区块链与电子病历系统设计文档

目 录

[1. 概述 2](#_Toc520207642)

[2. 电子病历的特点 2](#_Toc520207643)

[3. 基于区块链的电子病历结构设计 3](#_Toc520207644)

[3.1. 可授权电子病历结构设计 3](#_Toc520207645)

[3.2. 区块结构设计 3](#_Toc520207646)

[4. 业务功能 3](#_Toc520207647)

[4.1. 用户管理流程 3](#_Toc520207648)

[4.2. 授权流程 3](#_Toc520207649)

[5. 问题与挑战 3](#_Toc520207650)

# 概述

本文档主要探讨基于区块链的电子病历医疗系统的可行性及必要性。包括区块链的特点、适用场景以及电子病历系统初步设计。面向的读者为有一定计算机、数据库基础知识的技术人员。

# 电子病历的特点

电子病历归病人所有，病人可将电子病历赠与医院使用。数据不可修改，只可更新，即写新版本。

# 基于区块链的电子病历结构设计

## 可授权电子病历结构设计



本文提出的用于电子病历的结构如上图所示，该电子病历的结构可以同时用于诊疗数据的产生和病人对数据的授权。各个字段的解释如下：

|  |  |
| --- | --- |
| 字段名称 | 说明 |
| 写入者ID | 写入电子病历的用户ID，当时医生诊断病人时，写入者为医生；当病人授权医生（医院）时，写入者为病人 |
| 拥有者ID | 拥有数据的用户ID，当医生诊断病人是，拥有者为病人；当病人授权时，拥有者为医生（医院）。 |
| 安全等级 | 指示接下来的数据内容安全性，分为明文数据、脱敏数据和加密数据类型 |
| 数据类型 | 指示接下来的数据类型，如门诊数据，用药数据、体检数据、住院数据等 |
| 诊断内容 | 电子病历核心数据 |
| 签名 | 对[写入者、拥有者、安全等级、数据类型、诊断内容]的签名 |

## 区块结构设计



# 业务功能

## 用户管理流程

## 授权流程

在医疗系统中，电子病历的核心数据理应为病人所拥有，若未经病人允许，医生和医院不应当有权限读取数据内容。在我们的系统中，用户可以允许数据以三种方式保存：

1. 明文存储:

在明文存储模式下，电子病历中的核心数据以明文的方式存储。

2. 密文存储

在密文存储模式下，电子病历中的核心数据以密文的方式存储。

3. 脱敏处理

在脱敏存储模式下，和病人标志有关的信息被加密存储，其他一般医疗诊断信息采用明文的方式存储。

病人是数据的拥有者，只有病人才有权利将自己的数据授权给其他用户读取，而被授权的人也只能拥有对数据的读取能力，无法再将数据授权给其他用户。因此在授权流程中，需要检查用户是否具有授权能力。

医院或者医生如果想看到病人的数据，则需要病人先授权。在密文存储模式下，假设病人A想要授权电子病历X给医生B，则授权的过程如下：

1. A获得电子病历X，并用自己的私钥解密得到真实电子病历。
2. 检查A是否有授权能力（如果没有源病历ID则有授权能力），如果没有授权能力则授权失败。
3. A获得B的公钥。
4. A重新产生一个电子病历，写入者为A，拥有者为B，源病历ID为X的ID，同时将真实数据用B的公钥加密，并写入新的电子病历。
5. 将电子病历发送到处理节点。

# 问题与挑战