NFT 圣经

你需要了解的 NFT 的所有知识

目录

1.什么是非同质化代币？

非同质化的资产是常见的资产。同质化的资产才是奇怪的资产！

大多数关于非同质化代币的讨论都始于从介绍被定义为能够取代或者能被另一相同物品代替”的同质性概念。我们认为这使事情变得过于复杂。为了更好地理解什么可能构成非同质化资产，只需要想想你拥有的大多数东西。你坐着的椅子，你的手机，你的笔记本电脑，任何你可以去 eBay 上出售的东西。所有这些物品都属于非同质化物品的范畴。

事实证明，同质化资产其实才是奇怪的。货币就是一个典型的同质化资产的例子。五美元永远是五美元，不管这五美金纸币上具体的序号是多少，也不管这五美元是否在你的银行账户里。能够用另一张五美元的钞票（或五张一美金钞票）替换五美元的钞票，这就是货币同质化的原因。

请注意，同质性是相对的，它实际上只适用于用来对比多种事物的时候。可参考商务舱、经济舱和头等舱机票的情况。每张机票在其等级内大致都是可互换的，但你无法公平地用头等舱的机票换成商务舱机票。就连你坐的椅子也大致可以和同型号的椅子互换，除非你对自己的特定椅子产生了特殊的感情。

有趣的是，可互换性也可以是主观的。回到机票的例子：一个在意坐在靠窗座位或者靠过道座位的人，可能不会认为两张经济舱的机票可以互换。同样的，一枚稀有的一分钱对我来说可能只值 1 分钱，但对钱币收藏者来说却价值不菲。我们将看到，当在区块链上表示这些物品时，即使是一些细微的差别变得很重要。

1.1. 基于区块链的非同质化代币

就像在加密货币出现之前，我们就有了数字货币（例如航空积分、游戏内货币）一样，从互联网诞生之初，我们就有了非同质化数字资产。域名、活动门票、游戏内物品，甚至是在 Twitter 或 Facebook 等社交网络上拥有的昵称，都是不可互换的数字资产，只是它们的可交易性、流动性和互操作性有所不同。而它们其中很多都是非常有价值的。Epic Games 仅在 2018年就在其免费游戏《Fortnite》中靠销售游戏内的服饰获得了24亿美元的收入，预计2025年活动门票市场将达到680亿美元，而域名市场也将继续保持稳定的增长。

我们有大量的数字资产，但我们从未真正拥有过它们。

显而易见，我们已经拥有了大量的数字资产。但是我们在多大程度上 "拥有 "它们呢？如果数字领域内的所有权只意味着一件物品属于你而不是别人，那么你在某种意义上拥有它们。但如果数字所有权更像是物理世界中的所有权（有可以无限期持有和转让的自由），对数字资产来说似乎并不总是如此。相反，如果你在特定的情境中拥有这些资产，也许你并不能或者不能轻易地转移它们。当尝试在 eBay 上出售一款 Fortnite 皮肤，你就会感受到将数字资产从一个人转移给另一个人的困难。

这就是区块链诞生的原因! 区块链为数字资产提供了一个协调层，赋予用户所有权和管理权限。它为非同质化资产增加了一些独特的属性，从而改变了用户和开发者与这些资产的关系。

1.1.1. 标准化

传统的数字资产--从活动门票到域名，在数字领域内并没有统一的表示方式。游戏很可能使用与活动票务系统完全不同的方式来表示其游戏内的收藏品。通过在公共区块链上表示非同质化代币，开发者们可以建立与所有非同质化代币相关的通用、可重复利用的、可继承的标准。这些标准包含了所有权、转让和简单的访问控制等基本原语。额外的标准（例如，如何展示 NFT）可在上方分层以便更好地在应用程序内展示出来。

这些标准类似于数字领域的其他构件，例如用于图像的 JPEG 或 PNG 文件格式，用于计算机之间请求的 HTTP，以及用于在网页上显示内容的 HTML / CSS。区块链在上面增加了分层，为开发者提供了一套全新的有状态原语，可用于在此基础上构建应用程序。

1.1.2. 互通性

非同质化代币标准允许非同质化代币在多个生态系统中轻松转移。当一个开发者推出一个新 NFT 项目时，这些 NFT 可以立即在很多不同的钱包提供商内部被看到，可以在市场上交易的，而且最近 NFT 还可以在虚拟世界的内部展示出来。之这之所以可行，是因为开放标准提供了一个清晰、一致、可靠、有权限的 API 来读写数据。

1.1.3. 可交易性

互通性带来的最引人注目的功能是在开放市场上可进行自由贸易。这是用户第一次可以将物品移出原有场景然后进入市场，在市场内用户可以利用复杂的交易功能，例如 eBay式的拍卖、竞价、捆绑销售，以及可以出售如稳定币和特定应用货币的任何货币的能力。

具体到游戏开发者来说，资产的可交易性代表着从封闭经济到开放自由市场经济的转变。游戏开发者不再需要管理他们经济的每一个环节 :从资源的供应到定价，再到资本控制。取而代之的是，他们可以让自由市场来完成繁重的工作!

1.1.4. 流动性

非同质化代币的即时交易性将引领更高的流动性。NFT 市场可以满足到各种受众的需求--从核心交易者到更多的新手玩家--允许资产更大的曝光给更广泛的买家池。就像 2017 年的 ICO 热潮催生了由即时流动性代币驱动的新资产类别一样，NFT扩大了独特数字资产的市场。

1.1.5. 不可变性和可证明的稀缺性

智能合约允许开发者对非同质化代币的供应设置硬性上限，并且强制执行 NFT 发行后不可被修改的长久属性。例如，一个开发者可以通过编程强制执行一件特定稀有的物品只能被创建出特定的数量，并同时保持更常见物品的供应量是无穷的。开发者也可以通过在链上编码的方式来强制执行特定的属性不随时间而改变。这对于艺术来说特别有趣，因为艺术在很大程度上依赖于原创作品的可证明的稀缺性。

1.1.6. 可编程性

当然，和传统的数字资产一样，NFT 也是完全可编程的。CryptoKitties（我们后面会讲到）直接在代表加密猫的合约中内置了繁殖机制。如今很多 NFT 都有更复杂的机制，例如锻造、制作、兑换、随机生成等。其中的设计空间充满了可能性。

2.非同质化代币标准

标准是使非同质化代币变得强大的部分原因。它们给开发者提供了资产将以特定方式表现的保证，并且准确描述了如何与资产的基本功能进行交互。

2.1. ERC721

由 CryptoKitties 开创的，ERC721 是第一个表示非同质化数字资产的标准。ERC721 是一个可继承的 Solidity 智能合约标准，这意味着开发人员可以通过 从 OpenZeppelin 库中导入它来容易地创建新的符合 ERC721 标准的合约（我们在这里有一个很有用的关于创建第一个 ERC721 合约的教程）。ERC721 实

际上较为简单：它提供了一个独特标识符号（每个标识符号代表一个资产）到地址的映射，地址代表该标识符号的所有者。ERC721 还提供了一种被许可的方式来转移这些资产，使用 transferFrom 方法。

```
interface ERC721 {
  function ownerOf(uint256 _tokenId) external view returns (address);
  function transferFrom(address _from, address _to, uint256 _tokenId) external payable;
}
```

如果你思考一下，这两种方法就是你所需用来表示 NFT 的全部：一种检查谁拥有什么的方法和一种转移物品的方法。该标准还有一些其他的花哨功能（其中一些对 NFT 市场非常重要），但 ERC721 的核心是相当基础的。

2.2.ERC1155

ERC1155，由 Enjin 团队首创，将半同质化的理念带入 NFT 世界。通过 ERC1155，ID 代表的不是单一资产，而是资产的类别。例如，一个 ID 可能代表 "剑"，而一个钱包可以拥有 1000 把这样的剑。在这种情况下，balanceOf 方法将返回钱包所拥有的剑的数量，而用户可以通过使用 "剑 "ID 调用 transferFrom 来转移任何数量的剑。

```
interface ERC1155 {
    function balanceOf(address _owner, uint256 _id) external view returns (address);
    function transferFrom(address _from, address _to, uint256 _id, uint256 quantity) external payable;
```

```
}
```

这类系统的优势之一是效率：使用 ERC721，如果用户想转让 1000 把剑，需要修改智能合约的状态（通过调用 transferFrom 方法），以获得 1000 个独特的代币。使用 ERC1155，开发者只需要调用数量为 1000 的 transferFrom，并执行一次转移操作。当然，这增加了效率，但同时也带来了信息的损失：我们无法再追踪单个剑的历史。

还要注意的是，ERC1155 提供了 ERC721 功能的超集，意味着一个 ERC721 资产可以用ERC1155来构建(你只需要为每个资产准备不同的ID且数量为1)。由于这些优势，我们最近见证了越来越多的人采用 ERC1155 标准。OpenSea 最近在 Github 上开发了一个资源库，用于开始使用 ERC1155 标准。

剖析 ERC20、ERC721 和 ERC1155 标准。ERC20 将地址映射为金额，ERC721 将唯一的 ID 映射为所有者，ERC1155 则将 ID 与所有者和金额进行嵌套映射。

2.2.1.可组合性资产

以 ERC-998 标准引导的可组合资产，提供了一个 NFT 可以拥有非同质化资产和同质化资产的模板。目前只有几个可组合的 NFT 在主网络上，但我们认为有令人难以置信的机会将它们投入使用！

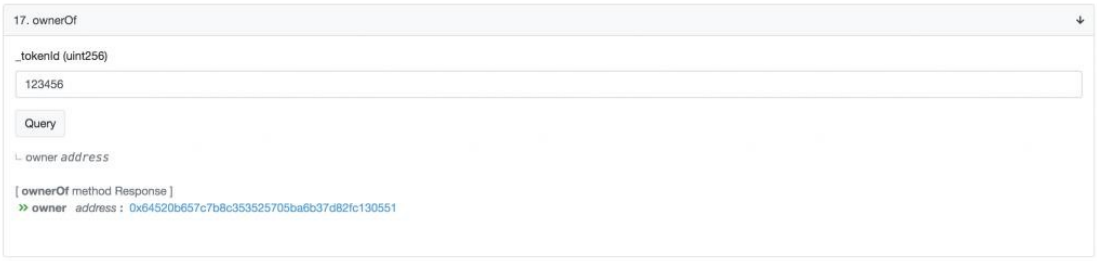
> ...一只 cryptokitty 可能拥有一个猫抓板和一个喂食用的盘子;盘子里可能有一定数量的同质化"chow "代币。如果我卖掉这只加密宠物，那么我就卖掉了这只 cryptokitty 所拥有的全部物品。

2.3.非 Ethereum 标准

虽然 Ethereum 是最热门的 NFT 所在公链，但还有其他的一些 NFT 标准正在出现在其他的链上。如由 MythicalGames团队开创的 DGoods，正专注于从 EOS 开始并提供一个功能丰富的跨链标准。Cosmos 项目也在开发一个 NFT模块，可以作为 CosmosSDK 的一部分加以利用。

3.非同质化代币元数据

像之前提到的，ownerOf 方法提供了一种方式去查询 NFT 的所有者。例如，通过在 CryptoKitties智能合约上查询 ownerOf(1500718)，我们可以看到，在写这篇文章的时候, CryptoKitty #1500718 在本文所写时的所有者是一个地址 为 0x6452 的账户.....这可以通过访问他们在 OpenSea 或 CryptoKitties.co 上的 CryptoKitty 来验证。



但是 OpenSea 和 CryptoKitties 是如何发现 CryptoKitty #1500718 的样子呢？它的名字和独特的属性又是什么呢？

这就是元数据的作用。元数据为特定代币 ID 提供描述性信息。在 CryptoKittty 的情况下，元数据是猫的名字、猫的图片、一段描述以及任何额外的特征（在 CryptoKitties 的情况下，称为"cattributes"）。如门票之类的应用，元数据除了名称和描述外，可能还包括了活动日期和门票类型。上面这只猫的元数据可能是这样的。

```
{

  "name": "Duke Khanplum",

"image":

"https://storage.googleapis.com/ck-kitty-image/0x06012c8cf97bead5deae2370
70f9587f8e7a266d/1500718.png",

  "description": "Heya. My name is Duke Khanplum, but I've always believed I'm King Henry
VIII reincarnated."

}
```

那么问题就变成如何以及在哪里储存这些数据，使得 NFT 的应用程序能够访问它们。

3.1.链上 vs.链下

对于开发者们来说，第一个决定是在链上或链下表示元数据。也就是说，你是要将元数据直接镶嵌到代表代币的智能合约中，还是单独托管它。

3.1.1.链上元数据

在链上表示元数据的好处是：1）元数据与代币一起永久存在，在任何应用的生命周期结束后仍会存在；2）元数据可以根据链上逻辑进行更改。如果资产意在拥有远超其原始创建的长期价值，那么第 1 点就很重要。例如，一件数字艺术作品被期望在整个时代中持续存在，不管用于创建该艺术作品的原始网站是否仍然存在。那么，其元数据必须与代币标识符的生命周期同时存在。

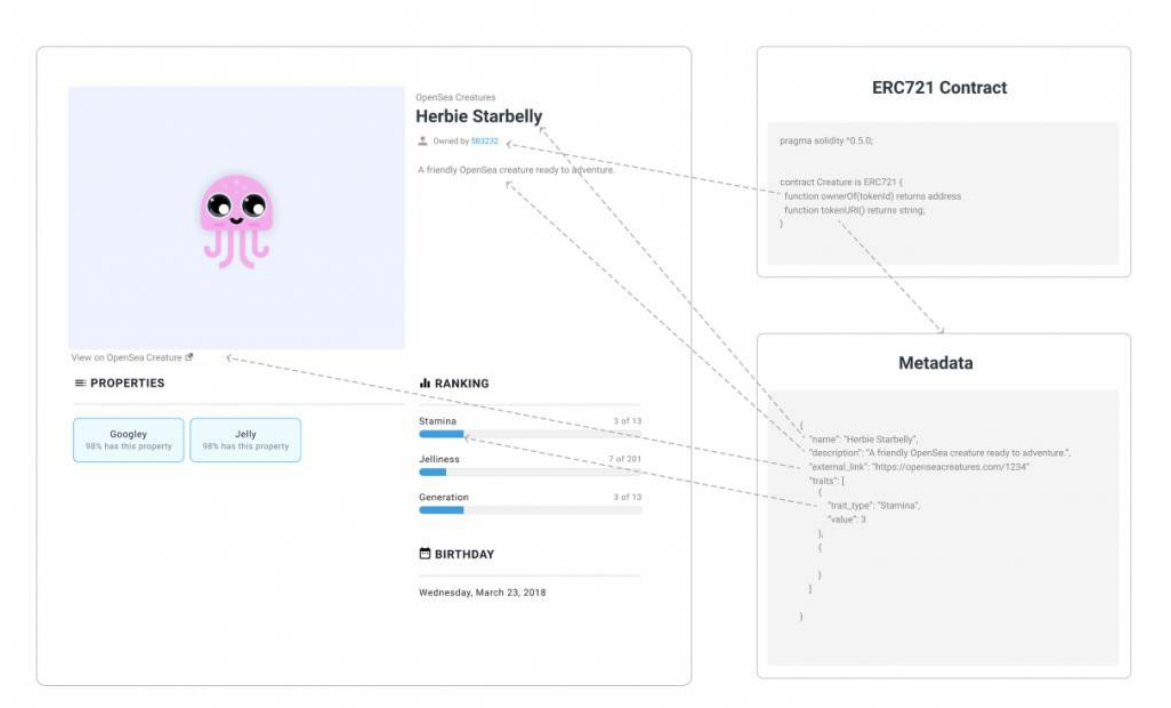
此外，链上逻辑可能需要与元数据进行交互。以 CryptoKitties 为例，CryptoKitty 的 "世代 "会影响 CryptoKitty 的繁殖速度，而繁殖都是在链上进行的（高世代猫繁殖更慢）。所以智能合约内部的逻辑需要能够从其内部状态读取元数据。

3.1.2 链下元数据

尽管链上元数据有这些好处，但大多数项目仅由于 Ethereum 区块链目前的存储限制而将其元数据存储在链下。因此，ERC721 标准包含了一个名为 tokenURI 的方法，开发人员可以用该方法来告诉应用程序从哪里可以找到给定项目的元数据。

```
function tokenURI(uint256 _tokenId) public view returns (string)
```

tokenURI 方法返回一个公共 URL。然后反过来又会返回一个 JSON 数据字典，就像上面 CryptoKitty 的示例字典一样。这个元数据应符合官方的 ERC721 元数据标准，然后才能被 OpenSea 这样的应用程序所使用。在 OpenSea，我们希望给开发者提供构建在我们市场内所展示的丰富元数据的能力，所以我们已添加了允许开发者加入诸如特征、动画和背景颜色等内容的 ERC721 元数据标准的扩展。



3.2.链下储存方式

如果你要在链下储存元数据，你有以下几个选项：

3.2.1.中心化服务器

最简单的办法是把元数据储存在某处的中心化服务器，或者像 AWS 一样的云储存方式。当然，这也有一些弊端：1）开发者如果想，他们可以改变元数据。2）

如果元数据的项目下线，该元数据可能从来源处消失。为了缓解第二个问题，现在有一些服务（包括 OpenSea）会在他们自己的服务器上缓存元数据，去确保即使在原始托管方案宕机的情况下，元数据也能很有效的被提供给用户。

3.2.2.IPFS

有越来越多的开发者，特别是在加密艺术市场领域，正在使用星际文件系统（IPFS）去线下储存元数据。IPFS 是一个允许内容在不同电脑上托管的点对点文件储存系统，即文件可被复制在多个不同的地点。这解决了 A）元数据是不可变的，因为它是被文件的哈希唯一寻址的，而 B），只要有节点愿意托管数据，该数据就会持续存在。现在已经有像 Pinata 这样的服务，通过处理部署和管理 IPFS 节点的基础设施，让开发者的操作过程变得更为简单，而备受期待的 Filecoin网络会（理论上）在 IPFS 上增加一个分层，以激励节点去托管文件。

4.非同质化代币的历史（2017-2020 年）

我们已经了解了什么是不非同质化代币以及如何构建它们，现在让我们深入了解它们是如何产生的。

4.1.纪元前 1 年：在 CryptoKitties 之前

NFT 的实验始于比特币网络上有色币的出现。建立在比特币竞争对手交易系统上的青蛙 Pepe 角色插画 RarePepes 是第一批。其中一些事实上已经在 eBay 上卖出了，后来有一套RarePepes在纽约的一次现场拍卖中卖出。

第一个基于 Ethereum 的 NFT 实验是 CryptoPunks，它由 1 万个独特的可收藏的 punk 组成，每个 punk 都有一套独特的特征。由 Larva Labs 构建的 CryptoPunks，特点是其链上市场可以与 MetaMask 等钱包一起使用，这降低了和 NFT 互动的门槛。今天，鉴于其有限的供应和在早期采用者社区中的强大品牌影响力，CryptoPunks 可能是现在真正数字古董的最佳候选人。此外，punks 生活在 Ethereum 网络上的事实，使得它们可以与市场和钱包进行互通（尽管比新的资产稍逊一筹，因为它们的出现早于 ERC721 标准）。

4.2.纪元前 0 年：加密猫的诞生

CryptoKitties 是第一个将 NFT 推向主流的项目。CryptoKitties 于 2017 年底在 ETH 滑铁卢黑客马拉松上被推出，它的特点在于是一个原始的链上游戏，允许用户一起繁殖加密猫以产生不同稀有度的新猫。"0 代 "猫咪在荷兰拍卖会上以递减的价格进行拍卖，而新猫咪也可以在二级市场上出售。

虽然后来游戏界有人给 CryptoKitties 贴上了 "不是真正的游戏 "的标签，但考虑到区块链的设计限制，该团队其实做了很多开创链上游戏机制的努力。其中，他们建立了一个链上繁殖算法，隐藏在一个决定了猫的遗传密码的闭源智能合约

内（进而决定了它的 "属性"）。CryptoKitties 团队甚至通过完善的激励系统保证了繁殖的随机性，并有远见地保留了某些 low-ID 的猫咪作为以后的推广工具。最后，他们开创了荷兰的拍卖合约，后来成为主要的 NFT 价格发现机制之一。CryptoKitties 团队卓越的远见，为早期的 NFT 领域带来了巨大的推动。

我们认为 CryptoKitties 的病毒性传播原因可以归结为：

4.2.1.投机机制

CryptoKitties 的繁殖和交易机制引导了一条清晰的盈利路线：买入几只猫，让它们繁殖出一只更稀有的猫，炒卖这只猫，重复（或者直接买入一只稀有猫，然后希望有人来买走它）。这就推动了饲养者社区的发展：那些致力于饲养和炒卖稀有猫咪的用户群体。只要有一批新用户加入并玩这个游戏，价格就会上涨。

在最狂热的时候，CryptoKitties 的成交量接近 5000ETH，其中 18号创世猫以253ETH（出售时为11万美元）的价格售出。这个销售额后来被 Dragon 猫的600ETH销售额所取代，当时（2018 年 9 月）的价格是 17 万美元，不过很多人猜测Dragon的销售是不合法的。这些高价格吸引了更多的用户参与淘金。

4.2.2.病毒性故事

加密猫的另一个成功之处在于它的故事。猫咪们可爱、可分享、有趣--而购买一只 1000 美元的数字猫的想法是如此荒谬，以至于促成了一个很好的新闻故事。此外，智能合约的迫切渴望的用户则 "打破了 Ethereum"，这本身就是一个故

事。由于 Ethereum 一次只能处理有限的交易数量（约 15 笔交易/秒,15tps），网络上较高的吞吐量导致了待处理交易池的不断扩大，和 gas 油价的增涨。日均挂单交易从 1500 笔上升到 11000 笔。新的潜在猫咪买家支付了天文数字的费用且要等上数小时去确认交易。

这些因素导致了 "CryptoKitty 泡沫"：新的需求进入 CryptoKitty 世界，价格上涨，而价格上涨带来新的需求。当然，所有的泡沫最终都会破灭。12 月初，猫咪的平均价格开始下降，且成交量也有所下降。许多人意识到，相对于 "真正的游戏 "来说，CryptoKitties 的玩法其实很原始，除了投机者之外，无法留住更多的受众。一旦新鲜感消失，它的市场就会受到影响。现在，CryptoKitties 每周的交易量在 50ETH 左右。