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，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，这是因为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;

1. INTRODUCTION

MediBloc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Medi-Bloc。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MediBloc平台提供的API和SDK来创建各种机遇医疗信息的服务。

**相关工作**。从立法的角度出发，已经进行了各种尝试来解决这些隐私问题。（[4]，[20]），以及从技术角度来看。 OpenPDS是最近开发的框架，它提供了用于PDS自主部署的模型，该模型包括一种用于返回数据上的计算从而返回的机制。回答而不是原始数据本身[6]。在整个行业中领先的公司选择实施自己的专有基于OAuth协议[19]的身份验证软件他们充当集中信任的权威。从安全角度来看，研究人员开发了各种针对隐私问题的技术侧重于个人数据。数据匿名化方法试图保护个人身份信息。 k-匿名，一个共同的属性匿名数据集要求每个记录与至少k-1个其他记录没有区别[24]。 k匿名性的相关扩展包括l-多样性，这样可以确保敏感数据由多种形式表示足够的可能值集[15]；和t紧密度着眼于敏感数据的分布[14]。最近的研究已经展示了如何使用这些数据来匿名化数据集可以将技术取消匿名[18]，[5]，即使是很小的数据点或高维数据的数量。其他隐私保护方法包括差分隐私，这种技术会干扰数据或在计算过程中增加噪声共享数据之前进行处理[7]，以及加密方案允许通过加密运行计算和查询数据。具体来说，完全同态加密（FHE）[9]方案允许任何计算运行在加密数据上但目前效率太低，无法在实践中广泛使用。近年来，一类新的责任制出现了。第一个这样的系统是比特币，它允许用户可以使用可公开验证的开放式分类帐来安全地转移货币（比特币），而无需中央监管机构区块链）。从那时起，其他项目（统称为到比特币2.0 [8]）展示了这些区块链如何可以满足需要可信计算的其他功能，并且可审核性。

MediBloc围绕平台发行的一种数字加密货币MED币来构建平台内的经济生态系统。为MediBloc平台生态系统作出贡献的用户和对医疗信息生成做出贡献的医疗服务提供者都会根据恭喜的大小来获得相应MED币奖励.MED币可在 MediBloc的合作多种机构中作为诊疗费、医药费和保险费等的支付手段。

MediBloc为医疗服务消费者、医疗服务提供者和研究机构等单位和个人提供了一个可以自由参与的医疗信息平台。MediBloc团队坚信，MediBloc平台通过重新分配医疗信息的所有权，将为医疗护理领域带来一场创新发展潮浪

**我们的贡献**。基于区块链系统，创造性的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。

1. **THE PRIVACY PROBLEM**

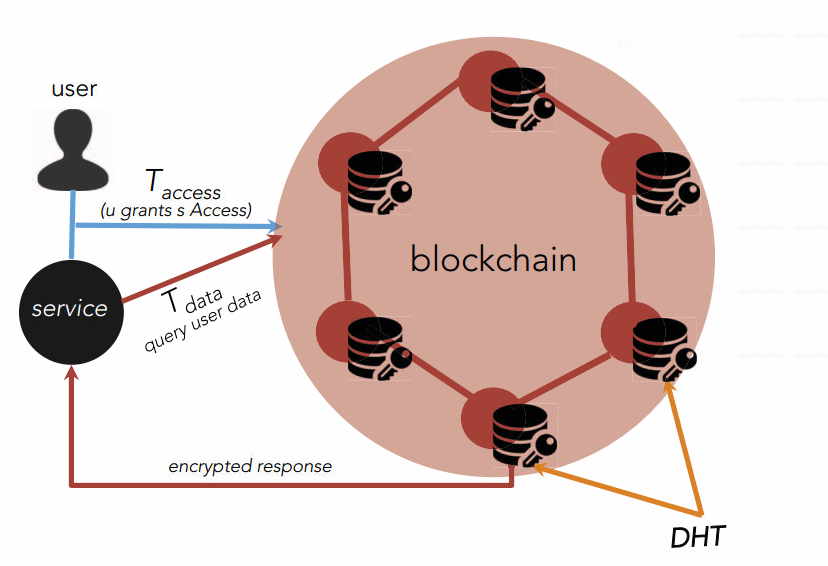
现有问题是，每天会产生大量的医疗信息，各个医疗系统相对独立，不能做到医疗诊断信息共享。患者到不同医院门诊是，需要自行携带医疗诊断信息，并且患者看不到一些医疗诊断信息，更不用说带出医院。患者到新的医院就诊的话，很多医疗过程重复且不必要，造成医疗资源的浪费，同时增加了患者的时间和精力投入。对于一些需要长期性治疗的患者，医生往往需要通过患者以往的治疗过程，用药习惯，开出针对性的诊疗方案，但由于各个医疗系统系统的隔离，医生只能通过患者带来的病历卡或者患者描述，来局部地了解患者诊疗过程，不能对患者整个治疗过程有个把控。

在整篇文章中，我们都会解决隐私问题用户在使用第三方服务时面临的问题。我们特别专注于移动平台，在该平台上服务可以部署应用程序供用户安装。这些应用程序不断收集用户没有特定信息的高分辨率个人数据知识或控制。在我们的分析中，我们假设服务是诚实而又好奇的（即它们遵循协议）。请注意，同一系统可用于其他数据隐私问题，例如患者共享其医疗数据用于科学研究，同时具有监控方法它具有立即退出的功能。有鉴于此，我们的系统可以防止以下常见的隐私问题：数据所有权。我们的框架致力于确保用户拥有并控制其个人数据。这样，系统将用户识别为数据和服务的所有者作为具有委派权限的访客。数据透明度和可审核性。每个用户都有关于收集哪些数据的完全透明她以及如何访问它们。细粒度的访问控制。一个主要关注点移动应用程序是要求用户授予一组注册时的权限设置。这些权限被授予无限期地更改协议的唯一方法是选择退出。相反，在我们的框架中，在任何给定时间用户可以更改权限集并撤消对先前收集的数据。该机制的一种应用将是改进移动设备中的现有权限对话框应用程序。虽然用户界面可能会保留同样，访问控制策略将安全地存储在区块链，仅允许用户更改它们。

1. **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手机用户应用；服务，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）；和节点，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。请注意，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。这些网络操作可以轻松地集成到服务可以使用的移动软件开发套件（SDK）在他们的发展过程中。为了说明，请考虑以下示例：用户安装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。手机上收集的数据（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。





IV. THE NETWORK PROTOCOL

现在我们详细描述所使用的底层协议在系统中。我们利用标准的密码学构建我们平台中的块：定义的对称加密方案由三元组（Genc，Eenc，Denc）–生成器，加密以及解密算法；数字签名三元组（Gsig，Ssig，Vsig）描述的方案（DSS）–生成器，签名和验证算法，分别使用带有secp256k1曲线的ECDSA实现[12]；和由SHA-256实例化的加密哈希函数H[11]实施。

1. *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：区块链利用伪身份机制。本质上是公共密钥，每个用户都可以生成她想要增加许多这样的伪身份隐私。现在我们引入复合身份，这是扩展在我们的系统中使用了该模型。复合身份是两个或多个参与方的共享身份，其中一些各方（至少一个）拥有身份（所有者），其余限制访问它（来宾）。协议1说明了单个所有者（用户）和单个来宾的实现（服务）。如图所示，身份由签名组成所有者和来宾的密钥对，以及对称的用于加密（和解密）数据的密钥，以便数据受系统其他所有玩家的保护。正式地，复合身份在外部（如网络所见）由2元组观察：