除了以上这些，还有未来的新增或更改而引入的安全问题，我们经常说“安全是动态的、不是静态的”，指的就是这点。比如现在很多项目方都有安全审计及漂亮的安全审计报告，但如果认真阅读质量不错的报告就会发现，这些报告会说明清楚，什么时间范围安全审计了什么内容，内容的唯一标记是什么（比如链上开源验证后的地址或 GitHub 仓库的 commit 地址，再或者目标代码文件的哈希值）。所以报告是静态的，如果你发现目标项目有不符合报告里的描述内容，就可以指出。

NFT 安全

前面提的 DeFi 安全几乎内容都可以应用到 NFT 安全上，但 NFT 又有自己独特的安全点，比如：

- Metadata 安全
- 签名安全

Metadata 指的主要就是图片、动图等内容，关于 Metadata 的具体标准建议可以参考 OpenSea 出的：

> https://docs.opensea.io/docs/metadata-standards

这里可能带来的安全问题主要有两点：

- 一个是图片（或动图）所在的 URI 是不可信的，比如随便的中心化服务，一方面不稳定，另一方面项目方随便改图片都行，那么 NFT 的数字藏品能力也就没了。一般都会用 IPFS、Arweave 这些去中心化存储，并且用知名的 URI 网关服务。
- 另一个问题是可能造成隐私泄露，随便的 URI 是可以采集用户的基本隐私的（如 IP、User-Agent 等）。