摘要-目前，所有的医疗信息系统都是以医疗机构为导向来进行管理和运营的。为保护患者隐私，除患者本人要求调出并查看自己的个人信息外，原则上不允许进行医疗机构以外的信息转移和共享，这种以医疗机构为导向的患者医疗信息管理系统必然会造成医疗数据分散在不同的医院，碎片化的医疗数据降低了医疗服务的质量。另一方面，医疗研究和人工智能领域对医疗信息的需求日益增加，可以供医学研究的数据却很少，而且数据的可靠性也很难得到保证。虽然每天都有大量的医疗数据产生，但是由于数据分散在不同的医疗机构，导致实际上只有一小部分数据可用。

Keywords--*blockchain; privacy; bitcoin;*

I. INTRODUCTION

社会快速发展，每日新增医疗诊断信息几何增长，但同时由于各医疗系统的独立性，不同医院甚至不同科室的医生都不能共享这些医疗信息，同时也加重了患者的成本负担。随着大数据，人工智能的发展，区块链技术给了我们新的方向。Medical BLockchain 是一个基于区块链技术开发的开放式信息服务平台，能够对包括智能手机在内的多种设备产生的以及分散在不同医疗机构的医疗信息安全地整合在一起进行管理。医疗消费者可根据需要对每项个人信息设置不同的读取权限，从而完全拥有对自己的医疗信息的所有权和控制权，医疗服务提供者可以在消费者同意的情况下将医疗对象的医疗记录输入 Medical BLockchain。希望获得他人医疗信息的个人、研究机构或企业在得到信息所有者的同意后，可获得所需的医疗信息资源。同时，软件开发人员可以使用 Medical BLockchain 平台提供的 API 和 SDK 来创建各种机遇医疗信息的服务。区块链技术的发展及应用 为解决医疗数据存储与共享的问题提供了新的方向 。

Medical Blockchain 基于中央服务器和节点服务器架构。中央服务器负责接入节点服务器，保证各个节点服务器的数据一致性，并为同步节点服务器的区块链数据提供支持。各个节点服务器接入中央服务器，向中央服务器发送区块链增加消息，然后由中央服务器广播到各个节点服务器，以此达到同步的目的。节点服务器彼此信息独立，互相不知道对方的存在，保证了医疗诊断过程的独立性和私密性。每个节点服务器独立维护每个医疗体系的医生和患者信息。节点服务器对用户提供 web 访问接口，可适配手机，电脑等多种接入设备。

相关工作。本系统使用 python 语言，基于 flask 框架，使用中央服务器和节点服务器架构对整个医疗区块链进行更新和维护。每个节点服务器独立接入中央服务器。节点服务器提供用户访问 web 服务。医生使用该平台对用户进行医疗信息的查看和修改和提交，患者可查看自身医疗信息，可以通过不同节点服务器访问到整个区块链信息。医疗信息使用 AES 对称加密技术，使用患者名称作为秘钥，医生和患者均可查看自身医疗诊断信息。

我们的贡献。基于区块链系统，使用中央服务器和节点服务器模型管理整个医疗区块链模型；传统区块链使用 hash 和工作量证明来验证区块的可用性，但在本系统中，不需要工作量证明，只使用 hash 来验证区块链，避免多余的开销；由于区块链的唯一性，使用医疗诊断账单的形式来记录医生对个特性病人的诊断情况，最后以账单形式汇总出病人医疗信息；由节点服务器保存医生信息和病人信息，节点服务器之间相互隔离，保证了多节点服务器彼此信息的保密性；医疗信息使用 AES 加密算法，密码默认使用病人信息。

组织。 第二部分讨论了我们的隐私问题解决本文； 第三节概述了平台，而第四节详细介绍了技术实施；第五节讨论了将来的扩展 第六节中找到了区块链及其结论。

II. THE PRIVACY PROBLEM

对于某些疑难杂症，需要很多科室的专家进行集体会诊，甚至不同医院的医生进行同步会诊。但是由于各个医疗系统相对独立，很难做到医疗诊断信息共享。专家会诊时候需要共享各种资料。如果患者到不同医院门诊，需要自行携带医疗诊断信息，从医学诊断角度上说，患者看不到，也不应该看到某些太过具体的医疗诊断信息，这就需要新接手的医生重新根据目前情况作出诊断，不仅增加了误诊的概率，还造成医疗资源的浪费,同时增加了患者的时间和精力投入。对于一些需要长期性治疗的患者，医生往往需要通过患者以往的治疗过程，用药习惯，开出针对性的诊疗方案，但由于各个医疗系统系统的隔离，医生只能通过患者带来的病历卡或者患者描述，来局部地了解患者诊疗过程，不能对患者整个治疗过程有个较为完整地把控。对于患者来说，治疗期间，更换医生的成本比较高。区块链技术可以很好的解决以上由于医疗结

构相互独立，医疗信息不能很好共享的问题。每个医疗系统作为一个区块链服务中心，记录下本系统下的所有医疗诊断信息，同时记录下每次用药和当时的诊疗情况；区块链服务中心会把数据更新情况提交给中央服务器，中央服务器把数据更新消息广播到所有注册到中央服务器的节点服务器。这样不仅能保证整个系统的区块链的唯一性，还能同步所有的区块链节点服务器。

III. PROPOSED SOLUTION

我们从系统概述开始。如图所示在图 1 中，构成我们系统的三个实体是有兴趣下载和使用的医院用户；此类应用程序的提供者出于运营和业务相关原因要求处理个人数据（例如，定向广告，个性化服务）；节点负责维护区块链的实体和分布式私有键值数据存储，以换取激励。

虽然系统中的用户通常会保留（伪）匿名，我们可以将服务配置文件存储在区块链上并验证其身份。系统本身的设计如下。区块链接受两种新的交易类型：Taccess，用于访问控制管理；和 Tdata，用于数据存储和检索。对于用户来说可以轻松使用这些这些网络操作来完成区块链的访问和修改。同时提供 resultAPI 接口，支持个别客户的专用定时服务。

为了说明，请考虑以下示例：用户使用我们平台保护她隐私的应用程序。当用户首次注册时，一个新的共享（用户，生成服务身份并将其与关联的权限一起发送到 Taccess 交易中的区块链。服务器上收集的数据（例如位置等传感器数据）使用共享的加密密钥加密并发送到 Tdata 交易中的区块链，随后将其路由到区块链外的键值存储，同时仅保留指向公共分类帐上的数据的指针（该指针是数据的 SHA-256 哈希值）。服务和用户现在都可以使用以下方法查询数据关联了指针（键）的 Tdata 事务。的区块链然后验证数字签名属于用户或服务。对于服务，其权限访问数据也会被检查。最后，用户可以随时通过以下方式更改授予服务的权限发出具有一组新权限的 Taccess 事务，包括撤消对以前存储的数据的访问。发展基于 Web 的(或移动的）仪表板，可进行概述数据和更改权限的能力相当微不足道，类似于开发集中式钱包，例如比特币的 Coinbase1。区块链外键值存储是一个实现 Kademilia [16]，一个分布式哈希表（或 DHT ），添加了使用 LevelDB2 和与区块链的接口实现持久性 DHT 由节点网络维护（可能与区块链网络脱节）读/写事务。数据在节点并进行复制以确保高可用性。它是有启发性的指出替代区块链解决方案可以考虑用于存储。例如，集中式云可能用于存储数据。虽然这需要一些对第三方的信任程度，它在某些方面具有优势可扩展性和易于部署的特性。

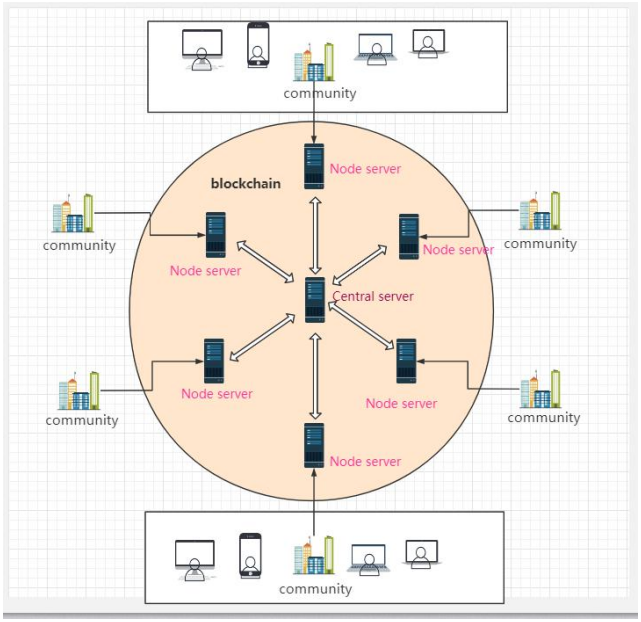

Fig. 1. Overview of the decentralized platform.

IV. THE NETWORK PROTOCOL

现在我们详细描述所使用的底层协议在系统中。使用基于 AES 加密算法，对区块的描述项进行加密，并对上一个区块的全部信息进行 hash 加密,用来保证区块链的唯一性。

A. Building Blocks

现在，我们简要介绍相关的构建基贯穿本文的其余部分。我们假设熟悉比特币[17]和区块链。

1）身份：中央服务器没有用户数据库，只有缓存的区块链数据，不进行权限管理。节点服务器有三种身份类型，分别是 doctor ，patient ，admin。patient 只能查看自身医疗数据，没有更改自身医疗数据和查看更改他人医疗信息的权限。Doctor 可查看全部医疗数据，并对医疗信息进行追加更改。同时，doctor 身份还有增加 patent 和 doctor 的权限。Admin 作为超级管理员，具有最高级权限，可访问并追加所有用户的信息。

2）区块链存储：初始情况下，只有中央服务器，所以区块链的头部区块链节点是由中央服务器创建的，其

中 hash 索引字段,是不包括自身字段的其他所有数据字符串的 hash 值。当有节点服务器启动，则节点服务器自动向中央服务器注册自身信息。然后中央服务器会自动发送自身缓存的所有区块信息。节点服务器响应中央服务器的添加节点命令，顺次完成所有区块链信息的添加和更新。至此，节点服务器注册成功，可进行正常的添加医疗信息区块的操作。区块链信息是分布式存储在各个节点服务器上，彼此相互独立，相互监督，保证区块链的唯一性。理论上整个区块链信息不包含中央服务器存储的区块链信息，中央服务器的区块链信息只用作分发缓存，但中央服务器也是必不可少的。去中心化，顾名思义就是去掉中央服务器，但由于各个节点服务器可能在不同网段，很难达到信息互通，同时也是为了形成单个节点服务器的孤岛效应。

3）策略：用户 u 授予服务的一组权限，用 POLICYu，s 表示。例如，如果您安装了手机
需要访问用户的位置和联系人的应用程序，然后政策 u，s = {位置，联系人}。这对请注意，任何类型的数据都可以通过这种方式安全地存储，假设服务不会破坏协议和标签数据不正确。可以部分防止这种情况发生的保障措施引入移动 SDK，但无论如何，用户可以轻松检测到欺骗的服务,因为所有更改都是对她可见。

4）辅助功能：Parse（x）反序列化发送到事务的消息，其中包含参数；协议 2 中所示的 CheckP olicy（pksigk，xp）验证了发起者具有适当的权限。

B.区块链协议

患者的 PHR 信息包含患者身份、性别、年龄、临床诊断、用药情况等信息为了在实现医学数据有效共享的同时保护患 者隐私，我们将患者的 PHR 信息进行敏感度分级,以键值对 的形式对不同敏感等级的信息进行存储，针对不同的密钥给 予不同的访问权限，确保只有数据拥有者 （ 患者 ） 或者经数 据拥有着授权 的申请方能够获得完整的 PHR 信息。为了实现高效的医疗数据的共享，通过分级加密和密钥管理来控制不同的访问权限,联盟链上的权威节点可以在不 向患者发送数据请求的情况下访问患者部分医疗信息，为了保护患者的隐私，其中不包含患者身份信息。

C.隐私和安全性分析

其一，区块链的特点使数据均以密文形式进行传输，并且在数据传输过程中,数据拥有者通过其在区 块链中的地址发送和接受数据包。由于区块链账户具有匿名性，因此，在数据共享时用户之间无法获取对 方的真实身份。其二，本文采用算法 3 对关键字索引进行了加密，在关键字搜索过程中不会显示任何关于数据拥有者的电子病历信息。其三，本文在数据共享时采用代理重加密技术确保用户数据的隐私性。一个 合法的用户 想要获取数据拥有者 在区块链中存储的电子病历，首先，征得同意后 将自己加密后的
最后，为每个用户服务对生成新的复合标识可确保仅一小部分数据如果对手同时获得两个
签名和加密密钥。如果对手仅获得一名键，则数据仍然安全。注意在实践中我们可以进一步分离身份，以限制单一受损的化合物身份。例如，我们可以为每存储一百条记录生成新密钥。在本节中，我们略微介绍了可能的方法未来对区块链的扩展。这些可以发挥重要作用在塑造更成熟的分布式可信计算中的作用平台，而不是当前最先进的系统。更多具体来说，它们将大大提高较早提出的平台。

A.从存储到处理

本文的主要贡献之一是演示如何克服区块链的公共性。所以到目前为止，我们的分析重点是存储指向加密数据的指针。尽管此方法适用于存储和随机查询，它对于处理数据不是很有效。更重要的是，服务一旦查询了一些原始数据，便可以将其存储为未来分析。更好的方法可能是永远不要让服务观察原始数据，但允许其运行计算直接在网络上获取最终结果。如果我们分裂数据共享（例如，使用 Shamir 的秘密共享[23]），而不是加密它们，然后我们可以使用安全的多方计算（MPC）安全地评估任何功能。

在图 2 中，我们说明了 MPC 如何与区块链，特别是在我们的框架中。考虑一个一个简单的例子，其中一个城市举行选举并祝愿允许在线秘密投票。它开发了一个移动应用程序利用我们的系统进行投票，现在增强了具有建议的 MPC 功能。在线选举后发生后，城市随后提交其后端代码汇总结果。网络选择节点的子集随机地，解释器将代码转换成安全的 MPC 协议。最终，结果被公开存储分类帐，可以安全地防止篡改。结果，没有人们可以了解个人投票是什么，但每个人都可以查看选举结果。

区块链网络中安全计算流程的示例。的左上方的块（EVote 过程）是不安全的代码，其中的参数（*）中标记的是私有的，并作为共享存储在 DHT 中。网络随机选择一个节点子集以计算 EVote 的安全版本，然

后将结果广播回整个网络，然后将其存储在分类帐中。

B.区块链中的信任和决策

POW 共识算法安全性极高，想要破坏系统需要掌握系统 51% 的算力，能够保障系统安全性，但是节点服务器需要消 耗大量资源存储数据，且数据入链时间长，对于医疗数据存 储和共享平台来说，这会造成没有必要的资源浪费。POS 共 识机制减轻了对算力的依赖，但本身医疗数据平台并不产生和使用代币，且 POS 机制易造成中心化，增加安全风险。 DPOS 进一步降低了资源浪费，代理人轮流当值的机制降低了中心化风险，加强了系统安全性。P

VI。CONCLUSION

区块链技术的分散性和抗篡改性等特点使其非常适用于医疗数据进行共享。笔者提出了一种基于区块链的电子病 历共享模型，适用于用户在不同医疗机构之间对自身电子病历便捷、匿名与安全共享的场景。首先，在其中引入并设 计了两种类型的区块链，此外，将分布式密钥生成技术与基于类型和身份的代理重加密方案相结合实现用户之间数据 的安全共享，采用 DPoS 共识算法对区块链进行维护。在该方案中，数据拥有者通过对电子健康记录类型的分类实 现细粒度的访问控制策略。最后，从防篡改、数据保护和应对安全协议的攻击进行了分析，从通信开销和计算开销等方面对本方案的性能进行了评估。结果表明，该方案能够很好的满足隐私性与共享性等多种要求，算力需求和通信成 本较现存方案更低。但本文模型只从安全性和性能方面进行了分析与改进，未考虑减少存储开销与提高共识效率等方面，在未来的工作中，可以对此进行更全面、深入的研究。

REFERENCES

[1] Craig Gentry. Fully homomorphic encryption using ideal lattices. In STOC, volume 9, pages 169–178, 2009.

[2] Scaling the facebook data warehouse to 300 pb, 2014.