

不久前，一件拥有5000幅作品的数字合成的图像：《每一天：前5000天》，就是那坨看似像素点的图片，被佳士得拍卖行以4.5亿元的巨额拍出，但与此同月，梵高的大作《蒙马特尔街景》只以1亿元的价格卖出。

而推特联合创始人第一条推特做成NFT拍出1888万，你要知道这个NFT却只有一句话“just setting up my twtr（刚刚设置好我的推特）”

11月初的时候，国际足球协会FIFA宣布将制作世足赛的web 3游戏。

其实不止FIFA，今年同时有不少公司也都抢进区块链，加密货币，NFT等web 3.0服务。像是Nike跟Adidas在年初也开始跨足NFT等web 3.0的服务。

那到底什么NFT？这需要从各位网络大佬提到的下一代网络：web3.0 说起.....

这次我就把web 3.0以及NFT，区块链，加密货币,还有Defi，一篇文章让您了解清楚。

写作不易，欢迎关注，点赞并转发给您身边的朋友分享其中的知识。

开始前要澄清所有的web 1.0，web 2.0，web3.0只是一种概念，而不是一种技术。而这种概念上的转变从历史脉络来看会比较简单。

我们先简单了解一下：什么是web1.0，web2.0，web3.0。

web 1.0是内容单向传输且资料集中于单一服务器

web 2.0则是内容能双向互动，但资料集中于多个服务器

而现在提倡的web 3.0不希望资料集中于任何服务器中，也就是去中心化，或者说所有网络使用者本身就是服务器。

举个例子：

web1.0就类似早期的电视台，内容都是电视台决定的，观众只能被动接收节目。只有管理者能够修改或新增内容。

随着网路普及以及速度提升发展出可以交互的动态网页与数据库。从而进入到了web2.0时代：简单来说就像是博客，只要进入后台输入内容就能够在网络上发布。现在任何需要账号密码的网路服务像是西瓜视频，今日头条等甚至是线上购物，网路游戏的背后都有这么一套数据库系统都属于Web2.0的范畴。

不过web2.0的出现也让这些网络平台或服务器，收集了大量的使用者与数据，形成了中心化的资料管理模式。导致这些平台或服务器可以分析这些数据，精准的插播广告也随之出现了。（也就是为什么购物网站在你一次搜索过后，就不断推送你想购买的东西）

另外在网络平台累积了大量使用者之后，也让他们掌握了可观的流量分配权，这使得平台间接获得了筛选内容的权利，具体来说就是所谓的“审查机制”。而创作者必须配合演算法才能够从平台获得流量被其他人看见。

web 2.0的出现让使用者可以自由发布内容，但现在又面临了大公司平台垄断内容曝光的权利，仿佛回到了web 1.0的时代。虽然使用者并不是没有平台发布，但发表之后又被另一个平台所限制。许多人认为这样的环境牵制了网路的可能性和言论的自由。

为了让网路回到web 2.0找回最初和自由的状态，Web3.0的概念开始成型：

web 3.0的倡议者跟开发者吸取了web 2.0的经验，他们发现中心化的资料管理方式正是为何web 2.0会从分散走向集中的原因。因此web3.0强调去中心化的资料管理。而区块链技术的诞生给了web 3.0成真的契机。这是一种不需要公司或权威机构，而且能永久保存资料在网路上的技术。

再简单点理解：1.0只能读--->2.0可读写--->3.0能确权（可读，可写，可拥有）

听完刚刚的介绍你是否觉得web 3.0是想象很美好但也很复杂充满新名词呢？

实际上到底要怎么运作来达成所声称的去中心化目标？

为什么会有矿可挖还有币可以拿？

怎么会有人想买完全看不懂意义跟价值在哪的nft图片呢？

就算办了钱包接下来又可以干嘛呢？

我们带着这些问题继续来寻找答案.....

说到web 3.0首先要讲的就是区块链，这可是一切的基础。关于区块链网上已经有非常多的文章跟视频了。这边稍微重点整理一下：区块链最开始是一种公开且分散的记账系统，每个人都可以写入或读取资料，但也有一套特殊的加密机制来确保资料不能被篡改，然后区块链会传送到网路的每个节点上是一种分散式的储存系统。不会因为特定的服务器出现问题资料就消失。这个特色也可用来验证区块链本身是否有被篡改。

假如要更新区块内的资料，例如验证一笔交易，必须把之前的区块放入更新资料中再打包成新的区块，接回原有的区块，一个接着一个形成区块链。上述打包资料的行为就是俗称的挖矿，包含了验证跟添加区块，完成挖矿之后会由系统发放加密货币当做奖励。

加密货币就类似现实生活中的纪念币。如同银行发行的纪念币是为了纪念特殊节庆所发行的货币，而加密货币则是为了纪念新区块上链所发行的货币。

纪念币因为发行数量有限，随着时间过去价格会上涨。而加密货币也是同样道理。

以比特币来说借由逐年递减挖矿奖励来限制比特币的发行数量，这就让比特币有了稀缺性，从而让加密货币有条件成为一种有价值的货币。

加密货币也称为同质化代币，就像上面提到的纪念币。

而我们现在常听到的nft则称为非同质化代币，有点类似纪念币上面还有了明星签名。

因此这个纪念币的价值就跟一般的纪念币有差别。

nft也能追踪艺术作品在网路上散布的起始点以及其交易的过程。讲白了NFT是一种虚拟产品的正版证明书，类似“奇幻式卡牌游戏”的防伪设计。

例如像游戏王，宝可梦卡或是NBA球员卡，这类卡牌不只有防伪设计，也会推出功能相同但卡面不同的“稀有卡”。因此在玩家以及收集者的眼里具有特殊的价值。

一般来说要做成一个nft除了付费给作者之外还必须付费给矿工进行铸造，也就是将艺术品打包成区块上传才能够得到一个nft。

你可能发现区块链加密货币，nft这些交易好像有点单调，难道号称未来的金融就只是买卖虚拟商品吗？这跟线上游戏买虚拟感觉没太大差别啊，有没有更进阶的应用方式呢？

因此DFI（decentralized finance）诞生了，翻译为“去中心化金融”，它包含前面讲的区块链加密货币NFT，以及各种更多元更便捷的非传统金融服务。而要做到Defi，需要用区块链技术建立“智能合约”。这是一种没合双方条件便会自动执行而且不能变更的合约。

举例来说：我手上有闲钱想要借人赚利息，我可以在智能合约写下租借的天数跟期望的利息发布成智能合约，而需要钱的人也可以写下他自己期望的天数跟应付的利息。当两者一致时智能合约就会生效，之后借钱与还钱的流程便会自动进行。通过上面借钱的例子也能看到Defi与过往中心化金融的差异。

以前要合法借钱必须跟银行借，而银行借给你的钱其实也是用其他人存在银行的闲钱，少了银行等第三方单位的中介，无论是出借人或是借款人理论上都能拿到更多的利益。

正所谓富贵险中求，Defi虽然有获利更多与快速交易的特性，但风险也比起过往与银行交易来的高。例如，智能合约的相关法律尚未完善，也曾发生过黑客利用智能合约的漏洞来窃取加密货币。

要如何保障加密货币的安全呢？

当下现成的解决方案就是去中心化钱包，去中心化钱包并不储存使用者的私钥和助记词，而是将这个核心机密完全交给使用者。

除了Defi许多透过智能合约来达到去中心化的服务或项目会在原有的词汇前面加上“D”或是“D1”。

例如：去中心化组织的DAO（分散式自治组织），以及去中心化应用的Dapp（分散式应用程序）。但并不是加上个D就跟海贼王里头的D之一族一样厉害哦。

去中心化的服务也有缺点：像是运作速度慢，使用者体验通常比较差，而且运作的的环境分散且复杂，维护跟更新还有开发都更困难等等。对已经被web2华顺体验宠坏的使用者来说门槛实在太高了。像是加密货币最初也因为界面难用让加密货币金融市场乏人问津。

一直到交易所以及去中心化钱包提供了好用的界面才让加密货币市场开始兴盛。

有人认为交易所的出现会把虚拟金融市场再次带向中心化，事实也确实如此。

但不可否认的是也因为交易所的出现加密货币金融市场才开始被大家重视。

最近因为中心化交易所运营不良的事件频繁发生，加上交易所存在潜在的资金不透明风险，使得大众对加密市场的信任下降了。

最后我想问问大家：如果要尝试web3区块链跟加密货币的世界你会想先从哪里开始呢？

1. 买一个喜欢的nft？
2. 存一点比特币以太方
3. 玩一款GameFi游戏？
4. 还是直接加入一个DAO去中心化组织的运作观摩观摩呢

如果你其他的点子，欢迎与我分享！

[#头号有新人#](#)

