据WHO统计，世界上10%~15%的药物是假的，在发展中国家这一比率甚是高达30%。假药每年会造成20万人的死亡。这些假药或盗用大品牌的商标，或者通过仿造标签来出售，这导致他的流通范围很广，随着技术的进步，假药的销售手段也越来越多。为了解决这一问题，需要加强对各级分销商，市场的控制和管理。追踪药品的走向。区块链能够处理供应链和产品追踪的问题，区块链可以确保供应链过程的安全，并非常有效地跟踪交付情况。DSCMR是一种基于区块链和机器学习的药物供应链和推荐系统。改系统包括两个主要模块：基于区块链的药品供应链管理和基于机器学习的消费者药品推荐系统。在第一个模块中，使用Hyperledger fabrics部署了药物供应链管理系统，该系统能够连续监测和跟踪智能制药行业的药物输送过程。 另一方面，在机器学习模块中使用N-gram、LightGBM模型向制药行业的客户推荐最佳药物。在RESTAPI的帮助下，机器学习模块与区块链系统集成。

大多数行业之所以希望转向区块链技术，是因为它提供了分布线上分布式存储账本，网络中的所有对节点都可以看到和验证交易相关信息。 还有就是它的共识算法，它授权网络将唯一验证的信息存储，解决了重复交易的问题。 此外，由于来自故障阈值的节点较多，而且容错性很强，网络故障概率很低。DSCMR能够持续监测和跟踪药品交付过程，以解决伪造问题。它的机器学习推荐系统可以推荐最好的药品，还可以通过用户反馈不断升级。它用Couch-DB存储大量的交易记录，消除数据冗余问题并为区块链网络中的每个节点提供单独存储。

区块链的去中心化分布式特性，扩展了医药行业药品供应链的安全性和隐私性。DSCMR的区块链上存储着供应商、制造商、分销商、药房、医院、医生和病人的信息。系统的所有相关参与者都可以使用客户端应用程序跟踪药物的状态。另外该系统还有一个单独的数据库，被称作stored-off blockchain。这个数据库可以供外部使用，在该系统中，机器学习的智能推荐系统就使用的这个数据库。这个数据库存储了各种信息的全部细节。系统中的每一步操作都需要其他节点的认证，才可以被认证存储到链上。

区块链分布式的存储信息，每个块都包含多个交易。交易通过加密和哈希方式存储确保安全。DSCMR系统分为药品供应链和推荐系统两个模块，这里只分析基于区块链的供应链系统。每个用户可以使用前端的web应用程序执行交易，包括药品订单、原材料供应、更新药品数据、更新订单、更新记录、交付药品、数据共享、跟踪药品供应、药品管理、客户管理等功能。为了安全，系统引入了通道，通道可以使网络处于私有的状态，通过通道传递的数据可以指定接收人，不被暴露于其他节点。区块链中每个节点都有智能合约和账本，智能合约提供了一种透明无冲突的方式交换财产、金钱、股票或任何东西，而不需任何第三方。从技术上讲，智能合约是多行计算机代码，它执行双方之间的协议，而不向中间人支付任何金额。 此代码由预定义的规则集组成，其中两组彼此达成一致。 当指定的条件与数据库交易相同时，自动触发此合约。该系统解决了交易执行率低的问题，只给指定节点部署智能合约。

这个药物供应链系统的交易过程如下：首先，用户通过前端应用程序注册身份信息，连接到区块链系统，并完成交易请求。然后，将交易发送到所有对等节点。 这些对等节点分为两类：提交者或背书者。 背书者执行或签署过渡提议，并给予批准，如果是有效的，就履行智能合同标准，否则拒绝它。另一方面，提交者的对等节点验证交易结果，然后写入交易块中。背书者是有预定义智能合约的提交者的特殊对等节点。背书者在自己的虚拟环境中模拟智能合约然后更新账本。背书者读取所有历史记录，然后在自己的虚拟环境中将数据写入。完成后把签名返回给客户端应用程序，客户端再把所有的背书者的签名通过共识算法交付给提交节点，把数据排序放入块中。然后提交节点通过匹配当前链的状态验证交易，再将交易写入整个账本。最后，根据写入的数据更新账本。这时提交者的对等节点向客户端发送通知，获取提交或不提交的状态。通过REST API和SDK建立客户端应用与区块链网络的通信。

[1] Khizar Abbas,A Blockchain and Machine Learning-Based Drug

Supply Chain Management and Recommendation

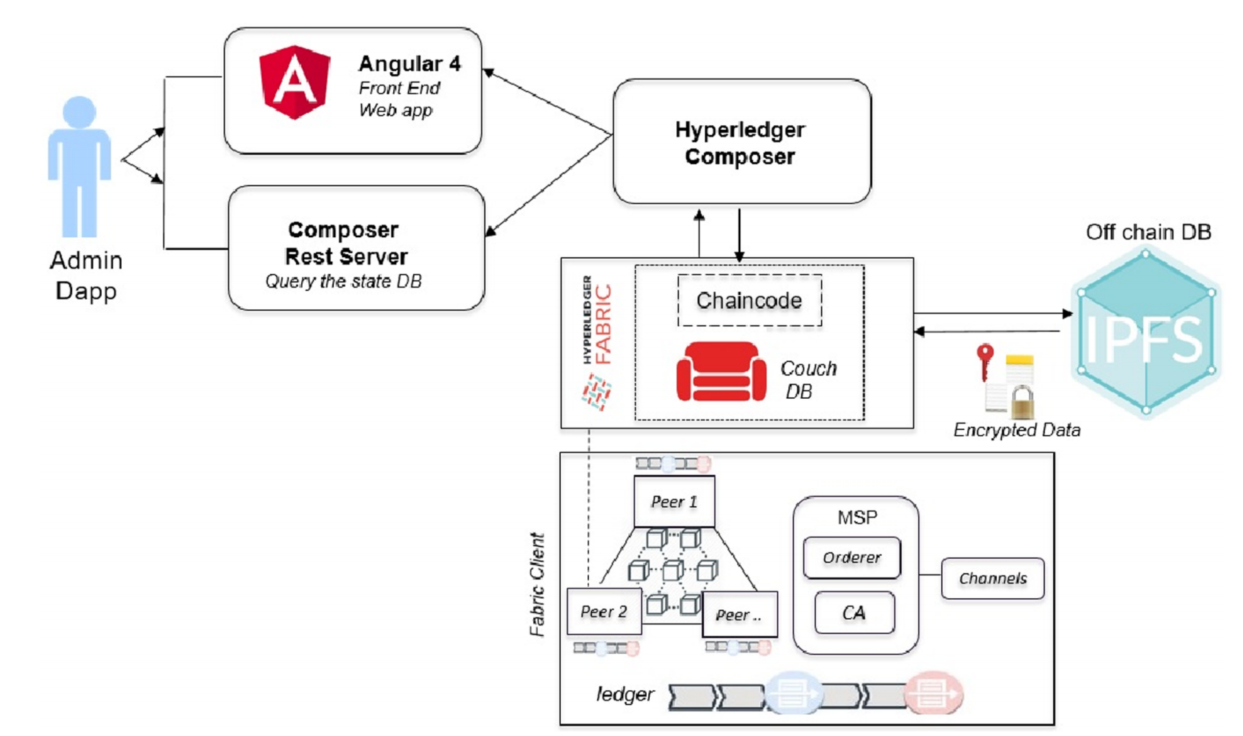
System for Smart Pharmaceutical Industry

Healthchain是一个注重隐私保护的区块链医疗电子病历的框架。它的重点是确保病人的隐私和数据安全，同时在分布式环境中共享组织以及医疗提供者的敏感数据。Healthchain是基于区块链的隐私保护框架，维护电子病历的安全性、隐私性、可扩展性，解决了现有系统单点故障的问题。该框架基于Hyperledger Fabric，并使用IPFS技术存储电子病历，把大量的医疗记录存储在离链IPFS数据库中，通过独特的加密算法对IPFS中存储的数据进行加密。大量的医疗数据存储在第三方集中式服务器上会加大安全的成本，使用区块链能显著提高效率。

Healthchain建立了一个以病人为中心的框架，在这个框架中，病人将对他们的医疗记录有完全控制权，拥有安全性、隐私性、可伸缩性和防篡改的性能。Healthchain框架建立在Hyperledger Fabric上，使用CouchDB作为链上数据库，利用Hyperledger Composer并将电子病例存储在IPFS中来构建这个私有的Healthchain网络。此框架使用智能合约处理交易系统的应用逻辑，特别是数据传输、访问管理、请求处理（如更新病历）、允许医生书写、向其他医生提交报告、更新所有权、与药剂师沟通[1]。 智能合同将在用户交互期间执行，以识别请求、验证请求和授予访问权限、更新病历权限。由于其去中心化的特性，该框架解决了单点故障的问题，并且对区块链的更改将对区块链的节点是透明的。同时为了保证区块链的读写效率，此框架只在链上存储数据的哈希值，真实的完整数据存储在IPFS中的离线存储框架中加密后去中心化存储。链上的数据通过PBFT共识协议认证进行添加。存储在IPFS中的数据通过独特的加密算法进行加密。该框架侧重与保证病人的权力，病人对自己的数据有完全的控制权，可以授权给医院访问，且没有挖掘激励的机制影响系统使用。

下图是Healthchain的架构，Angular4是DApp的前端框架，连接着Composer Rest Server，Composer Rest Server将CouchDB数据库可视化并公开。DApp通过Angular框架与用户界面交互，通过Composer Rest Server的REST API处理用户对Fabric的请求。REST API用于检索链上数据库CouchDB的当前状态，其中Angular框架通过对Composer Rest API的GET调用检索数据。Hyperledger Composer构建区块链网络，为应用程序创建智能合约。Healthchain的框架在Hyperledger fabric中利用CouchDB存储链上数据，离链则使用IPFS存储。Healthchain上的交易记录会被完整的保存在链上，且仅对相关人员可见。一旦数据被篡改，就会导致链上哈希值与数据不匹配。工作原型是在Hyperledger fabric区块链上实现的，方法是使用Hyperledger Composer为单个组织创建Web应用程序，方法是合并三个对等节点，三个节点分别用于验证、排序和注册网络参与者的公共通道，使用Kafka排序算法。通过CouchDB和IPFS可以扩展到其他的多个节点中，具有可伸缩性。通过分布式账本和其智能合约更新与其他节点的连接。设计了一个单通道，以便Hyperledger Composer可以通过该通道通信对等点。当交易执行时，链码将安装到对等节点，通过交互调用链码查询修改账本。交易存储在块中，每个块中主要包括交易的工作量，前块的哈希值和当前交易的哈希。

该系统使用特殊的公钥密码技术对IPFS中的数据进行加密，当医生请求访问存储在IPFS中的患者数据时，通过算法生成加密的记录存储在IPFS中，并将密钥发给医生和患者。医生用会话密钥对更新的记录进行加密并上传到IPFS后，完成此次会诊。系统将通知患者记录更新。系统使用会话密钥解密更新的加密数据，从IPFS中用病人的私钥解密加密的医疗记录。最后，系统将更新提交给原始记录，用病人的公钥加密原始记录并上传到IPFS。每个会话的会话密钥和加密数据将在会话完成后到期。



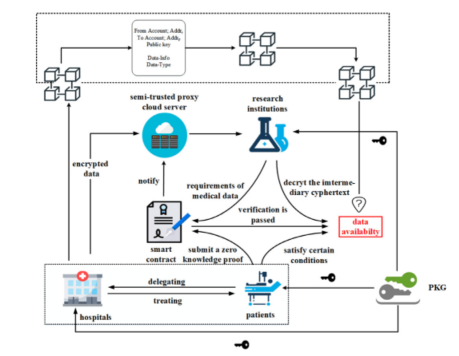
[1] Chenthara S, Ahmed K, Wang H, Whittaker F. A Novel Blockchain Based Smart Contract System for eReferral in Healthcare: HealthChain. In: International Conference on Health Information Science. Springer; 2020. p. 91–102.

<https://doi.org/10.1371/journal.pone.0243043.g005>

<https://doi.org/10.1371/journal.pone.0243043.g006>

[1]提出了一种基于区块链的隐私保护方案，特别是当多个实体与智能合约交互时，这个方案主要是涉及患者，研究机构和半信任云服务器的几个实体之间医疗数据的安全共享。该方案采用PBFT共识算法和零知识证明来验证患者的医疗数据是否符合研究机构提出的要求，不会暴露患者的隐私，然后采用代理再加密技术，确保研究机构能够解密中介密文。

在方案中，患者可以通过构建基于zk-SNARK的可信零知识证明并提供给智能合约进行验证，从而证明其医疗数据满足研究机构的要求而不泄露任何隐私。 一旦验证通过，患者和研究机构之间的交易将根据先前的协议在区块链中发布，以获得分布式共识，PBFT共识算法的计算成本低，所以选择PBFT共识算法。系统模型如图所示。



系统模型共涉及七个实体：1)患者；2)医院；3)研究机构；4)私钥生成(PKG)；5)半信任代理云服务器；6)区块链；7)智能合约。

私钥生成中心PKG是完全可信的，它不会执行非法操作。 此外，解决方案中的块只存储一个索引，其中包含指向病人记录的哈希指针，相应的加密数据被外包并存储在代理云服务器中。

该方案的步骤如下：1）研究机构根据满足其要求的医疗数据生成zk-SNARK的零知识证明，然后记录相关的计算结果、零知识证明和智能合约的哈希值。最后，在区块链系统中发布智能合约。2）患者只能安全加密算法，通过公钥对其数据进行加密，然后将密文发送半信任的代理云服务器。3）患者提交交易给块，然后对交易签名。系统会将医疗数据的哈希值存储在Hyperledger fabric的区块链上。4）患者可以提交符合医疗机构要求的数据换取奖励，这一过程需要根据医疗数据生成可信的零知识证明。5）病人提交零知识证明从而通过智能合约，智能合约会自动将患者的零知识证明和计算结果和哈希值分别与研究机计算的零知识证明、计算结果和哈希值比较。6）通过验证后，智能合约会通知病人生成新的密钥，再把密钥发送给半信任代理云服务器，服务器公钥会对新生成的密钥加密。7）半信任代理云服务器解密再加密新的密钥，再把密文转化为研究机构可以解密的中介密文，然后发送给研究机构。8）研究机构对收到的密文用私钥进行解密，获得医疗数据。在此过程中，半信任代理云服务器无法获取任何详细的医疗信息。9）最后，通过智能合约向验证节点提交交易。 该交易记录患者与研究机构之间的这次数据共享信息，并将用PBFT共识算法验证后在区块链上发布。

在此方案中，所有的医疗数据都是由患者在上传到半信任的代理云服务器之前使用安全加密算法进行加密的。 假设医疗数据加密算法在安全模型中是足够安全的，无论是内部还是外部都不能在不获得解密密钥的情况下破解密文。因此，半信任的代理云服务器或其他恶意攻击者无法推断任何密文内容的任何信息。可以使用患者提供的转换密钥将加密的医疗数据重新加密为中介密文。只有经过数据所有者授权的研究机构才能解密中介密文以获得有价值的真实数据。智能合约和其他实体甚至没有机会接触加密的医疗数据。

只有授权的实体才能使用他们的私钥来解密病人的医疗数据。此外，患者可以根据自己的医疗数据生成完全可信的零知识证明，并将其提交给区块链上的智能合同。零知识证明可以用来验证患者的医疗数据是否符合研究机构建议的某些条件。这一特性确保了具有供需匹配的数据可用性。

患者需要将其数字签名附加到由其医疗数据生成的零知识证明上，而数字签名的私钥只能由自己保存，不能由其他实体获得，从而保证了零知识证明的真实性。患者在区块链中记录的医疗数据已经通过PBFT算法达成共识。块的顺序和交易用哈希保护，每个块的哈希值是唯一的，一旦对抗篡改攻击，其他块的哈希值就会改变。

在注册阶段，患者或研究机构将严格接受fabric检查，以确保区块链的所有参与者都是合法的，然后fabric将为每个参与者生成伪身份。因此，参与者的隐私将受到保护，因为在随后的过程中使用伪身份而不是真实身份。在数据共享过程中，任何参与与智能合约交互的实体都不会披露患者的数据隐私，智能合约只能获得零知识证明而不是原始私有数据。此外，研究机构只是发布一些关键词，而不是整个要求，以实现部分隐私保护。这种方式防止对手根据整个要求伪造医疗数据。

一旦患者和医疗机构达成共识，他们共享医疗数据的行为将存储在区块链中。例如，如果任何一方有非法操作，患者在没有遵循先前的独家许可协议的情况下将其医疗数据出售给其他研究机构，则将追究其责任。

[1] A blockchain-based scheme for privacy-preserving and secure sharing of medical data