对 Web 3.0 的理解

2022-06-19

Web 3.0 开发

Web 3.0 是一个几年前就存在的概念，可能随着区块链的推广越来越有名了。当人们还不知道 3.0 版本的 Web 会是什么样子的时候，区块链出现了，尤其是以太坊的 dApp 提供了一种很大的可能性，于是 Web 3.0 就和区块链、去中心化、自我主权这些概念绑定在一起。

前几天提到说。「Web 3.0 开发」是可以作为一种职业定位去描述的，而且这个词可以涵盖区块链开发的范畴，立意比「区块链开发」这个描述高一点。

Web 2.0 时代，我们说的 Web 开发指普通的前后端开发，前端用所谓的三大框架 React.js、Vue.js、Angular.js 结合组件库，后端用 Spring 全家桶，加上各种中间件 Zookeeper、Kafka、Elasticsearch 之类，还有常用的数据库 MySQL、Oracle，就是 Web 开发的常用技术栈。

Web 3.0 开发的技术栈，可能会演进为 Remix、Hardhat、Ruffle 这些智能合约的开发工具和框架，人们像关注 Java 的语言特性一样去关注 Solidity，以及各种区块链节点的搭建运行调用、二次开发，甚至及区块链节点本身的开发等等。当然，很难简单地把这些技术栈去和 Web 2.0 一一对应。一个简单的例子是，当你从事区块链开发的工作，你已经很难用前端开发或者后端开发来形容自己的工作内容了，就只能是区块链开发，或者智能合约开发，或者其他的描述方式。

现在已经有一些岗位在用「web3 开发」的形容了，不过我们要区分清楚 Web 3.0 和 web3 不是一回事，目前很多岗位说的 web3 指以太坊的那个 web3 框架。我们需要一个新的描述，同时我们需要有一个更好的、更有前景的职业定位，那就是 Web 3.0 开发。

我这里想说的是，要相信我们走在正确的道路上。

一级市场和二级市场

区块链的一级市场，指比特币、以太坊这种原生的链。二级市场更多是基于这些链，衍生出的一些项目，基于以太坊的项目尤其多，Layer 2、预言机、NFT、ENS，都属于二级市场。

有一些团队是做一级市场也就是区块链开发的，Solana、Filecoin、Neo 都是在以太坊之后出现的，Dfinity 的 IC 也是处于活跃的一种一级市场的例子，再比如像 Bitcoin SV 是在做 “支持智能合约的比特币” 这样的事情。

还有很多创业团队是在做二级市场，比如有从 360 出来的去做智能合约的安全，把合约扫描一遍报出安全漏洞给你；还有做 NFT 的交易协议，去定制一些类似 NFT 交易所的 API，想建立通用的交易网络；还有炒元宇宙概念的，给虚拟人物定制不同样式的衣服；也有基于 IC 做去中心化邮箱的等等。以太坊的各种扩容方案当然也算二级市场，OP 前段时间还发行 token 了。

从商业角度没有什么高下之分，从技术角度也不好说简单和难，不过我觉得还是一级市场更基础一些，但是技术上的发展相对缓慢，花样没那么多。具体倾向于哪一种看个人意愿了，这里想提醒的是，Web 3.0 开发是统称，要了解这些不同层级市场的区别。

去中心化是历史的倒退

刚才说希望 Web 3.0 是有前景的方向，这个部分想说的是 Web 3.0 的前景也没有那么好。

想到这个话题是在关心钱包安全的时候，意识到一个问题，就是账户的私钥一旦泄露，你就永远失去了对账户资产的控制权，或者说别人永远拥有了你账户资产的控制权。

因为我们知道，账户地址是可以从私钥解码出来的，私钥就是你的资产，在备份钱包的时候，备份的就是私钥。你的私钥泄露，就相当于把金钱摆到别人手里，至于别人会不会及时拿走，你能

不能在对方动手之前抢回来，那就是另外的问题了。

这个和传统的账户模型是不一样的，你不可能说你的用户密码是你的财产，因为中心化账户是基于 KYC 的，你只要能证明自己的身份，身份证或者指纹或者长相，都可以找回你的财产，因为财产是和你绑定在一起，而不是你的账户，你的账户密码是可以修改的，即使泄露，别人也只能在短时间内拥有你账户的控制权，你把密码改掉，别人就没办法了。

私钥是不可能更改的，你能做的，就是及时把资产转移到另外的私钥。去中心化的世界有意区分了身份和数字身份的概念，增加了数字身份的主权，但同时也削弱了身份对数字身份的控制能力。

这里衍生出的问题就是，去中心化的资产安全吗？把钱拿在自己手里，比把钱存到银行，更加安全吗？考虑到比特币诞生的背景，是出于对中心化机构的不信任，才有了去中心化的理念。

想想吧！一开始就是没有中心化机构的，人们以物换物，打一开始，就是去中心化的世界。后来为了降低个人保护自己财产的成本，为了增加对坏人作恶更有力的惩罚机制，人们共同组建起中心化机构，保护大部分人的利益。

现在炒作去中心化的理念，不正是一种历史的倒退吗？去中心化并非新产生的事物，而是早就已经存在的、被人们选择性抛弃的东西。

不过现在的去中心化和以前的去中心化，最大的不同就是现在的技术手段更为先进，有可能做到之前做不到的事情，把世界推到一种新的愿景上。但是也要注意现在的技术不是那么先进，还远没有发展到那种程度，区块链的技术瓶颈非常多。

所以我的观点是，现在的去中心化理念不是中心化世界的演进，而是中心化世界的补充。在接下来的时间，中心化和去中心化会同时存在。

要注意的是，去中心化不等于 Web 3.0，Web 3.0 是 Web 2.0 的演进，因为版本号增加了。Web 3.0 将是中心化和去中心化同时存在的时代。

LUNA 归零

前段时间有一件搞笑的事情，有一天，LUNA 的价格早上还是 80 美元一个，晚上的时候就跌到 1 美元一个了。在接下来的三四天，LUNA 的价格从 1 美元，跌到了 0.00001 美元。几天之内，近万倍的跌幅。曾经号称前十的加密货币，突然归零了。

我粗浅的理解是，UST 有一个交易池，当短时间有大量卖出的时候，交易池会有小幅的倾斜。当时先是小幅的波动，然后随着社交媒体的传播，大量散户失去了对 UST 的信任，开始大幅卖出，越卖价格越低。Terra 团队是有 5 万个比特币作为储备的，当时也及时打进去想把平衡拉回来，结果比特币也在跌，质押进去的比特币在结算的时候已经不值预期那么多钱了，没能把价格拉回来，后来 Terra 团队也放弃了，任由价格下跌。

LUNA 的事情发生后不久，看到有的人讨论说，LUNA 还有机会吗？有一种机会是，Terra 团队还有 20 亿，等 UST 的价格跌到总市值小于 20 亿的时候，Terra 团队可以把市场上所有 UST 都买下来，销毁掉多余的 UST，只留 20 亿个，UST 的价格就可以回到 1 美元了。不过 Terra 团队可能没打算那么做，后来发行了新的 LUNA。

LUNA 的失败不意味着算法稳定币的失败，有的团队也在研发新的算法稳定币，据说是想把美联储的运行模式，用算法模拟出来，正在写白皮书。

在 Web 3.0 宏大的时代背景下，LUNA 的事情就算是先行的笑料吧。

Web5

最近新出一个 Web5 的概念，就是 Web 5.0 的意思。提出这个概念的人说，跳过 Web4 是因为 Web2 + Web3 = Web5。好家伙，不愧是 Web5，提出 Web5 的能是一般人吗？但凡对软件工程有了解的敢这么说？

简而言之，我的结论是，Web5 一定不会成功。不管它叫 Web5 还是 Web6、Web7，它的理念还是围绕去中心化、SSI 那一套，还在我理解的 Web 3.0 的范畴之内。如果认真了解过 DIDs 的理念，就知道现阶段所谓的 Web5 完全是噱头了。