Patientory:一种医疗保健点对点EMR存储网络v1.1

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

2017年5月

这篇文章仅作为传播信息，而不是Patientory用来作为合同或任何相关联公司股份的报价。任何形式的合同都是通过私下的报价备忘录，并且符合证券业法律和法规。

摘要

一种使用区块链的医疗健康信息交换(HIE)能够利用交流和电子安全的真正价值。这个系统能够降低摩擦

1 介绍

1.1 什么是区块链？

数字货币比特币所使用的技术 - 区块链, 它的创建者中本聪（**Satoshi Nakamoto**）的身份至今还是一个谜团。从**2009**年以来，区块链在金融领域的应用越来越广泛，各种各样新的区块链相关企业和服务商进入市场。区块链技术不受任何机构的控制，他在自己商业化的网络上，共享交易的分类账簿。分布式的分类账簿让创建费用低廉的商业化联系更容易，实际上任何物品的价值都能够追踪，交易也更加容易，而不受任何人的控制。这些技术让私人机构拥有数据的隐私和控制权。建立信任和完整性，而不需要第三方机构。

1.2 目前医疗护理的基本架构

从针对**"**阶段**"**调整到**"**个人的全面护理**"**需要护理机构形成一个**"**网络**"**，在其中各方人员致力于提升对病人的护理质量，特别针对急性病发作后期的护理。**T**需要使用数字货币，各方面护理人员才会协调合作，人员包括专家，主要护理外科医生，护理给予者，健身提供者（像营养学家和康复护士）。但是这些解决方案改进和提高医疗护理的追踪方法和效率，目标主要是在电子医疗记录**(EMR)** 系统上记录健康信息。

医疗和政府组织花了大量的时间和金钱建立和管理传统的信息系统和数据交换平台；一直都需要资源进行分析和解决问题，更新现场参数，进行备份和还原操作，提取并报告信息。
联邦法律和刺激项目让民众更容易接触医疗保健数据，是由于医院在部署**EMR**方面对政府施压。然而，大多数的医院所使用的系统还不能共享数据。所以，医生花更多的时间在输入病人资料，而不是跟病人聊病情。从**2011** 到 **2014**年，出席外科医生筋疲力竭的事例从**45% to 54% [1].**。

众所周知的是，有一种说法，个人的临床和健身的健康信息没有转化成针对性的保健计划。即使有许多的数据，整个医疗保健系统还没有能力为了改善病人的医疗状况而对大数据进行整合管理。

这样目前的医疗行业使用的健康解决方案无法兼顾病人的隐私和护理效果。随着行业数据的膨胀，这个问题越来越严重。**区块链技术的安全，具有的属性，分布式的本质有助于减少费用和增加运营的效率，还有提供切实可行的安全的基础架构。**

1.3 病人和医疗机构的关系

病人要求高效和最佳的治疗方式，得到最好医疗保健效果。这要求大型的医疗机构能够跟其他关联医疗机构，附属医疗组织比如实验室和药剂房配合提供医疗保健。最终，病人的记录需要一段时间更新和修改。

EMR 软件影响了病人和医疗机构之间的联系。病人门户网站比较少融入病人中，体验比较差。还有就是，这个软件不利于信息在不同系统之间转移，要是想实现转移，需要专门的人进行信息掉配。导致了跨机构对病人治疗和保健的延误，对病人治疗和保健的时间，治疗效果也影响了。治疗机构花费更多的时间在沟通上，为了提高对病人的治疗效果，工作量显著地提高了。对病人治疗产生了反面的效果.

除此之外，鉴于许多医生不想要让病人访问**EHRs**，病人在追踪个人健康方面占据被动的地位。最后会导致病人感觉对自己的健康状况缺乏控制和失去了知情权，病人可能会觉得沮丧。但是最近越来越多人使用移动健康治疗软件（**Mobile Health Care apps**），帮助个人追踪自己的健康状况，这个软件还是没有起到提高病人医疗水平或者产生任何好的效果，可能会被集成到**EHRs**中。

2 系统概况

使用 Patientory 区块链网络就能解决目前存在的问题。旧的 EMR 采用中心化的架构，容易被黑客攻击，还必须符合证券法规和承担高昂的费用。部署 Patientory 区块架构，系统上面有访问控制选项，医疗机构会减少触犯法规的风险；能够促进医疗护理保持同步，促进医疗护理的效果。上面有一幅图解，解释 Patientory 区块链的基础架构和病人跟医疗机构之接的协调过程。

3 部署系统

3.1 在开始讨论之前看一下 HIPAA Regulations 和 Compliance Guidelines，他们来自the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 。主要考虑的问题是隐私条款，安全条款，云计算规则。这个白皮书不是研究HIPAA 法规。跟部署相关的元素应当提前定义，可以在应用的时候再进一步的讨论。

A. Privacy Rule 隐私条款

Patientory 的商业模型要求我们关注隐私条款，这是因为涉及到私人医疗信息的存储和交流方式。应用隐私条款可以归纳为“隐私条款. . .（应用于）医疗护理计划，医疗护理清算中心，或者任何其他的医疗护理机构，只要他们传递电子形式的健康信息”[2].这些机构的代表团体，作为服务提供商，也需要遵循 HIPAA 法规。后面间接的关联团体被称为商业关联(BA)，BA必须遵循的法律文件有一个专门的词是商业关联合约(BAC).HIPAA 对这些团体设有严格的要求条款。

从最初的调查来看，这些协议的详细要点包括医疗信息的授权使用、医疗信息脱敏以及隐私信息的定义。隐私医疗信息（PHI和电子ePHI）被定义为所有可以被识别的个人健康信息或由受保机构或其业务伙伴以任何形式或媒介（包括电子、纸质或其他）进行传播的信息[2]。脱敏的医疗信息是指那些不包含个人隐私信息和不会被任何医疗机构利用的个人健康信息[2]。脱敏医疗信息的使用限制包括：不会被披露和没有使用限制的医疗数据、脱敏医疗信息也不会以任何理由提供给个人做医疗鉴定[3]。敏感信息和脱敏医疗信息的边界，被定义为会限制不到美国人口总数0.04%个人医疗信息的集合。

B.安全防护规则和云计算指导意见

由于本文篇幅有限，本章节只列举被重点关注的问题。这些被重点关注的问题如下，受保医疗机构要使用CSP提供的服务去创建、接收、维护或传送电子隐私医疗信息ePHI（如处理和存储），另一方面，CSP是HIPAA法案中相关的商业合作伙伴。此外，当某个商业伙伴把服务转包给CSP去建立、接收、维护或传输相关电子在隐私医疗信息，CSP分包商这时候本身就成为HIPAA法案中的监管对象。即使CSP处理或存储的是加密的电子隐私医疗信息，但其仍然缺少对数据的加密密钥。仅仅是缺少这种加密密钥CSP是无法规避HIPAA法案中规定的商业责任和义务。因此，当受保医疗机构（商业伙伴）和CSP必须遵从HIPAA商业伙伴协议（BAA），并且，CPS不仅要对BAA协议内容负直接负责，同时也要遵从HIPAA法案下的条款和承担相关责任[3]。

受保医疗机构大多使用云存储提供商（CSP）提供的云服务来存储医疗信息，并对外宣称利用云储存服务能够提升处理效能，降低IT投入成本。但是，由于消费者们选择云服务商提供的云存储对个人数据进行存储，他们就无法直接管控自己的个人数据，用户也无法得知哪些人拥有数据的访问权和数据真正存储在哪里。即使商业伙伴BA和云存储提供商签订了商业合作协议，但这也仅仅能让他们不违约合同条款中的隐私性和安全性问题。而实际上，客户已经无法控制数据的泄露，并且只能寄希望于云存储服务商们能够加强对数据的监管权限。
虽然云存储的使用很受欢迎，但消费者们将个人资料存储在云端，仍然是承担不小的风险。在基于云的基础架构中，数据会被复制和频繁转移，所以数据未经授权的使用风险增加。另外还有很多人间接的拥有对数据的访问权限，例如系统管理员、网络工程师以及管理数据服务器的技术专家们。这些也增加了数据未经授权使用和访问的风险。

然而，即使严格控制数据的访问权限并在数据源进行加密，但数据在运输过程中，仍然面临患者病例报告管理（PROMs）的问题。患者病例报告管理（PROM）的概念是要制定一个相应的管理办法，该办法以患者为本或专注于患者所关心的焦点问题上，为了让该办法成功实施，需要让患者们积极参与并进行反馈。从如今物联网中所使用的各类设备中获取大数据流，并结合基于云端的服务，可以初步建立PROM的基础逻辑架构，但仍然很难得知存储在云端的数据，是否能够将病人的数据形成管理和进行关联。

区块链技术的实现能够确保和增强各类医疗记录数据的安全性，并且可以降低医疗违规和分布式记录医疗数据所有权。在把加密数据导入数据库的过程中用到了不同的加密算法，同样，恢复数据时也会用到不同的解密算法。在数据传输或恢复过程中，采用了符合国家标准与技术协会（NIST）规定和受法律监管的加密算法对医疗数据进行加密。因此，所有信息的交换，都能够遵守国家标准与技术协会（NIST）条例中的最佳实践。

随着医疗行业中的数据泄漏事件不断发生，区块链技术的出现能够使HIPAA法案对患者和医疗机构的同步监管切实可行。

C.区块链系统分析和HIPAA法案限制的局限性

以太坊区块链平台，通过在以太坊虚拟机（EVM）上执行可编程化的具有图灵完备性的机器语言，可使各种类型的区块链应用易于实现开发。这些运行在虚拟机中的系统应用仍然有局限性，如果不使用预言(Oracle)服务，这些应用就不会直接连接到广阔的互联网中去。另外，区块链的存储空间也存在局限性，以太坊上的gas浪费了存储空间，限制了数据访问权限。正如本文所提到的，目前进行区块确认所需要的状态请求校验的打包时间至少需要15秒。
区块链用于存储隐私信息需要解决数据模糊处理的局限性，比如，加密过程，如果不小心泄露了解密密钥，那么就没有办法删除掉区块链中存放的隐私信息。而出于HIPAA法案关于数据监管的要求，区块链本身数据无法被篡改的特点，可能会导致出现无法纠正的数据泄露问题。虽然，理论上脱敏的数据可以存储在太坊的公有链上，但是一旦出现数据脱敏的清洗规则失效或者与区块链交互的相关数据没有达成一致性，都会导致发生灾难性的后果。麻省理工大学的媒体实验室也在研究MedRec协议的形成过程中，得出了这一结论，并将其信息总结在MedRec的白皮书上[3]。挖掘边界信息可能就像观察时间戳和已知数据存储协议的交互一样简单。

通过上述分析，可以将个人患者与相关机构建立起联系，更重要的是，在这个阶段中也形成了工具化。鉴于这些工具的专业性，观察者有能力去获取足够多的违反HIPAA法案规则的信息，如用户的身份、位置、交易时间以及可能的诊断病例等。

这种情况本质上是不太可能发生的，所以缩减到美国人口的0.04%变得微不足道。但是需要特别注意到的是现实情况中由不明原因导致的单点故障。此外，如果直接在区块链中存储加密数据，数据库管理员DBA有责任按照HIPAA法案中数据存储条例中的规定签，订商业伙伴协议(BAC)(参见安全防护规则、和云计算指导意一章)。而要求每个矿工和个人拥有的计算节点都符合HIPAA法案标准，是一个不合乎情理的要求。鉴于这些问题，我们利用基于以太坊私有链实现了一种可持续存储敏感数据的机制。

D.可用性和安全性的实施目标
任何系统的首要安全准则都可以归结为一致性、完整性、可用性、可计算和信息/身份保障。攻击者和用户都必须要适应这些准则要求。他们也都需要一定的能力。从用户的角度看，系统需要足够的透明并且不需要精通更多的知识就可以使用。另外，由于普通用户无法掌握很多网络安全的复杂知识，所以操作过程需要对用户来说尽可能得友好简单。
在发生网络攻击的情况下，我们必须让所创建的系统能够保持资源的可访问，这样发挥的价值远远超过了这些资源本身。由于我们的认知程度有限，任何系统上都有可能会发生攻击现象，所以，我们要持续投入时间和精力去优化系统。更简单的说，没有完美无瑕的防御系统。考虑到这些限制条件，接下来，我们要详细讨论前面提到的本项目要实现的所有目标。

3.2硬件和网络的实现
为了满足上述设计目标，需要把整个系统拆分成几个独立的子系统。每个子系统又细分权限，确保只有经受保机构授权批准后才可以进行交互，同时也提供了一种提高安

全性又同时保证可用性的机制。该系统也备设计成可扩展性，即在需要提升响应级别时，能够轻松实现扩容。下面，将详细描述该系统。
公共医疗机构通过在以太坊区块链（私有链）上为个人用户提供远程过程调用（RPC）服务器接口。网络中的区块链节点，只有被授权后才能与其他块链节点进行交互。这里有一个重要的认证机构就是HIPAA合规性存储工具和RPC服务器。这个重要认证机构是在区块链上生成公有/私有密钥对的资源。HIPAA合规性存储工具里面存储着构成电子隐私医疗信息(ePHI)的实际数据。
当发生数据请求时，HIPAA合规系统可能会被代理转发进行访问授权，然后会重新把数据到发送回RPC服务器。或者，可以使HIPAA合规存储直接与RPC服务器通信。每个实现方案的优点需要在最后选择前考虑好。任何一种访问方式，HIPAA合规存储工具都会根据要求解密数据库的相关内容。而这些解密后的信息又会被交易的请求方使用公钥进行再次加密。这个公钥也是区块链上运行HIPAA数据控制接口的合约所使用的公钥。
具体的网络拓扑图可以参加图2所示。

互联网<-->RPC服务器<-->区块链物理节点数据集合机<-->区块链挖矿节点<-->HIPAA区块链物理机 安全vpn私有链<--> HIPAA合规性数据库

图2：Patientory区块链网络拓扑

3.3软件实现解析
系统除了在硬件和网络中的实现了物理隔离外，软件的访问控制方式也有助于请求机构的认证授权和数据的完整性。下面详细描述，软件系统的访问控制原理和数据加密。

HIPAA合规性数据库仅接收HIPAA代理机转发过来的入站连接。这确保了通讯数据流能够被已知可控的路径所隔离。而HIPAA代理仅仅会转发，在区块链上没有被处理的有效交易访问HIPAA存储工具的请求，同时交易的处理也会出发请求事件。该请求事件需要包含请求方的公钥和被请求的数据。最后，RPC服务器使用访问控制应用程序界面（API），使得只有认证的用户才可以与服务器进行交互。
为了弄清楚系统的调用层次结构，首先就必须要强调下访问控制合约的结构。系统中的每个用户都会在私有链上映射出一个私有地址。每个私人地址都仅能被授权直接与区块链上的一个合约交互。这样的合约是用户类的合约。而机构、机构雇员和客户是类对象。

这些类对象拥有基于权限的接口。机构合约具有已授予浏览权限的所有客户的列表；同样，每个客户的合约中有所有他有权访问的机构列表。机构持有的合约可以从用户那里撤销该机构所拥有的任何权限。机构合约不会自行更改此列表，以防止未经授权

访问个人病例记录。此外，机构合约还拥有经过授权且有维护权限的雇员名单。这个权限清单有较为健全的运行机制，会自动撤销掉不经常使用的权限，以防止机构无意中保留了前雇员的进入权限。

在这个系统中，所有外部各方通过提交调用请求的编码签名交易进行交互。这些交易在用户验证后提交给RPC服务器处理。RPC服务器把这些请求转发到数据集合机中，然后通过负载均衡机制去转发这些请求，提供给矿工。矿工收到请求后，通过交易的请求方各自控制的合约，提交事务处理响应。该合约是唯一能够从外部请求中接受交易的实体。因此，完全控制区块链调用操作的机制就建立起来了。
对于任何给定的交易，调用方都会产生一个不可改变的记录。这样就可以记录所有尝试访问的信息。在用户合约中存储的实际数据是通过HIPAA存储服务器解析完成的hash指针，所匹配的回应数据。该信息会通过执行一个有效的请求交易绑定到HIPAA代理中。这一通讯过程是间接实现的，并通过区块链事件信息系统显示出来。请求者只能通过有效的交易来查询数据库，用户也不能直接修改自己的信息，访问控制是可以证明的。从机构的角度来看，机制都是相似的，除了机构合约中承载的用户列表，该列表包含可以请求数据的用户和能够与机构交互的雇员清单。当某个请求交易由合约中的一个机构雇员发起，这时候控制合约会调用机构合约，而机构合约又会去调用用户合约，通过请求数据指针在电子隐私健康信息ePHI中解析到要查询的数据。直到该机构出现在用户正式批准的机构清单上，合约就会指向到正确的hash地址上。然后这些数据指针会在HIPAA存储工具上再次绑定生成出来的信息。

3 系统实现

3.1 HIPAA规章制度和指导意见

在对系统实现进行卓有成效的讨论之前，我们必须要关注1996年颁布的美国健康保险流通与责任法**(HIPAA)**中对医疗系统的限制条件。该法案关注的焦点主要集中在隐私保护规则、安全防护规则、和云计算的指导意见上。本白皮书的意图不是对**HIPAA**法案进行全面阐述。这些实现系统功能的细节描述将会在后续应用开发中进一步的讨论。

A.隐私保护规则

Patientory商业模式中，隐私保护规则是根据私人医疗信息的电子存储和传输过程所制定的。隐私规则的适用范围概括如下：医疗卫生计划、医疗信息交换和任何以电子化存储和传播医疗信息的相关机构[2]。除了这些代理机构外，HIPAA法案也对医疗机构的当事方和供应商进行制约。这些中间商被称为商业伙伴（**BA**），该法案文件规定，**BA**要按照商业协会协议（**BAC**）的制约。**HIPAA**法案对这些协议提出了严格的要求。
从最初的调查来看，这些协议的详细要点包括医疗信息的授权使用、医疗信息脱敏以及隐私信息的定义。隐私医疗信息（PHI和电子**ePHI**）被定义为所有可以被识别的个人健康信息或由受保机构或其业务伙伴以任何形式或媒介（包括电子、纸质或其他）进行传播的信息[2]。脱敏的医疗信息是指那些不包含个人隐私信息和不会被任何医疗机构利用的个人健康信息[2]。脱敏医疗信息的使

用限制包括：不会被披露和没有使用限制的医疗数据、脱敏医疗信息也不会以任何理由提供给个人做医疗鉴定[3]。敏感信息和脱敏医疗信息的边界，被定义为会限制不到美国人口总数0.04%个人医疗信息的集合。

B.安全防护规则和云计算指导意见

由于本文篇幅有限，本章节只列举被重点关注的问题。这些被重点关注的问题如下，受保医疗机构要使用CSP提供的服务去创建、接收、维护或传送电子隐私医疗信息**ePHI**（如处理和存储），另一方面，**CSP**是**HIPAA**法案中相关的商业合作伙伴。此外，当某个商业伙伴把服务转包给**CSP**去建立、接收、维护或传输相关电子在隐私医疗信息，**CSP**分包商这时候本身就成为**HIPAA**法案中的监管对象。即使**CSP**处理或存储的是加密的电子隐私医疗信息，但其仍然缺少对数据的加密密钥。仅仅是缺少这种加密密钥**CSP**是无法规避**HIPAA**法案中规定的商业责任和义务。因此，当受保医疗机构（商业伙伴）和**CSP**必须遵从**HIPAA**商业伙伴协议（**BAA**），并且，**CPS**不仅要对**BAA**协议内容负直接负责，同时也要遵从**HIPAA**法案下的条款和承担相关责任[3]。

受保医疗机构大多使用云存储提供商（CSP）提供的云服务来存储医疗信息，并对外宣称利用云储存服务能够提升处理效能，降低**IT**投入成本。但是，由于消费者们选择云服务商提供的云存储对个人数据进行存储，他们就无法直接管控自己的个人数据，用户也无法得知哪些人拥有数据的访问权和数据真正存储在哪里。即使商业伙伴**BA**和云存储提供商签订了商业合作协议，但这也仅仅能让他们不违约合同条款中的隐私性和安全性问题。而实际上，客户已经无法控制数据的泄露，并且只能寄希望于云存储服务商们能够加强对数据的监管权限。

虽然云存储的使用很受欢迎，但消费者们将个人资料存储在云端，仍然是承担不小的风险。在基于云的基础架构中，数据会被复制和频繁转移，所以数据未经授权的使用风险增加。另外还有很多人间接的拥有对数据的访问权限，例如系统管理员、网络工程师以及管理数据服务器的技术专家们。这些也增加了数据未经授权使用和访问的风险。

然而，即使严格控制数据的访问权限并在数据源进行加密，但数据在运输过程中，仍然面临患者病例报告管理（PROMs）的问题。患者病例报告管理（**PROM**）的概念是要制定一个相应的管理办法，该办法以患者为本或专注于患者所关心的焦点问题上，为了让该办法成功实施，需要让患者们积极参与并进行反馈。从如今物联网中所使用的各类设备中获取大数据流，并结合基于云端的服务，可以初步建立**PROM**的基础逻辑架构，但仍然很难得知存储在云端的数据，是否能够将病人的数据形成管理和进行关联。

区块链技术的实现能够确保和增强各类医疗记录数据的安全性，并且可以降低医疗违规和分布式记录医疗数据所有权。在把加密数据导入数据库的过程中用到了不同的加密算法，同样，恢复数据时也会用到不同的解密算法。在数据传输或恢复过程中，采用了符合国家标准与技术协会（NIST）规定和受法律监管的加密算法对医疗数据进行加密。因此，所有信息的交换，都能够遵守国家标准与技术协会（**NIST**）条例中的最佳实践。

随着医疗行业中的数据泄漏事件不断发生，区块链技术的出现能够使HIPAA法案对患者和医疗机构的同步监管切实可行。

C.区块链系统分析和HIPAA法案限制的局限性

以太坊区块链平台，通过在以太坊虚拟机（EVM）上执行可编程化的具有图灵完备性的机器语言，可使各种类型的区块链应用易于实现开发。这些运行在虚拟机中的系统应用仍然有局限性，如果不使用预言**(Oracle)**服务，这些应用就不会直接连接到广阔的互联网中去。另外，区块链的存储空间也存在局限性，以太坊上的**gas**浪费了存储空间，限制了数据访问权限。正如本文所提到的，目前进行区块确认所需要的状态请求校验的打包时间至少需要**15**秒。

区块链用于存储隐私信息需要解决数据模糊处理的局限性，比如，加密过程，如果不小心泄露了解密密钥，那么就没有办法删除掉区块链中存放的隐私信息。而出于HIPAA法案关于数据监管的要求，区块链本身数据无法被篡改的特点，可能会导致出现无法纠正的数据泄露问题。虽然，理论上脱敏的数据可以存储在太坊的公有链上，但是一旦出现数据脱敏的清洗规则失效或者与区块链交互的相关数据没有达成一致性，都会导致发生灾难性的后果。麻省理工大学的媒体实验室也在研究**MedRec**协议的形成过程中，得出了这一结论，并将其信息总结在**MedRec**的白皮书上[3]。

挖掘边界信息可能就像观察时间戳和已知数据存储协议的交互一样简单。
通过上述分析，可以将个人患者与相关机构建立起联系，更重要的是，在这个阶段中也形成了工具化。鉴于这些工具的专业性，观察者有能力去获取足够多的违反HIPAA法案规则的信息，如用户的身份、位置、交易时间以及可能的诊断病例等。
这种情况本质上是不太可能发生的，所以缩减到美国人口的0.04%变得微不足道。但是需要特别注意到的是现实情况中由不明原因导致的单点故障。此外，如果直接在区块链中存储加密数据，数据库管理员**DBA**有责任按照**HIPAA**法案中数据存储条例中的规定签，订商业伙伴协议**(BAC)(**参见安全防护规则、和云计算指导意一章**)**。而要求每个矿工和个人拥有的计算节点都符合**HIPAA**法案标准，是一个不合乎情理的要求。鉴于这些问题，我们利用基于以太坊私有链实现了一种可持续存储敏感数据的机制。

D.可用性和安全性的实施目标

任何系统的首要安全准则都可以归结为一致性、完整性、可用性、可计算和信息/身份保障。攻击者和用户都必须要适应这些准则要求。他们也都需要一定的能力。从用户的角度看，系统需要足够的透明并且不需要精通更多的知识就可以使用。另外，由于普通用户无法掌握很多网络安全的复杂知识，所以操作过程需要对用户来说尽可能得友好简单。
在发生网络攻击的情况下，我们必须让所创建的系统能够保持资源的可访问，这样发挥的价值远远超过了这些资源本身。由于我们的认知程度有限，任何系统上都有可能会发生攻击现象，所以，我们要持续投入时间和精力去优化系统。更简单的说，没有完美无瑕的防御系统。考虑到这些限制条件，接下来，我们要详细讨论前面提到的本项目要实现的所有目标。

3.2硬件和网络的实现

为了满足上述设计目标，需要把整个系统拆分成几个独立的子系统。每个子系统又细分权限，确保只有经受保机构授权批准后才可以进行交互，同时也提供了一种提高安全性又同时保证可用性的机制。该系统也备设计成可扩展性，即在需要提升响应级别时，能够轻松实现扩容。下面，将详细描述该系统。
公共医疗机构通过在以太坊区块链（私有链）上为个人用户提供远程过程调用（RPC）服务器接口。网络中的区块链节点，只有被授权后才能与其他块链节点进行交互。这里有一个重要的认证机构就是**HIPAA**合规性存储工具和**RPC**服务器。这个重要认证机构是在区块链上生成公有**/**私有密钥对的资源。**HIPAA**合规性存储工具里面存储着构成电子隐私医疗信息**(ePHI)**的实际数据。
当发生数据请求时，HIPAA合规系统可能会被代理转发进行访问授权，然后会重新把数据到发送回**RPC**服务器。或者，可以使**HIPAA**合规存储直接与**RPC**服务器通信。每个实现方案的优点需要在最后选择前考虑好。任何一种访问方式，**HIPAA**合规存储工具都会根据要求解密数据库的相关内容。而这些解密后的信息又会被交易的请求方使用公钥进行再次加密。这个公钥也是区块链上运行**HIPAA**数据控制接口的合约所使用的公钥。
具体的网络拓扑图可以参加图2所示。

互联网<-->RPC服务器<-->区块链物理节点数据集合机<-->区块链挖矿节点<-->HIPAA区块链物理机安全vpn私有链<--> HIPAA合规性数据库

图2：Patientory区块链网络拓扑

3.3软件实现解析

系统除了在硬件和网络中的实现了物理隔离外，软件的访问控制方式也有助于请求机构的认证授权和数据的完整性。下面详细描述，软件系统的访问控制原理和数据加密。

HIPAA合规性数据库仅接收HIPAA代理机转发过来的入站连接。这确保了通讯数据流能够被已知可控的路径所隔离。而HIPAA代理仅仅会转发，在区块链上没有被处理的有效交易访问HIPAA存储工具的请求，同时交易的处理也会出发请求事件。该请求事件需要包含请求方的公钥和被请求的数据。最后，RPC服务器使用访问控制应用程序界面（API），使得只有认证的用户才可以与服务器进行交互。

为了弄清楚系统的调用层次结构，首先就必须要强调下访问控制合约的结构。系统中的每个用户都会在私有链上映射出一个私有地址。每个私人地址都仅能被授权直接与区块链上的一个合约交互。这样的合约是用户类的合约。而机构、机构雇员和客户是类对象。

这些类对象拥有基于权限的接口。机构合约具有已授予浏览权限的所有客户的列表；同样，每个客户的合约中有所有他有权访问的机构列表。机构持有的合约可以从用户那里撤销该机构所拥有的任何权限。机构合约不会自行更改此列表，以防止未经授权访问个人病例记录。此外，机构合约还拥有经过授权且有维护权限的雇员名单。这个权限清单有较为健全的运行机制，会自动撤销掉不经常使用的权限，以防止机构无意中保留了前雇员的进入权限。

在这个系统中，所有外部各方通过提交调用请求的编码签名交易进行交互。这些交易在用户验证后提交给RPC服务器处理。RPC服务器把这些请求转发到数据集合机中，然后通过负载均衡机制去转发这些请求，提供给矿工。矿工收到请求后，通过交易的请求方各自控制的合约，提交事务处理响应。该合约是唯一能够从外部请求中接受交易的实体。因此，完全控制区块链调用操作的机制就建立起来了。

对于任何给定的交易，调用方都会产生一个不可改变的记录。这样就可以记录所有尝试访问的信息。在用户合约中存储的实际数据是通过HIPAA存储服务器解析完成的hash指针，所匹配的回应数据。该信息会通过执行一个有效的请求交易绑定到HIPAA代理中。这一通讯过程是间接实现的，并通过区块链事件信息系统显示出来。请求者只能通过有效的交易来查询数据库，用户也不能直接修改自己的信息，访问控制是可以证明的。从机构的角度来看，机制都是相似的，除了机构合约中承载的用户列表，该列表包含可以请求数据的用户和能够与机构交互的雇员清单。当某个请求交易由合约中的一个机构雇员发起，这时候控制合约会调用机构合约，而机构合约又会去调用用户合约，通过请求数据指针在电子隐私健康信息ePHI中解析到要查询的数据。直到该机构出现在用户正式批准的机构清单上，合约就会指向到正确的hash地址上。然后这些数据指针会在HIPAA存储工具上再次绑定生成出来的信息。

3.4 交互性

EHR系统是一个基于独立受信的验证结构，患者数据被保存在每一个互相隔离的单独系统中。这就导致那些一对一的诊疗机构需要在软件中增加“额外”的解决方案才能够使系统和其他医疗合作组织或者附属的医疗机构开展合作。但是，医疗主体机构能够给其他组织提供的医疗信息权限是有限制的，例如只读、提交、发送或通知。并且，患者/消费者在这种信息交换中的可交互性和参与度非常有限。此外，数据交换的机制还存在一个缺点，就是在数据提交后要进行修改是很困难的。

而主要通过部署区块链和它的智能合约，参数就会立即生效。患者就成为收发信息的主要媒介，就不能进行频繁的更新和排查软件故障。由于区块链中的记录是不可篡改的，并存储在所有参与

记账的用户中，是不需要进行灾难恢复的。而且，区块链透明的信息结构可以消除数据交换过程中产生的差异和时延报告事件。

3.5 进程和可扩展性

用户可以控制他们所有的信息，并确保能够传输具有完整性、一致性、时效性、准确性和广泛性的高质量数据。从而使数据可持续和可信赖。由于使用了分布式的数据库技术，区块链不存在中心节点故障，也更有能力去地抵御恶意攻击。

门诊为病人提供服务<--->患者的医疗信息可以被追踪<--->标准数据字段和病人ID编号发送至区块链中<--->系统处理进来的交易<--->交易被存储在包含不可识别患者ID标号的区块链中<--->区块链<--->诊所和医疗机构提交他们的查询请求<--->可以查看到不可识别的患者信息<--->数据可以被分析和使用<--->患者的私钥地址关联到区块链中的数据<--->新的诊所和医疗机构可以共享私钥地址<--->诊所可以使用私钥地址恢复患者数据<--->没有私钥的机构无法追踪和发现数据

图3：区块链进程流图

在所有的医疗护理网络中，都有必要确保参与者们可以依赖彼此提供各自所需的服务而共同协作。要实现这一点，必须要有办法能够确保及时交付任务并对其所提供的服务负责，如果不能及时交付，那么就要确保高质量的服务水准。因此，任何医疗保健基础设施都必须能够对所需要的信息进行无缝监控和对接，以此来驱使主要的医疗护理提供商能够正确评估他的医疗护理网络。而且，随着医疗护理网络的发展，医疗机构会和医疗网络提供商之间有越来越多的交互，这也增进了医护网络基础架构规模的发展和效率的不断提高。

构建高度可扩展和分布式医疗管理系统的关键点在于一个点对点的基础架构。这样的架构已被广泛应用于多个行业，如媒体、体育、房地产、供应链、这些都展示了区块链可以很轻松得成为一款连接现有中心化基础架构的优秀软件扩展组件[7]。这也指引我们探索使用区块链框架的应用场景来实现医疗保健行业的点对点基础架构。

区块链可以允许两个或两个以上的机构进行“医疗保健交易”的确认。与传统集中认证模型不同的是，区块链提供了两个关键属性。第一个是，有兴趣的一方可以根据彼此双方“信任关系”的”交易级别“来与对方建立友好关系;第二个是，这种关系中的责任风险遵循于双方签订合约的“交易级别”。这两个属性是非常有用的，因为这种属性限制了相关各方之间的信息和责任的权限，让医疗机构可以根据对方的能力特点和病患人员护理类型等，同时与其他多家供应商建立起交易关系。这种方式比要限制供应商数量的传统集中式系统更具优点，传统系统中会根据供应商的责任和能力来确定供应商的范围和患者的需求。

3.6 医疗信息交易和代币

Patientory的代币**PTOY**是驱动区块链基础设施的燃料。代币的主要用途是规范网络存储空间分配、管理医疗护理质量和在收支周期使用。

在Patientory网络中，已经给患者分配了免费的存储空间用来存储病例信息。代币**PTOY**可以让他们从医院系统建立的节点上购买额外的存储空间。**PTOY**可以通过加密货币交易所或其他平台购买。同样，医疗机构也会使用代币PTOY。代币也被用于和医疗保险公司签订智能合约后的支付环节，也被作为调节价值模型指标的机制。

为了使美国成功地从费用服务模式转换到目前的价值型模式，就必须要搭建一个医疗信息技术的基础设施，使社会组织可通过其声誉模型去链接高质量、有价值、高效能的医疗协助中去。

补偿收益与供应商工作网络的效率相关，这样做是为了确保能改善医疗护理质量和健康状况，同时也能降低相关的护理成本。使用共享储蓄（医疗费用偿还方式）收益显现出的一个优势，就是能够要真正激励网络中的不同参与者积极创造出更好的医疗护理服务。通过在区块链网络上执行

智能合约，可以明确的追踪供应商的贡献度，这样就能有效地在网络中控制能提供最大效能节省整体医疗费用的供应商可以存在一个合适的比例。
新医疗护理模式的另一个关键影响点是，医疗供应商可以在提升医疗护理水平后获得额外的补偿收益。这种补偿收益的多少是根据供应商管理患者健康效果（激励措施）来评估的。作为新医疗护理模式共享储蓄收益方面的一部分，医疗供应商及其网络合作伙伴可以保留对病人信息电子管理所产生的收益。
我们对代币使用的建议是，有支付能力的付款人可以向医疗供应商支付代币，作为对供应商提供服务的激励方式。这种能够轻松兑换优惠福利的智能合约，有着无缝跟踪和管理医疗数据的能力，能够为医疗供应商和患者提供了必要的"报酬"，从而达成共赢的局面。相反，如果一个或多个参与者被罚款，背负了债务，也可用同样的方式进行征税，这种"报酬/惩罚"的方法将为医疗保健行业从疾病管理理念转变为健康生活理念，提供十足的推动力。
Patientory发出的代币（**PTOY**）是**Patientory**平台上的本地代币。为了交换**PTOY**代币，用户能够使用代币在网络上租用健康电子信息的存储空间，并通过执行健康规范智能合约进行支付和交易。我们认为，在可预见的未来，使用代币这种最佳的支付方式，能够支持该医疗基础设施的发展。未来的生态系统中将会诞生很多有活力的代币，而医疗保健领域也需要一个闭环的支付系统。付款欺诈行为，对医疗保健领域造成了数十亿美元的损失，而我们的代币系统将对病患护理的全生命周期起到积极管理和良性循环的作用[4]。

该系统还激励那些拥有大量服务器和存储的大型组织与中小型医疗机构进行代币交易，这些组织可以直接接入到区块链卫生网络中，而无需直接运行相关节点。尽管如此，新医疗护理政策提供了鼓励有能力的医疗供应商共同努力来改善医疗护理环境，但目前使用的EHR体系结构普遍缺乏实现这一目标的能力，所以授予或接收代币将有助于实现这一目标。
因此，代币的价值与网络中执行的交易量相关。随着Patientory网络中持续增加的代币交易，会增加代币的需求，使得代币升值。

3.7 如何获得代币PTOY

PTOY可以通过**Patientory**的本地应用程序、加密货币交易所获得，也可以通过与其他患者、医生或保险公司的交易中获得。在预售期间，平台用户将能够通过发送以太币（**Ether**）到**PTOY**区块链上的智能合约中，获得**PTOY**。**Patientory**界面将集成第三方场外交易解决方案（如**Shapeshift**和**Coinbase**），以便不持有**ETH**的交易者进行交易。
Patientory代币将采用预售形式进行初始分配。任何人都可以通过抵押**ETH**到代币销售的智能合约中，以优惠的折扣认购到**PTOY**。如果使用其他加密货币（如**ETC**或**BTC**）参与认购，可以通过预售页面上的第三方转换服务来认购**PTOY**。
创始团队将保留10%的**PTOY**份额，进行十二个月的持有期。这些代币将成为**Patientory**创始团队的长期激励。另外**20%**的份额将被分配**Patientory**基金会，用于医疗保健领域区块链技术的研发和调研。

3.8智能合约、如何处理保险索赔

A.自动裁决

医疗费用账单繁琐、患者的第三方报销流程复杂，往往导致病人、医疗机构和保险公司之间的误解和推诿。这些复杂的情况也让一些消费者不知道该什么时候、与何人、以及什么原因进行费用结算，甚至弄不清楚这些费用该由患者自身付款还是应该要求保险公司承担。
Patientory是一个利用以太坊区块链技术和快速医疗互通资源（**FHIR**）兼容的应用程序接口（**API**）共同搭建的平台，**Patientory**平台旨在增加医疗电子化程度、实现近乎实时的索赔裁决、在利益相关者之间提供透明公正的协议并减少欺诈行为。

FHIR作为行业标准的格式化数据，它的建立降低了医疗保健和保险遗产系统集成的复杂性。考虑到将数据添加到区块链中的成本，我们解决方案中的一个关键点是通过执行智能合约来确定需要上链的数据。
医疗费用账单和相关的保险费用预计在2018年达到**315**亿美元，医疗机构每周要花费约**3.8**个小时用于和付款人之间的工作，我们的**Patientory**平台可以大大减轻这些运营成本。
诊断信息互相之间的关联关系分析方法，也可被用于分析欺诈活动的索赔数据。这种分析也会揭示例如多重理赔性质所引起的用药行为。这两个例子都能说明，使用Patientory系统会提升保险公司的价值，当然最根本的效益也会远远超过这些。
Patientory系统中的相关规则是通过智能合约系统执行的，全部涉及的协议都是针对末端用户所编写的智能合约。这使医疗机构能够在系统查询和验证之前就交付服务。使用系统所需花费的成本可以在医疗机构和个人之间使用代币**PTOY**自动计费。因此，医疗机构和个人会很清楚地了解所产生的成本。这也消除了会计部门的工作量，增加了使用**Patientory**系统产生的价值。

Patientory是一个闭环的支付系统。它允许通过以太坊公链进行跨链的安全价值交换。这种机制也解决了比特币中交易的共识问题，这里它确实是需要一个信任的实体来充当预言机（Oracle）。

B.可行性

通过使用现有机制，可以容易地构建出这种架构。举个这样的例子，亚马逊网页服务（Amazon Web Service）中的**HIPAA**合规性数据存储系统和易于部署的**ErisDB**。这类的软件即服务（**SAAS**）的平台可以快速部署出具有以太坊智能合约功能的区块链，并具有访问控制和上文中提到的功能。虽然这种方式需要额外搭建节点，但与开发完整架构相比，这还是一个较小的成本方案。
Patientory的三层智能合约架构中，只有一小部分特性是需要在以太坊区块链中实现的。而较为复杂的业务逻辑已经从相关实施路径中移除掉了，并对数据层进行了优化，实现了分布式网络的特性。
以太坊区块链中智能合约的组件包括：数据库图式（schema）、验证和账本交易验证以及用于读取分布式账本的查询优化逻辑。
以太坊区块链中业务逻辑是其单独的一层中间（业务）层。该逻辑代码可访问各类服务，包括安全执行、证据留存、身份认证、支持加密，数据格式化、可靠的消息传递、触发器以及可将该代码绑定到区块链中任意数量的智能合约上，使Patientory在各类医疗保健机构协会中具有热插拔的功能。这些都是在**fabric**中提供的服务，其支持执行智能合约中各个代码段，并把交易发送到区块链节点中，绑定数据库图式（**schema**）到数据层中。

3.9其他独特的优势

虽然像医院这样的医疗机构无法访问未经授权的医疗记录，但在紧急情况下患者可预先授权进行信息共享，所以末端用户可以参与到服务中，获得更多的好处。考虑到这一点，医疗机构在紧急情况下，可以根据用户之前的授权来升级访问权限，访问无响应患者的相关记录。如果某个用户没有进行响应，但是留有他们的手机，该医疗机构就可以从锁屏的智能手机中获得辅助签名，来证明患者身份。该辅助密钥不能与用户的主帐户相同。因此，如果医疗机构的帐户向区块链提交了包含患者公钥或该患者智能手机中的紧急辅助密钥的请求，那么，区块链就会升级患者医疗记录的级别，以供该医疗机构进行访问，否则该医疗机构是没有访问权限的。**这个私钥被设计成了可替换的方式，并可由患者尽快更换。使用这种方式，可以在紧急情况下，提升个人和授权医疗机构之间信息交换的安全性。**
如果医疗机构在没有正确授权的情况下要访问这些信息，那么系统将会向患者通知医疗机构的这些行为。如果患者设定了阈值拒绝此请求，则不会共享数据。此外，如果机构多次尝试欺诈的请求，平台可以撤销该机构权限，并对其处以罚款。本系统需要同时使用移动设备和医疗机构的密钥才能够请求数据，因此丢失通讯设备所带来的影响也能降低至最小。在可预见的未来，所有保

险卡都将和现代信用卡一样，会嵌入密码微控制器，这将有助于其像智能手机一样独立完成相关的操作。

4国家/国际化医疗护理重点项目

4.1个性化护理

为了实现优质化医疗护理，以人为本的方法很重要。这种方法不仅要考虑临床方面，还要考虑到阻碍人们享受到合格医疗护理和维持健康生活的社会和经济因素。
为了达到有效的医疗护理效果，需要找到阻碍个人健康和生活状况的因素。越来越多的患者都患有两种以上的综合症，所以，“简化式”的单项护理服务不利于激励和达成有效的护理效果。因此，要结合患者多方面的身体状况和健康需求，来定制更加灵活的护理模式。让患者能够积极跟踪、管理和参与到个人的护理中至关重要，因此，这就需要一个全面、可动态调整的互动似的护理计划。

4.2临床效果

与患者自身密切相关的患者病例管理（PROMs），在过去几年中有着更加重要的意义和更高的重要性。部分原因是因为患者护理得到了越来越多的关注，而且能够评估患者所患疾病的负担和影响。患者病例管理（**PROM**）可以包括病症和其他生活质量健康指标，如身体状况或社会功能、诊疗配合程度和诊疗满意度这些方面。他们还可以对诸如癌症或多发性硬化症等疾病的治疗提供更加详细和完整的评估，从而促进患者和医师之间在治疗相关疾病方面能够进行更准确的沟通。
PROM不同于传统的临床治疗方式（例如癌症治疗，戒烟），因为它们从患者的角度出发，直接反映出疾病及治疗的影响。这些措施可以在医治疗效和患者的费用负担之间起到平衡作用。**PROM**在监控患者体力活动或身体总体状况等方面也有着重要的意义，与传统临床治疗方式相比，它更能够体现出医疗的整体效果和安全性。因为这些方式都是从患者的角度出发，这样可以促进患者更多地参与到治疗决策过程中，为医疗保健决策提供指导意见。所以说，加强区块链上的**PROM**基础设施建设，就是在加强建设医疗供应商和患者之间医护标准。

5结论

区块链技术将在医疗行业IT领域中发挥越来越重要的作用，为医疗生态系统中的每个参与者带来带来利益和新效能。对医疗机构来说，了解区块链技术的核心尤为重要，要为技术变革做好储备。而基于区块链的新一代功能强大的应用程序，将会塑造下一代医疗保健业务。为了充分发挥区块链在医疗领域中的潜力，必须要建立相关标准，确保在医疗领域中实现兼容性和互通性。