解构 NFT

2021，NFT 大火。

从朋克头像、混血猫咪到无聊的大猩猩，各路风格的 CG 作品“你方唱罢我登场”，纷纷乘着 NFT 的风口“上链”。第一个 Twitter、第一条手机短信、NBA 明星球员的“精彩瞬间”……似乎没什么不能 NFT，没什么不能“上链”。佳士得 6900 多万美元的成交天价更是将 NFT 一举送上神坛。

NFT 是什么？持有 NFT，到底会获得哪些权益？它跟“区块链”有什么关系？跟“元宇宙”、Web3.0 这些概念又有什么关联？

一切答案，其实都要从定义 NFT 的“智能合约”谈起。

NFT，全称叫 Non-Fungible Token， 翻译成中文是“非同质化通证”，与之相对的概念就是“同质化通证”（Fungible Token，“FT”）。

FT 属于“种类物”，人们关注的是它们的面值和数量，并不在意它们彼此之间的区别（比如序列号），所以，相同数量的 FT 价值相同，可相互替代；NFT 相当于“特定物”，每一枚都具备与众不同的属性和特点，因此，不同的 NFT 彼此不能等价互换。

不论 FT 还是 NFT，其实都是在区块链上用智能合约定义的簿记权益，通俗点说就是在数字化账本上存储的关于财产归属和财产数量的权益记录。FT 的簿记，类似于银行给储户开立的分户余额账，核心就是记录每个账户有多少余额；NFT 的簿记，则类似于不动产登记中心的房产档案，核心在

于记录每个房屋的权利人是谁，以及房屋坐落、面积等属性。

所以，FT 的智能合约，核心内容是一个由“账户”指向“余额”的映射集合，通过“账户”编号能快速地检索出“余额”的数量；而“转账”，就是把“转出”账户的余额减少特定数量，同时把“接收”账户的余额增加相应数量。

而 NFT 的智能合约，其核心内容则是一个由“Token 编号”指向“账户”的映射集合，通过“Token 编号”能快速检索出持有这枚 Token 的“账户”；而 NFT 的“转让”，就是把特定 Token 编号所指向的“账户”从“转出”账户修改为“接收”账户。

智能合约的其余内容，NFT 与 FT 都差不多：定义 Token 的名称、符号、发行总量等等。然而，NFT 会有一个非常独特的描述性变量或字段，详细地界定每一枚 NFT 所指向的“标的数据”的属性特征，那就是——“元数据”。

元数据（Metadata），听起来是个很玄、很科幻的名字，总让人联想到“元亨利贞”或者“N 次元空间”之类的名词。其实，它本质上就是对某个数据集合或者数据对象的结构、位置、内容等特征的描述，特别类似于《房产证》上对房屋坐落、面积等房屋特点的描述。

根据《房产证》上对房屋特点的描述，人们很容易就能找到房屋的位置，理解房屋的结构、大小等基本属性。与之类似，根据“元数据”的描

述，计算机程序就可以找到“标的数据”的位置或索引，了解其数据类别和编码规则，从而实现对“标的数据”的访问和解析。当然，也可以在“元数据”中加入各种“注释”类的信息，从而让每一枚 NFT 都显得“与众不同”或者具备“私人订制”的特点。比如，在 NFT 发行时，将艺术品作者的名字或者 NFT 认购者的 ID 写入其中。

不同的 NFT 项目，其“元数据”的设计方案并不完全相同。比如，著名的朋克头像项目，其实是将 1 万个 24x24 点阵的朋克头像拼合成一个 PNG 图片，然后将这个图片文件的哈希值（详细解释见下文）作为一个特殊的不能修改的属性变量写入智能合约，结合着每个头像的编号，在逻辑上共同构成每枚 NFT 的“元数据”。这样，每枚 NFT 都会对应着一个特定编号的头像，而每一个头像都可以凭编号从拼合的大图中找到相应位置的显示单元。大图片的内容通过智能合约的哈希值可验证真伪，从而间接存证每枚 NFT 对应的朋克头像的数据内容。

无聊猩猩（Bored Ape Yacht Club，“BAYC”）是个非常有诚意的 NFT 项目，其“元数据”的设计理念和标的数据的存储方式非常严谨。首先，计算每个猩猩头像图片的哈希值，然后将这个哈希值与对应的 Token ID 连接成字符串再进行第二次哈希计算，最终结果作为该枚 Token 的“元数据”写入智能合约。同时，标的数据，即每枚 Token 所对应的猩猩头像图片，再以“内容寻址”的 IPFS 协议（详细解释见下文）存入 IPFS 分布式存储网络。这样，NFT 的“元数据”，既能验证猩猩头像的数据内容，又

能验证头像图片与 Token ID 之间的映射关系，还能进一步通过哈希表查找到图片的存储位置。区块链存储的 NFT 智能合约与分布式存储的头像图片相互协同，真正意义上实现了“图片及其权属信息”可永久性保存且不可篡改的目标。

哈希算法，是目前在数据加密、数据完整性验证、数字签名、区块链等领域非常常用的一项技术。它的基本功能就是将任意长度的源数据转换为特定长度的摘要值（“哈希值”），而且可以保证源数据的任何细微变化都会导致其摘要值发生明显改变。同时，哈希算法还满足一般加密函数的基本要求，那就是从源数据推导出哈希值很容易，而从哈希值反推源数据却几乎不可能。也就是说，哈希函数不能被轻易“破解”。

哈希函数的功能特点，就好像给数据录制“身份指纹”，不同的源数据必定会生成不同的哈希值，而不同的哈希值绝不会对应相同的源数据。所以，人们就可以利用哈希值来标记、识别数据的“身份”，校验数据存储、传输过程中是否完整，是否发生丢失或被篡改。

哈希算法有很多种，区块链领域中常见的有 SHA256、keccak256 等，中国密码局推出的商用密码杂凑算法 SM3 也是一种摘要值长度为 256 位的哈希算法。计算机能识别和计算的文件最终都是以二进制形式存储、传输、运算的，数据文件的大小最终体现为序列化二进制数据的不同长度，也就是在计算机内存、硬盘等存储介质中所占用的比特位数。不论源数据多大、长度上占据多少比特位，经过前述这些哈希函数的计算，获得的计

算结果都会是占据 256 位这么长的摘要数据，按 8 位一个字节折算，就是 32 字节。当然，不同算法获得的哈希值会彼此不同。

设计严谨的 NFT 项目，会在“元数据”中写入每一枚 Token 对应的多媒体文件的哈希值，从而标记、锁定不同 Token 所指向的“标的数据”的具体内容。

NFT 其实并不存储图片、视频或音频文件，只是在“元数据”属性中记录了这些文件的数据特征。换句话说，NFT 本身并不具备任何可直接转变为画面、影音的数据，既不能“观赏”，也不能“聆听”，完全是一个抽象的信息记录。

所谓“上链”，并不是能展现艺术品影音特点的多媒体文件“上链”，其实只是数据文件的“权益簿记”以智能合约的形式写入了区块链。人们通常对于 NFT 的感性认识，无论是卡通图片、3D 动图、短视频，还是音乐，其实都是另一个多媒体文件经软件解析处理后通过屏幕、喇叭等外部设备呈现的，而这个多媒体文件就是 NFT 的元数据所描述的“标的数据”。

所以，NFT 的“标的数据”在哪里存储，谁负责存储，可以存储多长时间，存储的成本由谁承担，这些问题直接关系着 NFT 的核心价值。试想，如果数千万美元拍卖取得的 NFT，突然有一天“看不见了”，投资人将会是种什么感受？

当代网民应该非常熟悉 HTTP 这个词，几乎每天都会在浏览器的地址

栏中输入几十次以 http 开头的网址来访问、浏览网页。这其实就是一个寻找、下载数据文件的过程。首先，浏览器会将网址发送给域名解析服务器，将域名地址解析为 IP 地址，然后根据 IP 地址找到特定的服务器，再从服务器下载网页文件到本地，最后通过浏览器将网页文件解析为包含文字、图片、动画、音乐、链接的多媒体页面，通过计算机屏幕、喇叭呈现出来。

在线多媒体文件被存储在特定地点的特定服务器上，全球用户所能看到、听到的信息都源自这个特定服务器，一旦服务器宕机、掉线，或者控制这台服务器的网站运营者倒闭、破产，用户就无法访问相关文件，这就是当前万维网的“中心化”文件存储模式。

目前很多 NFT 项目，都是采用这种中心化存储模式来存储“标的文件”的，然后，通过 HTTP 协议和域名地址来寻找、访问它。所以，在这些 NFT 项目的元数据描述中，域名地址都会是一个必备内容，协助与区块链交互的应用程序快速定位并找到多媒体文件，进而让用户对 NFT 产生图画、影音等感性认识。（然而，很少有项目会说明 NFT 与其“标的数据”之间的区别，以及多媒体数据文件并没有“上链”的事实，更少有项目会提示数字商品可能随标的数据一道灭失的风险。）

IPFS，是前述中心化文件存储模式的强有力挑战者，全称是“InterPlanetary File System （星际文件系统）”。它最本质的特征有三个，一是将中心化存储改为分布式存储，让全网的每个计算机节点都能提供文件存储服务；二是将传统的 IP 寻址方案改为内容寻址，以哈希值为

依据寻找、访问数据资源；三是将数据文件拆分成小块单元数据，分散存储在多个计算机节点上。

IPFS 的分布式、数据拆分存储方案，可以彻底摆脱中心化存储模式带来的数据毁损灭失风险。文件一旦存入 IPFS 网络，一个或几个节点的故障或灭失，很难破坏文件的数据完整性。同时，以哈希值为依据的内容寻址模式，又可以有效固定和验证文件内容，自动排除篡改、伪造数据对原始内容的消极影响。

所以，无聊猩猩的头像，将永久性保存在 IPFS 的网络当中（除非全网节点同时宕机或同时删除特定文件），只要正确地输入其哈希值地址，永远都能找到它，而且是那个每个比特都没有被改动过的最最“真实”的“大猩猩”。

NFT 的权益簿记、交易规则是智能合约定义的，而不同区块链系统之间，智能合约的存储方式、访问策略却差别很大。其中，最主流的是“以太坊”模式，将智能合约编译后直接存储在区块链上，合约内容不能被篡改，所有的用户都能访问、获取合约内容，从而可以公开透明地了解智能