**项目计划书**

FACOS-ES：基于区块链隐私保护系统的自动化视力初筛平台

|  |  |
| --- | --- |
| 队长 | 蒋天宇 |
| 团队成员 | 侯灿坤、王文卓、陈柏熹 |

目录

[第一章 实践过程 1](#_Toc163646177)

[1.1 市场调研 1](#_Toc163646178)

[1.2 政策分析 2](#_Toc163646179)

[1.3 行业难点 3](#_Toc163646180)

[1.3.1趋势 3](#_Toc163646181)

[1.3.2痛点 3](#_Toc163646182)

[1.4 技术难点 4](#_Toc163646183)

[第二章 创新意义 4](#_Toc163646184)

[2.1 项目产品 4](#_Toc163646185)

[2.2 核心技术 5](#_Toc163646186)

[2.3.1 FACOS系统工作流程 5](#_Toc163646187)

[2.3.2拥有者上传协议算法实现 7](#_Toc163646188)

[2.3.3链下Storage BFT方案实现 8](#_Toc163646189)

[2.3 研发历程 10](#_Toc163646190)

[2.4 主要专利 11](#_Toc163646191)

[2.5 应用成效 11](#_Toc163646192)

[2.5.1测试平台 11](#_Toc163646193)

[2.5.2 测试数据 12](#_Toc163646194)

[2.6 竞品分析 13](#_Toc163646195)

[第三章 发展前景 13](#_Toc163646196)

[2.2 商业模式 13](#_Toc163646197)

[3.1.1 目标市场 13](#_Toc163646198)

[3.1.2 目标人群 13](#_Toc163646199)

[3.1.3 核心价值主张 14](#_Toc163646200)

[3.1.4 收入来源 14](#_Toc163646201)

[3.1.5 关键合作伙伴 14](#_Toc163646202)

[3.1.6 关键资源 14](#_Toc163646203)

[3.1.7 潜在挑战 14](#_Toc163646204)

[3.1.8 潜在机会 15](#_Toc163646205)

[2.3 客群容量 15](#_Toc163646206)

[2.4 营销模式 15](#_Toc163646207)

[2.5 财务预测 15](#_Toc163646208)

[3.5.1 收入预测 16](#_Toc163646209)

[2.6 发展规划 16](#_Toc163646210)

[2.7 融资计划 16](#_Toc163646211)

[第四章 团队协助 17](#_Toc163646212)

[4.1 创始团队 17](#_Toc163646213)

[4.2 执行团队 17](#_Toc163646214)

[4.3 组织架构 17](#_Toc163646215)

[4.4 顾问团队 18](#_Toc163646216)

[第五章 社会价值 18](#_Toc163646217)

[5.1 产业升级 18](#_Toc163646218)

[5.2 带动就业 18](#_Toc163646219)

[5.3 未来规划 19](#_Toc163646220)

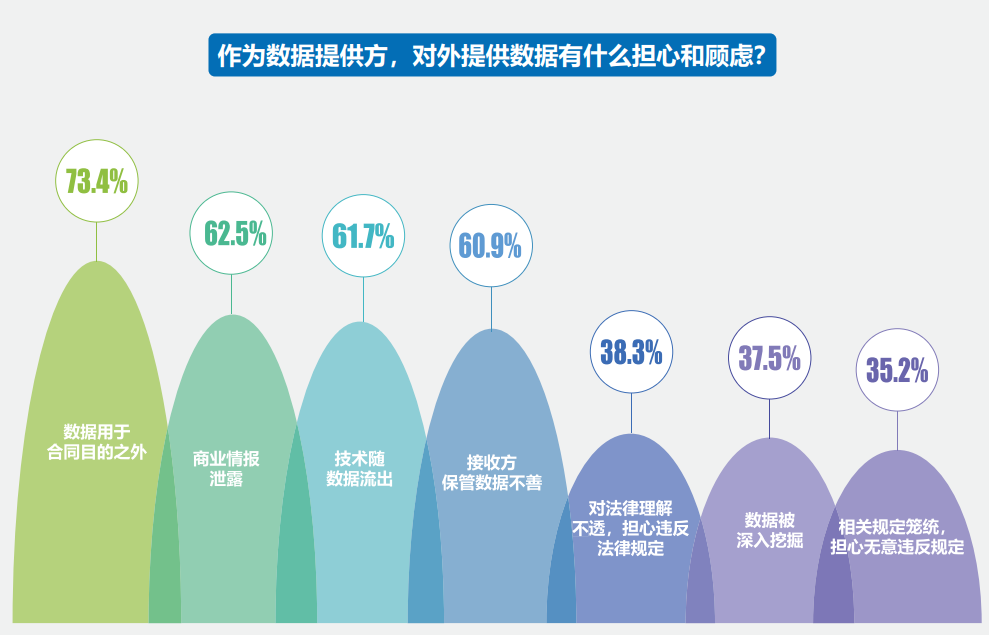
[5.4 风险对策 20](#_Toc163646221)

# 实践过程

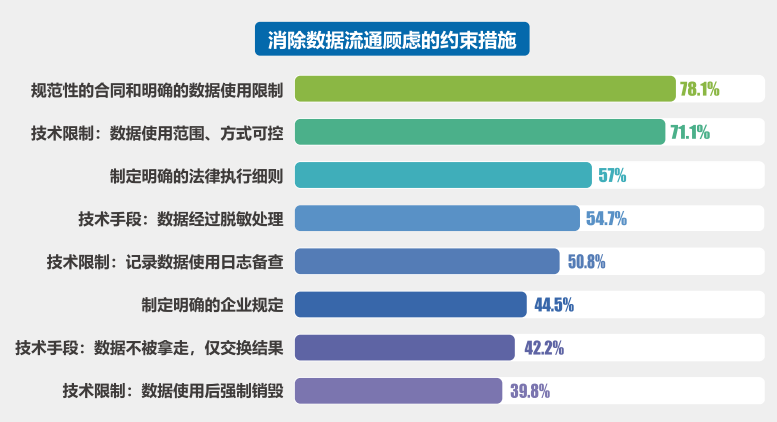
## 市场调研

根据MarketsandMarkets调研数据显示，2022年全球区块链市场规模达到74亿美元，到2027年，区块链市场规模将增长到940亿美元，年复合增长率将达到66%。市场观察，2023年区块链在能源领域为2.7亿美元、身份管理13亿美元以及医疗健康领域为8.2亿美元。

在当前快速发展的医疗领域，医疗信息系统扮演着至关重要的角色，它们为医疗机构提供了必要的工具和平台，用于管理患者数据、诊断结果、医疗记录等信息。然而，尽管医疗信息系统在不同医疗机构中得到了广泛应用，但仍然存在着一个普遍的问题：医疗信息系统之间缺乏互通性，医疗数据难以共享和获取。



这种缺乏互通性导致了医疗信息的碎片化和不完整性，患者的医疗数据可能分布在不同的医疗机构或医疗信息系统中，医生往往无法获取到完整的、全面的患者信息。这种情况不仅给医生的诊断和治疗带来了困难，也影响了医疗服务的质量和效率。



在现有的医疗信息系统中，医疗数据的共享通常受到技术标准、数据格式、安全性等诸多限制。医疗机构可能使用不同的信息系统、数据库或软件，这些系统之间缺乏标准化的接口和协议，使得医疗数据难以跨系统进行共享和交换。此外，由于涉及患者隐私和医疗机密等敏感信息，医疗数据的共享还需要满足严格的安全和隐私要求，这增加了医疗信息共享的难度。



因此，解决医疗信息系统之间缺乏互通性的问题，实现医疗数据的共享和获取，对于提高医疗服务的质量和效率具有重要意义。建立起统一的、标准化的医疗信息交换平台，促进不同医疗机构之间的数据互通和共享，将为医疗行业带来更大的便利和效益。区块链系统可用于患者数据的安全管理和共享，确保医疗数据的隐私性和完整性，促进医疗健康领域的数据互操作性和共享。我们开发了FACOS将解决以上问题。

## 实地调研

项目小队前往泉州市儿童医院进行实地调研。我们发现医院在眼科方面，每天的人流量都在200人以上，节假日更甚，这个意味着医生需要重复大量的普通的“视标法”进行视力检查。同时数据登记也存在一些问题，需要进行人工登记，并且无法进行数据流通，这意味着假如换另一家医院，则同样的操作需要重新进行，我们视为这些操作相当于一种冗余。同样的问题也普遍存在在一些中小学，因为这些学校会委托医院的眼科前往学校进行视力检查。

## 政策分析

2021年6月7日，工业和信息化部、中央网络安全和信息化委员会办公室发布的《关于加快推动区块链技术应用和产业发展的指导意见》中要求建立基于区块链技术的政务数据共享平台，促进政务数据跨部门、跨区域的共同维护和利用，在医疗健康等公共服务领域开展应用，促进业务协同办理，深化“一网通办”改革，为人民群众带来更好的政务服务体验。

2023年7月25日,国家卫健委等六部门印发深化医药卫生体制改革2023年下半年重点工作任务,明确提到要开展全国医疗卫生机构信息互通共享三年攻坚行动,推进“区块链+卫生健康”试点。

## 行业难点

## 1.4.1趋势

|  |  |
| --- | --- |
| 区块链服务（BaaS）市场已经进入技术深化、多行业渗透、场景应用为核心驱动的发展阶段 | |
| 技术持续迭代，性能提升、技术融合仍为核心 | 区块链性能决定着去中心化模式下的并发交易处理及效率,一直是厂商进行技术提升的焦点。在保证安全性的前提下，技术提供商不断进行共识算法、编译技术、大规模组网方向上的创新与能力，目前业界区块链TPS普遍达到10万级。 |
| 金融及政府核心行业增长减缓，制造及公共事业行业用户开始区块链部署 | IDC调研发现，政府和金融仍是在BaS产品投资的前两大行业但与此同时，制造业与公共事业（电力行业）在区块链平台的建设开始凸显。 |
| 政务从试水到加入顶层设计 | 政府对于区块链应用的发展已经不单单满足于政务方面的试水，将区块链技术加入整个政府或央行的顶层设计成为各国下一步研究的方向。其中一个成功的案例就是我们的数字人民币。截至2022年上半年，15个省市的试点地区通过数字人民币累计交易笔数大约是2.64亿笔，金额大约是830亿人民币，支持数字人民币支付的商户门店数量达到456.7万个。 |
| 区块链将在医疗健康行业发展 | 传统的医疗健康行业中仍然存在很多问题，例如看病难、看病贵，市场流通假冒伪劣医疗产品、医疗检查结果不互认、药品研发试验阶段样本不足等问题，这些问题的主要原因之一就是数据未能实现有效共享。区块链具有分布式记账和不可篡改的特点，可为数据确权和使用方式提供技术支持，这也是中共中央对区块链发展的指导思想——着重定位在其对产业的赋能和变革。 |

## 1.4.2痛点

|  |  |
| --- | --- |
| 中心化系统的效率和成本问题 | 传统的中心化系统通常需要大量的中介机构来进行数据验证、交易处理等，这不仅增加了操作成本，也导致了效率低下。 |
| 医疗信息孤岛 | 医疗信息系统之间缺乏互通性，医疗数据难以共享和获取。这导致了医疗信息的碎片化和不完整性，影响了医疗服务的质量和效率。 |
| 医疗数据安全问题 | 医疗数据的安全性和隐私保护仍然是一个挑战。医疗数据可能面临被窃取、篡改或滥用的风险，导致患者隐私泄露和信任危机。 |

## 技术难点

FACOS系统面临的技术难点包括医疗数据的隐私保护和安全共享。在医疗数据隐私保护方面，难点主要在于如何实现个人医疗数据的加密存储和传输，确保数据在共享的同时不泄露患者的身份信息。另外，如何设计匿名身份管理系统，确保医疗数据与个人身份之间的隔离和匿名化也是一大挑战。在安全共享方面，难点在于如何建立可信的数据共享机制，确保数据在多个医疗机构之间的安全传输和合法访问，同时防止数据被篡改或盗窃。解决这些技术难点需要综合运用加密算法、智能合约技术、身份认证技术等多种技术手段，同时兼顾用户体验和系统性能。

ES系统面临的技术难点包括计算机视觉对学生面部的扫描和身份的识别，同时在测试视力的过程中，我们需要对学生进行手势识别和准确地判断。同时我们需要遵循医院“视标法”的准确流程，并合理打包数据，并进行数据上链操作。

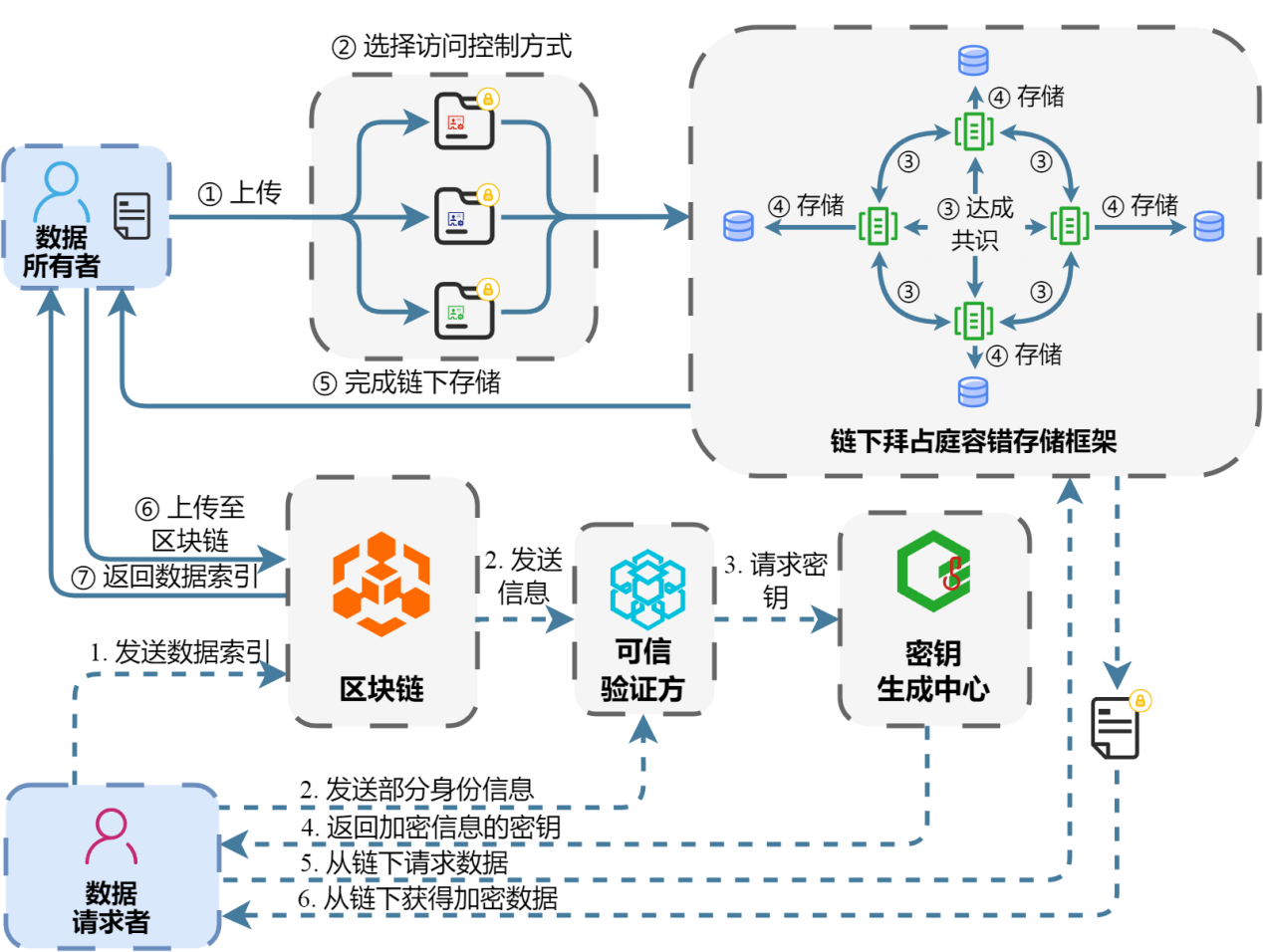
# 创新意义

## 项目产品

|  |  |
| --- | --- |
| 摘要 | 金融、政府和医疗保健等领域面对日益严峻的数据管理挑战。这些领域每天产生海量数据，包括金融交易、政府记录和医疗数据，而这些数据的敏感性要求安全存储、高效传输和便捷访问。现有的存储系统，普遍存在数据安全和隐私问题。同时，现在的“视标法”普遍存在需要大量人力且数据不流通或者无法保证数据隐私的问题。  我们的链上链下系统（**FACOS**），这个可以容忍 *f*（N >= 3*f* +1，N 为总节点，*f* 为可容错节点）个网络通信故障、抵抗恶意网络节点的任意破环，可以保障我们的存储系统在互联网环境下良好运行。本系统还设计了基于隐私保护控制下的访问控制协议，其中包含：混合加密，广播加密，属性加密等。通过隐私保护下的访问控制算法以及异步 BFT 容错协议，使得本系统更加健壮、可信以及安全。  我们的视力检测系统（**ES**），可以自动化进行用户管理，通过面部识别以身份的识别。同时，系统会自动判断用户是否佩戴眼镜，从而分别进行普通视力检测和矫正视力检测。同时根据算法进行手势识别，并依据“视标法”准确流程进行视力的初步筛查。 |
| 系统概要 | “链上链下系统” 是一种创新的复合系统，将区块链技术与异步BFT（拜占庭容错）共识算法相结合，旨在提供高度安全性和隐私性的数据存储与验证解决方案。这个系统通过将区块链的分散性、透明性和不可篡改性与异步 BFT 共识算法的高度安全性相融合，实现了数据的全面保护和可信性。  在链上（On-Chain）部分，区块链技术被用于存储和验证各种数据。这一部分利用区块链的去中心化特性，确保数据不受篡改，从而提供了高度可信的数据存储和传输机制。此部分强调隐私保护和访问控制协议，确保只有经过授权的用户才能访问数据。各种应用密码学方案被广泛应用，包括属性加密、广播加密和门限加密，以增强数据的隐私性和完整性。  链下（Off-Chain）部分采用了异步 BFT 共识算法，这是一种极为强大的共识机制，特别适用于对安全性和隐私性要求很高的场景。能够在异步网络环境下运行，无需担心消息到达的时间限制。这确保了数据能够安全传输，即使在不可预测的网络状况下也能保持系统的可靠性。系统还具备抵御分布式拒绝服务（DDOS）攻击的能力，确保系统在面对网络攻击时能够继续正常运行。  视力初筛系统（ES）是一个AI+混合系统可以在保证视力初步筛查的准确性的同时，也保证了筛查的效率，同时此系统也不需要或者需要很少的人力重复劳动的参与。面部识别部分用到了InsightFace技术，手势识别部分用到了Mediapipe技术。  链上链下系统不仅解决了数据的安全性和隐私性问题，还提供了高度可靠的分布式数据存储，即使在极端网络条件下也不会丢失数据。然而，系统面临算法时间复杂度较高的挑战，这可能会导致计算资源的浪费和系统效率下降。因此，未来的工作需要继续优化系统以提高性能和效率，同时维持其高度安全和隐私保护的特性。链上链下系统代表了区块链和密码学技术的创新应用，为数据安全性和隐私性提供了前景广阔的解决方案。 |
| 创新点 | FACOS系统的设计注重了客户端访问控制和安全存储，在提供个性化权限管理的同时，采用了异步拜占庭容错存储方案和可信执行环境验证器等关键技术。这种综合方法保障了数据安全、隐私保护，并且在应对数据存储和传输挑战方面展现了出色的有效性和可靠性。  ES系统的设计注重检测的精确性和效率，并且注重对过程的高度自动化，在效率方面相比较传统解决方案大大提高，同时大大节省了人力资源，在控制眼科医院人流量方面展现出非常乐观的一面。 |
| 关键词 | 区块链、隐私和安全、数据共享、容错、细粒度访问控制、面部识别、手势识别 |

## 核心技术

### 2.2.1 FACOS系统工作流程



#### 2.2.1.1 上传阶段

（1）数据拥有者输入数据*m*（**医疗数据**）。

（2）数据拥有者选择一种访问控制方法（广播加密、属性加密、门限加密），对 m 进行加密。

（3）数据拥有者将消息 *m* 的哈希 *h* 和 *m* 的密文 *c* 上传到链下 BFT 存储。

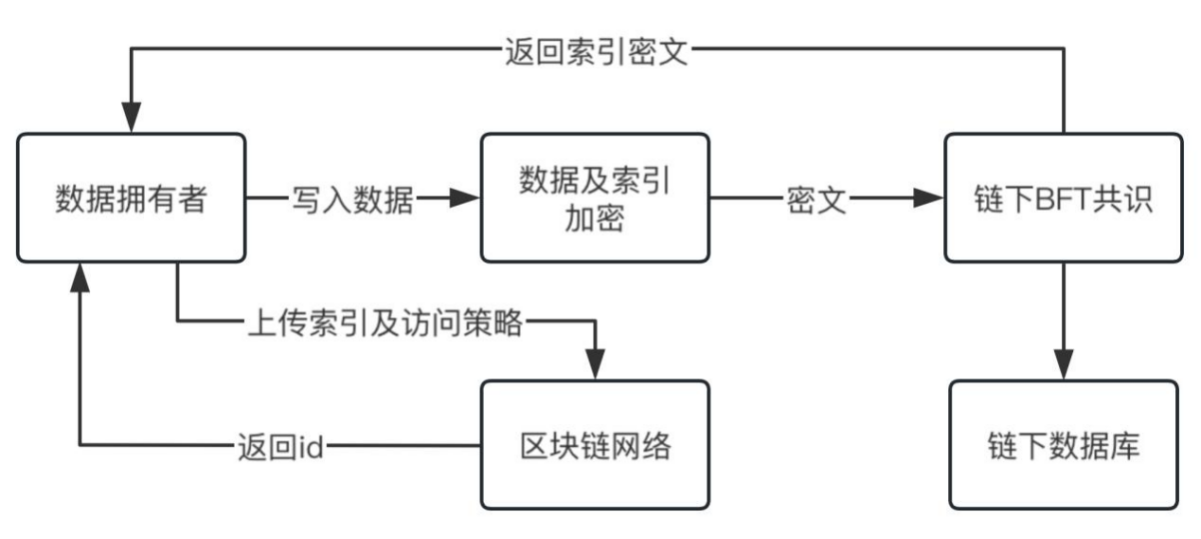
（4）BFT 存储副本对 *h* 和 *c* 达成共识。

（5）BFT 存储副本以键值格式（leveldb）存储 *h* 和 *c*。

（6）当链下阶段完成时，BFT 存储副本向数据拥有者返回“done”。

（7）当数据拥有者从链下 BFT 副本中收到足够数量的“done”回复时，数据拥有者将数据信息（访问控制类型、数据大小和策略密文等）和哈希值 *h* 的密文上传到区块链网络。

（8）在链上阶段完成后，区块链将 *id* 返回给数据拥有者。数据拥有者可以根据自己的意愿将 *id* 分享给一些数据请求者。



#### 2.2.1.2 下载阶段

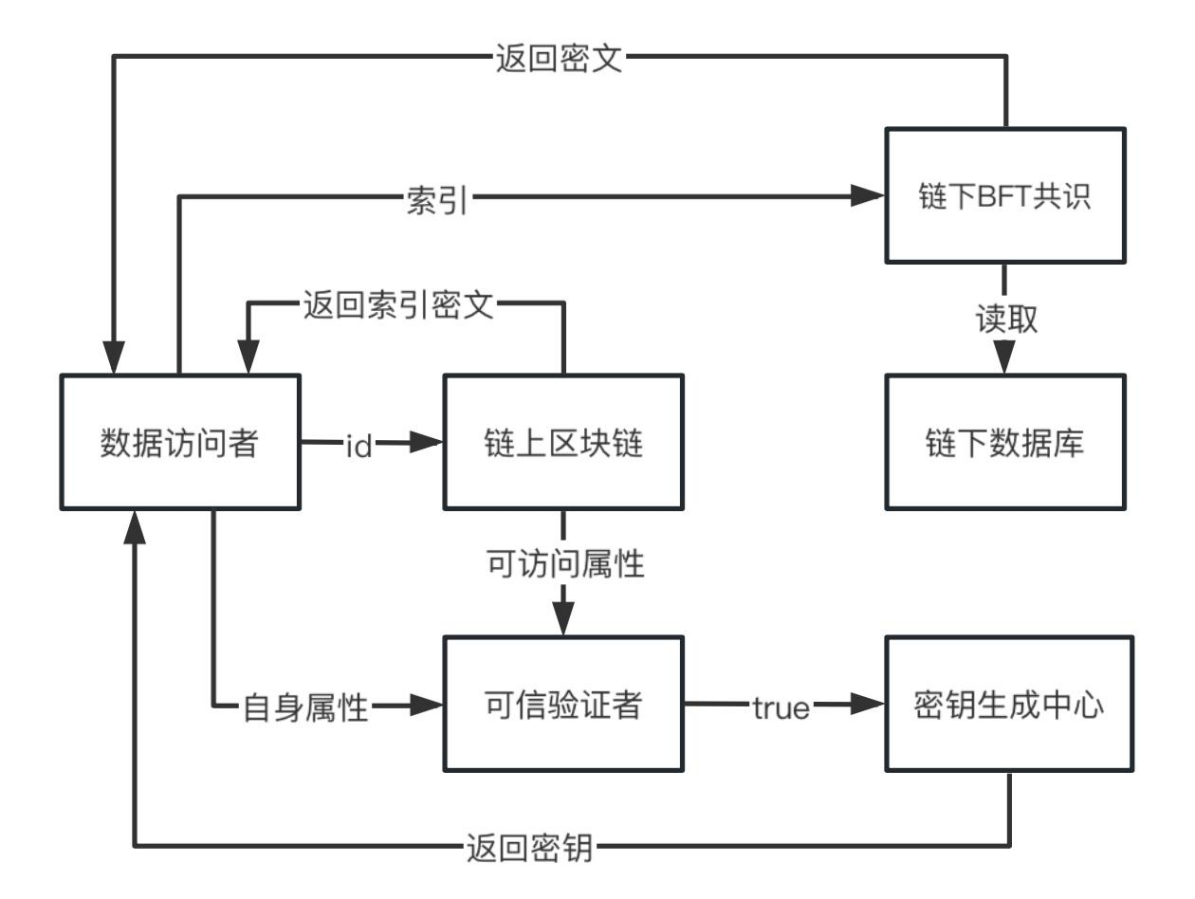
（1）数据请求者将数据拥有者共享的 *id* 发送给区块链。

（2）区块链网络将id索引的访问类型和策略密文发送给可信验证者。数据请求者还将自己的与自己对应的部分策略发送给可信验证者。

（3）可信验证者将部分策略与数据拥有者设置的策略进行满足后，数据请求者可以在步骤 4 中从密钥生成中心获取密钥。

（4）当数据请求者用从密钥生成中心接收到的密钥解密 *h* 后，将 *h* 发送到链下 BFT 存储。

（5）数据请求者可以从链下 BFT 副本中下载密文 *c*，并使用相应的访问控制方法最终获取医疗数据 *m*。



### 2.2.2拥有者上传协议算法实现



在协议中，数据所有者对消息 m 进行加密，并将(h，σ)发送到链外的 BFT存储。伪代码如图 9 所示，涵盖了从第 1 行到第 16 行的步骤。第 1-4 行初始化了数据所有者的消息缓冲区、消息属性列表、访问控制类型以及访问策略。

属性列表与访问策略不同，在一般情况下，访问控制列表可以用来生成访问策略。例如，属性列表是一个无序集合，如[男性，女性，年龄 > 60，30 岁 < 年龄 < 45 岁，医院，医生，专科医生，福建，中国，... ]，访问策略可以由上述列表生成，类似[((男性 ∩ (年龄 > 40) ∩ 医院 A) ∪ (女性 ∩ (35 岁 < 年龄 <45) ∩ 医院 B)) ∩ 福建 ∩ 中国 ∩ ... ]。

第 5-7 行，数据所有者生成其 PKABE 和 keyAES，并获取可信验证者的公钥 PKVerifier。加密阶段包含了第 8-16 行。数据所有者从其缓冲区中选择第一批消息 m。利用混合加密方法，消息 m 在第 10 行由 keyAES 使用 AES-CBC 算法加密，keyAES 在第 12 行由 PKABE 密钥使用 CPA-ABE 算法加密。第 13-14 行，哈希值 h 也通过 PKABE 使用 CPA-ABE 算法加密。第 15-16 行，数据所有者将密文 c 和 x 打包，并随机将(h，σ)发送到 BFT 存储副本。

### 2.2.3链下Storage BFT方案实现

Storage BFT 是一个基于异步 BFT（Honey badger BFT 共识算法）的存储系统，具有比一般存储系统更高的安全性和隐私性。即使部分节点出现故障或受到攻击，系统仍能保持数据的可靠性和完整性，在异步网络下，保证了消息最终能到达，没有到达时间的限制，可以有效的防御 DDOS（分布式拒绝服务）攻击。

Storage BFT 可以对用户的敏感数据进行加密，确保数据在存储和传输过程中得到保护。只有经过授权的用户才能解密和访问数据，从而保护用户的隐私不被未经授权的访问者获取。Storage BFT 提供安全的数据存储和传输机制，采用安全的通信通道和加密技术，防止数据被篡改、窃取或中间人攻击。用户可以放心地将敏感数据存储在系统中，并安全地传输数据。

#### 2.2.3.1准备

创建 N 个 buf [i]（FIFO 队列），buf [i]为第 i 个节的消息队列；创建一个PK（公钥）和 N 个 SKi（私钥），SKi 为第 i 个节点的私钥。

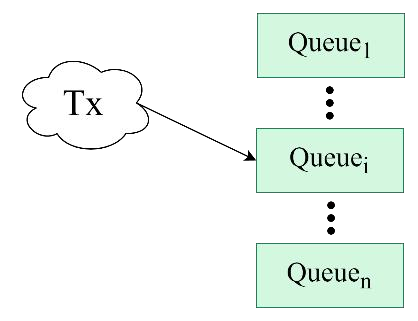
#### 2.2.3.2用户存入或读取数据

用户将存入或读取命令和使用广播加密或属性加密后的数据发送至随机个服务器中，服务器收到密文后，将将密文放入共识队列。

#### 2.2.3.3共识

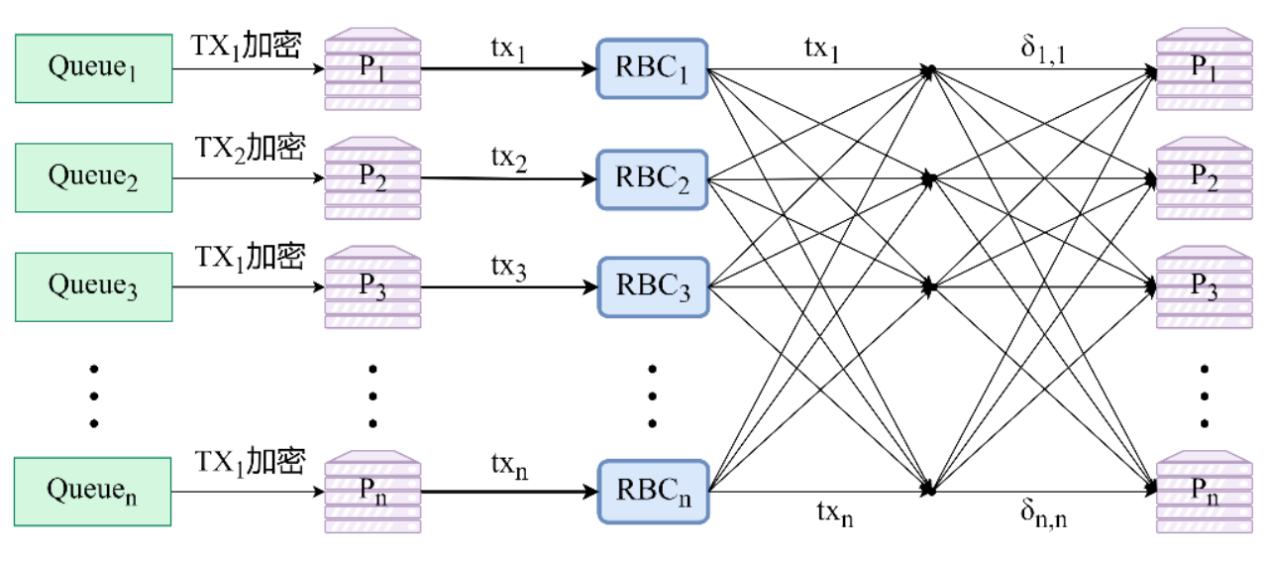
（1）选择数据

N 个节点从共识队列中随机选择 B/N 的数据，作为𝑡x输入。用Storage BFT算法选择数据。



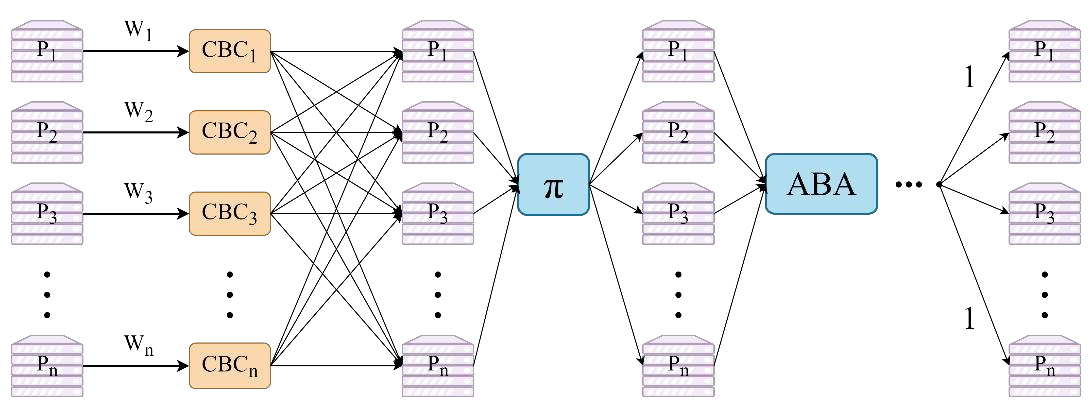
（2）PRBC阶段

将vi输入给RBCi 。使用纠删码将txi分成N块sj数据块，设置为N - 2f 块数据块就能复原txi。使用默克尔树计算出VAL并分别发至N个节点，每个节点收到后，把VALi发至N个节点，每个节点收到后验证是否为默克尔树分支，否则丢弃。每个节点收到N - 2f个消息后将数据复原为vi。节点将共享签名id发送给所有节点。节点接收到f + 1个有效的id共享签名，可以将这些共享签名组合成id的签名σ，然后输出σ。



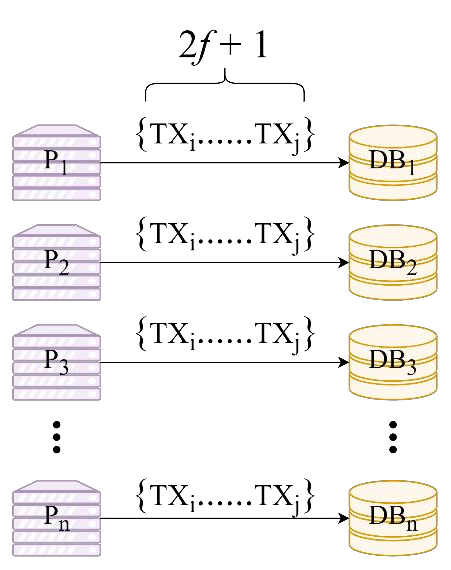
（3）MVBA阶段

N - f个PRBC完成后，将N - f个数据输入，调用MVBA协议并等待从MVBA获得输出Wi，MVBA对Wi整体进行投票，如果Wi满足N - f个正确，对Wi输入1。最后进行ABA，获得2f +1个数据输出，对2f +1个数据对应门限加密进行解密。把剩下f个数据进行第2步操作存入消息队列。



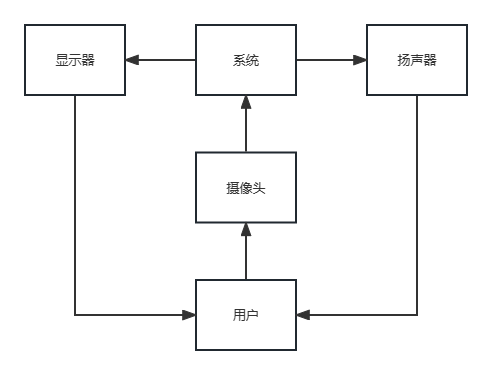
#### 2.2.3.4存储或访问数据

将MVBA中2f +1个数据进行解析，如果是存入命令，将命令存入；如果是读取命令，将读取后的密文放入一个临时数据库，用户可直接访问，用户获得数据后需要用自己的私钥进行解密，即可获得原数据，如此用户没有访问此数据的权限，即无法对密文进行解密。



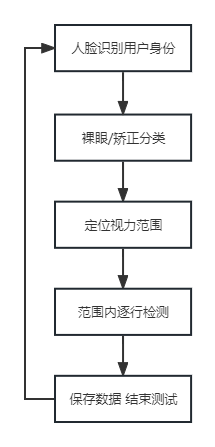
### 2.2.4 ES系统

#### 2.2.4.1 系统组成



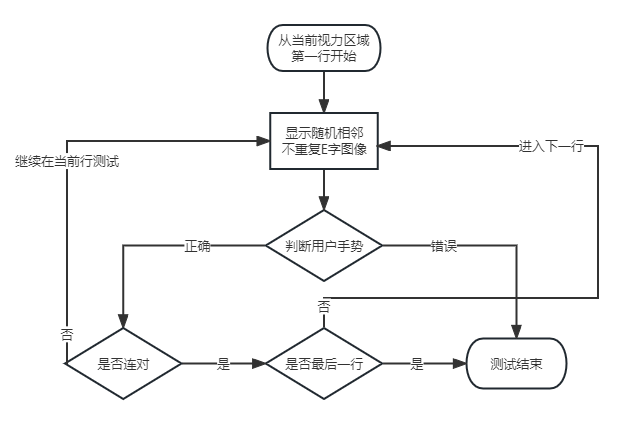
本系统由若干个硬件构成，最终会将图片传入我们的系统内，让系统来识别图像，并做出一些操作。同时，使用扬声器和显示屏为用户提供友好的交互环境，从而方便用户使用我们的系统。

#### 2.2.4.1 系统总体流程



ES系统从人脸识别用户身份开始运行，再到眼镜佩戴识别判断应该执行矫正视力识别还是普通视力识别。之后再进行视力检测，并根据传统视标法推断出被测用户的视力。之后对数据进行一次诊断，判断用户是否需要进行更进一步的检测，最后进行打包和上链操作。

#### 2.2.4.1 系统判定具体流程



ES系统中的视力判断逻辑，我们根据传统“视标法”的准确流程对应用的开发和测试。

## 研发历程

|  |  |
| --- | --- |
| 需求分析和规划阶段 | 在这个阶段，团队对医疗数据隐私保护和共享的需求进行深入调研和分析，了解市场需求和用户需求，确定FACOS系统的主要功能和特性，制定详细的项目规划和技术路线图。 |
| 技术选型和架构设计阶段 | 在这个阶段，团队进行技术选型，选择适合FACOS系统的区块链平台、加密算法、智能合约技术等关键技术。然后，团队设计系统的整体架构，包括链上链下结构、数据存储和处理方案等。 |
| 核心功能开发阶段 | 在这个阶段，团队着重开发FACOS系统的核心功能，包括匿名身份管理、医疗数据加密和共享、智能合约逻辑等。团队采用敏捷开发方法，不断迭代和优化系统功能，确保系统能够满足用户需求。 |
| 安全性和隐私保护加固阶段 | 在这个阶段，团队注重提升系统的安全性和隐私保护能力，采用先进的加密算法、多重身份验证、隐私保护技术等手段，确保用户医疗数据的安全和隐私不受侵犯。 |
| 测试和优化阶段 | 在这个阶段，团队进行系统的功能测试、性能测试、安全测试等，发现并修复系统存在的问题和漏洞，不断优化系统的性能和用户体验，确保系统能够稳定运行和满足用户需求。 |
| 部署和推广阶段 | 在这个阶段，团队将FACOS系统部署到实际环境中，与医疗机构和用户进行合作，推广和应用系统。团队积极开展市场推广活动，提升系统的知名度和影响力，吸引更多的用户和合作伙伴加入系统。 |
| 持续改进和迭代阶段 | FACOS系统的研发过程并不是一次性的，团队将持续关注用户反馈和市场变化，不断改进和优化系统功能，引入新的技术和功能，保持系统的竞争力和创新性，实现持续发展和成长。 |

## 主要专利

以FACOS为技术的专利以提交申请。

## 应用成效

FACOS系统预计的应用成效，有效保护个人医疗数据隐私的同时实现了数据的安全共享。医疗机构和患者可以安全地共享医疗数据，提升了医疗服务的质量和效率，促进了医患沟通与合作，为医疗行业的数字化转型和智能化发展提供了重要支持。

### 2.5.1测试平台

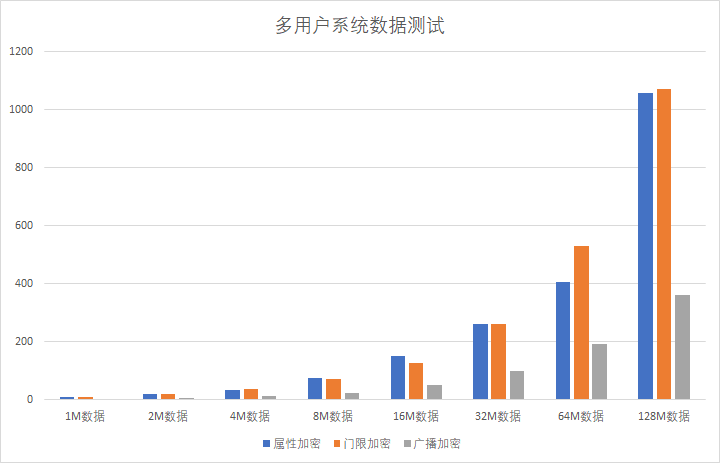
我们在阿里云和腾讯云上进行了测试，使用了 11 台虚拟机，每台虚拟机配备 2 个 vCPU 和 4GB 内存，都运行在 Ubuntu 20.04 上。虚拟机均匀分布在不同的区域。

我们的系统测试基于不同的网络规模和批处理大小。SGX 在阿里巴巴服务器上的部署规格如下：架构为 x86\_64，CPU 配置为 2 个逻辑 CPU 和 1 个物理 CPU，每个核心设计为处理 2 个线程。服务器拥有英特尔 Xeon Platinum 8369B CPU，主频为 2.70GHz，带宽维持在 10 Mbps。内存总共为 8GB，其中 4GB 用于物理内存，其余 4GB 用作加密内存。服务器上的内核版本为 5.19.0。应用程序选用了以与英特尔 SGX 高度兼容性而著名的 Gramine 1.2 的 Library 操作系统。

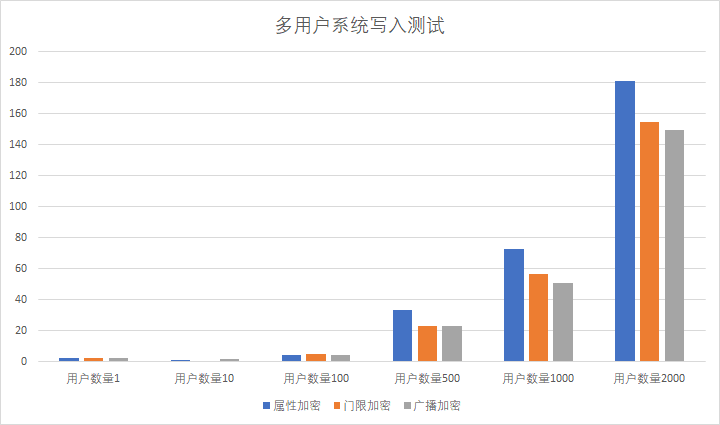
对于区块链网络，我们使用了 Hyperledger Fabric V2.3。Fabric 部署在单台服务器上，使用的共识算法是 RAFT 协议。链码中我们只模拟了 300 行代码内的读写函数。

我们使用 f 来表示容错网络个数，链下副本的总数为 n = 3f + 1。b 为 B/n 的下取整，B、b 分别是协议的批量大小和每个副本提出的交易的批量大小。K 表示要商定的数据总数。我们设定 f =1, n=4, B=40, b =10, K=1000。

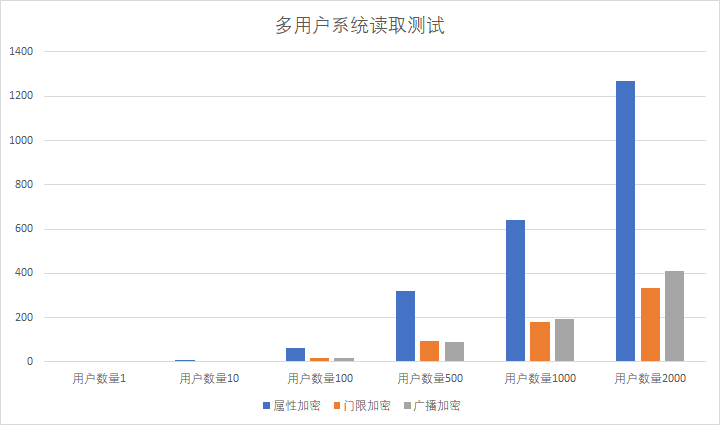
### 2.5.2 测试数据



FACOS 数据大小写入测试/s



FACOS 多用户写入测试/s



FACOS 多用户读取测试/s

## 竞品分析

FACOS系统的竞品分析主要包括与类似的医疗数据管理平台进行比较，如MediBloc和Medicalchain。与竞品相比，FACOS系统在医疗数据隐私保护方面可能采用更先进的加密技术和匿名身份管理，确保用户数据安全性和隐私性。此外，FACOS系统可能在用户体验和界面设计上更加友好和直观，提供更便捷的数据共享和访问方式。另外，FACOS可能具有更高的可扩展性和互操作性，能够与其他医疗信息系统无缝集成，为用户提供更全面的医疗服务。综合来看，FACOS系统有望在医疗数据隐私保护和共享方面取得竞争优势。

# 发展前景

## 商业模式

在医疗健康领域，医疗数据的安全共享一直是一个关键问题。患者的医疗数据分散在不同的医疗机构和系统中，跨系统共享存在挑战，包括数据安全性、隐私保护和数据完整性。

### 3.1.1 目标市场

医疗保健机构、患者、保险公司、研究机构等。

### 3.1.2 目标人群

|  |  |
| --- | --- |
| **医疗机构和医生** | 医疗机构和医生是使用区块链技术的重要用户。他们可以利用FACOS来管理患者的医疗记录、病例、诊断结果等信息，实现数据的安全共享和医疗信息的透明性。 |
| **患者** | 患者是医疗健康领域中最终的用户。他们可以通过FACOS更好地管理自己的医疗信息，包括个人健康档案、诊断结果、用药情况等，同时保护隐私和数据安全。 |
| **保险公司** | 保险公司可以利用FACOS来管理索赔数据、验证患者的医疗信息，从而提高审核效率、降低欺诈风险，并为客户提供更准确的保险服务。 |
| **制药公司** | 制药公司可以利用FACOS来追踪药物的生产、流通和销售过程，确保药物的真实性和安全性，同时提高供应链的透明度和效率。 |
| **医疗研究机构** | 医疗研究机构可以利用FACOS管理和共享研究数据，加强数据安全性和可信度，促进医疗研究的开展和合作。 |

### 3.1.3 核心价值主张

|  |  |
| --- | --- |
| **提供安全的数据共享平台** | 基于区块链技术建立一个安全、去中心化的平台，医疗机构可以在其中安全地共享医疗数据 |
| **保护隐私和数据安全** | 采用加密技术确保数据的隐私性，只有经过授权的用户才能访问和查看数据 |
| **提供可追溯性和透明性** | 所有的数据交换和访问记录都被记录在区块链上，可以追溯数据的来源和访问历史，提高数据的透明度 |

### 3.1.4 收入来源

|  |  |
| --- | --- |
| **许可费用** | 医疗机构需要支付许可费用来使用平台进行数据共享和访问 |
| **定制服务** | 提供定制化的解决方案，根据客户的需求提供额外的功能和服务，收取额外费用 |
| **数据分析和洞察** | 利用医疗数据进行数据分析和洞察，并向客户提供相关的报告和洞察服务，收取费用 |

### 

### 3.1.5 关键合作伙伴

|  |  |
| --- | --- |
| **医疗保健机构** | 与医疗机构合作建立数据共享合作关系，共享医疗数据 |
| **技术提供商** | 与区块链技术提供商合作，确保平台的技术稳定性和安全性 |
| **法律顾问** | 与法律顾问合作确保平台的合规性和数据隐私保护 |

### 3.1.6 关键资源

|  |  |
| --- | --- |
| **技术团队** | 负责开发和维护区块链平台的技术团队 |
| **医疗数据** | 医疗健康数据是平台的核心资源，需要与医疗机构合作获取和管理数据 |
| **客户关系** | 建立和维护与客户的良好关系，了解客户需求并提供相应的解决方案 |

### 3.1.7 潜在挑战

|  |  |
| --- | --- |
| **法律和监管问题** | 医疗数据涉及敏感信息，需要符合法律和监管的要求，包括HIPAA等相关法规 |
| **数据标准化** | 医疗数据的标准化程度不高，需要解决数据格式和标准的统一性问题 |
| **用户采纳度** | 医疗机构和患者可能对新技术的采纳存在一定抵触心理，需要做好推广和培训工作 |

### 3.1.8 潜在机会

|  |  |
| --- | --- |
| **市场需求** | 医疗健康数据安全共享是一个迫切的市场需求，有很大的市场潜力 |
| **技术创新** | 区块链技术的应用为医疗健康领域带来了新的技术创新和解决方案，有望引领行业发展 |

通过以上商业模式，基于区块链的医疗健康数据安全共享平台可以为医疗行业提供安全、透明、高效的数据管理解决方案，从而促进医疗数据的共享与应用，提高医疗服务的质量和效率。

## 客群容量

针对我们的医疗信息系统项目，我们的目标用户主要包括各类医疗机构、医生、护士以及患者等。我们预计在项目上线后的第一年，我们能够吸引到本地医疗机构作为我们的用户，并且预计每家医疗机构平均有50名医生和护士使用我们的系统。此外，预计每家医疗机构每天能服务100名患者。

## 营销模式

系统市场规模不断扩大，预计未来几年将保持稳定增长。随着人口老龄化和医疗技术的不断进步，医疗信息系统的市场需求将进一步提升。在国内市场方面，随着医疗改革的深入推进和医疗服务水平的不断提高，医疗信息系统在各级医疗机构中的应用也将得到进一步普及和推广。

FACOS系统的营销模式将采用多元化的策略，包括以下几个方面：首先，通过线上渠道，包括社交媒体、搜索引擎优化等，提升品牌知名度和用户曝光率。其次，与医疗机构和合作伙伴建立合作关系，共同推广和应用FACOS系统，拓展用户群体。另外，举办线下活动，如行业会议、研讨会等，提升产品认知度并与潜在客户进行面对面的交流。同时，针对不同用户群体，制定个性化的营销策略，提供定制化的解决方案，满足用户需求。通过综合运用线上线下渠道和个性化服务，提升市场竞争力，实现FACOS系统的广泛应用和市场份额增长。

## 财务预测

3.5.1成本预测

单位：万元

|  |  |  |
| --- | --- | --- |
| 项目 | 具体内容 | 预测金额 |
| 编程人员工资 | 根据项目的复杂程度和开发周期 | 4 |
| 设计人员费用 | 包括UI/UX设计师的费用，根据设计工作量和设计师的收费标准 | 1.2 |
| 测试人员费用 | 用于测试和质量保证的人员的工资 | 1.6 |
| 研发工具及其软件许可证 | 购买开发所需的软件和工具的费用 | 0.5 |
| 硬件设备费用 | 例如测试设备等的购置费用。 | 0.4 |
| 云服务器成本 | 如果选择使用云服务提供商提供的计算和存储资源，则需要考虑云服务费用，如云主机、存储空间等。 | 1.4 |
| 广告费用 | 包括线上和线下广告的投入费用，例如搜索引擎广告、社交媒体广告、电视广告等 | 0.6 |
| 市场营销团队费用 | 雇佣市场营销团队的费用，包括市场策划、推广活动执行等 | 3 |
| 总计 | 12.7 | |

### 3.5.1 收入预测

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 总投资额 12.7万元 | | | | | |
| 预期第6个月 | 利润3万元 | 预期第9个月 | 利润6万元 | 预期第一年 | 利润10万元 |
| 投资收益率 | 23.6% | 投资收益率 | 55% | 投资收益率 | 79% |

## 发展规划

FACOS系统的发展规划包括以下几个方面：进一步优化系统功能，提升医疗数据隐私保护和安全共享能力；拓展应用场景，扩大到远程医疗、健康管理等领域；加强全国合作，拓展全国市场；持续投入研发，跟进新技术发展，保持竞争优势；建立健全的生态系统，吸引更多合作伙伴加入，共同推动系统发展。通过持续创新和合作，实现FACOS系统的长期稳健发展，为医疗健康领域带来更多价值和便利。

## 融资计划

FACOS系统的融资计划旨在支持其技术研发、市场推广和生态系统建设。我们计划通过多种渠道融资，包括风险投资、创业孵化器、政府补助等。首先，我们将寻求风险投资机构的投资，以获得资金支持和行业资源。其次，我们将积极参与创业孵化器和加速器项目，获取更多的资源和指导。同时，我们也将申请政府科技创新项目的资助，以支持技术研发和市场拓展。通过多渠道融资，我们将确保足够的资金支持，实现FACOS系统的持续发展和壮大。

# 团队协助

## 4.1 创始团队

|  |  |
| --- | --- |
| 蒋天宇  （项目负责人、后端工程师、运维工程师） | 负责后端开发和系统运维工作，确保系统的稳定性和安全性 |
| 侯灿坤  （算法开发负责人、系统架构师） | 具备全面的技术能力和项目管理经验，负责项目的整体规划和技术实现 |
| 王文卓  （资源管理负责人） | 负责项目资源的统筹管理和优化分配，提高团队的工作效率和资源利用率 |
| 陈柏熹  （销售推广负责人） | 负责项目的销售推广工作，拓展客户渠道，提升项目的知名度 |
| （指导老师） | 他们为团队提供技术指导和项目建议，帮助团队克服困难，推动项目顺利进行 |

## 4.2 执行团队

|  |  |
| --- | --- |
| 项目负责人 | 侯灿坤 |
| 算法开发负责人 | 侯灿坤 |
| 后端工程师 | 蒋天宇 |
| 算法优化负责人 | 侯灿坤 |
| 资源管理负责人 | 王文卓 |
| 测试运维工程师 | 蒋天宇 |
| 销售推广负责人 | 陈柏熹 |

## 4.3 组织架构

|  |  |
| --- | --- |
| 项目负责人 | 负责项目的整体规划、协调和管理，监督项目的执行进度和质量，对项目的整体责任和成果负责。 |
| 技术团队 | 算法开发负责人：负责算法开发团队，指导和管理算法开发工作。 |
| 前端工程师：负责前端界面设计和开发工作。 |
| 后端工程师：负责后端系统架构和开发工作。 |
| 算法优化负责人：负责优化算法性能和效率。 |
| 测试运维工程师：负责系统测试和运维工作。 |
| 支持团队 | 资源管理负责人：负责项目资源的管理和调配。 |
| 财务管理负责人：负责项目的财务预算和管理。 |
| 销售推广负责人：负责项目的销售推广和市场拓展工作。 |

## 4.4 顾问团队

指导老师为项目提供技术指导和建议，协助解决项目中的技术和管理问题。

# 社会价值

## 5.1 产业升级

|  |  |
| --- | --- |
| **提高医疗服务效率和质量** | 通过提供安全、透明、高效的医疗数据管理平台，医疗机构可以更有效地共享和访问医疗数据，从而提高医疗服务的效率和质量。医疗数据的准确性和完整性也将得到提升，有助于提供更精准的诊断和治疗方案。 |
| **促进医疗研究和创新** | 通过医疗健康数据的安全共享，可以为医学研究和创新提供更多的数据资源。医疗研究人员可以更方便地获取大量的医疗数据进行分析和研究，从而推动医学科学的进步和创新。 |
| **增强患者参与和控制权** | 患者可以更方便地访问和管理自己的医疗数据，有助于增强他们对个人健康状况的了解和控制。患者可以更积极地参与医疗决策，与医疗专业人员共同制定个性化的治疗方案。 |
| **保护医疗数据隐私和安全** | 基于区块链技术的医疗健康数据管理平台可以提供更高级别的数据安全和隐私保护机制，确保医疗数据的安全性和隐私性。这有助于减少医疗数据泄露和滥用的风险，保护患者的隐私权益。 |
| **降低医疗成本和提高效率** | 通过提高医疗服务的效率和质量，以及促进医疗研究和创新，可以为医疗行业带来更多的效益。这有助于降低医疗服务的成本，提高医疗资源的利用效率，从而使医疗服务更加可及和可持续。 |

## 5.2 带动就业

|  |  |
| --- | --- |
| 技术人才需求 | 随着FACOS系统的不断发展和完善，对于具有区块链技术、数据安全、智能合约等方面专业知识的技术人才的需求将会增加。这包括区块链开发工程师、数据科学家、信息安全专家等，他们将参与系统的设计、开发、维护和安全保障工作。 |
| 运营和管理岗位 | FACOS系统的运营和管理需要一定数量的人力资源，包括项目经理、运营专员、数据分析师等，他们将负责平台的日常运营管理、用户服务、数据分析等工作。 |
| 医疗健康行业人才 | FACOS系统的应用将带动医疗健康行业相关人才的需求增加，例如医生、护士、健康管理师等，他们将参与医疗数据的采集、处理、分析和应用，为患者提供更好的医疗服务。 |
| 市场推广和销售人员 | 随着FACOS系统的推广应用，将需要一定数量的市场推广和销售人员，他们将负责平台的推广宣传、客户拓展、合作伙伴开发等工作。 |
| 技能培训与人才发展 | FACOS系统的发展也将带动相关领域的技能培训和人才发展，各种培训机构和教育机构将提供相关的培训课程和学习资源，培养更多具备相关技能的人才。 |

FACOS系统的发展和应用将在技术、医疗健康行业以及市场推广等领域带动就业增长，为社会创造更多的就业机会，同时也为劳动者提供了更多的职业选择和发展空间。

## 5.3 未来规划

|  |  |
| --- | --- |
| 技术创新与升级 | FACOS将不断进行技术创新和升级，采用先进的加密算法、安全多方计算、零知识证明等隐私保护技术，以应对不断演进的安全挑战和隐私威胁。 |
| 功能丰富化 | FACOS将进一步完善智能功能，支持更多的医疗数据操作和共享场景，如授权访问、数据交换、数据审计等，以满足不同医疗机构和用户的需求。 |
| 跨行业合作与整合 | FACOS可能与其他行业合作，如保险、生物科技等，整合更多医疗数据来源，实现医疗数据的全面共享和跨领域应用，为医疗健康产业的发展提供更多支持。 |
| 国际化拓展 | 随着全球医疗健康数据交流的需求增加，FACOS可能拓展国际市场，与国际医疗机构、政府部门合作，推动医疗数据跨境共享和合作研究，促进全球医疗健康事业的发展。 |
| 社会责任和公共治理 | FACOS将积极参与社会责任和公共治理，加强对医疗数据隐私保护、伦理规范、法律合规等方面的研究和实践，为医疗数据安全和合理使用建立良好的制度和机制。 |
| 用户教育与参与 | FACOS将加强对用户的教育和参与，提高用户对医疗数据隐私保护的意识和能力，促进用户积极参与医疗数据管理和共享，共同维护医疗数据的安全和合法使用。 |
| 生态系统建设与社区发展 | FACOS将建设完善的生态系统，吸引更多的合作伙伴和开发者加入，共同推动系统的发展和应用。同时，建立开放、包容的社区，促进技术交流与创新，形成良性发展的社区生态。 |

FACOS系统有望在医疗数据隐私保护与共享领域持续发展，为医疗健康产业的数字化转型和智能化发展提供坚实支撑，为社会健康事业的进步做出积极贡献。

## 5.4 风险对策

|  |  |
| --- | --- |
| 风险 | 对策 |
| 数据安全风险 | 采用高级加密技术确保数据安全，包括数据加密、数据脱敏、多重身份验证等措施。建立完善的数据备份和恢复机制，以应对数据丢失或损坏的情况。 |
| 隐私泄露风险 | 严格遵守相关隐私法规，如GDPR、HIPAA等，制定隐私政策并加强用户授权和访问控制。采用零知识证明等隐私保护技术，确保用户医疗数据的隐私安全。 |
| 技术漏洞和攻击风险 | 进行定期的安全审计和漏洞扫描，及时修补系统漏洞，更新安全补丁。建立安全事件响应机制，及时发现并应对可能的安全威胁和攻击。 |
| 合规风险 | 遵守国家和地区的法律法规，确保系统的合规性。与相关监管部门保持密切联系，及时了解并遵守监管政策和规定，以降低合规风险。 |
| 市场竞争风险 | 加强市场调研和竞争分析，了解竞争对手的优势和劣势。不断提升产品和服务的质量和竞争力，积极开展市场推广和品牌建设，以应对市场竞争风险。 |
| 金融风险 | 制定合理的财务预算和资金管理计划，确保项目资金的有效使用和充分控制成本。建立健全的风险管理制度，及时识别和应对可能的金融风险。 |