**患者隐私处理：**

患者数据上链之后会进行隐私化处理，采用**哈希算法**将患者的个人信息，既往病史和诊断记录进行隐私化，其中链上的数据只显示相关的**病历元数据模板**信息。患者也可以对自己隐私的数据开放给专业的医生或医疗机构。

**患者病历链：**

患者病历链用于存储患者院外数据、诊疗数据、化验数据、影像数据等。

1. **数据结构：**

1）每一个患者都有唯一的**元数据，**元数据可以包括（由患者身份证号生成的唯一ID，患者年龄范围，患者性别，患者病种，患者的地域范围。

2）数据病历模板（病历模板编号，病例模板结构），

3）模板病例数据（患者唯一ID，模板病例编号，病例数据）。

1. **数据业务：**

1）患者生成：患者通过进入医院扫描码，填写基本信息后，生成患者公钥+私钥。基本信息填写完毕后，出块节点会将此数据标记为某患者初始病例数据打包到区块中。

2）费用：创建数据需给平台支付代币费用，通过代币费用能避免垃圾数据上传。

3）数据提交：医生可以使用某个表单请求患者提交数据，每次数据请求需要给平台支付代币费用，这笔费用主要是给患者提供。

4）模板：医生可以通过平台发布模板，模板的主要作用为患者填写数据的表单项，表单的创建是无需花费任何费用，而且此时的表单，也无需上链。

5）数据上链：医生请求患者的表单，患者数据。

6）费用：为了平台能够安全稳定，凡事节点中的帐户需要支付相关费用，这些费用主要用于请求数据，请求医疗服务等。

7）病历链包含了数据：交易双方公钥地址、交易费用数目、交易内容（元数据、模板、原始数据、医疗服务请求等）。

**数据影像中心：**

MCL链平台准备利用IPFS建立分布式医疗数据影像存储。

**帐户：**

1. **患者帐户：**扫描医院的二维码，患者填写个人基本信息，姓名、出生日期、年龄、性别、病种、地址。信息填写完毕后提交，提交后生成患者帐户的公钥+私钥，医疗端接收到提交信息，医生帐户进行审核，审核完毕后会给与费用奖励。

**患者帐户信息：**帐户名称，帐户地址（此地址也就是帐户的公钥，公钥地址应有患者身份证号生成，用于确定其唯一性），帐户费用余额，患者联系方式。

**患者数据保存：**患者数据上链之后，个人的病例数据也要保存在本地，一是方便查看个人病例，二是能够进行病例信息的授权。

**患者的私钥存储：**患者的私钥数据应保存在本地客户端数据库中。

1. **医生帐户：**医生帐户是存在医院的节点上的，医院的节点是作为我们联盟链接最关键的一环，节点的作用主要作为将各种交易打包出块。医生的帐户在节点服务器中生成，因此每个参与的医院都需要部署一个服务器作为联盟节点。医生帐户的生成规则，医生需要填写，身份证号ID，手机号。系统会根据医生的身份证号生成公钥+私钥。帐户内容包括（帐户名称，帐户地址，帐户余额，联系方式），其实医生帐户和患者帐户基本上一致。

**注意：医生帐户和患者帐户本质上是一致的，唯一区别是在业务流程上有区分。在某些情况下医生帐户有可能变为患者帐户，同理患者帐户也可以变更为医生帐户。**

1. **帐户数据存储：**

帐户信息分为两种存储方式，1）存储到中心化的管理平台，2）存储到本地客户端。

1. 中心化的存储：主要存的是登录账号，以及登录账号的密码以及私钥信息。
2. 本地存储：将登录账号信息，登录密码，以及私钥信息等，以Berkeley DB的形式存储（仅限于PC端）。移动端App以文件的形式存储。

**病历链生成：**

1. **交易：**

数据交易要分为两种，一个是第一次需要患者的元数据，第二个是病历记录信息。元数据并不是用医生创建，而是是由患者自己填写信息，由医生审核，通过审核则需要给患者一定的tocken。病历记录的数据信息，需要医生主动给患者发起，每个发起求需要同tocken支付，否则无法创建。

数据交易的格式为：（交易双方帐户地址、数据类型（元数据、病例数据）、模板结构、数据内容、交易时间戳、交易数额）。

1. **出块：**

共识结构主要采用的是PBFT，采用主从节点配置，出块是由主节点完成，默认的出块时间为60分钟之内，将60分钟范围内经过验证的数据交易打包到区块中。打包到区块中后各个从节点进行数据块的同步。

1. **激励机制：**

系统提供了1，000，000，000个tocken积分，tocken分配必须按照一定的机制完成。

* 出块的奖励机制
* 提交数据的奖励机制
* 交易验证的奖励机制

1. **索引：**

交易索引主要展示交易数据交易记录，索引数据的存储采用Level DB，主要存储交易帐户信息，所在的区块，交易类型，交易时间，交易积分值。

1. **元数据：**

系统能够展示患者的基本元数据信息，元数据展示的内容（患者公钥地址、年龄范围、地址区域、病种类型、生成数据节点、生成数据帐户）

**节点管理：**

1. **CA证书：**

系统通过CA+PBFT共识机制来分配证书，通过CA证书分配，能够实现动态PBFT节点。