有两种用户，政府用户和普通用户。

普通用户有两种证件，身份证和护照。

身份证：

|  |  |  |
| --- | --- | --- |
| 参数 | 类型 | 字节大小(B) |
| 姓名 | char[] | 30 |
| 性别 | char[] | 1 |
| 民族 | char[] | 5 |
| 出生年月日 | date | 8 |
| 居住地址 | char[] | 70 |
| 身份证号 | char[] | 18 |
| 颁发机构 | char[] | 40 |
| 有效期起始日 | date | 8 |
| 有效期终止日 | date | 8 |
| 照片 | char[] | 358×441×3 |
| 证件编号 | char[] | 64 |
| 指针 | char[] | 64×3 |

有效期就是创建证件的时间，然后终止日就是根据出生年月日算年龄，十六岁以下五年，十六到二十五岁十年，二十五岁以上二十年（项目中写的统一十年了）

还有一个外键是用户的公钥。用户和两种证件是一对多关系。

护照：

|  |  |  |
| --- | --- | --- |
| 参数 | 类型 | 字节大小(B) |
| 姓名 | char[] | 30 |
| 性别 | char[] | 1 |
| 国籍 | char[] | 5 |
| 出生年月日 | date | 8 |
| 护照号码 | char[] | 18 |
| 颁发国家 | char[] | 8 |
| 颁发机构 | char[] | 40 |
| 有效期起始日 | date | 8 |
| 有效期终止日 | date | 8 |
| 照片 | char[] | 358×441×3 |
| 证件编号 | char[] | 64 |
| 指针 | char[] | 64×3 |

护照有效期就算十年吧。

证件编号相当于证件的主键。三个指针（起到指示作用，不是C的那个指针）分别是（以身份证为例，护照一个道理）：指向同一个人前一个身份证，未来可能存在的新身份证，和当时持有的最新护照。

指针的获取逻辑是：第一个证件由证件内容经过sha256得到，它指向前一个证件的指针设为全零，指向未来证件的指针是自己编号的sha256。第二个证件的编号是根据前一个证件的未来指针得到，它的指向前一个证件的指针内容是前一个证件的编号，未来指针是这个证件编号的sha256。然后如果当时没有另一个证件，它指向另一个证件的指针就为空。

**政府：**

政府这边只有一个用户，可以不写登录（只是模拟政府操作，不用太严谨），有一个固定的公钥作为标志，用来上传区块链用。

政府用户可以创建两种证件，身份证和护照，也可以创建新的普通用户。创建后会将数据存入mysql数据库。身份证和护照会根据其所有者的公钥加密之后上传到区块链。

政府页面的大概划分可以参考项目里的样子。

左侧功能栏选择主页面，操作身份证，操作护照。

主页面：

显示每一个普通用户的公钥（存在数据库里的）

可以添加普通用户（这部分是区块链，可以通过接口获得公私钥，你写一个方法名称在那里留着就行），将公私钥存入数据库。（目前项目里面用户只有公钥，想加个私钥属性，主键还是公钥，位数可能有变化）。有一个添加按钮，什么都不用输入就可以创建用户，创建成功后弹出窗口，显示公钥是什么，私钥是什么。

身份证：

一个表，可以显示每个有身份证的用户的公钥，后面接着一个按钮，可以点击查看该用户的身份证信息。点进去后显示该用户的所有身份证列表，显示一些主要信息，比如身份证的姓名，性别，身份证号，有效起止日这些。表的末尾有个按钮可以点击查看这张身份证的详细信息（即一个页面，显示出这个证件的所有属性，希望有点排版）。

在显示该用户所有身份证列表的那个页面，有个按钮可以点击添加身份证，点进去输入身份证的信息（有效期这种就是获得当前年月日），然后存入数据库（最好有一个弹窗，确认输入的信息）。还要用这个用户的公钥加密，上传区块链（上传区块链不用写）

护照：类比身份证，一样

政府页面右上角要有一个显示政府身份的文字。（我的项目前端里面有，可以参考板块样式，感觉颜色要改改，不知道怎么才能像一个正经管理系统）

**用户：**

用户不能访问本地的mysql，只能根据自己的公钥从区块链上获取数据，再根据私钥解密获得原始信息。（公私钥是webase区块链平台提供的）

左侧功能栏也可以选择身份证和护照。以身份证为例：

身份证页面也可以选择显示当前最新的身份证的详细信息（排版可以类比政府那边），和所有拥有过的身份证列表（根据外键获取）（列表样式也可以参考政府那边）。列表末尾也有一个详细信息的按钮，点进去可以看这个证件的所有属性信息。

用户页面右上角除了登出按键还要显示用户的公钥。