

# C-Card 的去中心化身份实现

从上个世纪互联网应用出现开始，数字身份就伴随着互联网的发展而发展，数字身份可能是 Email 地址、IP 或者域名、QQ 号/微信号、网易游戏账号、Facebook 账号、Twitter 账号等等，通常由互联网应用的服务商提供，服务商不同，数字身份一般也不同。

## 传统数字身份的弊端

随着计算机科学技术以及互联网应用的蓬勃发展，越来越多的工作和生活线上化，人们越来越多的从物理世界向数字世界迁徙，以服务提供商为中心的账户管理方式也暴露出越来越多的弊端：

- 1.造成数据孤岛，数字身份从属于服务商，决定了用户要重复注册很多的账号和密码，每个用户都在不同的服务商上生产数据，且不同服务商上的数据并不互联互通，或者很难流通。
- 2.造成数据垄断，互联网巨头依靠平台效应垄断市场，利用用户数据作为护城河，产生大量价值，但用户对于自己的数据却没有话语权和价值分配，更甚的，还有平台发生大数据杀熟的现象。
- 3.数据隐私安全的问题，Facebook 就多次爆出了用户数据泄露的问题。日常生活中，各种数据泄露、收集以及买卖的行为防不胜防，损害用户的利益。
- 4.数字身份所有权问题，数字身份由服务商控制，用户租借使用，没有所有权，只有使用权，服务商可以决定账号禁用，服务终止等等。

## ComingChat 的去中心化数字身份解决方案:CID

为了解决这些问题，ComingChat 推出了去中心化数字身份 CID(即 Coming ID，下文

简称 CID)，CID 是一段 1-12 位的数字，存储于 MinixChain 链中，兼具 NFT 属性，且每个 CID 可以绑定附有数据，CID 及其附有数据可以在 MinixChain 链中交易流通。

CID 具有以下优势：

- 1.是去中心化，CID 存储在区块链上，避免了身份数据被单一的中心化机构所控制。
- 2.是所有权归属用户自己，数字身份自主可控，个人数字身份以及相关数据的所有权都归用户自己所有，用户可以选择自由交易。
- 3.是保护用户的隐私安全，用户不用再担心个人信息泄露的问题，只要不泄露个人私钥，数据就不会泄露。
- 4.是可信的数据交换，由于身份相关数据存储在区块链上，认证过程将不再依赖中心化的机构。
- 5.数据可互联互通，通过跨链等技术手段，用户的身份数据可以在不同区块链之间使用，避免了传统的在不同服务提供商注册多个账号的重复操作。

要了解更多详细的 CID 实现方案需先了解 MinixChain，MinixChain 是一个基于 Substrate 框架，采用 aura + grandpa 共识的开放联盟链，后续会通过 Spider 跨链协议衍生为 ChainX 的平行链。为了防止链上的 DDOS 攻击，将发行 Mini 积分，用作该联盟链的手续费。

用户注册 CID 即在 MinixChain 上发起一笔交易，待该笔交易在链上确认后，该 CID 正式产生，所有权归属于用户。

```
pub fn register(
    origin: OriginFor<T>,
    cid: Cid,
    recipient: <T::Lookup as StaticLookup>::Source,
) -> DispatchResult {
    match cid {...};
    ensure!(!Self::is_distributed(cid), Error::::DistributedCid);
    let recipient :&&? = T::Lookup::lookup(s: recipient)?;

    Distributed::::try_mutate_exists( key: cid, f: |details :&mut Option<CidDetails<<...>::Accountid>| {
        *details = Some(CidDetails {
            owner: recipient.clone(),
            bonds: Vec::new(),
        });
    });
}
```

用户向他人转移 CID 的过程也是发起一笔交易，同样，待该笔交易在链上确认后，该 CID 的所有权转移给了目标用户。

```
pub fn transfer(
    origin: OriginFor<T>,
    cid: Cid,
    recipient: <T::Lookup as StaticLookup>::Source,
) -> DispatchResult {
    match cid {...}
    let who :T = ensure_signed(o: origin)?;
    let recipient :&&? = T::Lookup::lookup(s: recipient)?;

    Distributed::::try_mutate_exists( key: cid, f: |details :&mut Option<CidDetails<<...>::Accountid>| {
        let mut detail :&mut CidDetails<<...>::Accountid> = details.as_mut().ok_or( err: Error::::DistributedCid);

        ensure!(detail.owner == who, Error::::RequireOwner);
    });
}
```

ComingChat 推出的 C-CARD 就是基于 CID 实现的，每张 C-CARD 的数据都与对应的唯一 CID 进行绑定，并且所有数据都是存储在区块链上，CID 是唯一的，因此 C-CARD 也是唯一的。C-CARD 包含的数据包括卡名、卡面、铭记、志号、水印等等，所有数据都是存储于链上，一经发行，不可篡改，且所有权归属于用户自己，用户可以自由交易。

C-CARD 示例：



## CID 相比其他去中心化数字身份的优势

目前市面上也有很多做去中心化数字身份(DID)的项目，比较有代表性的比如 Weldentity，百度 DID 等，这类 DID 解决方案有以下几个弊端：

1. 可读性极差,类似 `did:ethr:0xf96486a6b0b77ca91ac59da659358fd5ead16557` 这种标识符作为自己的 DID 身份非常难以记忆。
2. DID 只能存储于 DID 发行方的特定区块链中，不能跨链，或者难以跨链。
3. 这类 DID 解决方案并没有实际的产品和用户做支撑，只是停留在概念阶段或者内部阶段。

再来看下 ComingChat 推出的 CID 这种 DID 解决方案的优势：

1. CID 是一段 1-12 位的数字，类似 QQ 号，方便记忆，且用户可以通过参与社区共建、特殊贡献等方式获得稀有 CID，极具有纪念和收藏价值。
2. CID 基于 MinixChain 联盟链，随着加入联盟链的成员越来越多，CID 支持的服务提供商也会越来越多。
3. MinixChain 的底层是 Substrate，天然支持跨链，CID 后续将完成跨链功能，用户可以将 MinixChain 链上的 CID 跨链到其他区块链，从而使得拥有其他区块链的私钥的用户

也可以使用 CID。

4. 目前 ComingChat 已经有大约 6 万用户，并且用户数还在不断增长，说明 CID 已经经过了几万用户的实战检验，大部分用户都表示了对 CID 极其浓厚的兴趣，CID 的链上交易数也每天在增加。

5. CID 作为 ComingChat 的身份标识，用户使用 CID 就可以使用 ComingChat 提供的服务。

随着区块链技术的不断发展，相关生态体系不断完善，web3.0 时代正在加速到来，越来越多的 Dapp 将进入广大用户的生产和生活中，而致力于构建 web3.0 世界的我们，后续将在 ComingChat 实现智能小程序平台，对于个人用户和企业用户而言，使用 CID 就可以在平台上创建各类 Dapp 以及使用各类服务，CID 将成为 web3.0 世界的通行证！

快来注册专属于你的 CID，领取专属于你的 C-CARD，成为在 web3.0 时代真正拥有数字身份的人，畅享下一代价值互联网！