



2018杭州·云栖大会

基于区块链 的病历服务系统

参赛队伍: Artificial Chain
2018.09.04

阿里云2018全球区块链大赛

我们是谁

Team: Artificial Chain

6

陶友贤 中国人民大学 系统架构、后台程序设计

吴龙影 哈尔滨工业大学深圳研究院 chaincode、小程序前端设计

赵守月 江南大学 Web端程序设计

张思宇 北京交通大学 产品原型、竞品分析、商业分析

张思航 昆明医科大学 病历顾问、应用分析

前言 / INTRODUCTION

首先感谢您在百忙之中审阅我。

当今时代，随着数字化医疗信息系统在全社会推广，电子病历已成为记录患者病情的主流载体。

虽然国内医院信息化建设在不断的发展完善，国外发达国家的先进水平相比还有很大差距，特别在人性化、精细化和标准化方面。尽管很多大型医院已经拥有了医护工作站、移动医护工作站、药房系统、全院PACS(Picture Archiving and Communication Systems 影像归档和通信系统)等系统，可以实现部分界面和工作流程的集成，但由于不在一个平台上，大量临床数据分散在不同的系统中，很难实现高效方便地获取患者信息系统。

建立一套覆盖整个行业的，且被认可的信息交换标准才能真正意义上的电子病历。

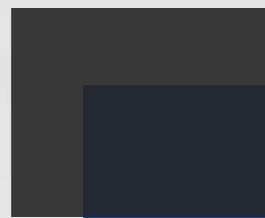
前言 / INTRODUCTION

电子病历的核心价值在于共享，病历的本质是医疗信息载体，信息才是最核心的部分，让信息流动起来，是电子共享的目标，也是信息化社会的共同趋势。

对于医生来说，由于具有数据化、信息化、方便化、详细化等特点。

对于患者来说，使用共享病历，不仅提高看病的准确性，而且可以避免很多重复检查，减少病人自付医疗的负担。

纵然电子病历的好处比比皆是，但病历共享仍然“在路上”。如何使患者信息在脱离数据库后仍然能够维持以个人为中心的结构并且随时可以获得，是我们目前思考的主要问题。



目 录

CONCENTS



商业概述



项目详解



创新点



方案架构图



项目演示



PART 01

商业概述

患者自述：



甲医院

三年前，我生了一场大病，在
甲城市的甲医院就诊，住了很
久的院。



在甲医院医生哥哥护士姐姐的
帮助下，可以出院啦！出院时，
甲医院给了我一份出院病历！



患者自述：



乙医院

昨日，身体突感不适，如今，我在乙城市，前往乙医院就诊。



医生询问之前详细的治疗内容，可没有带出院病历的我也忘了详细的诊疗过程（各种医学专业术语真的不记得...），该怎么办？



方 案

Plan A



缺点

- 1.患者治疗时间耽误
- 2.条件限制无法赶回家城市
- 3.来回奔波加重病情。

方 案

Plan B



缺点

- 1.一般医院不会发电子病历给病人，患者需要电子病历需带着病人的身份证到医院病案室调阅复印。
- 2.不是所有病历都能够复印 (<https://www.120ask.com/question/47766056.htm>)。

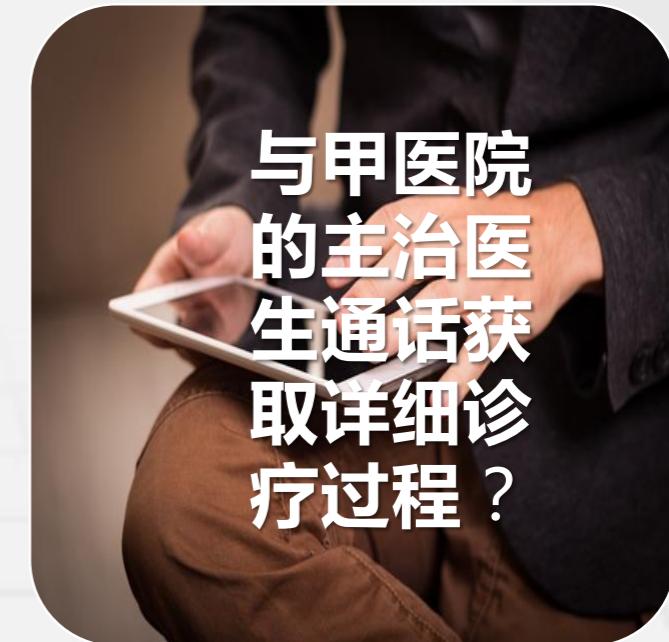
方 案

缺点

1. 医生时间有限（且通话有医患敏感性）
2. 病人因为知识差异听不明白
3. 通话容易遗漏很多关键信息。

Plan C

与甲医院的主治医生通话获取详细诊疗过程？



方 案

缺点

医生没有足够的信息，对某些急诊的病情的诊断和治疗产生延误治疗。

（比如病人近期脑卒中病史，但同时发作心肌梗塞时，就是介入和灌注就有相对的禁忌症。）

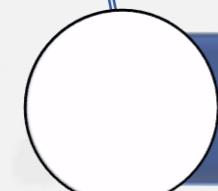
甚至——

直接无奈
告诉医生
丢失既往
就诊记录？

日常生活中，你是否遇到以下情况？



医院看病时，忘带或丢失纸质出院记录（病历）



医生无法确定患者是否将病史描述准确及完整



医患纠纷，医生和病人各执一词，难以决判

为什么？（痛点）



病人隐私无法保护



病历数据无法永久访问

病历可被篡改



医院信息系统标准不一
信息化建设程度差异
资源难整合



为什么？（痛点）



居民整体健康状况难掌握
各类疾病数据无法追踪

重复检查，浪费成本
病人医保双负担



急诊无法快速掌握
病史，无法做出最
准确的诊断和处理



基于区块链的病历服务系统

对患者

搭建资源获取平台
方便的病历保管，用户通过系统轻易访问
自己的信息，即时的病历获取与授权他人
查看



绝对的保密性

利用独特的区块链属性，以及内含
认证系统、保密系统、能够在处理敏
感信息时为用户提供强大保密技术

病历内容的不可变性与连续性

一旦记录，病人拥有无时限获取的权利
及医患双方均不可篡改病史内容

基于区块链的病历服务系统

对医院医生

搭建资源获取平台

详细病史的直接迅速获取
患者提供信息有据可循

节约时间资源

一定程度减少单个病患不必要的问诊时间，进行更切实的查体

降低医疗安全风险

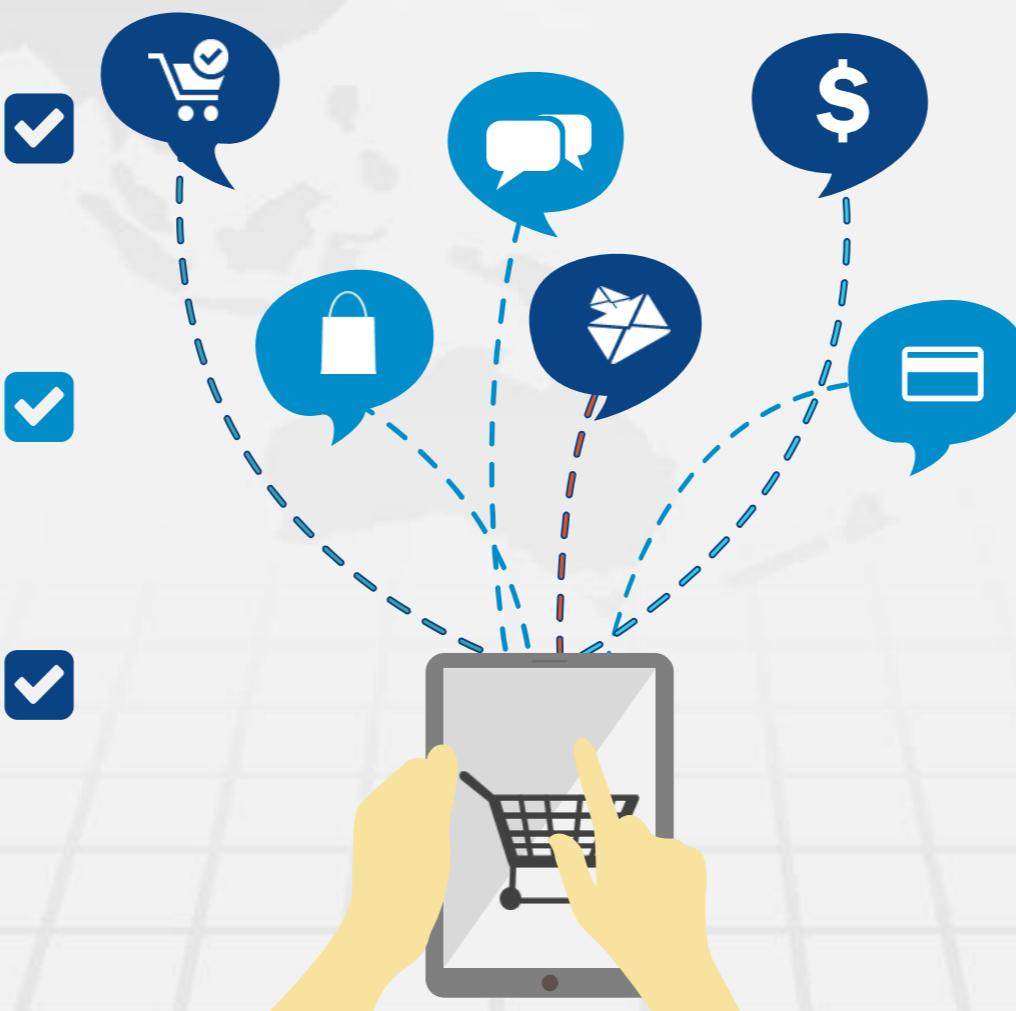
能更准确的下达诊断以及抢救的处理，不至于遗漏特殊病史，忽略禁忌症

资源整合平台

医生可以通过该平台，获取匿名的医疗数据，进行追踪和统计疾病、用药的纵横向比较

双向转诊更快捷

上级医院更快捷准确指导下级医院，病人不用集中在少数几个著名医院，既分解了病人庞大的流量，同时不用来回奔波也可以享受到优级医疗服务。



基于区块链的病历服务系统

对医疗行业



- 部分解决患者看病过程中的一些问题，为后续进一步解决打下基础
- 是医疗系统电子化、自动化、智能化、标准化实现的开端
- 医疗数据的大面积收集和统计，促进整个医疗事业的进步

我们的愿景



基础实现功能

1. 病历自由共享，区域（全国）一体化：作为统一数据格式的平台，保证网络健康安全的输送数据，病人可无限制获取自己信息，并分享给特定的对象查看。
2. 绝对隐私性：以特有的区块链技术解决现在的集成储存泄露的隐患，同时实现多份复制和永久保存。
3. 智能化应用：能缩短诊断所用时间，提高筛查的准确率，减少不必要的实验室检查等；能减少医疗差错和提高医疗质量

未来发展方向

目前实行患者对医生的一级，以后可考虑医院对医院的二级授权，便于医院间的授权信息分享，上级医院对下级医院的指导等

目前系统功能聚焦于病历共享与隐私保护，以后可进一步发展本系统功能，实现诸如智能提醒、医生预约等功能

随着本系统的使用，人们愈加能体会到病历共享和隐私保护的重要性。吸取本系统应用过程中的经验，可发展其他同样需要共享和隐私保护领域的相关系统建设

功能拓展

预约医生

可根据病人需求，推荐该科室最专业的医院及医生，并网上预约

生活广场

病人关注的话题讨论，病情讨论，心得交流，意见交换

数据统计

医生有权获得匿名医疗数据，支持循证医学和医学统计的发展



病情预测和分析

根据年龄性别职业等基本信息，提醒病人每年应当注意的体检项目

过敏病史

单独明显标识

提醒复诊和吃药

对病人的下次就诊时间提醒，每日用药时间提醒



PART 02

项目详解

技术背景



区块链技术

- 提供可信的去中心化存储，保证分布式的病历信息添加以及病历内容的不可变性
- 充分保护用户隐私
- 患者病历的授权可见

QUANJING.COM



技术背景



微信小程序

- 简单直观可操作，屏蔽区块链具体实现细节
- 二维码扫码查询保证了患者病历查询的一次性，再次保护病人隐私

QUANJING.COM

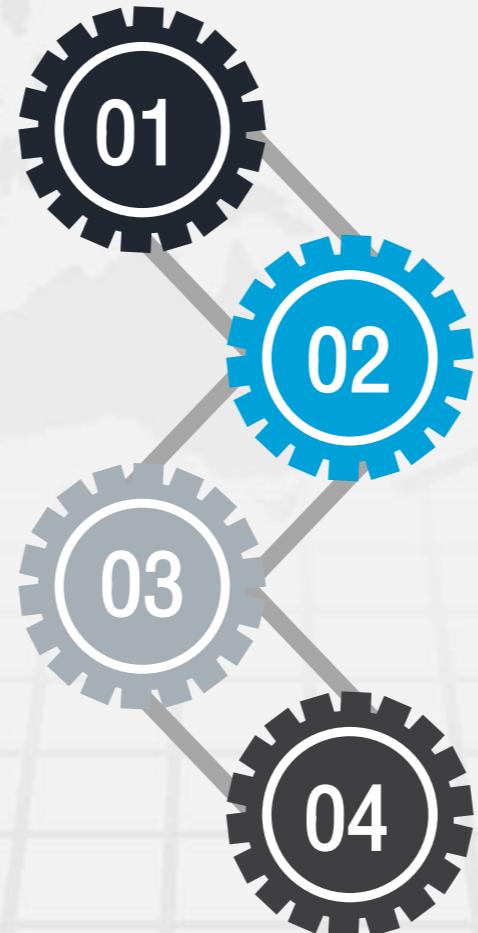


竞争优势

基于区块链的病历服务系统

- 1.实现了跨院的病历信息整合
- 2.医生可见患者全部病史
- 3.病历信息持久存储
- 4.患者病历信息的不可改变性与可信度得到保证
- 5.病历信息不易丢失

VS



医院电子病历共享调阅方式

- 1.由于各医院使用系统不同，跨院病历信息调用与整合是一个长期的过程。（北京市试点、健康云、丁香云管家）
- 2.部分病史不可见
- 3.可调阅的病历信息有时间限制
- 4.医院对患者病历信息具有绝对的控制权，有权限改变病历信息
- 5.病历信息中心化存储，存在丢失的风险

竞争优势

基于区块链的病历服务系统

6.面向患者，患者可在本系统查看自己的病历信息

7.逐步扩大功能的发展方向，目前先提供共享病历服务作为试点，后续再扩大功能

8.保留原医疗系统，本系统独立存在，执行过程中如发生意外对原医疗系统不会产生影响

9.利用差异性竞争优势

VS



医院电子病历共享调阅方式

6.主要面向医院，医院之间患者的信息的共享

7.逐步扩大规模的发展方向，现在试点医院实行较为完备的功能，后续逐渐扩大医院规模

8.对底层医疗架构进行改变，有利于改变当前医疗系统

差异性竞争优势



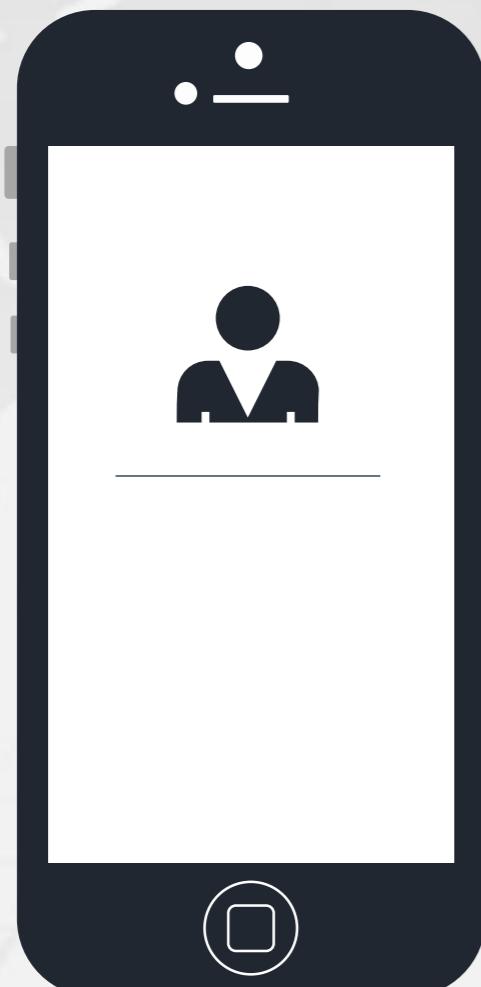
集中分布

目前的电子病历调阅式共享虽已成为医疗行业必然的趋势，但仍主要集中在[北京](#)、[上海](#)、[杭州](#)、[香港](#)等，数量较少并且模式功能单一（比如[北京30家试点](#)、[朝阳医院“健康云”](#)、[丁香云管家](#)），无任何一种模式可以实现全国一体化，大部分地区仍是一片空白。

差异性竞争优势



差异性竞争优势



独特的性能

区块链具有不可替代的优势，
1.录入信息的修改痕迹管理；
2.公钥私钥加密的绝对隐私性；
3.去中心化，任一节点权利与义务均等（节约时间成本）
4.开放性 匿名数据可以公开用于医学研究，循证医学，方便统计。

丢失程度

非常容易

纸质病历

容易

调阅式共享

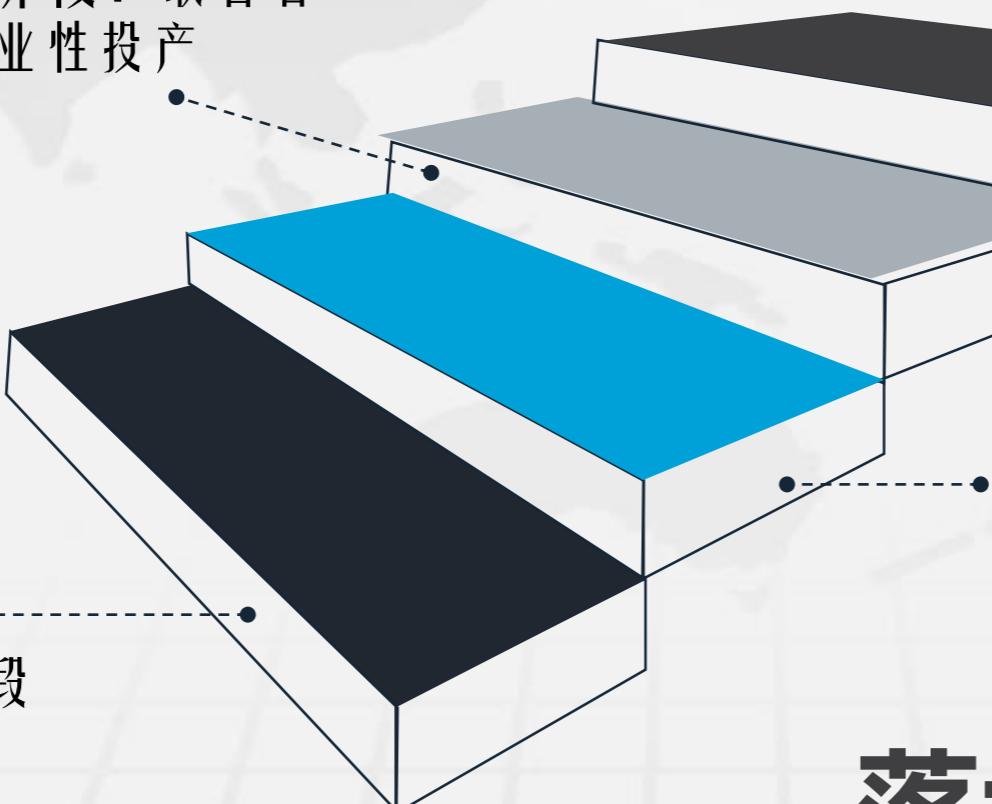
几乎不

区块链

第一阶段
开放决策：本阶段

第三阶段

开放后期阶段：联合各大行业、商业性投产



第二阶段
开发前期阶段：技术筹备、资金筹备、人员培训

第四阶段

开放反馈阶段：收集、整理新产品的市场信息

落地可行性分解

开发前期阶段——模式分析

和各大医院谈合作

医院数据端口输入病历

(需要医院支持)

病人手动输入

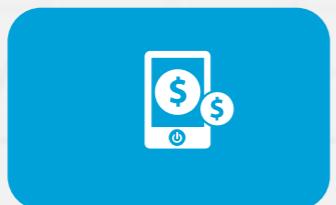
(存在输入误差)

注：本系统病历信息存储内容仅涉及病人基本信息、可获取的出院记录、医嘱、影像学检查结果单以及实验室检查结果单，不涉及病人不可获取的部分，保护医院及病人两方隐私，使双方对于信息内容都可接受

开发前期阶段——经费支持



争取风投企业的支持。本系统是区块链应用到实际生活中的一个重要案例，如获得成功，可为后续区块链的应用提供经验；同时，这是区块链应用到医疗行业的重要举措，后续医疗行业的应用可在本系统基础上发展；本系统对原有医疗系统几乎不产生影响，风险较小，同时发展前景良好、意义重大



争取政府的支持。本系统是解决患者就医的民生问题，出发点是便民利民，如能获得政府支持，可由政府拨出经费支持

开发后期阶段

战略

医疗行业

客户

合作伙伴

- 战略布局
- 重大合作
- 上下游资源连接

- 人才储备实力
- 政府、媒体背书
- 行业报告, 奖励合作
- 广告

- 行业数据报告
- 战略合作业务输出
- 大型合作伙伴合作

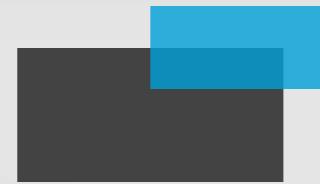
支持点

IT第三方服务未来生态
良性发展

互联网垂直应用到各行业

赋能合作伙伴

信息传递



开发反馈阶段



新产品开发的实践中，通过实验、鉴定，可以对新产品的决策方案不断地进行检验修改和完善

根据用户的意見和要求，进一步改进新产品，以便更好地打开市场营销路



PART 03

创新点

创新点

商业创新点

- 区块链技术于医疗行业的一次创新性应用，为后续持续地发展应用（医疗系统一体化、规范化等）奠定基础
- 为解决医疗等民生问题提供一种新的思路与方法，如“患者报销、医保异地结算”等问题，可以记录电子收据

技术创新点

- 区块链和微信小程序结合，简单易用，可传播性好
- 区块链和客户端加解密机制实现用户隐私的保护与可信机制



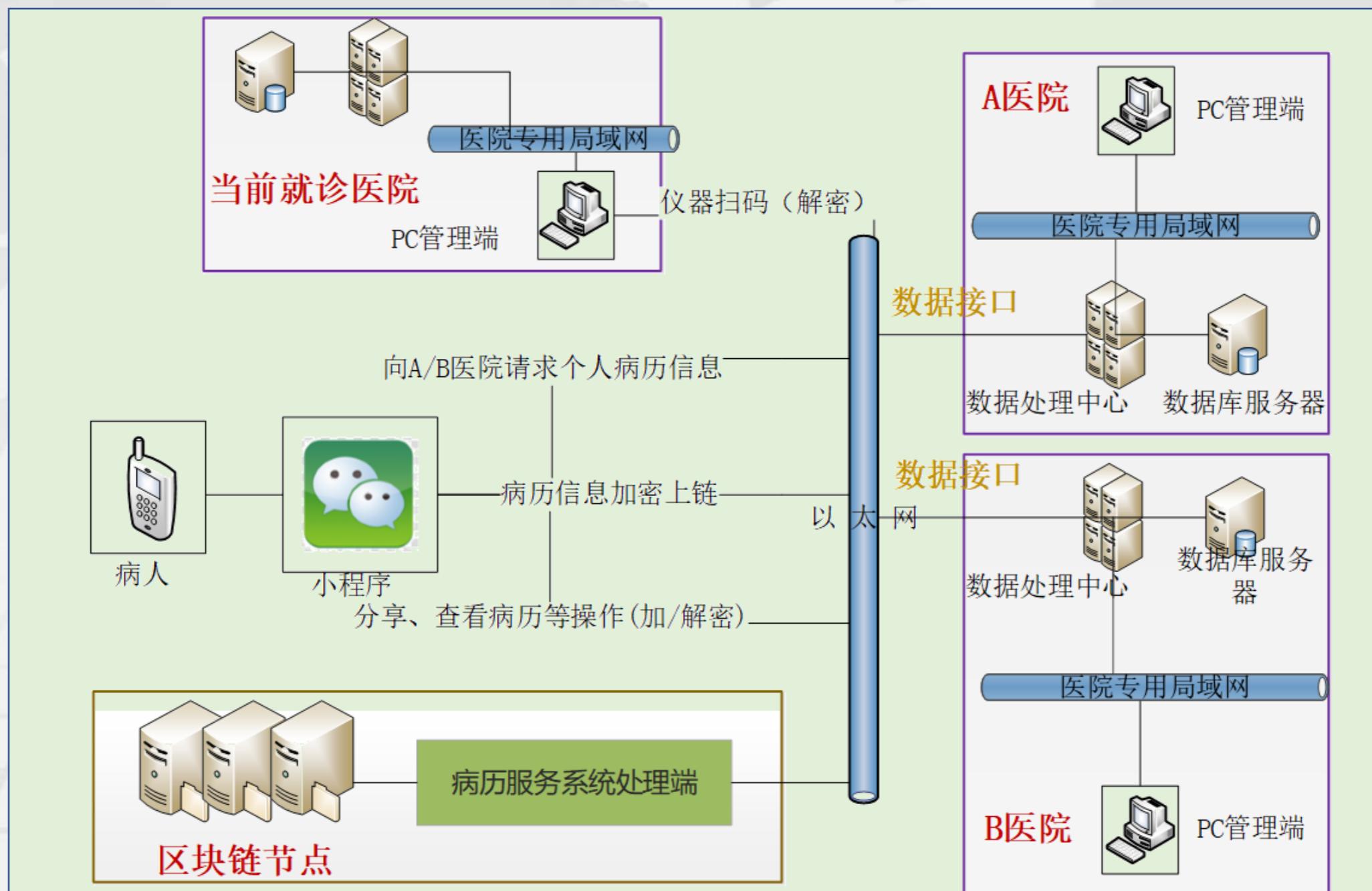
PART 04

方案架构图

方案架构图——整体布局



方案架构图——系统部署图



方案架构图——系统功能点

小程序入口



方案架构图——功能点技术路线

病历信息加密上链

01

- a. 用户登录后在客户端生成**RSA、AES两份秘钥**（保存在客户端）
- b. 从医院提供的接口查询出病历信息，将部分重要信息通过**AES对称秘钥加密**（连同不加密的用户公钥等个人信息），上链

02

医院扫码查看病历信息（解密）

病历码中是病人的AES对称秘钥和病人信息，便于通过查询到病人信息，直接用AES解密（**此处，展望通过硬件设备，查询出的电子病历信息可以显示在医院电脑上，便于入院做初始询问和记录**）；

备注：若为了保护病人对称秘钥起见，也可以通过病人的私钥加密，扫码后通过病人信息去获得病人公钥，从而解开对称秘钥

03

病历信息分享（加密）

病人可以将自己的既往病历分享给他人，a. 通过手机号搜索他人，b. 通过他人的公钥将自己的对称秘钥加密，并连同对称秘钥加密后的病历信息上传到链上。

方案架构图——功能点技术路线

04

查看分享病历信息（解密）

- a. 用户通过自己的手机号查询到被分享的列表
- b. 通过自己的私钥解开“被自己公钥”加密后的对称秘钥
- c. 用对称秘钥解开分享者的病历信息，得以查看

05

查看自己分享给他人的病历列表（解密）

- a. 用户通过自己的手机号查询到被分享的列表
- b. 通过自己的对称秘钥直接解开病历信息，得以查看

06

搜索链上用户、展示病历信息列表

直接根据key搜索链上数据

备注：本系统方案**基于区块链技术方式**进行实施，通过客户端将信息加密再上传至区块链，更好地保护了用户信息的隐私，且去中心化，后期将对加解密算法和其他流程方案进行思考。

方案架构图——加解密机制

01

RSA, 是公开密钥系统的代表，常用于签名和验签

特点：只需交换公钥；公/私钥机制，公钥加密，私钥解密；（或者私钥加密，公钥解密）；公钥负责加密，私钥负责解密；私钥负责签名，公钥负责验证。

02

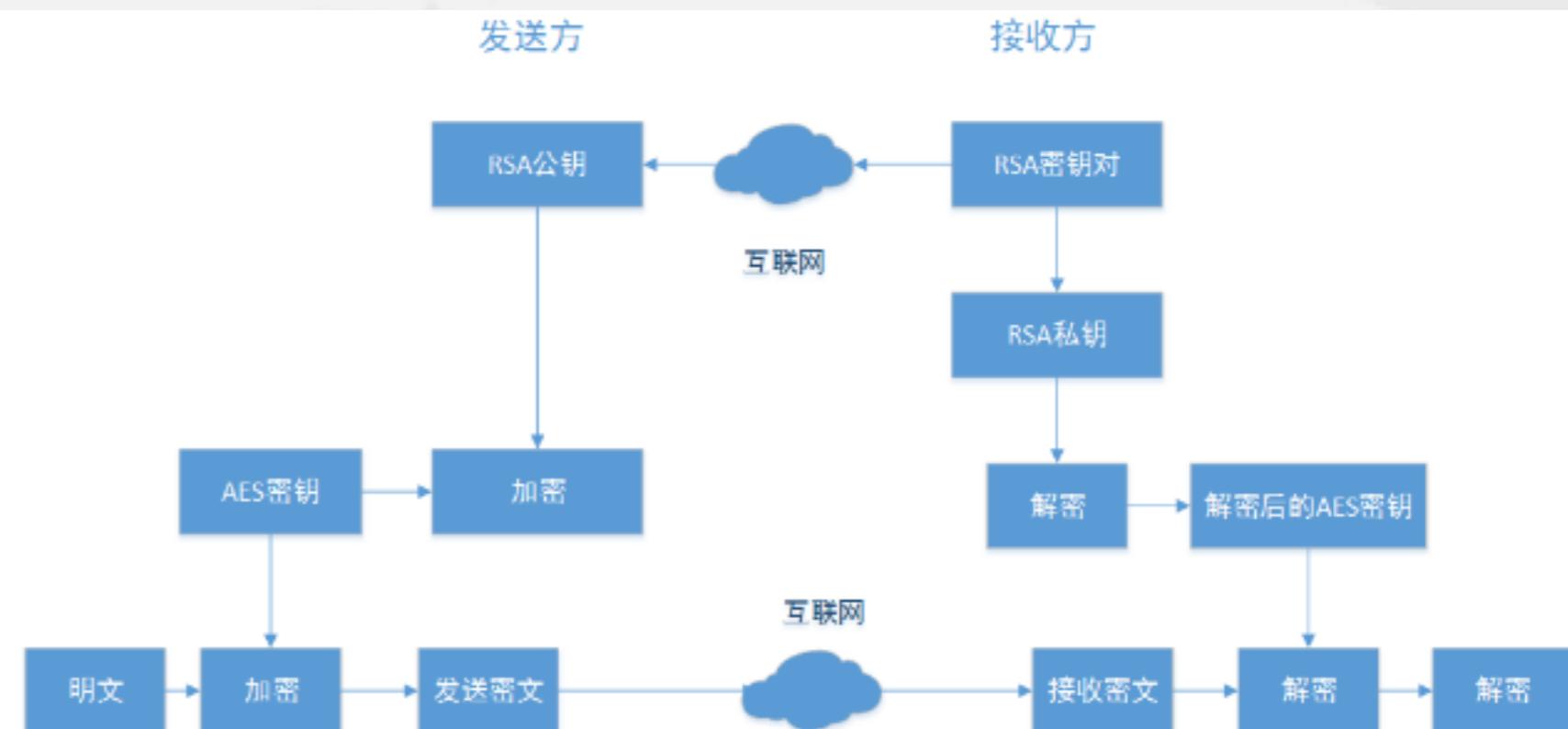
AES, 对称加密，密钥最长只有256个bit

特点：加解密用同一秘钥；执行速度快，效率高，易于硬件实现。由于是对称加密，密钥需要在传输前通讯双方获知。

03

AES+RSA=数据加密方

本系统是通过将AES用自己的私钥加密，再用对方的公钥解密，从而解开密文。





PART 05

项目演示

项目演示——医院管理平台

在线预览地址: <http://47.107.42.181:8080/ccweb/PcWeb/>

医疗病历服务管理平台

系统管理员
修改密码
退出登录

功能菜单

病人管理

病历管理

电子病历

在线测试

病人信息

姓名	李四	性别	男	出生日期	1965-08-03
联系方式	15061112861	证件号	340521199501013311	家庭住址	北京市海淀区XX大街Xx号
医保号	0001234	医保类型	城镇职工基本医疗保险	陈述者	患者妻子 可靠
主诉	患者1.5 h + 前因摔倒头痛、呕吐	是否有过敏史	青霉素过敏	是否有输血史	无
现病史	患者约1.5h+洗澡时摔倒，伴有头	既往史	患者为慢性阻塞性肺疾病患者，曾	个人史	嗜烟 1包/天，嗜酒
婚育史	已婚，1子1女	家族史	父母均有高血压、父亲曾是“哮喘”		
其他备注	暂无				

医院信息

医院代号	HDXX	医院名称	北京海淀XX医院	地址	北京海淀中关村大街XX号
住院号	HD00123456	登记号	000123456	科室	神经外科
入院时间	2016-03-01 14:25	出院时间	2016-03-28 15:57	住院周期	4周

入院诊断

1. 模拟医院电子病历的形成，可见附件中的“模拟电子病历”（已调研）

2. 医院愿意提供接口，病人在小程序端查询，并将数据信息上链（否则，病人填写信息等方案）

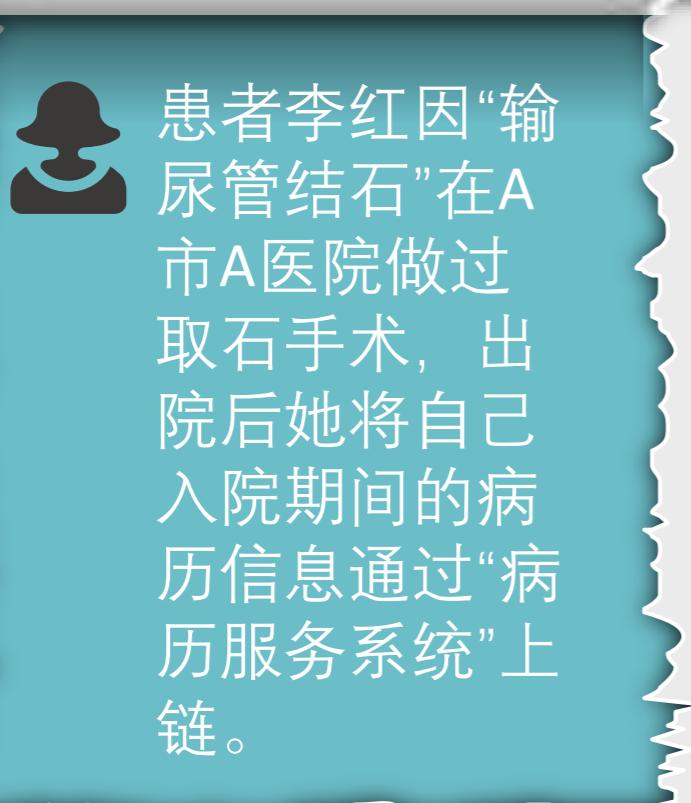
01

项目演示——小程序端

小程序入口



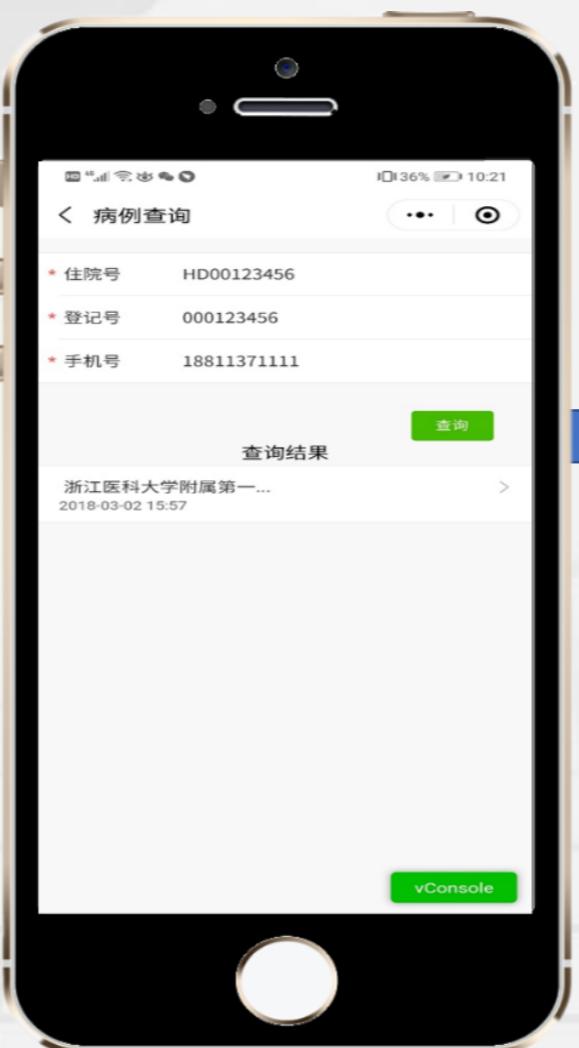
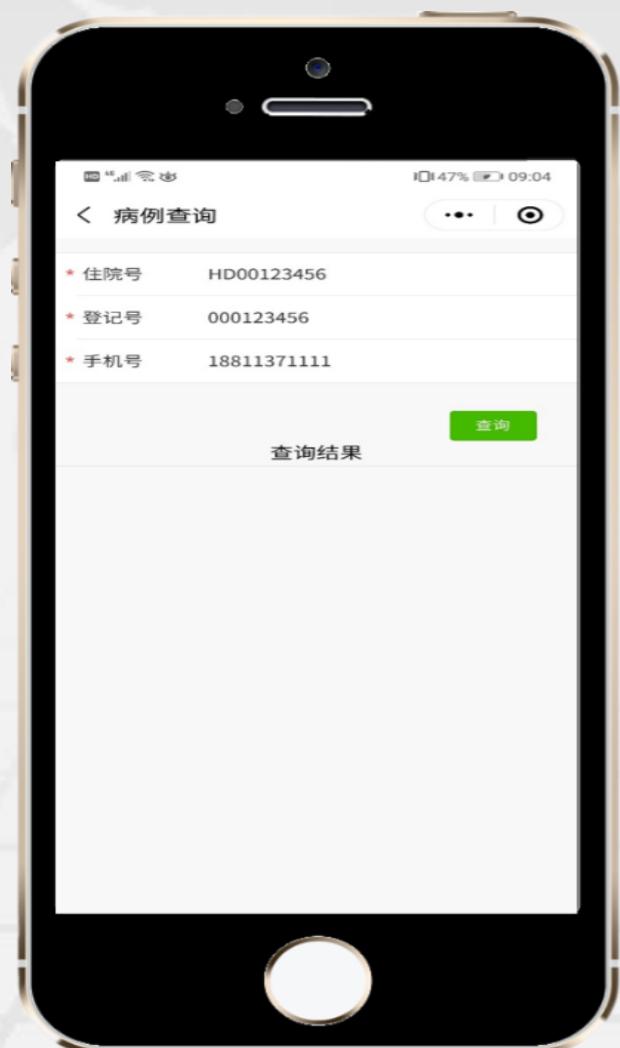
登记用户信息，
保存上链



01

项目演示——小程序端

点击顶部搜索，根据医院提供的接口查询本人在医院的病历信息，查询结果显示



查看病历最新信息，并上链



02

项目演示——小程序端



某日，李红在B市时旅游突感到剧烈刀割样腹痛，遂自行进入本市某医院就诊，之前从未到过B市。



医生开始询问，李红难以描述，就拿出手机，医生通过扫码，直接查看李红病史。

02

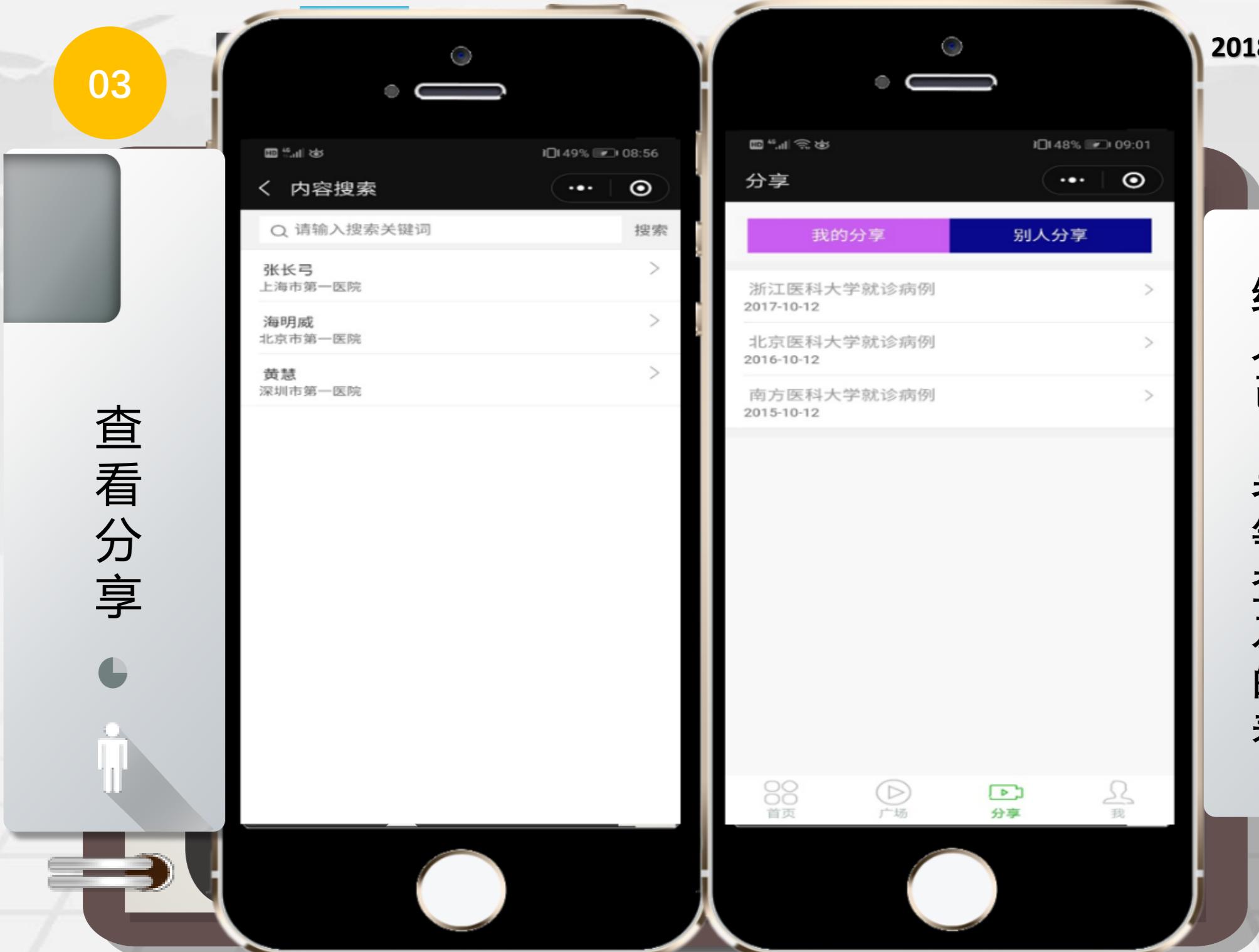
项目演示——小程序端

医院硬件



03

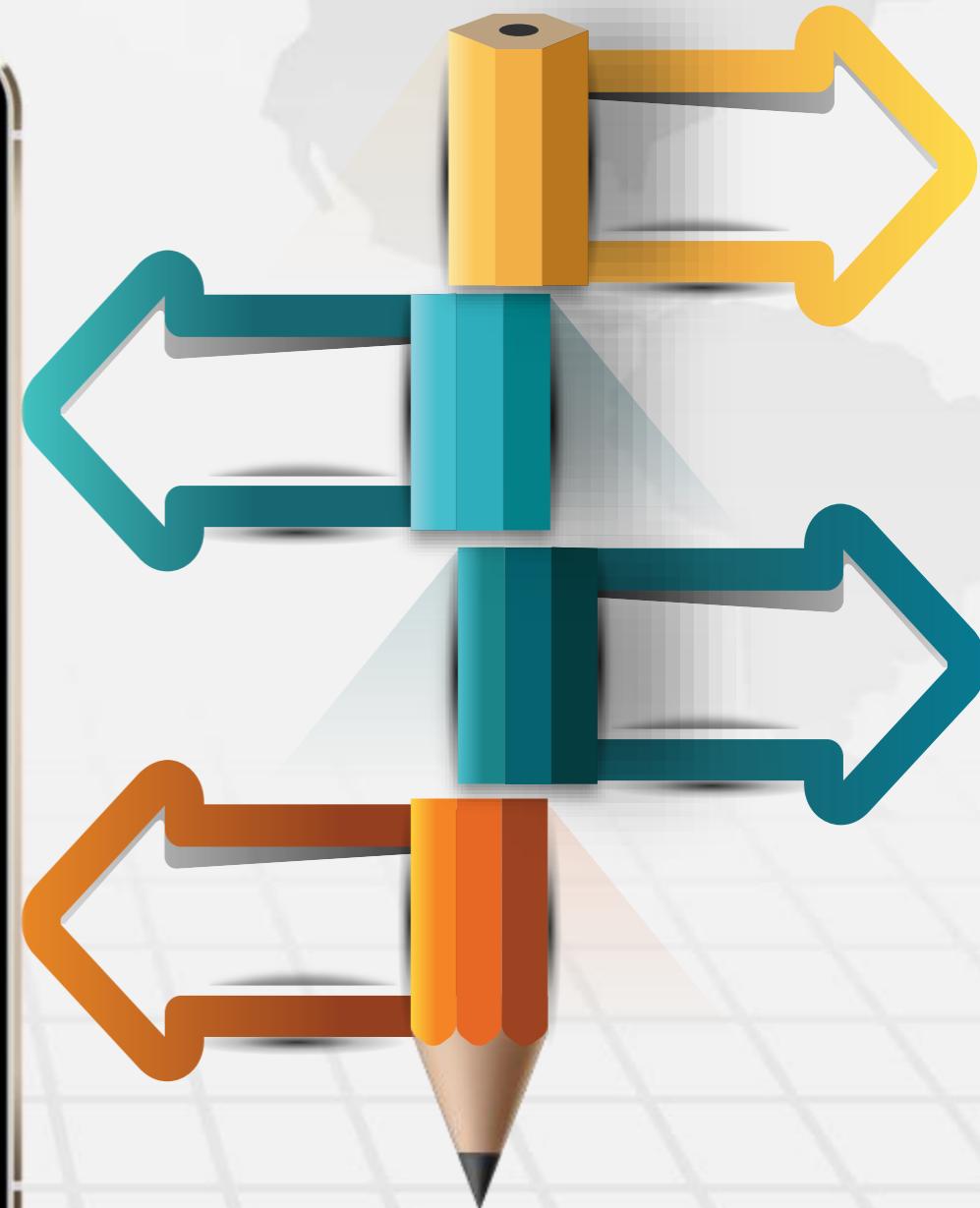
查看分享



给熟悉的人分享自己的病历
(朋友或者家人等)：
查看自己及被分享的病历列表

项目演示——小程序端

其他（生活广场：用于分享一些话题，后续计划更新；个人页面：个人查看个人信息、公私钥）：



谢谢聆听

参赛队伍: Artificial Chain
2018.09.04

阿里云2018全球区块链大赛

2018杭州·云栖大会