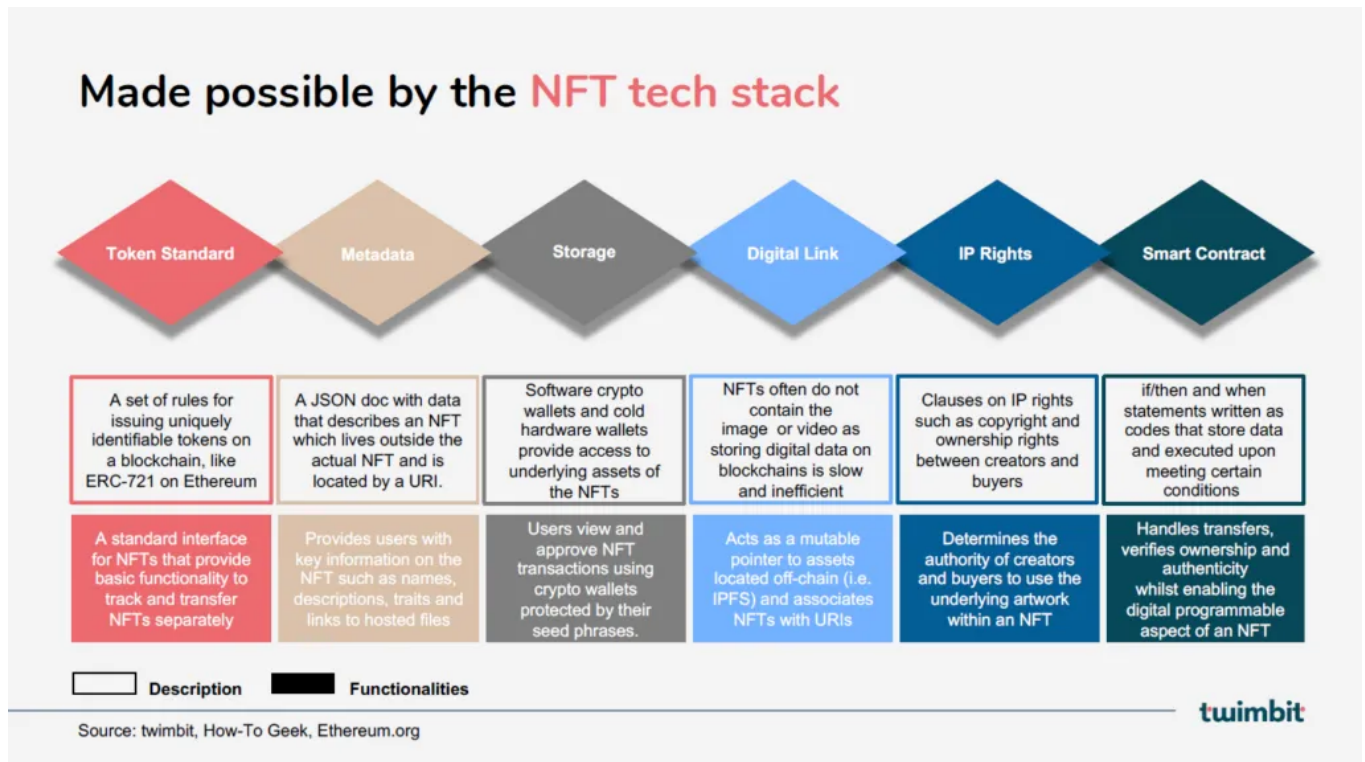


ML-driven Dynamic Pricing for New Metaverse Products

NFT Architecture



Insurance coverage for NFTs

- **Damage Insurance**
Provides coverage for damages caused by intervention on the blockchain,
- **Crime Insurance**
Provides coverage against crime such as theft or damage to property, or for fraudulent activities such as a third party placing a fake product in the NFT marketplaces.
- **Financial Risk Insurance**
Provides coverage for the value of NFT with respect to underlying blockchain currency or fiat currency.

Substitutes

- [Coincover](#)
Instead of calculating risks, they reduce risks by [Cryptocurrency Theft Protection](#) and [Disaster Recovery](#) technologies.
 - [IMA Financial Web3Labs in Decentraland](#)
 - [HARTi and Mitsui Sumitomo](#)
Marketplace Insurance
 - [Evertas](#)
-

Premium Prediction Model

[How to Calculate Insurance Premiums](#)

For a real world insurance ML model, [Boosting insights in insurance tariff plans with tree-based machine learning methods](#).

[Paper](#) | [Github](#) | [Slides](#) | [Presentation](#)

Calculating premium rates

A P&C insurance company is interested in the total loss amount L per unit of exposure-to risk e , where L is the total loss for the N claims reported by a policyholder during the exposure period e . P&C insurers usually opt for a so-called frequency-severity strategy to price a contract Claim frequency F is the number of claims N filed per unit of exposure-to-risk e . Claim severity S refers to the cost per claim and is defined by the average amount per claim filed, that is the total loss amount L divided by the number of claims N . The technical price π (or: pure/risk premium) then follows as:

$$\pi = \mathbb{E} \left(\frac{L}{e} \right) \stackrel{\text{indep.}}{=} \mathbb{E} \left(\frac{N}{e} \right) \times \mathbb{E} \left(\frac{L}{N} \mid N > 0 \right) = \mathbb{E}(F) \times \mathbb{E}(S)$$

assuming independence between the frequency and the severity component of the premium.

For an NFT insurance, N (No. of claims) = 0/1 only in the given year

And S (Claim severity) = $\min(x\% \text{ of NFT price as declared in policy, Maximum insured amount})$

Thus, L (Total loss amount) = $0/S$

$\therefore \pi$ (pure/risk premium) = $E(\text{claim is made in a given year}) \times \text{Insured NFT price}$

$E(\text{claim is made in a given year}) = P(\text{claim is made in a given year})$ since $\text{maxClaim} = 1$

Calculating claim probability

This should be between 0.8 to 1.2 . [Chandra mohan sir said this.]

Depending upon insurance coverage i.e. claims can be made due to whichever reasons,

$P(\text{claim is made in a given year}) = P(\text{NFT loss}) + P(\text{NFT theft})$

Risks associated with NFTs

- **NFT Valuation** [Use either dynamic pricing or valuation as a risk] #FinancialRisk💰
Valuation risk can be both due to drop in nft demand because of decline in popularity of related games or deflation of blockchain currency with respect to fiat currency.
- **Metadata & TokenUri integrity and availability** #DamageRisk🔨
Developers can change the metadata at any time, meaning there's a chance that your NFT will look different than when you bought it.
If the original hosting solution shuts down or is compromised, your digital assets are likely at risk of disappearing.

How to evaluate?

Data on chain is both tamper proof and permanently available than a decentralised solution (ipfs) or a centralised web server.

[OnChain/ IPFS/ Centralised web server]

In decreasing order of trustworthiness ->

- **Smart Contract Security** #CrimeRisk😈
Developer risks and possible human errors that may result in malicious or even vulnerable smart contracts that are targets for hackers.

How to evaluate?

Community tested standards more hack proof

[No token standard/ ERC721/ ERC998/ ERC1155]

- **Private Key theft** #CrimeRisk😈
Theft of private keys through cyberattacks, phishing, malware, and device theft

How to evaluate?

- Cold wallets difficult to hack and prevents private key theft
[Hot/ Cold]

- Wallet Security Score
Based on [Cryptocurrency Software Wallet Methodology](#) and reviews from [Cryptocurrency Wallets](#)

- Account Access Method
- Transaction Authorization Method
- Recovery Method
- Reputation
- Hierarchical Deterministic
- Open Source Code

- **Ecosystem security** #CrimeRisk 🐱

//...

How to evaluate?

Scores from [CertiK](#)

- Level-1 Blockchain Security
[Ethereum/ Polygon/ Binance Smart Chain/ ...]
- Metaverse
[Sandbox/ Decentraland/ ...]

- **Policyholder itself** #DamageRisk 🛠️ #CrimeRisk 🐱

Policyholders can fall prey to phishing attacks or lose private keys.

How to evaluate?

- Age
- Blockchain/ NFT Tech literacy
- [CreditWorthiness](#)

- **IP Rights ...Are they insured?**

Sources

- Extract from [Are NFTs insurable?](#)

NFTs are one-of-a-kind digital assets. As with cryptocurrencies, NFTs are stored in a blockchain. While anyone can explore the blockchain record to view the underlying asset only the holder of the NFT has the "private key" that verifies ownership. Therefore the holder of the NFT is recorded as the owner of the underlying asset unless the NFT is transferred to another person's digital wallet. Once an NFT transaction is made and assigned to a different private key, there is no way anyone can reverse the transaction: *"Not your private keys, not your NFTs"*.

Therein lies one of the main risks of NFTs. Owning an NFT requires a digital wallet that

contains "private keys" to transact on the blockchain. If you lose access to the digital wallet by forgetting passwords, damaging devices or due to getting hacked, NFTs from your digital wallet can be lost. Just recently users of the NFT marketplace "Nifty Gateway" [claimed that their entire NFT collection was "stolen"](#).

Another risk of NFTs is that they usually contain a link to the storage location of the underlying asset. If that link is broken or the company storing the asset goes out of business the owner of the NFT could be left with links to assets or files that no longer exist. Similar risks arise if a digital marketplace, storage wallet provider or a server farm involved in a NFT transaction suffer bankruptcy or service interruptions that damage the digital files. Further risks associated with NFTs include whether the seller had the necessary intellectual property rights associated with the digital asset. What happens if the creator or seller of the underlying asset fails to secure or verify necessary trademark or copyrights?

- Extract from [Developments in NFT Insurance | Ingram Yuzek Gainen Carroll & Bertolotti, LLP - JDSupra](#)

However, despite the similarity, a specie insurance for NFT(s) would still require a precise description for the core "risks" (which are the events where the insured are entitled to receive insurance proceeds from the insurer), and such description might not be easy to draft due to the nature of blockchain and the way NFTs are transacted. For instance, when defining the loss of a NFT, the insurer will not only consider what constitutes an event of loss but whether the assumption of the occurrence of such event is justified. On the one hand, an insurer might find it reasonable to assume the risk that a NFT might be stolen by a hacker without negligence on the side of the NFT holder and/or custodian, but, on the other hand, the same insurer might not find it reasonable to assume the risk of loss that occurs as a result of the underlying blockchain's forking event, because the chance of loss from such event might be incalculable and would affect a significant amount of NFTs based on that blockchain.

Another example is that an insurer might be willing to insure a NFT holder against certain events where the NFT becomes inaccessible, such as the loss of the holder's private key or the malfunction of the holder's cold wallet, as that risk and the likelihood of such events are more manageable and determinable. However, the same insurer might not be willing to assume the risk of such inaccessibility when a NFT is held by a DAO that lacks comprehensive rules and/or voting mechanisms governing the access to or transfer of the NFT. In short, an insurer's ability and willingness to provide insurance coverage might vary even if the outcome of the risk is the same, and it thus becomes important to keep an eye on how an insurer would phrase certain risks in its NFT insurance policy in response to the nature and the unique elements of blockchain and tokens.

- [NFT Insurance Is Coming, but Is There an Industry to Support It?](#)
- [An Emerging Sector: NFT Insurance - Lexology](#)
- [NFT Insurance: Understanding the Challenges and Solutions](#)
- [As NFT Scams Grow In Number, NFT Insurance Hits The Market](#)

- [Covering the Highlight Reel: The Need for Insurance Options to Protect NFT Owners | Pillsbury - Policyholder Pulse blog - JDSupra](#)
 - [Non-Fungible Tokens and Cyber Insurance](#)
 - [Security risks in the NFT ecosystem](#)
-

Calculating Insured NFT price

Same as Insured Declared Value

Insured NFT Price can be c% of

- Price at which NFT bought by insurer
- **Predicted price of NFT at the time of insurance <- working on this**
- Predicted price of NFT at the time of claim
- Adjusting for on-chain currency... i.e. insurance based on

How to calculate the current price of an NFT?

Sources

- **Upshot NFT Appraisal blog collection**
 - [How Real-Time NFT Pricing Can Increase NFT Adoption](#)

While models for predicting prices of liquid financial assets like stocks and cryptocurrencies often rely on **historical price trends**, such approaches may only partially help in the less liquid world of NFTs. **NFT characteristics or metadata (tags and labels which describe the features of an NFT and its creator)** are a valuable source of information.

Transformations of historical sales data based on these features give more dense and informative datasets than simply relying on an individual NFT's price trend alone. Our algorithms take these characteristics as inputs and can automatically identify and pool information from past sales of similar NFTs, helping resolve the issue of illiquidity.

We train machine learning models that are able to predict transaction prices based on variables constructed from NFT metadata and **proxies for the state of the**

market at different levels of granularity (Ethereum > NFT market > specific NFT project, etc.).

We validate the predictions by examining their accuracy on data not used in the training process and obtain error bounds by comparing our predictions to realized sale prices. Both the **predicted pricing and error bounds** provide useful information to NFT buyers, sellers, or developers building products on top of the NFT economy.


Our approach to valuation is similar to how art or real estate valuation works at a high level, although these traditional markets usually rely on simpler linear models with a known set of predictor variables, established from decades of research and observation. In contrast, the variables that determine NFT prices are not yet well understood.

- [Taking NFT Pricing to the Next Level with Machine Learning](#)
- [Determining What Matters for NFT Valuation](#)
- [Explaining NFT Pricing with Machine Learning](#)
- **Nansen Articles**
 - [NFT Index Methodology | Nansen](#)
 - [NFT Price Estimates Machine Learning Model | Nansen](#)
- [Here's Machine Learning for NFTs: DeepNFTValue | HackerNoon](#)

Research paper

- [\[2204.12932\] NFT Appraisal Prediction: Utilizing Search Trends, Public Market Data, Linear Regression and Recurrent Neural Networks](#)
- [Multimodal Learning for Improved NFT Price Prediction](#)
- [Prediction and interpretation of daily NFT and DeFi prices dynamics: Inspection through ensemble machine learning & XAI](#)
- [\(PDF\) Analysis of Non-Fungible Token Pricing Factors with Machine Learning](#)
- [Predictors of NFT Prices: An Automated Machine Learning Approach](#)
- [Mapping the NFT revolution: market trends, trade networks and...](#)
- [\(PDF\) PREDICTION WITH MACHINE LEARNING AND COMPARISON OF LAND PRICES IN THE METAVERSE UNIVERSE](#)
- [TweetBoost: Influence of Social Media on NFT Valuation](#)

Data

- Data crawled from
 - [Market Tracker | NFT Sales History & Trends | NonFungible.com](#)
 - [CryptoSlam](#)
- [NFT API Quickstart](#)
- [Worldwide NFT heists tracker - Comparitech](#)
 NFT Thefts Sources
- [Worldwide crypto & NFT rug pulls and scams tracker - Comparitech](#)
- [The Biggest Cryptocurrency Heists of All Time | Comparitech](#)

Colabs

- Non- fungible NFT sales data collection
<https://colab.research.google.com/drive/1WILQAYEL5eiSpe-4kFPdCGMIAP8Edf1K>
- Non- fungible NFT price prediction
https://colab.research.google.com/drive/1HUeDEE_PjwyQA9tptJk-cCu2Jw-8gJuk
- Cryptoslam NFT sales data collection and price prediction
<https://colab.research.google.com/drive/1AEpFPyx3iveQomB2GymQiq2w9WRyFWH1>