shared framework for interacting with the physical world using tokens.
- **Chain agnostic:** 4K’s physically-backed tokens can exist on any chain with an NFT standard.
- **Scalable:** The 4K Protocol is designed to bring in millions of assets on-chain quickly and efficiently.
- **Transparent:** Both the provenance of assets and the operations of guardians (including losses, damages, etc.) are publicly stored on-chain.

We will build the 4K Protocol governance and accountability system on Ethereum, though physically-backed 4K tokens will be implemented across all major layer 1s and 2s.

2.1 Key Components

The 4K Protocol is built around the following key components:

Physically-Backed Tokens: We present a novel concept of a *physically-backed token* — a token that can be redeemed for its respective physical asset by burning the token. These tokens will generally conform to the ERC-1155 standard, though they can also conform to the ERC-721 and ERC-20 standards.

Physical Guardian Protocol: We describe a protocol that ensures that a physically-backed token is truly backed by a physical asset.

Proof-of-Assets: We outline a system by which a decentralized network of guardians prove that they are holding a physical asset and are held accountable if that asset is lost or damaged. This protocol is what enables one to believe a physically-backed token can actually be redeemed for the original physical asset without needing to trust any single centralized entity.

Staking Pools: We introduce a mechanism to hold guardians financially accountable for lost assets, damaged assets, or failure to follow the standards of the protocol. This mechanism is also used to

quickly reimburse asset owners in the event of a loss or damage and serves as a layer of protection beyond the traditional legal system.

Physical Oracles: We describe a system for the state of physical assets to be routinely recorded on-chain.

2.2 Key Component Overview

- Physically-backed tokens are minted when a physical asset is placed in the care of a guardian. An asset owner can redeem their token for the physical asset by burning the token.
- Guardians are compensated for the cost and risk of holding physical assets with guardian fees. If an asset owner does not pay their guardian fee, the physically-backed token is sold in an English-style auction.
- In the event of a loss or damage claim, asset owners are immediately compensated through the staking pool. Guardians are required to stake and stakers earn governance rights, 4K token emissions, and a percentage of protocol fees. Payouts from the staking pool are a mechanism to provide immediate resolution for claims - guardians are required to pay back the full value of all payouts from the staking pool.

3 Physically-Backed Tokens

Physical assets are represented on-chain with tokens. A physically-backed token has the following attributes:

- **Asset metadata:** Each asset contains attributes that are common between assets (e.g., name, description, category) as well as arbitrary key-value pairs that can be defined by the asset owner. The 4K Protocol creates standards on attributes that must be present for given asset categories.
- **Guardian type:** Who the guardian is, where the guardian is located, and how the asset will be held (e.g., temperature control, location, security level, on-chain coverage caps).
- **Guardian rate:** The rate that the asset owner must pay the guardian to hold the asset.
- **Guardian fee balance:** A balance of tokens that guardian payments are paid from. Asset owners can top up this balance at any time. When the token is transferred to another owner, the remaining guardian fee balance for that asset is returned to the original owner.

Each token progresses through the lifecycle of minting, being held by a guardian, and redemption. In between, the token — and thus the asset itself — can be freely exchanged or used in financial platforms, both centralized and decentralized. There are fees associated with each stage of the lifecycle and a small portion of these fees accrue to the treasury and the staking pool. This fee accrual is described in detail below. The treasury also collects a marketplace fee whenever the asset is transferred between owners.

4 Physical Guardian Protocol

The purpose of the physical guardian protocol, a subset of the 4K Protocol, is to create a digital token that represents ownership of the physical asset.

For the token to represent ownership, transferring the token must also mean that one is transferring ownership of the physical asset. That ownership is only meaningful if the new owner of the token can redeem their token for the physical asset. If the holder of the token tries to take possession of the physical asset, the holder of the physical asset could refuse out of maliciousness, incompetence, loss, damage, or any other reason. The 4K Protocol is built to solve this agency problem by aligning incentives between the guardian and the owner of the token to securely store the asset and return it when requested.

Guardians are entities in the 4K Protocol who are responsible for securing a physical asset. The physical guardian protocol governs how guardians interact with physical assets in two respects:

- **Compensation:** In exchange for the risk and cost of securing the physical asset, guardians are compensated.
- **Accountability:** Guardians are required to provide proof-of-assets and are held accountable for mishandled assets.

4.1 Compensation

Guardians are compensated for securing physical assets through guardian fees, minting fees, audit fees, and redemption fees. All of these fees are paid in USD stablecoins. Stablecoins that can be used for payment of fees are approved by protocol governance.

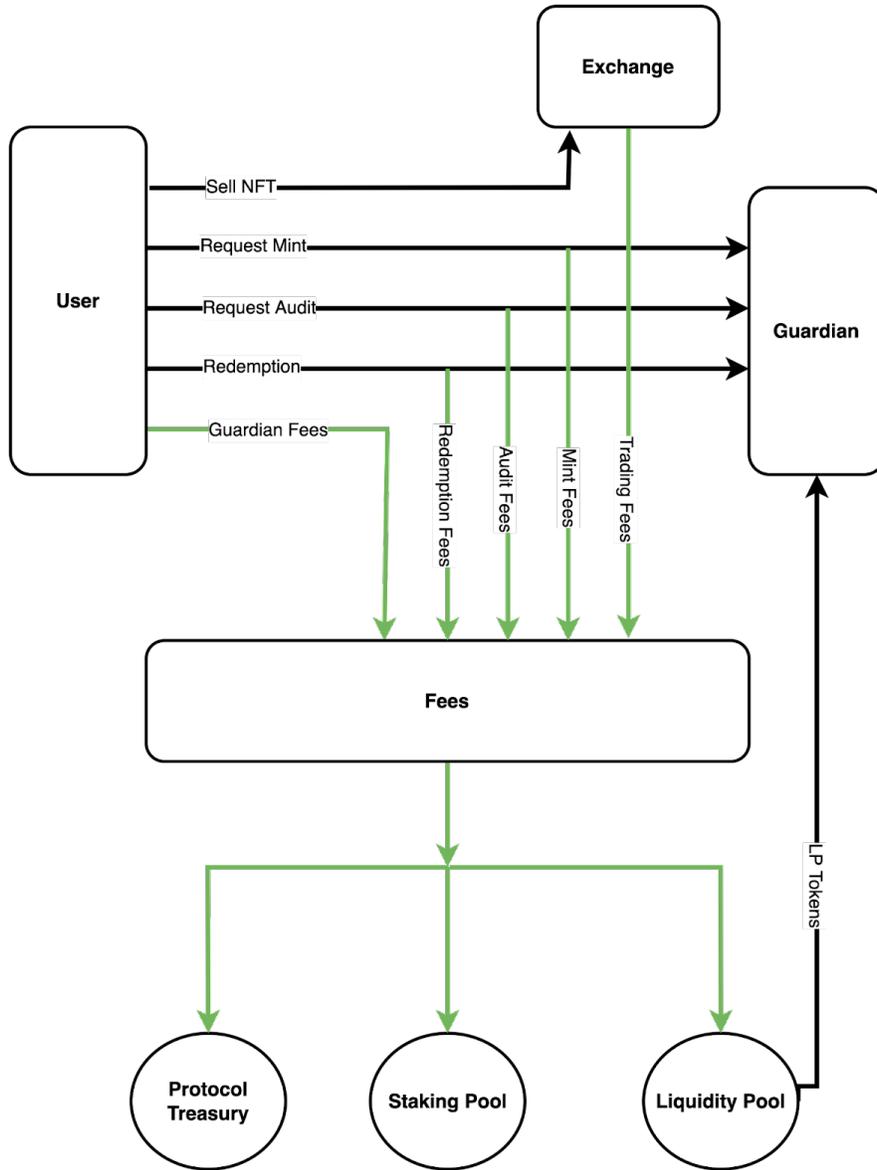


Figure 1: Protocol Fee Distribution

4.1.1 Liquidity Pool

Guardian fees, minting fees, audit fees, and redemption fees are paid to guardians in stablecoins, but the guardian does not directly receive stablecoins for their rendered services. Instead, fees are automatically deposited into a liquidity pool of stablecoins and 4K tokens. This liquidity pool will initially be seeded by 4K and kept in balance by market arbitrage. The guardian receives liquidity pool tokens for their rendered services that they can later trade for either stablecoins or 4K tokens. We expect the impact of slippage to be low since the average value of 4K tokens being paid into the pool will be relatively low. The intent of this design is to:

1. Insulate the asset owner and the guardian from currency risk.
2. Since Balancer [1] style pools can support an arbitrary number of currencies, the user and guardian have flexibility in which currency they want to use to pay and receive their guardian fees.
3. Create liquidity for the 4K token.
4. Provides a sustainable source of demand for the 4K token via a steady inflow of stablecoins into the liquidity pool.
5. Give guardians yield on their guardian fees by default.

4.1.2 Guardian fees

Guardians charge fees for securely storing an asset. While the asset is held by the guardian, guardian fees are continuously charged on-chain with each block. Guardian fees are charged on each asset individually, and each asset has its own balance. The asset owner (i.e. token holder) pays their guardian fees upfront by topping up the balance on their assets. As guardian fees accrue, the fees for an asset are automatically deducted from that asset's balance.

For example, a guardian could set their guardian fee for a given class of assets at 1 USDC per day. If the asset owner wants to top up their balance for that asset for the next year, they would prepay 365 USDC for that physically-backed token and that payment would be reflected on the token's balance. After five days have passed, five tokens would be paid out of this balance to pay the guardian, and the other 360 tokens would remain locked in the token's balance. This example is simplified for the sake of clarity. In reality, the guardian will be paid in LP tokens which the guardian can choose to trade in for 4K tokens or stablecoins.

The price of guardian fees is determined competitively between guardians who compete on:

- Price
- Reputation (e.g., number of on-chain audits the node has failed and passed, whether the node has unpaid claims)
- Total on-chain claim coverage
- Ability to provide specialized services (e.g., high security, temperature control)
- On-chain coverage caps via the staking pool
- Off-chain insurance

While guardians have full autonomy in setting the fee rates for new physical assets entering their care, they are limited in how quickly they can raise limits, which is expressed as a percentage increase over time, for existing assets in their care. The maximum rate at which fees can be raised for existing assets held by guardians is determined by protocol governance.

4.1.3 Guardian Asset Classes

The guardian fee is determined via the *guardian class*. Each *guardian class* is a specification on the level of service a given asset will receive (e.g., temperature control, security, handling precautions), the maximum on-chain coverage payout for that asset in the event of a loss/damage, the redemption fee cost, and the guardian fee (USD fee per block) for that asset. The guardian class is selected by the asset owner when the physically-backed token minting request is created.

$$\text{Guardian fees} = \text{Fee per block as defined by guardian class} \times \text{Number of elapsed blocks} \quad (1)$$

A guardian can choose to activate or deactivate guardian classes for *new* assets at any time, though guardian classes for existing assets cannot be deactivated.

4.1.4 Minting

Before an asset is minted, the asset owner pays a minting fee to create an on-chain record of their selected guardian, guardian type, and asset metadata (e.g., asset pictures, description). This on-chain record is not to be confused with the physically-backed token, which is created once the guardian receives the asset. The owner of the physical asset then sends their asset to the guardian.

The purpose of the minting fee is to compensate guardians for the one-time cost of inventorying an item and disincentivize people from spamming guardians with low-quality physical assets. The minting fee is set by the guardian for each guardian asset class. Each guardian is responsible for setting its own minting fee. A percentage of the minting fee is sent to the protocol's treasury and staking pool and the rest goes to the guardian.

When an asset is received, there is a mandatory on-chain audit of that asset. During the initial audit, the auditor places a unique identifier on the asset and photographs the asset. The audit process is described below in detail. Once the on-chain record of the audit is created, the token is automatically minted, which enables the guardian to collect the minting fee and begin collecting guardian fees on the asset.

4.1.5 Redemption

When a token owner wants to redeem their token for a physical asset, the token owner pays a *redemption fee* to use the protocol's redemption mechanism and enters the physical address where the asset must be sent via an off-chain process. Once this occurs, the token is burned and the asset no longer accrues guardian fees.

Redemption fees are set by the guardian for each class individually. A percentage of the redemption fee is sent to the treasury and the rest goes to the guardian.

Once an asset is redeemed, there is a mandatory final on-chain audit of that asset in which the asset is photographed with its unique identifier. The audits at the beginning and end of an asset's lifecycle with a guardian are foundational elements of the accountability system described in detail below.

4.1.6 Auctions

If an asset reaches a negative balance, a 90-day grace period begins. Fees continue to accrue during the grace period. If the asset owner does not resolve the asset's negative balance within the grace period, the asset is automatically sold on the open market via an English auction (similar to MakerDAO's [2] CDP system).

Assets purchased in the auction are paid for with 4K tokens. Proceeds from the auction are first used to pay the negative balance. The remainder is split between the prior asset owner who failed to pay their guardian fees (85%), the guardian (10%), and the protocol's treasury (5%). This split can be changed by protocol governance. If no one purchases the asset in the auction, the guardian becomes the owner of the asset.

The 4K Protocol's auction mechanism is far more efficient than how delinquent accounts are handled in the traditional warehousing industry. Whereas traditional auctions are opaque with high transaction costs, the 4K auction is fully automated and transparent. Auction participants can find all relevant details about an asset without seeing the asset in person, and the asset can change hands without needing to physically move.

4.2 Proof-of-Assets

Guardians are required to provide proof-of-assets to prove that physically-backed tokens in their care are actually backed by physical assets. Guardians are held accountable via a combination of the audit oracle and self-staking.

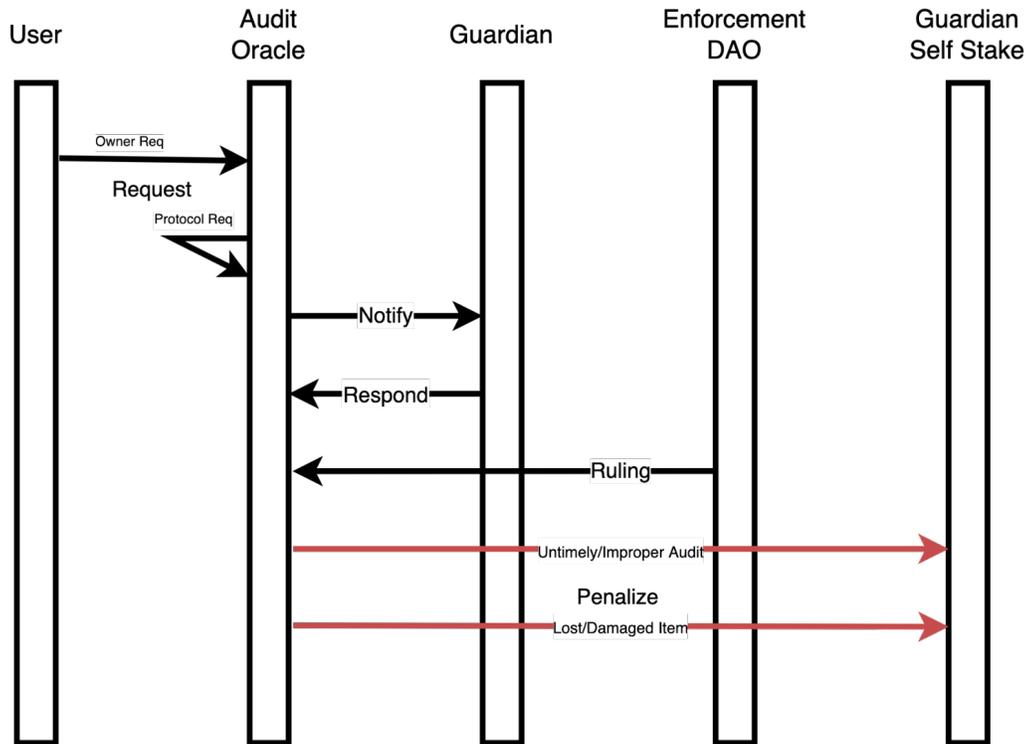


Figure 2: Audit, Review, and Enforcement Process

4.2.1 The Audit Oracle

Guardians supply proof on whether an asset is truly backing a physically-backed token through the *audit oracle*. The audit oracle is used to hold guardians accountable for losing or damaging physical assets. The audit record for each physically-backed token is publicly stored on-chain.

All assets are audited when the asset first enters the care of the guardian and again when the asset is finally redeemed. Audits are performed regularly and can be initiated in multiple ways:

- **Initiated by the owner:** The owner can initiate an audit for a fee. This fee is set by each guardian individually. There is a cap on the maximum fee a guardian can charge for an audit. There is also a cap on the maximum number of audits an owner can request per asset per time period. The audit fee and maximum audit frequency are set by protocol governance.
- **Randomly initiated by the protocol:** Every week, the protocol will randomly select a small percentage of assets for each guardian to audit. This percentage is set by protocol governance. The guardian will not earn an audit fee for audits initiated by the protocol.
- **During asset inventory and redemption:** An audit is required on any asset 1) once it enters the guardian's care and 2) when the asset is redeemed. These audits are free of charge.

Audits are performed remotely via video, though later the protocol may also support in-person audits. During an audit, the guardian is required to display a unique identifier of the asset, the asset itself, and the hash of a block that was added to the blockchain no more than 4 hours prior

to the creation of the on-chain audit record. The unique identifier attached to the asset can have varying levels of security (e.g., RFID, tamper-evident seals, diamond-dust identifiers [3]). Guardians compete with each other to offer robust unique identifiers that are not prone to tampering, hacks, or cloning. The video recording is stored off-chain, while a hash of the video is stored in the on-chain audit record.

The audit is a request for proof, not a final determination, that an asset remains intact and in possession of the guardian. Owners of the physical asset are only reimbursed through the on-chain staking pool after a *review* has taken place. Reviews are described in detail below.

The protocol sets on-chain standards to ensure high-quality audits:

- **Automatic penalties for untimely audits:** Guardians set service level agreements (SLAs) for each guardian class on how long audits and redemptions will take to complete. The guardian's self-stake will automatically be charged a penalty for each day that the requested audit has not been completed. This penalty can be changed by protocol governance.
- **Quality reviews:** Anyone can initiate a review of an audit that doesn't meet the standards of the protocol (e.g., blurry images, missing unique identifiers). If the Enforcement DAO finds the audit has not been properly conducted, a penalty will automatically be charged to the guardian's self-stake. This penalty is set by protocol governance.
- **When in doubt, rule on the side of the asset owner:** If an asset is being reviewed as a suspected loss, the Enforcement DAO will interpret failure to produce an audit or poor quality audits as evidence that the asset is lost.

4.2.2 DAO Review

The community is incentivized to proactively monitor audits to see if there is evidence of lost assets, damaged assets, or improperly conducted audits. Anyone can initiate a *review* of an asset from the protocol's Enforcement DAO. During a review, the Enforcement DAO determines whether there has been loss or damage of an asset and how much that loss or damage is worth. If the Enforcement DAO levies a penalty on the guardian, the individual who initiated the review will receive a portion of that penalty as a reward. The fee to initiate a review and the reward for correctly identifying an issue are both set by protocol governance.

There are different types of review:

- **Audit review:** When an audit was not performed correctly (e.g., blurry images, unique identifier not present on the asset). The penalty for an improperly conducted audit is set by protocol governance.
- **Asset review:** Asset reviews are initiated when an asset is suspected to be damaged or lost. The maximum amount a guardian will be responsible for is defined by the coverage payout cap. The coverage payout cap is defined by the guardian on each guardian class. For example, a guardian may have a "Class A" guardian class that covers an asset up to \$50K. If, during the Enforcement DAO's review, there is determined to be a loss or damage, a *claim* is created. The value of the claim is then automatically removed from the staking pool and sent to the token owner's address. If the asset has been lost, the token is burned.

- **Guardian review:** This review is initiated when the guardian is suspected of systematically being deceptive and not acting in the best interest of the protocol. Penalties for the guardian review are determined by Enforcement DAO.

4.2.3 Audits and reviews are publicly stored on-chain. Asset owners will review this transparent record of loss rates, damage rates, and Enforcement DAO penalties to evaluate whether a guardian is reliable.

4.3 Staking and Accountability

The 4K protocol implements a novel staking pool design that connects staking rewards to the core-economic driver of the Protocol - guardian fees. This design is inspired by the veToken design of Curve [4] and validator slashing design of Tendermint [5]. This design is intended to accomplish the following goals:

- **Build trust:** An on-chain mechanism to immediately compensate asset owners in the event that the Enforcement DAO determines there are losses or damages.
- **Create accountability:** Guardians are required to have skin in the game, and are held accountable on-chain for losses, damages, and process violations.
- **Align incentives:** Long-term stakers are rewarded with both higher emissions, governance rights, and allocations of protocol fees.

Staking pools are created with 4K tokens and payouts from the staking pool are made with 4K tokens.

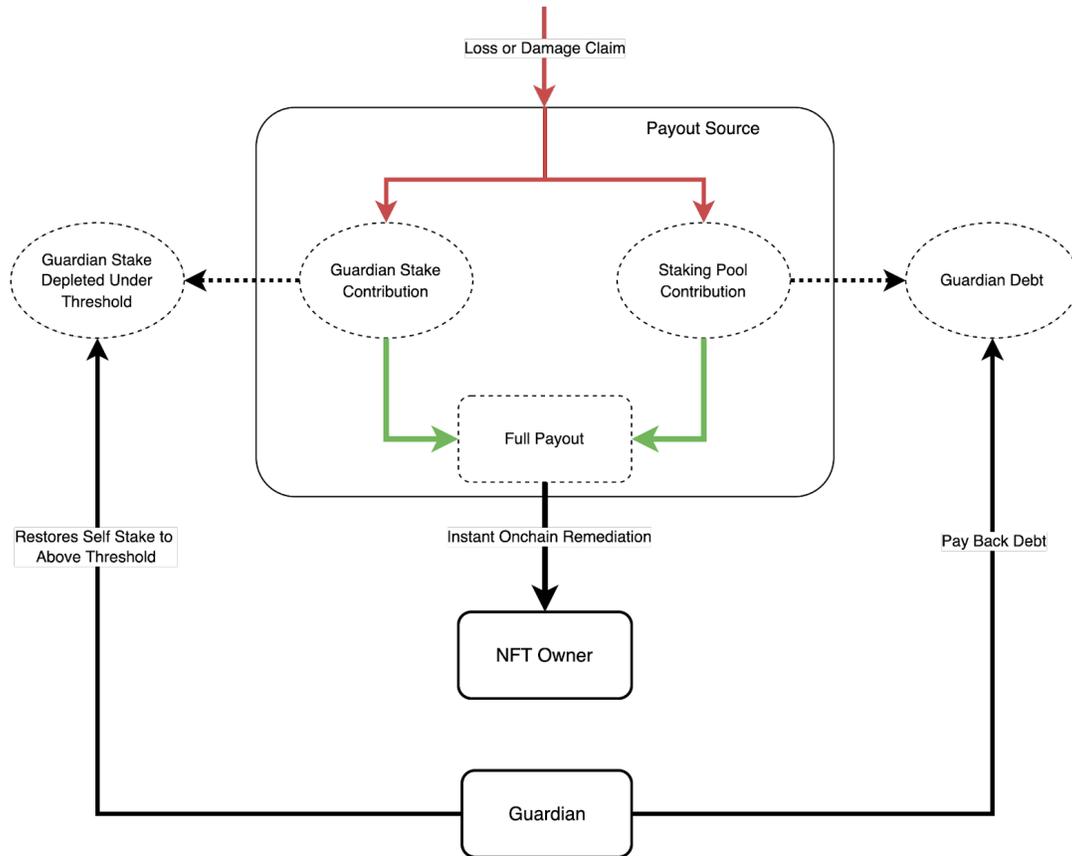


Figure 3: Loss or Damage Remediation

4.3.1 Staking and Locking

4K tokens are staked and locked in the staking pool in return for ve4K tokens. ve4K tokens are the sole unit by which protocol token emissions and protocol fees are distributed and governance power is determined.

The minimum locking period is 28 days and the maximum locking period is 4 years. A 4K token locked in the staking pool for 4 years will receive 1 ve4K token in return and shorter locking periods will receive fewer ve4K tokens.

veTokens are also how protocol fees - guardian fees, minting fees, redemption fees, etc - are distributed to token holders. A percentage of all protocol fees is awarded to veToken holders. This percentage is determined by protocol governance. In the long term, as 4K token emissions decrease, this percentage of protocol fees will become the primary way in which 4K stakers are rewarded.

The ve4K token system rewards stakers invested in the long-term success of the 4K protocol with both higher rewards and a more of a say in the direction of the protocol. The veToken system also plays an important function in locking capital as a temporary remediation mechanism in the event of losses or damages. This remediation mechanism is described in detail below.

4.3.2 Self-staking and Remediation

In addition to rewarding long-term stakers, the staking pool is also designed to act as an instant remediation and accountability mechanism in the event of a loss, damage, or process failure.

To participate in the protocol, guardians need to stake a minimum threshold of 4K tokens into their staking pool. The minimum requirement is determined by protocol governance. The guardian must continue to meet this staking requirement to participate as a guardian.

In the event of a process failure - incomplete or improperly completed audits, unprocessed redemptions, etc - penalties are levied fully against the guardian's self-stake.

In the event that the Enforcement DAO determines there is a damage or loss, temporary remediation for that damage or loss is taken partially from the guardian's self-stake and partially from the full staking pool. The percentage that comes from the guardian's stake - the *coverage ratio* - is set individually for each guardian by protocol governance according to the guardian's level of risk. This allows the protocol to control the aggregate risk taken on by the staking pool. Any remediation taken from the staking pool is temporary, and the guardian is required to repay remediation taken paid for by the broader staking pool. Protocol governance can also set a *risk cap* on the total amount that each guardian can be in debt to the broader staking pool at any given time. When the value of the total outstanding debt of a guardian exceeds the risk cap for that guardian, claims will not be paid out from the broader staking pool.

The intention of this design is to increase the total value of guaranteed on-chain payouts for losses and damages while also minimizing the risk taken on by stakers in the staking pool.

$$\text{Total coverage for a guardian} = \text{Value of the guardian's stake} \div \text{Guardian's coverage ratio} \quad (2)$$

Since the total on-chain coverage a guardian can offer is proportional to their self-stake, this system encourages guardians to increase their skin in the game. An example of how this would work in practice:

- An audit discovers there is a lost item and the Enforcement DAO determines the value of this lost item is \$1000. When the Enforcement DAO's decision is finalized, \$1000 will immediately be sent to the owner of the lost item.
- This \$1000 is sourced from both the guardian's self-stake and the total staking pool. Let's imagine that the protocol governance set the coverage ratio for this guardian at 40%. This means that \$400 in ve4K tokens will be taken from the guardian's self-stake and the remaining \$600 is taken from the larger staking pool. Since all guardians need to have a minimum self-staking threshold to operate on the network, the slashed guardian may need to increase their self stake to be in good standing in the network.
- The guardian would be required to pay back \$600 to the staking pool to be in good standing with the network and guardians that refuse to pay back will be penalized by the Enforcement DAO. This debt is on-chain and is a signal to the network of whether this node can be trusted. Guardians ultimately have 100% responsibility for covering damages and claims, and guardians will have their own off-chain coverage to cover losses from damages and claims.

If a guardian's self-stake is depleted (i.e. there's a catastrophic event), the guardian will no longer have access to the larger staking pool for reimbursing asset owners. However, if a guardian runs out of self-stake, they are still on the hook for reimbursing asset owners with outstanding claims. These debts are logged on-chain and ultimately need to be paid back into the staking pool by the guardian.

In other words, the larger staking pool acts as a temporary means to provide immediate remediation in the event that a guardian has many claims against it in a short amount of time. Guardians are ultimately fully responsible for covering losses and damages.

The purpose of this mechanism design is to ensure guardians have skin in the game, give asset owners who have a lost/damaged item the best user experience possible through instant remediation, and put the onus on the guardian for coordinating off-chain insurance.

4.3.3 Joining and Leaving the Protocol

Initially, joining the protocol will be determined by protocol governance. To join the protocol, a prospective guardian must have at least the minimum threshold of their own tokens staked to their staking pool.

The ultimate vision, however, is for joining the network as a validator to be a fully decentralized process. There will eventually be "community nodes" which have lower self-staking and process requirements but will not have access to the larger staking pool in the event of a loss or damage.

A guardian can be "jailed" when it is no longer acting in the best interest of the protocol. Jailed guardians have the following restrictions placed on them:

- Guardian fees and redemption fees will continue to accrue, but they cannot be collected by the guardian.
- The guardian's self-stake will not accrue inflation rewards while the guardian is jailed.
- The guardian cannot accept new assets.

A guardian can enter and leave jail in two ways:

1. The DAO can vote to jail guardians that are acting against the best interest of the protocol. The DAO can also vote to remove a guardian from jail.
2. Guardians will automatically be jailed if they no longer meet their minimum token staking threshold or if the guardian fails a certain threshold of reviews in a given time period. Both of these thresholds are set by protocol governance. Once a guardian meets these thresholds, they will be removed from jail.

4.3.4 Preventing malicious nodes

The staking pool mechanism is optimized for holding guardians accountable for lost and damaged assets, not necessarily to prevent malicious guardians from stealing the assets under their care. The only way to fully prevent malicious guardians from stealing assets under their care is to require them

to over-collateralize (i.e. self-staking more than the total value of the assets under management) and we believe this solution is unworkable.

The ultimate backstop to prevent a malicious guardian from running off with a guardian's assets is legal action taken by a DAO representative. Asset owners will need to decide whether they believe that a guardian resides in a jurisdiction with an acceptably reliable rule of law.

5 Interoperability

For 4K physically-backed tokens to gain mainstream adoption, they need the ability to be sent cross-chain with minimal effort. As blockchain ecosystems evolve, interoperability will become a necessary ingredient to any liquid protocol. In this section, we describe a phased approach to cross-chain interoperability for the 4K Protocol.

5.1 Phase I: Centralized Physically-Backed Token Bridging

4K physically-backed tokens have the claim rights to the underlying real-world assets they represent. This means that the community inherently trusts the protocol to store its underlying assets. Unlike traditional bridging of unbacked ERC20 tokens, this unique attribute allows for centralized bridging with little controversy. Initially, the 4K Foundation will bootstrap cross-chain interoperability by burning and minting the tokens in a centralized manner. A user can send the physically-backed tokens back to 4K on its source blockchain at any time and specify the desired target blockchain to be minted. 4K will then verify the authenticity and re-validate its custody status before burning the original token and minting the new token on the target blockchain. This process ensures that at any given time, only one instance of the token that represents the underlying asset exists on any blockchain. Essentially, 4K will operate like a centralized exchange that allows for multi-chain deposits and withdrawals. This solution does not require a custodian as all transaction metadata can be encoded in the transactions themselves on-chain via smart contracts. This phase would be the MVP for cross-chain 4K physically-backed token transfers.

5.2 Phase II: Decentralized Token Bridging

Many ERC20 bridges are being built across blockchains. Multi-party computing bridges such as the Multichain router [6] provide strong security guarantees, though, in their current state, they do not support NFT standards such as ERC1155. Harmony's Horizon [7] bridge allows for ERC1155 bridging but has little adoption. We believe that, in the near future, there will be many more NFT-compliant bridges built across various blockchains. 4K is not a bridging protocol and it is in 4K's best interest to partner with various bridges rather than building the bridges ourselves. As the technology matures, 4K will integrate with suitable decentralized bridges to enable decentralized NFT bridging. In this phase, 4K NFTs would be able to trustlessly bridge across blockchains. Novice users can still continue using the centralized bridging provided by 4K in phase 1.

5.3 Phase III: Cross-Chain NFT Marketplace

With decentralized bridging of 4K physically-backed tokens, liquidity would become fragmented. An NFT listed on one blockchain's marketplace can only attract liquidity from that one specific blockchain. This inhibits the NFT's price discovery. 4K plans to enable a cross-chain physically-backed token market through a multi-chain concurrent listing. An asset can be sold across various

blockchains at the same time. The 4K physically-backed token would then be minted on the buyer's target chain. For example, 4K could integrate with Chainlink's upcoming cross-chain interoperability protocol (CCIP) [8], which would serve as the messaging layer for required metadata passing. This feature is currently an R&D effort since CCIP is still in active development.

6 The 4K Token

The 4K governance token has multiple purposes across the protocol:

- **Governance and long-term incentive alignment:** 4K token holders can lock their 4K tokens in return for ve4K tokens which earn both more governance rights, emissions, and a cut of protocol fees. Longer locking periods result in more ve4K tokens. This aligns 4K token holders with the long-term interests of the protocol.
- **Accountability and remediation:** 4K tokens are how claims and penalties are paid by guardians.
- **Auctions:** Physically-backed tokens with a negative guardian fee balance are automatically auctioned in the open market.

Consequently, the 4K token also accrues value in multiple ways.

- **Fees:** All fees (guardian, minting, redemption, bridging, etc) are paid in stablecoin and into a 4K / stablecoin liquidity pool, which creates a sustainable source of demand for the 4K token.
- **Locking stakes:** The protocol incentivizes long locking periods for 4K tokens, which reduces the velocity of the token. Guardians are required to have a minimum threshold of locked 4K tokens to participate in the network. Long-term locking/staking incentives are sustainable because stakers receive a portion of protocol fees.
- **Paying penalties and claims:** All penalties and claims are paid out in 4K tokens, and guardians are required to pay back the value of all claims/penalties in 4K tokens.

7 Marketplace

To demonstrate the utility of the physically-backed tokens, 4K is building a marketplace for physically-backed tokens.

Exchanges on the marketplace are charged a 1% marketplace fee. This fee is split between the protocol treasury (80%) and the guardian storing the exchanged asset (20%).

In addition, owners of 4K collections can set royalty fees for their collections up to 10%. Royalty fees accrue to the original minter of the token.

This split is our current model though this model may change in the near future. Protocol governance can also change both the marketplace fee and how that fee is split.

8 Risk Mitigation Strategies

8.1 Summary

The 4K Protocol is designed to address the unique risks of operating in the physical world. The primary risk mitigation strategies include:

- **Guardians are required to stake tokens:** These staked tokens are slashed when guardians lose assets, damage assets, or fail to follow the standards of the protocol (e.g., timely redemptions and audits).
- **Assets held by guardians are routinely audited:** Each asset has a trail of audits from when it enters the care of a guardian to when it's finally redeemed. These audits allow the Enforcement DAO to determine whether a guardian was responsible for damaging or losing an asset.
- **Guardian performance data is publicly available on-chain:** Failed audits, lost or damaged inventory, and penalties from the Enforcement DAO are publicly viewable on-chain. This performance data will be a major factor in how asset owners choose which guardian to send their assets to and which guardians the Enforcement DAO allows to continue operating as a node in the network.
- **Guardians who aren't meeting the requirements of the network are temporarily "jailed":** While guardians are in jail, they will no longer receive inflationary rewards and their earned guardian fees will be withheld.
- **Legal action is the final recourse for grossly negligent or malicious behavior:** The protocol is designed to handle accountability on-chain and outside the legal system. However, in the event of grossly negligent or criminal behavior (e.g., stealing inventory), the guardian would be held responsible under the traditional legal system.

8.2 Strategies

Asset degrades over time while in the care of the guardian: The guardian is fully accountable for any unreasonable asset degradation in between initial receipt and handoff to the shipper. Damage claims are adjudicated through the on-chain review process.

A large number of assets are lost or damaged at once and a guardian's staking pool cannot cover losses: The staking pool is designed to provide instant remediation for infrequent losses and damages that may occur during the course of operations. However, in the event of large-scale losses or damages, the guardian's self-stake may be depleted before it can fully cover the claims levied by the Enforcement DAO. In this situation, the guardian would need to increase their self-stake again before the rest of the claims can be paid out. This means that some asset owners would not get paid out immediately after the Enforcement DAO creates their claim. Guardians will be expected (and in the early days of the protocol, required), to have off-chain coverage to cover these losses. Protocol governance controls the catastrophic risk that the staking pool takes on through the *coverage ratio* and *risk cap* parameters of each guardian. The total amount of unpaid claims is publicly visible on-chain and will be an important signal for determining whether a node is trustworthy. The Enforcement DAO can decide to jail guardians who fail to increase their self-stake in a timely manner.

Assets may be lost or damaged in transit to or from the guardian: Every asset is audited, at a minimum, at the time it enters the care of the guardian and at the time the asset is redeemed. Since there will be photo documentation of every asset across the full lifecycle with the guardian, there is a high degree of certainty as to whether damage or loss occurred with the guardian or in transit. Asset owners are responsible for coordinating transit to and from the guardian. Asset owners assume the full risk for losses or damages in transit so we recommend for asset owners to pay for shipping insurance.

A guardian may claim they never received an asset when they actually did receive the asset: When shipping, the guardian's signature is required when assets are initially delivered to the guardian and the asset owner's signature is required when assets are redeemed.

Guardian refuses to redeem the token, goes bankrupt, or steals the physical asset: Under U.S. law, a physically-backed token is considered a warehousing receipt. The guardian is legally responsible for bankruptcy or theft according to existing case law for warehousing receipts. The incentives baked into the 4K Protocol offer a layer of protection in addition to the local court system.

Guardian pretends they have inventory that they don't have: A guardian could attempt to game the audit system by reusing a single physical asset during audits for multiple tokens. Though we can't fully eliminate this risk, under the proposed system, this scheme would be exceedingly difficult and against the interests of the guardian. Every asset is audited when it enters and leaves the care of the guardian. Each audit includes photographic proof of the asset along with the asset's unique identifier physically attached to the asset. This identifier attached to the asset can have varying levels of security (e.g. RFID, tamper-evident seals, diamond-dust identifiers). Guardians compete with each other to offer robust unique identifiers that are not prone to tampering, hacks, or cloning. Guardians who are suspected of systematic manipulation may be required, at the discretion of the Enforcement DAO, to cover the expense of in-person audits.

Guardian doesn't process an audit or redemption or doesn't do so in a timely manner: Each guardian sets their own on-chain SLAs for each guardian class on how long audits and redemptions will take to be completed. For each day that a guardian is late, 4K tokens are automatically slashed from the guardian's self-stake. This penalty is set by protocol governance.

An audit is not done in a timely manner or at all: This risk is mitigated in two ways. First, guardians set SLAs for each guardian class on how long audits and redemptions will take to be complete. The guardian's staking pool will automatically be charged a penalty for each day that the requested audit has been completed. Second, if an asset is being reviewed as a suspected loss, the Enforcement DAO will interpret the absence of proof (i.e. failure to produce an audit) as proof of absence (i.e. the asset is lost).

A guardian may not properly perform the audit: If a guardian does not properly perform an audit (e.g., the photograph is blurry, a unique identifier is not placed on the asset, a recent block hash is not in the photograph) it is more difficult to know if and when a guardian damaged or lost an asset. This risk is mitigated by allowing anyone to initiate an Enforcement DAO review of an audit. If the Enforcement DAO finds the audit has not been properly conducted, a penalty will automatically be charged to the guardian's staking pool. This penalty is set by protocol governance. If an asset is put up for review for the Enforcement DAO and the audit trail contains improperly performed audits, the Enforcement DAO will err on the side of ruling in favor of the asset owner.

Asset owners could collude to overwhelm the guardian with audit requests that cannot be filled: The cost of an audit will be set by protocol governance such that an attack to overwhelm a guardian would be cost-prohibitive. Protocol governance can also set limits on the frequency of audit requests.

An asset owner may send in inauthentic assets: In the early days of the 4K Protocol, the 4K marketplace will take steps to verify the authenticity of any assets submitted claiming to be authentic. In the future, we will build the *authentication protocol*, a decentralized way to verify the authenticity of a physical asset.

Asset owner sends the wrong asset to a guardian or misrepresents information about the submitted asset: If an asset owner intentionally or unintentionally sends the wrong asset to a guardian, the metadata for that physically-backed token will not match the asset that's actually being held by the guardian. However, since all assets are audited when they are initially inventoried by the guardian, there will always be photo documentation of the actual asset being held by the guardian. It would be obvious if the asset held by the guardian doesn't match the metadata of the physically-backed token.

Guardian commits on-chain fraud: A guardian could send an asset to themselves, intentionally lose the asset, and collect the on-chain remediation payment. This scheme would be short-sighted. Records of lost and damaged assets are publicly available on-chain, and high loss and damage rates would ruin the guardian's reputation. Guardians who lose too many assets will be automatically jailed, in which case they stop receiving inflationary rewards.

There may be frontend vulnerabilities: 4K will create a front-end for guardians and asset owners to manage their inventory. Frontend vulnerabilities could compromise the assets of guardians and asset owners. 4K will mitigate this risk by open-sourcing its frontend products and creating bug bounties.

Centralized hosting of data: 4K will create frontend products for asset owners and guardians that will be hosted on traditional web servers. In addition, some data (e.g., photos from audits) may be stored off-chain. Using a traditional web hosting service increases the risk of outages and criticism from the community of 4K being too centralized. 4K will mitigate this risk by storing data on-chain as much as possible and heavily investing in the resiliency of our traditionally hosted web products. 4K continuously evaluates its web3 technology stack and, when possible, will move from centralized technologies to decentralized technologies (Arweave, Filecoin, Akash, ENS/HNS, etc).

9 The DAO

4K's will progressively decentralize, starting by moving governance to a DAO. We will detail DAO governance architecture at a later date, but will likely use a framework like Aragon [9] or Kleros [10].

The DAO will initially have two core committees:

- **Enforcement:** Acts as the court system for determining losses, damages, process failures, and malicious behavior.

- **Economics:** Proposes upgrades and changes in the economic structure of the protocol.

10 Future work

10.1 Authentication Protocol

The current design of the physical guardian protocol is optimized to give certainty on whether a physically-backed token is truly backed by the corresponding physical asset. However, it's possible that the original asset owner who minted the physically-backed token could have misrepresented the attributes of that token (e.g., claiming a cheap clone of a watch is an authentic watch).

In the early days of the protocol, the 4K Protocol governance may help users distinguish trusted assets by 1) denoting whether the physically-backed token was minted by a trusted party (e.g., directly from the brand itself) and 2) performing additional authenticity checks on assets as they are received by guardians. However, we ultimately want authentication to be a decentralized process managed by the *authentication protocol*.

The goal of the authentication protocol is to give users the information they need to determine the likelihood that an asset is authentic. The authentication protocol will coordinate a network of *authenticators* to determine whether an asset is actually what the original minter represented it to be. This determination is recorded in an on-chain *authentication*. An authentication is simply an on-chain record from an authenticator with a determination of an asset's authenticity. Assets can be authenticated an arbitrary number of times. Authentications allow the community to come to a consensus that an asset is what its metadata claims to be.

A possible implementation of the authentication protocol could be:

- 4K Protocol governance votes who can be an authenticator. For an authenticator to participate in the 4K Protocol, they must stake a minimum threshold of 4K tokens.
- Asset owners can request an in-person or remote authentication to be completed by an authenticator. Authenticators earn a fee for each authentication they process. The amount of the fee is determined by each authenticator individually. The authentication can be completed before or after the asset enters the care of the guardian. If an authenticator accepts the request, they create an on-chain authentication record with their determination of that asset's authenticity.
- If the Enforcement DAO suspects that authenticators are deliberately creating false authentications, the authenticator will have their staked tokens slashed and/or will be kicked out of the protocol.

10.2 Valuation Protocol

The ability to reliably value physically-backed tokens is important for both facilitating transactions and for using these NFTs as collateral in decentralized finance.

The valuation protocol will likely consist of the following parties:

Physical Asset Pricing Oracles: Collect data on various websites and manually update the estimated pricing of assets on a time interval basis.

On-chain Appraisers: Professionals or anyone the community designates as a credible appraiser for specific classes. On-chain appraisals will have a similar design to the authentication protocol. Each on-chain appraisal allows the community to come to a consensus on the value of an asset.

10.3 Advanced Enforcement DAO

Under the current design, guardians are held accountable through a review process. For a fee, anyone can initiate a review, which is completed by the Enforcement DAO.

There are limitations with using the Enforcement DAO as the primary mechanism for completing reviews. First, it may be difficult for the Enforcement DAO to scale their reviews as adoption of the 4K Protocol grows. Second, since review determinations are made by a limited set of individuals in the Enforcement DAO, these individuals could produce false determinations.

In the future, we will create a fully decentralized mechanism for reviewing audits. A potential implementation could work as follows:

- Reviews are judged by a decentralized panel of *judges*. The protocol randomly selects which judges will be on the panel of any given review. Judges are paid in 4K tokens.
- Anyone can become a *judge* by staking 4K tokens. The 4K Protocol publishes clear criteria for how judges are to adjudicate different situations (e.g., damaged assets or audits that were not done correctly).
- During a panel’s review, each judge submits their vote for the outcome of the review. The outcome of the review is determined by the majority vote. Judges can only get paid for the review if their vote conforms to the majority vote. The judge’s staked 4K tokens are slashed if their vote doesn’t conform to the majority vote. There would be mechanisms in place to prevent collusion between judges.
- There would still be an Enforcement DAO, but the DAO would no longer be responsible for adjudicating user-initiated reviews. Instead, the Enforcement DAO would be responsible for investigating and levying penalties when the guardians or judges are suspected of gaming the protocol.

11 Tokenomics

Seed	10.00%
Private	8.00%
Strategic	2.50%
Public	5.00%
Team and Advisors	19.5%
Ecosystem, Foundation and Liquidity Incentives	55.00%

Table 1: Initial Token Distribution

Ecosystem, foundation, and liquidity incentives are incentives to both users and dApps to bring items onto the 4K protocol. ve4K token holders can vote to apply liquidity incentives to specific asset classes (e.g. watches, sneakers, trading cards, art, etc).

Newly released tokens will be distributed to a combination of staking rewards (40%), team vesting (10%), and Ecosystem, Foundation, and Liquidity (50%).

The genesis supply will be 4 BN tokens and the total supply at year 20 will be 10 BN tokens.

Y1	30%	Y11	4%
Y2	25%	Y12	3%
Y3	20%	Y13	2%
Y4	15%	Y14	1%
Y5	10%	Y15	1%
Y6	9%	Y16	1%
Y7	8%	Y17	1%
Y8	7%	Y18	1%
Y9	6%	Y19	1%
Y10	5%	Y20	0%

Table 2: 4K Token Inflation Schedule

4K uses a veTokenomics design that is inspired by and similar to Curve. veTokens are locked for up to 4 years, and longer locking periods increase a user’s voting power, share of protocol fees, and share of inflationary rewards. veTokens are non-transferrable and decay linearly. veToken stakers can unlock their tokens with a 50% penalty.

12 Roadmap

1. **Build a physically-backed token ecosystem:** Our immediate focus is enabling new use cases for physically-backed tokens across the EVM ecosystem.
2. **Create core protocol on Ethereum:** We will build our token, staking pools, and governance on Ethereum.
3. **Create Tendermint-Based Layer 1 chain on Cosmos:** Given our highly unique use case, we will eventually build our own Tendermint L1 on Cosmos to give us stronger flexibility, performance, and sovereignty.

References

- [1] Fernando Martinelli and Nikolai Mushegian. *Balancer Whitepaper: A non-custodial portfolio manager, liquidity provider, and price sensor*. 2019.
- [2] The Maker Team. “The Dai Stablecoin System”. In: (2017). URL: <https://makerdao.com/en/whitepaper/sai>.

- [3] Dust Identity Inc. *Dust Identity*. 2022. URL: <https://dustidentity.com/>.
- [4] Curve.fi. *Curve Documentation*. Version 1.0.0. 2022. URL: https://curve.readthedocs.io/_/downloads/en/latest/pdf/.
- [5] Jae Kwon and Ethan Buchman. *Cosmos Whitepaper*. 2022. URL: <https://v1.cosmos.network/resources/whitepaper>.
- [6] Multichain. *Multichain Documentation*. 2022. URL: <https://docs.multichain.org/>.
- [7] Rongjian Lan et al. *Horizon: A Gas-Efficient Trustless Bridge for Cross-Chain Transactions*. 2020.
- [8] Chainlink. *Introducing the Cross-Chain Interoperability Protocol (CCIP) for Decentralized Inter-Chain Messaging and Token Movements*. 2021. URL: <https://blog.chain.link/introducing-the-cross-chain-interoperability-protocol-ccip/>.
- [9] Luis Cuende and Jorge Izquierdo. *Aragon Network: A Decentralized Infrastructure for Value Exchange*. Version 1.1. 2017.
- [10] Clement Lesaege, Federico Ast, and William George. *Kleros White Paper*. Version 1.0.7. 2019.