

# NFT介绍 副本

💡 2021年被称为 NFT 的“元年”，Uniswap一双袜子卖16万美元，推特创始人五个单词拍出250万美元，加密艺术家Beeple的数字作品“First 5000 Days”在佳士得单一拍品网上以6900万美元价格成交；

## 背景知识

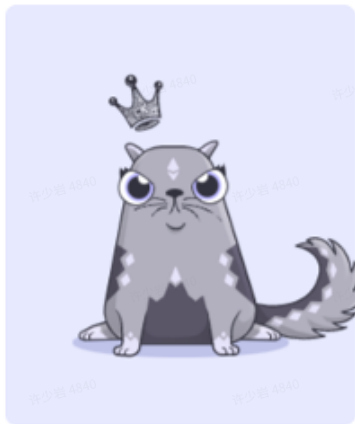
**区块链：**是一种技术。分布式账本，你的数据不存在中心化地方（银行、公司数据库），而是每个使用者都拥有一份完整的数据，且每份数据都是不可篡改，可追溯，只有拥有私钥的人才能操作。

**比特币、以太坊、IPFS：**分别是第一代、第二代、第三代代表性的区块链**应用**。第一代比特币是用区块链来作为分布式记账（可以看做是数据库），以太坊用区块链打造分布式应用平台（EVM分布式操作系统有逻辑运算能力，在上面搭建DAPP等应用），第三代是打造了一个数据库+操作系统+文件系统的星际协议~（这里就扯淡了）

**DeFi：**以太坊上的去中心化 金融借贷应用。场景是对于所有的token进行操作（BTC，ETH）SOL），替代银行的工作。与传统金融相比，DeFi有更强的开放性和包容性：第一，DeFi不需要依赖任何中心化的主体来提供信用中介或者背书;第二，没有准入限制，即任何一个联网的人都可进入;第三，任何第三方均无法阻止任何一笔交易，也不能逆转任何一笔交易。

**Web3.0：**基于区块链的应用。分布式、去中心化、匿名安全。

**加密猫：**NFT的前身，养不同的小猫，同时能生小猫，一个游戏火爆出圈。



Suki Grimskibear

🔒 1971779

♡ 2

🔪 Gen 20 ⌚ Catatonic (1w)



Boots Bippoppins

# 1972016

♡ 1

🔪 Gen 13 ⌚ Catatonic (1w)



Mittens Greenwuv

# 1972430

♡ 1

🔪 Gen 13 ⌚ Catatonic (1w)



Minka Delibear

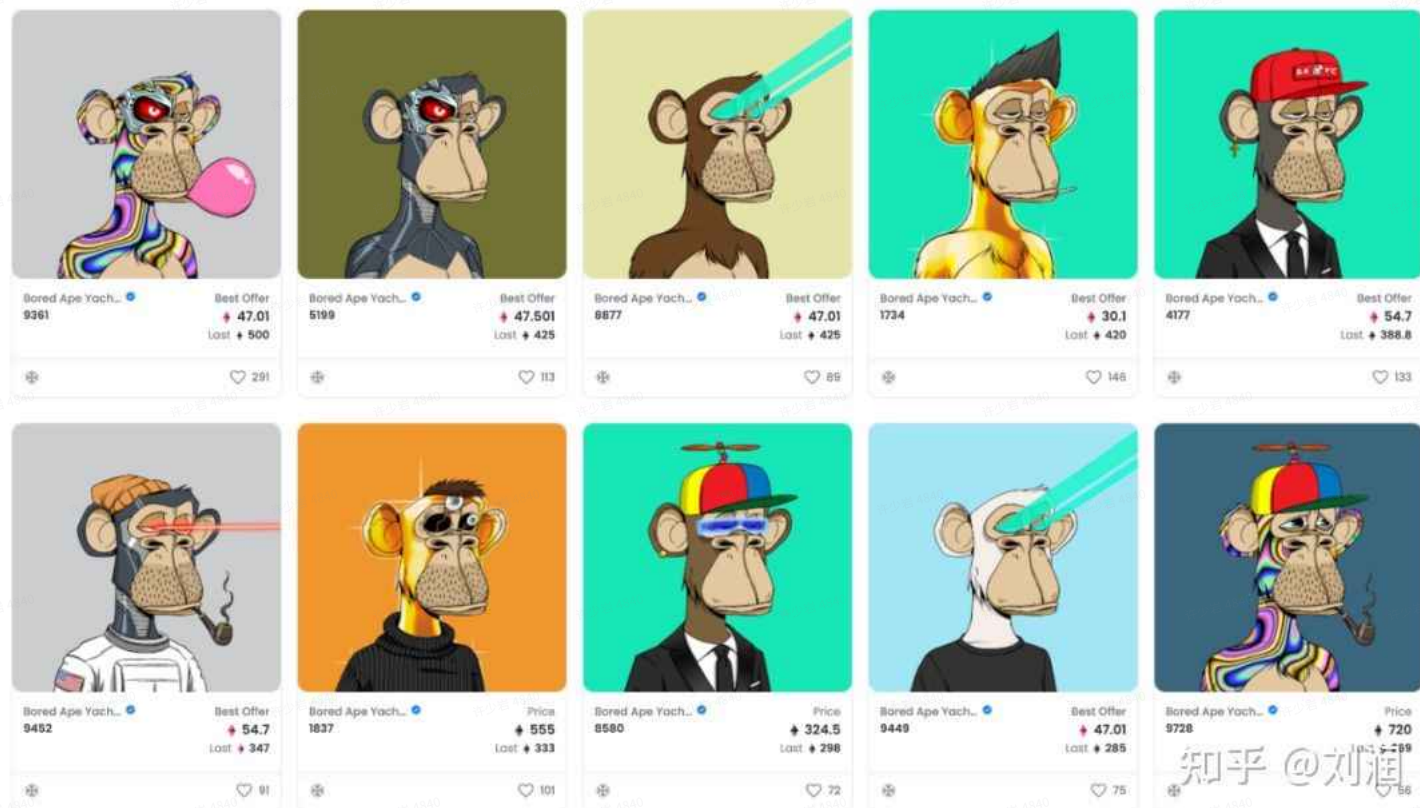


Myeong Yodelrum



Felis Liondork

NFT是什么？



NFT 的概念是由加密猫CryptoKitties 的创始人兼 CTO Dieter Shirley 在 2017 年正式提出的。

随着加密猫的火爆，NFT 的概念迅速走进了大众视野。由此，数字资产不再只是指代加密货币，而是由同质化的加密货币与非同质化的 NFT 代表的加密资产组合而成。

- 同质化代币（Fungible Token，FT）

同质化代币同样如此，同种类的一个比特币和另一个比特币没有任何区别，规格相同，具有统一性。在交易中，只需关注代币交接的数量即可，其价值可能会根据交换的时间间隔而改变，但其本质并没有发生变化。同质化代币是一种能够替换、具有统一性、可接近无穷拆分的代币。

- 非同质化代币（Non-Fungible Token）

非同质化代币包含了记录在其智能合约中的识别信息。这些信息使每种代币具有其独特性，因此不能被另一种代币直接取代。它们不能以一换一，因为没有两个 NFT 是相同的。

核心是在数字世界进行确权，目前我们对于房产，期权，汽车等证明核心是依赖政府、依赖公司成本非常高。

**“数字内容资产化”是其最核心的价值**

打破了以往对互联网时代信息的认识：**我们可以传递信息，但无法传递价值。**

## 能做什么？

允许用户和公司将其个人数据（如其个人 ID，证书，公司财产数据，注册数据，房地产数据以及其他有关现实世界资产的重要信息）放置在区块链网络上

一个例子：张三，他20岁的时候，画了一幅画。那时他还是学生，不出名。这张画5000块卖给了李四。张三很努力，越画越好，也办了很多画展，慢慢越来越有名了，就在几年后，他曾经的这张画一路被炒到了1万、2万、10万、100万、1000万。

他画卖出去的时候只有5000块，而现在这画暴涨卖到1000万，结果都跟他没关系。

现在既然可以确权，那它就可以同时设定交易规则。

这个交易规则在NFT世界里，理论上是可以随便定的。

但现在大家所普遍制定和遵守的交易规则就是，每次交易分给创作者10%。

## NFT性质

- **独一无二，且真实性可被证明：**由于智能合约的详细属性，每一种 NFT 只有一个存在，无法被复制或拷贝，不存在盗版，具有天然稀缺性
- **不可互换：**由于非同质化
- **不可分割：**只能作为单一整体存在
- **所有权和使用权分离：**NFT代表个人对数字资产的所有权，无法阻止他人查看、阅读和使用。NFT只是捕捉信息记录持有人的信息并且标记在区块链上，让全世界知道数字资产的所有人是谁。
- **精神资产化：**将一种象征意义的精神资产化并固定下来，使其可以被收藏或转让。NFT的投资逻辑建立在 NFT 玩家的精神消费上
- **一级半市场&二级市场：**
  - 一级市场：NFT 中心化项目方发行 NFT
  - 一级半市场：一级市场发行之后，允许所有的一级发行获得的收藏者在一定范围内重新做交易。但不允许其他的外部平台的一级发行商进入平台
  - 二级市场：一级发行商和收藏商进行交易的市场，完全去中心化，满足用户超域的身份认同

数字艺术家 Beeple 从 2007 年开始每天作图一张，最终把 5000 张图片拼接成一个 316 MB 的 JPG 文件，并将其作为 NFT 出售。这个耗时 14 年创作的作品《Everydays: The First 5000 Days》，最终以 6934 万美元的价格在英国著名拍卖平台佳士得上卖出。





Beeple 创纪录拍卖后，Zion Lateef Williamson、村上隆、Snoop Dogg、Eminem、Twitter CEO、Edward Joseph Snowden、Paris Hilton、姚明等各界明星、艺术家纷纷通过各种 NFT 平台发布了 NFT，再一次将 NFT 推向大众视野。

## 国内跟进

2021

6月23日，支付宝发行了一批“NFT”版付款码皮肤，每款NFT限量8000份，售价为10支付宝积分+9.9元，每日分两批抢购。活动一发出，发售的NFT就被一抢而空。

而随着活动热度的攀升，闲鱼等二手平台上出现了天价买卖NFT的现象，连黄牛都开始进入，并直接在闲鱼发帖：“高价回收支付宝NFT 敦煌美术研究所NFT编号0001或者6666的，十万一张，其他编号500一张。”而网截图显示，闲鱼同款NFT最高标价已到150万元

7月30日，QQ音乐称将推出NFT加密艺术品服务“TME数字藏品”，向用户发行虚拟的收藏品，开启内测，后续该项平台技术或将在TME内各家产品中同步上线。

8月2日，号称国内首个NFT交易平台的“幻核”正式上线APP，该产品正出自腾讯PCG事业群。

QQ音乐紧随其后，8月9日，QQ音乐上线了首只音乐数字藏品——胡彦斌二十周年黑胶NFT《和尚》。该专辑限量发售2001张，发售前预约人数超过了4万。

此后再进场的互联网大厂，包括京东、B站、网易、小红书在内的平台，都强调自身是数字藏品，很少再见到NFT字样，在介绍相关产品时也纷纷强调其与虚拟货币的不同。

随着起数字藏品业务的蓬勃发展，从支付宝小程序“蚂蚁链粉丝粒”为品牌载体开始升级成“鲸探”，而这是一个独立的APP,目前早已上线各大应用商店，但蚂蚁集团并未对“鲸探”的上线进行大幅宣传

## 生态板块



目前 NFT 项目主要集中在数字收藏品、游戏资产和虚拟世界三个领域：

数字收藏品往往是具有特定的文化印记和艺术美感的多媒体内容，如 NBA Top Shot 是 NBA 球星的短视频视频剪辑收藏品 NFT；游戏资产则更强调用途，如区块链卡牌游戏 Gods Unchained 的卡牌 NFT 可以用到实际的对战中；

虚拟世界一般拍卖其中的地块和特殊物品，如 Decentraland 中的地块 NFT，用户拥有该 NFT 就可以建设改造相应的虚拟土地。除此之外，还有形形色色 NFT 项目，他们往往都具备稀缺性、属于某些文化圈子、或是有着相应的用途。

在交易流通层：以 OpenSea 为首的综合性交易平台，为用户提供了稳定且方便的多品类，NFT 资产交易体验。OpenSea 支持交易多个项目平台的 NFT 资产交易，被称为“NFT 的亚马逊”，并且用户可在平台内上传数据内容免费铸造 NFT。

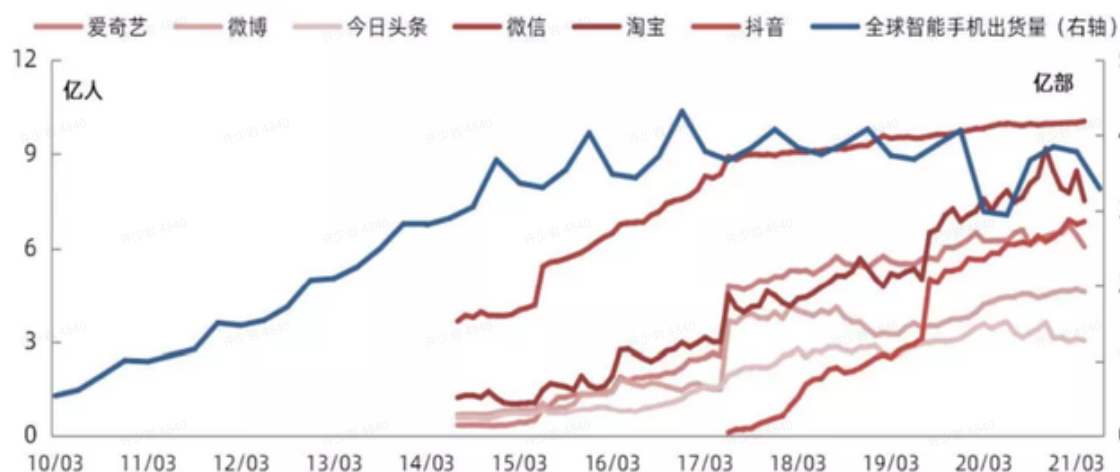
而以 Nifty Gateway 为首的数字艺术交易平台，专注于服务艺术家与艺术品爱好者，业务重点在于通过 NFT 与数字艺术的结合，解决传统数字艺术作品的缺少交易实体的痛点，带来全新的数字艺术交易模式。

## 巨头为什么看重？

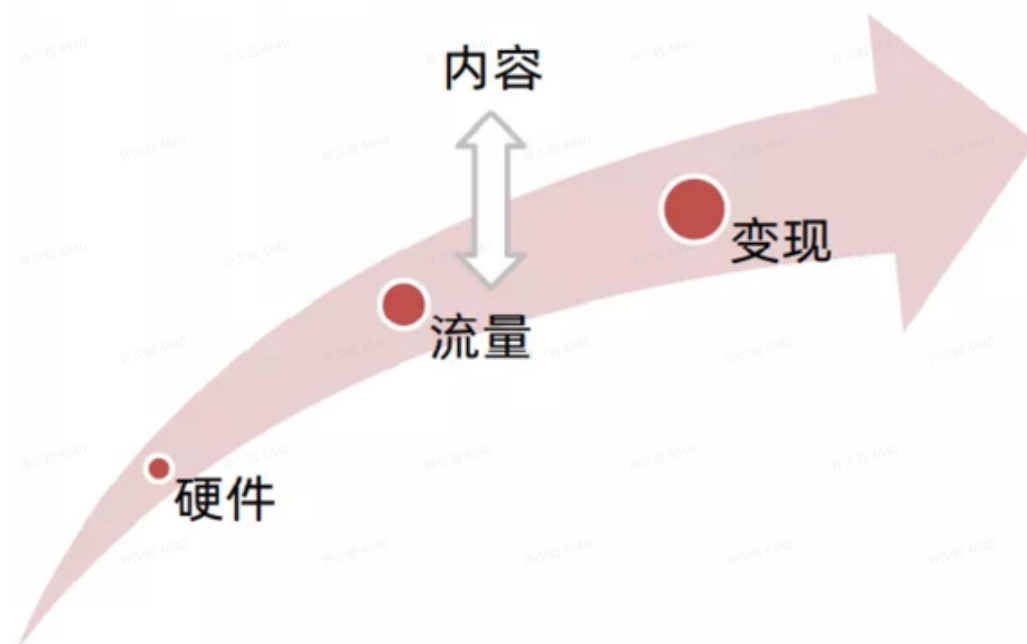
智能手机出货量的提升带来移动互联网渗透率的提升，社交、游戏、视频、购物等应用端的供给输入带来了内容大爆发，流媒体、直播等商业模式创新改变了原有的内容分发规则。这些分别对应着硬件、流量、内容与变现，但内容本身的无法变现，导致移动互联网商业的底层逻辑仍是流量。



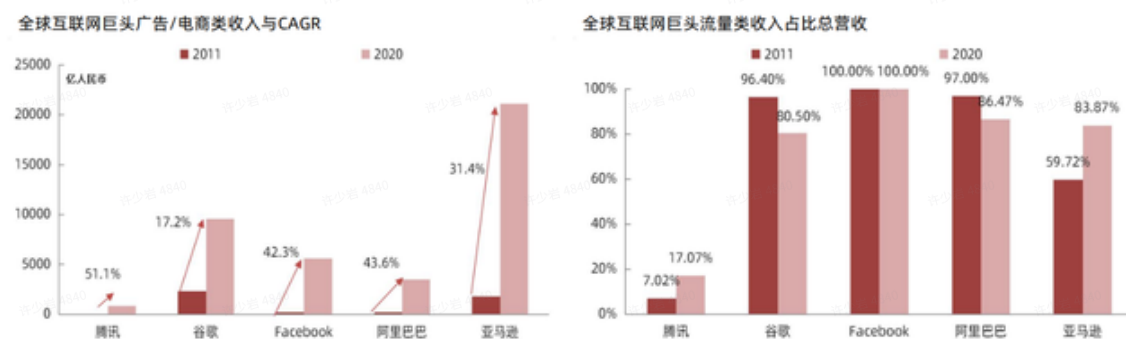
## 从硬件到流量（移动端MAU）



## 移动互联网时代的发展脉络



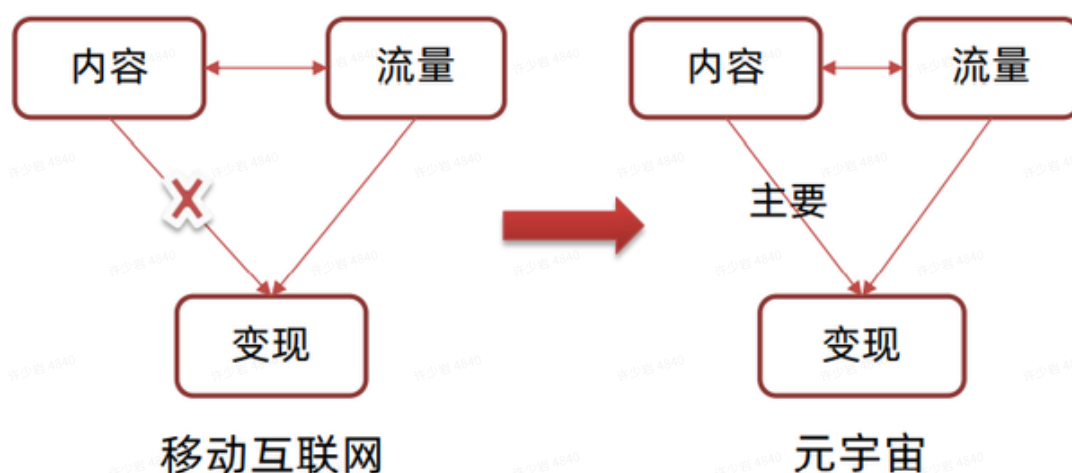
当前巨头的核心变现方式还是广告 CAGR（复合年均增长率）



资料来源：公司公告，中泰证券研究所（注：阿里巴巴初始年份为2012年数据）

元宇宙是在移动互联网渗透率达到天花板后互联网企业选择的新增长点。元宇宙是社会大众所选择的形态，用户在元宇宙中能够利用底层技术生产自身期望的内容，打破了PGC（专业生产内容）时代限定场景与内容、限定规则的诸多框架，实现了内容本身的可变现性，而企业在这一形态下，以提供底层技术、场景、IP为基本盘，也可以参与到内容创作的过程中。这重塑了新的商业逻辑，从内容必须要借助流量这一相辅相成的载体才能实现变现，到内容本身即可变现。

### 元宇宙形态下的商业逻辑



## 购买心理

NFT购买者的心理，将NFT为消费者创造的价值分为功能价值、社会价值、情绪价值、认知价值和条件价值，探究NFT如何实现二级市场流动性。Discord社区问卷调研和豆瓣小组问卷，结论如下：

1. 功能价值明显：实现收入和数字资产储备是目前玩家入局NFT的主要动机
2. 认知价值突出：玩家将参与NFT的购买作为元宇宙和区块链相对简易的认知渠道
3. 情感价值和社会价值相对不突出：玩家对NFT商品的价值认知目前投机程度大于共情程度，基于内容的NFT价值待发掘，因NFT产生的社群连接尚不紧密→可能由于此次调研并未深入NFT核心社群

## 发展未来

### • 元宇宙+社会实验

真正意义上的元宇宙何时才能落地应用还是未知数，但可以想象的一个非常有趣且可实施性较强的落地是——低成本社会实验。一些研究和实验在真实世界需要极高的世界、资本和社会成本，元宇宙为这类需求提供了非常好的替代选择，具体场景可以假设一方出于研究和学术需要出资设立虚拟实验项目，承接方负责按照实验需求的逻辑搭建特定虚拟世界并招募志愿者，志愿者进行虚拟实验并在成功完成后获得酬劳。一些人会将目前的区块链经济生态看做一场社会实验，但这个“实验”明显缺乏独立性且无法控制变量。元宇宙中的社会实验是与外界隔绝的、可回档、可重复的。

### • 社交与展示



NFT的持有者和价值信仰者需要一个“Show off”的舞台，这类社交聚集地对稳固NFT价值共识和吸引新鲜血液加入都非常有效。将NFT从重投机转向自我实现的有效方式便是为价值鼓吹者和价值信仰者提供表达和聆听的渠道。行业内的先行者和KOL需要一个属于NFT的“小红书”来向他人展示自己的爱好和格调。

## 制作原理

### 知识点

- 区块链
- IPFS
- 智能合约

### 过程

#### 第一步: 制作id

制作id，这是把物质制作成 NFT 的第一步。物质有哪些？一段文字、一张图片，一件衣服等，夸张的说，现实世界的物质，无论是虚拟的(游戏装备)或实质物质，都可以被通证化。

#### 如何操作？

通过 **第三方技术手段** 获取物质的唯一标志性中间产物。

因此制作 NFT 第一步，广义于下面等式：

- $id = F(I)$ 
  - a.  $I$  = 输入的物质
  - b.  $F$  = 处理函数，代表一种方法
  - c. id 唯一标志性的中间产物

最简单的例子就是哈希函数，不考虑哈希碰撞，它就可以根据不同的内容输出不同的哈希值。 **思维在这里不要局限于哈希函数。**

#### 获取图片的唯一id

这里用图片代表一系列的文件类数据。

1. 我们可以将图片转换成 []byte 字节数组，然后计算其哈希值。这种操作虽然比较简单，但是图片别人却不能访问，看不到；
2. 如果我们想向外部任何人提供图片的读权限，在计算完 id 后，有两种做法：
  - a. 上传图片到文件服务器，任何人可以通过 url 链接访问。这里的服务器是中心化的；
  - b. 增加区块链属性。上传文件到 IPFS (ipfs是什么，自行搜索)，如此一来，文件别人能访问，同时还具备了区块链的去中心化等属性。其中 IPFS 会在上传完文件后，会使用它的算法，帮你计算好哈希值返回，可以直接用它的作为id。

#### 获取衣服的唯一id

这里用衣服来代表一系列的实际物质。如果获取它们的唯一id呢？做法可以放飞思维去思考，比如可以：

- 衣服的出厂信息、扫描内容、照片，等系列关于它的信息，数据化，然后用这些数据制作成文件，最后参考图片的做法。

## 第二步：通证化

第一步中获取了物质的id，现在要把它们通证化。切记一点：目前公认的 NFT 都是基于区块链公链的，那么以后是不是会一直这样呢？不一定，说不准出来了新的共识。

### 基于不同公链的流程

通证化的流程如下：

1. 选择一条区块链公链。这里的选择会决定后面 **智能合约** 等系统组件的技术栈，这一点很核心；
2. 在所选的公链上开发智能合约；
3. 所开发的智能合约需要遵循一些基础约定，比如至少能保证物质的id能达到验证去重，什么意思呢？意思是，如果 A 在今天上传了 id=1 到链上，明天 B 也上传同个 id=1 到链上，合约要能告诉 B，你不能上传了，id 已经存在；
4. 部署智能合约到链上，此时它变成 DApp；
5. 通过发交易的方式，调用该智能合约的方法，将id等相关数据存储到链上。

### NFT 的智能合约

NFT 智能合约可以基于不同的公链开发，它不局限于任何一条公链。不同公链的智能合约方案实现也不同，下面以以太坊公链举例说明。

在以太坊上面，开发 NFT 智能合约，已经有很多标准，比如 ERC-721 \1155 \998，各有各的特点，但它们的特点是在基础属性上拓展而来的。(各标准文档: <https://eips.ethereum.org/EIPS/eip-721>)

如果选择 ERC-721 标准开发 NFT 智能合约，在元数据存储部分，就有 tokenUrl 这项，它相当于物质的唯一 id，像下面的样子，**\_tokenURIs** 存储的就是通证当前计数id与其对应的 tokenUrl，这里的tokenUrl 是字符串格式，一般是文件url，存储在 IPFS 或其他服务上面的文件的链接，但不局限于链接，也可以是其它的内容。

```

1 // 伪代码
2 contract MyERC721 is IERC721Metadata, ... {
3     ...
4     mapping(uint256 => address) private _tokenOwner;
5     mapping(uint256 => string) private _tokenURIs;
6
7     uint256 public tokenCounter; // 计数, 当前总的 NFT 的数量, 累增
8
9     constructor () public ERC721 ("name", "symbol"){
10         tokenCounter = 0;
11     }
12     // 外部调用方, 调用这个函数, 传参数: tokenId 即物质的id, tokenId 唯一
13     function createNFT(string memory tokenId) public returns (uint256) {
14         uint256 tokenId = tokenCounter;
15         _mint(msg.sender, tokenId); // 将交易发送者和当前的 tokenId 绑定
16         _setTokenURI(tokenId, tokenId); // tokenId 映射到 tokenId
17         tokenCounter = tokenCounter + 1; // 累加
18         return tokenId;
19     }
20     // _exists 函数判断 tokenId 是否存在, _tokenOwner[tokenId]
21     // 根据 id 读取对应的 url
22     function tokenId(uint256 tokenId) external view returns (string memory) {
23         require(_exists(tokenId));
24         return _tokenURIs[tokenId];
25     }
26     // 根据 tokenId 和 url 建立 map 数据关系
27     function _setTokenURI(uint256 tokenId, string memory uri) internal {
28         require(_exists(tokenId)); // _exists
29         _tokenURIs[tokenId] = uri;
30     }
31     ... // 省略系列接口, 包含读接口
32 }

```

上面的 tokenId 是标准要求的存储数据项。整个合约具备下面约束功能：

1. NFT 持有者，即 msg.sender(owner) 和 tokenId 一对多关系，代表一个人可以拥有多个 NFT；
2. tokenId 和 tokenId 一对一关系，代表每份数据一个链上的唯一id，同时 tokenId 没要求是唯一，但在调用方，一般会把 tokenId 设置唯一，即使不唯一也没关系，冲突的时候，tokenId 越小的，其当初被设置的时间就越早；
3. NFT 持有者在将数据写入链上后，能够获取 NFT 的链上唯一 id，后续可以根据 id 进行系列的读写操作。

一般来说，我们常规的 NFT 有一个和数据建立关系的项就足够了，但并不局限于此，合约在实现了标准要求的接口后，完全 **可以自己添加自定义数据项及其读写函数。**

### 第三步：展示与修改

#### 展示 NFT 内容

所谓展示，就是对 NFT 的数据进行读取再展示。一般的流程如下：

1. 根据当初设置 NFT 数据到链上时获得的 id 去智能合约读取信息；
2. 将获得的信息通过某介质应用还原出原始的 NFT 数据。

比如将图片 NFT 展示出来。(借助上面的 721 合约标准和 IPFS 结合为例)

3. 假设调用合约存储数据时候得到的 tokenId 是 3，那么使用这个 tokenId 去调用合约的读数据方法；
4. 执行完 1 步骤，可以得到 tokenUrl，即文件存储在 IPFS 中所得到的链接；
5. 直接将 tokenUrl 链接在浏览器打开，看到图片。

## 修改 NFT 内容

修改是一项 NFT 智能合约的拓展功能，可有可无，具体是怎样的方式，完全看需求的实现。比如：

6. 允许重置 tokenId 所对应的内容；
7. 在 NFT 原数据中增加其他字段内容，再允许修改这些字段；
8. 转让 NFT，可以把某 tokenId 对应的 NFT 信息转让给其他 owner，达到转让目的；
9. **出售 NFT**、**拍卖 NFT** 等操作....

## 所有权共识

目前 NFT，非同质化通证。本质是想借助区块链的属性来表示一种资产的所有权证明。

比如曾拍卖出 6000 多万美金的数字作品(图片)《Everydays: The First 5000 Days》，中标者能获得原图 和 该图的 NFT。这两样东西，一样是实质的作品，一样是它的所有权者的证明。

我们假设下，如果持有某作品的人，是一位匿名者 A，过了多年后，该作品本身不小心被盗并被找回。那么如何证明 A 是真正的拥有者，此时 A 只需要展示他对该作品的 NFT 拥有权，就可以证明。

那么 NFT 是不是类似于我们现实中的证书？不全是，分两点：

10. NFT 和证书都能证明某资产的所有权；
11. 对比的存储介质与永恒时效：
  - a. 证书可能要找保险柜保养放着，但它终究占据一方土地，仅受一方土地容纳的保险柜保证安全，在时过境迁的影响下，持续性存储下去的时间会较短；
  - b. NFT 存储在区块链上，受整个互联网的链节点所保护。它能够存活到整个链网络垮掉那天，对于节点数量众多的公链来说，这个概率几乎等同于互联网终结那天。

## 价值判断

两个维度：

外在：大众对这个东西价值的认同程度，即，有多广泛的人会承认这个东西的价值。

内在：这个东西本身的成本、稀有程度、不可复制程度、品牌价值等等……



通过NFT，区块链将成为一个虚拟物品的开放市场。

紧密度低的东西，价值和NFT关系不大，更多可以被称作 **数字纪念品**

## 参考

<https://www.jinse.com/blockchain/974350.html>

<https://mp.weixin.qq.com/s/mRPB2MQkBI8YDrT5T4dJDw>

<https://www.cnblogs.com/linguanh/p/15163809.html>

<https://zhuanlan.zhihu.com/p/32615963>

<https://zhuanlan.zhihu.com/p/365263479>

<https://www.jianshu.com/p/a9ccc643b6db>

<https://baijiahao.baidu.com/s?id=1724999323929672290&wfr=spider&for=pc>