Web3 5Degrees Protocol - Make all DApps socializing

一、 当前背景

2008年中本聪发布比特币的白皮书，标志着人类未来个人资产的所有权从不可信第三方转移到个人自身的开始;行业早期由于BTC等虚拟币与金融强相关的，行业早期充满了投机、炒作、诈骗、传销等行为;但是经过十多年的社会实验，行业的进步大家有目共睹，从早期个人台式机电脑挖矿，到后来开发专有矿机挖矿，到最终大家合力通过矿池挖矿然后按劳分配收益;以及随着以太坊主网的上线，ERC-20、ERC-721、ERC-1155等协议标准的确立，到ICO的兴起再破灭，到2020年的DEFI崛起，2021年的NFT、DAO、Web3.0[1]等概念崛起，持续对市场对年轻一代人进行资产、数据所有权的教育，让个体能更加重视资产所有权，数据的所有权的意义;行业每一步的发展都是在重塑人类价值网络底层的架构。

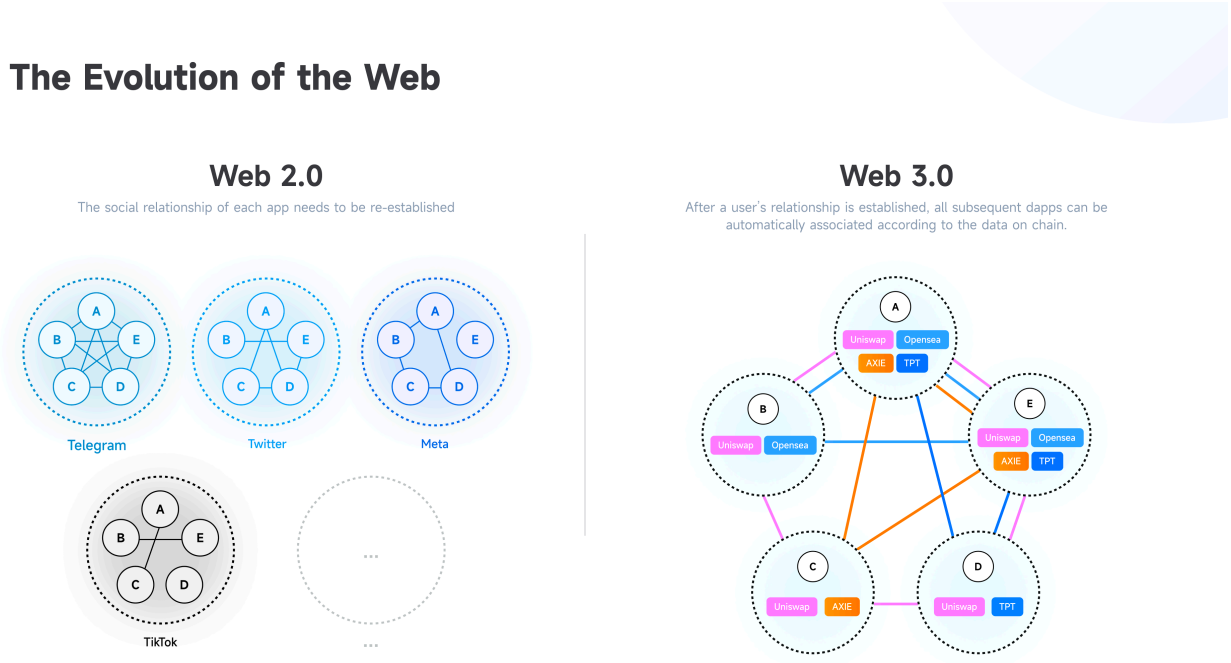
二、现状与思考

在互联网时代大家并没有形成一个统一的身份系统，用户在每个网站或者应用程序中都要重复一套个人的账号密码;每个产品都是孤立的账户信息，但随着现在数十亿人上网，它的缺点变得越来越明显，尽管他已经被证明是一套不安全，不便捷，不高效的方案。原生的互联网人都可能需要掌握70到80个账号密码，导致用户的体验急剧下降;当然也有一些有价值的互联网产品尝试帮人们更方便的管理他零散的账户信息，例如Okta、1Password和LastPass;最重要的是，用户实际上并不拥有他们的在线身份。相反，他们只是从公司和中心化实体那里租用使用权。因此，他们很容易面临数字身份被黑客攻击、操纵、审查或简单丢失的风险。

Web3.0[1]的出现，人们尝试通过构建ENS[2]、DAS这类对标互联网时代DNS协议的产品来解决目前大家遇到的统一身份问题;但是这套方案也有一定的局限性，它通过模仿互联网DNS模式来试图改革现有互联网的问题，并没有从互联网底层核心问题进行革新。试想如果做为一个社区因为推特某个功能对他们存在一定的偏见，导致整个群体不满，但是作为这个群体你又没有任何办法可以去反抗他们，因为你并不能简单的只是用类似ENS[2]这套统一的别名系统就可以轻松的切换到另一个平台;这里的核心问题是个人的身份系统并不是一个简单的别名系统;它应该包括个人名字的唯一性加上个人整个社会关系。所以你用ENS[2]这类别名系统看似是解决了一部分问题，但是并没有完全解决。那我们是否有更好的方案来解决这类问题呢，我想我们应该从更深层次去思Web3.0[1]给人类带来的是什么;Web2.0当前面临的困境是什么。

我们认为Web2.0面临的表象问题是恶意垄断问题，本质是因为数据所有权的问题，导致互联网整个生态的权利义务发生了严重的错位;一些本该属于个体用户的被平台牢牢地抓在手里，个体无法得到公平反对的权利，平台还可以无节制的利用这些本不属于平台的权力打压萌芽中竞品并进一步延长恶意垄断的周期或者直接让竞品死于萌芽，如果平台体量大到一定程度可能会导致大而倒不了的问题对社会产生一定地绑架。

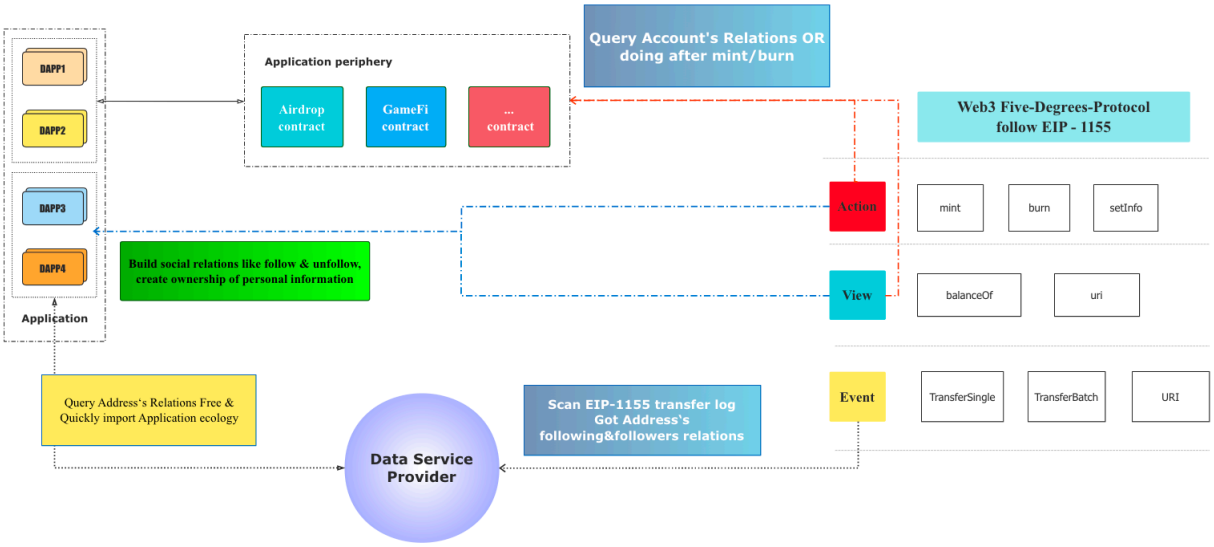
所以我们认为Web3.0[1]核心应该尝试解决Web2.0用户数据所有权问题，通过区块链技术将数据所有权还给用户，所有的DAPP在用户授权的情况下共享这套数据，既然用户数据所有权这个底层的机制发生了转移，上层的各种结构会翻天地覆的巨变自然不用多说。巨头无法利用本不属于自己的数据优势来恶意竞争，上层表像出来的也能解决当前互联网巨头恶意垄断问题，让市场主体回归到提高服务质量的正常竞争轨道。当然这块也跟当前各国政府打击垄断，提高数据要素的地位的政策不谋而合。



三、解决方案

针对前文描述的Web2.0当前面临的核心问题，我们提出给一个简单实体数据所有权协议，用协议将这些核心数据资产化;为了让协议足够易用、无需许以及可组合性，我们选择在现有ERC-1155[3]标准下来构建协议。兼容ERC-1155[3]标准的情况下可以非常简单的植入到Web3.0[1]的任何协议层或者是业务层，协议中产生的NFT可以在任意的NFT市场里面交易或者任何需要用户关系的智能合约可以链上确认用户关系，集成协议的应用只需要支持ERC-1155[3]标准即可快速支持本协议。

随着整个Web3.0[1]行业的发展，实体通过铸造目标NFT的方式构建一个个关系网络，从而形成一个巨大的透明的，统一的，无需许可的实体关系网络基础设施。所有的DAPP专注于业务，结合这套关系网络实现各种产品，比如可以在Uniswap里增加一个社交模块，让用户可以直观的知道自己关注的人交易的详细数据，或者可以在OpenSea上增加一个朋友圈模块，这样用户在OpenSea里能轻松地知道朋友圈在玩什么NFT并快速找到指定社群，类似将Twitter或者Discord很好的整合到OpenSea，再或者如果校内网使用了这套解决方案，在校内网挂了后用户在那里的好友关系你可以在Sandbox的校内元宇宙看到老同学们。



核心方法介绍

设置实体的相关信息:调用合约的setInfo方法即可设置当前实体相关信息。
获取实体的相关信息:调用合约的uri方法即可获取当前实体相关信息。
设置实体的反向关系数量上限:调用合约的increaseMaxSupply方法即可。
建立实体之间的正向关系:调用合约mint方法铸造被关注的实体的一个NFT，持有对方的NFT即表示实体之间建立了连接关系。
销毁实体之间的正向关系:调用合约burn方法销毁被关注的实体的一个NFT，销毁对方的NFT即表示实体之间建立了连接关系。
获取实体的正向关系列表:通过查询当前实体持有的这种NFT的列表既可。
获取实体的反向关系列表:通过查询那些地址持有当前实体的这个NFT的列表既可。

Web3 5Degrees协议

```
//This protocol follows ERC-1155 standard, EIP-1155 refers to: https://eips.ethereum.org/EIPS/eip-1155
[EIP]

pragma solidity >= 0.8.0;

import "@openzeppelin/contracts/token/ERC1155/IERC1155.sol";

interface IFiveDegrees is IERC1155 {

    struct TokenURIInfo {
        string name;
        string image;
        uint256 maxSupply;
        string properties;
    }

    event Mint(address indexed account, address indexed owner, uint256 tokenId);
    event MintBatch(address[] indexed accounts, address indexed owner, uint256[] tokenIds);
    event Burn(address indexed account, address indexed owner, uint256 tokenId);
    event BurnBatch(address[] indexed accounts, address indexed owner, uint256[] tokenIds);
    function setProtocolInfo(string memory name, string memory image, string memory properties) external;
    function uri(uint256 tokenId) external view returns (string memory);
    function baseInfo(address account) external view returns (string memory, string memory);
    function metrics(address account) external view returns (uint256 tokenSupply, uint256 totalBalance);
    function setPayProxy(address proxy) external;
    function setInfo(string memory name, string memory image, string memory properties) external;
    function increaseMaxSupply(uint newMax) external payable;
    function decreaseMaxSupply(uint256 newMax) external;
    function mint(address account) external;
    function mintByOrigin(address account) external;
    function mintBatch(address[] memory accounts) external;
    function mintBatchByOrigin(address[] memory accounts) external;
    function burn(address account) external;
    function burnOrigin(address account) external;
    function burnBatch(address[] memory accounts) external;
    function burnBatchByOrigin(address[] memory accounts) external;
}
```

引用

[1] Web3 [https://en.wikipedia.org/wiki/Web3]

[2] Decentralised naming for wallets, websites, & more [https://docs.ens.domains/ens-migration-february-2020/technical-description]

[3] EIP-1155: Multi Token Standard [https://eips.ethereum.org/EIPS/eip-1155]