

基于区块链的医疗药品溯源

目录

[1、背景 3](#_Toc8205)

[2、现状 3](#_Toc9787)

[3、区块链帮助解决医疗数据平台痛点 5](#_Toc21788)

[4、区块链医疗的亮点 11](#_Toc16038)

[1.分布式账本，去中心化 11](#_Toc12340)

[2. 非对称加密，数据不可篡改 12](#_Toc24315)

[5、区块链医疗的挑战 12](#_Toc24198)

[3.智能合约 14](#_Toc14769)

[4.通证生态激励 15](#_Toc25207)

[6、区块链技术在医疗中应用场景 17](#_Toc8772)

[1.电子健康病例（EHR） 17](#_Toc14766)

[2.DNA钱包 18](#_Toc8046)

[3.医疗支付与理赔 18](#_Toc6376)

[4.药品的回溯与防伪 19](#_Toc24629)

[5.身份认证 19](#_Toc4941)

[6.健康管理 20](#_Toc12922)

[一、设计方案 21](#_Toc28996)

[二、架构设计 24](#_Toc20202)

1、背景

医疗行业是一个与居民生命和健康息息相关的产业。目前，我国城市医疗体系已基本健全，农村以及社区医疗体系正在逐步完善中，医疗行业平稳发展。过去五年，由于新型农村合作医疗制度的推进、城市社区和农村卫生服务体系的完善，医疗行业平稳发展。

2、现状

1、需求现状:人均医疗保健支出大幅增加，门诊和住院人数持续增加，医疗机构诊疗人次达近年高峰;费用方面，人均医疗费用继续增加，但涨幅呈下降趋势;门诊及住院病人药费比重下降,检查治疗费比重上升，“以药养医”比重下降。

2、民众对于医疗的重视程度与日俱增，矛盾也日益增多，如何才能缓解，甚至化解这些矛盾，成了众多医疗健康领域从业者都承认的痛点与难点。前几年，互联网发展势头强劲，孕育出了很多互联网医疗产品，如好大夫、春雨医生等，这些产品都是从某些角度使寻医问诊的流程更加扁平化，但仍未能解决医患之间的最基本矛盾――信任问题。

一方面这些医疗平台收入不稳定、时间不固定，医生不愿在上面倾注过多时间和精力。另一方面，在线问询的效果十分有限，很多时候并不能满足患者的需求，从而降低了持续获客能力。看病难、看病贵、医患信任难题,这一切矛盾都源于医疗服务本身具有极高的信息不对称性，以及医疗资源的稀缺性。

3、医疗数据平台存在的问题

医疗数据平台工作是收集数据，核心是为了数据应用与共享。但医疗数据平台在收集与共享方面也有许多问题,包括数据质量不高、存在信息孤岛、篡改失真、记录遗漏、泄露个体隐私、数据灰色交易等等。这些问题阻碍了数据平台的发展,信息不能得到流通和共享，对新医改的政策没有帮助。

数据收集缺乏统一标准，无法形成患者完整画像

目前，每个平台都有一套自己的标准但都不完善，收集的信息也大多是零散信息，异结构化、半结构化数据偏多，而这些不完善的数据汇集到一起时又会存在整合困难的问题。总体来看，信息收集缺乏统一标准，忽略信息收集的全面性，导致各机构只收集需要的信息，对患者不能形成完整画像。最终，也就无法形成一套记录患者完整医疗信息的数据系统。数据分类模糊，缺乏价值数据等级

医疗数据有很多细分，如医院信息、器械信息、医生诊断信息、患者信息、健康信息等，现阶段在处理数据时对细分信息的归类还有待改进。类似于患者服药量、临床数据、影像资料等有价值的数据比较匮乏，因此需要建立数据价值标准从而形成数据等级的划分。

网络安全压力大，获取信息成本降低

虽然法律法规明确保障了医疗健康领域的数据安全和隐私，但互联网领域的快速发展,使得越来越多的设备接入到网络,给网络安全带来极大隐患。据调查，防止医疗数据泄露的费用有所增加，平均每个记录为380美元，而数据维护成本也下降了10%。由此可见，盗取信息的成本在降低，患者信息数据泄露的风险在加大。

3、区块链帮助解决医疗数据平台痛点

区块链天然适合记录数据信息。医疗数据行业完全能利用这一优点，把不准确和存在差异影响的医疗记录上链。

目前，区块链技术在医疗行业中，应用得最多的就是医疗健康数据的分布式账本记录。如果在建立病历时，由医疗专业人员负责确保敏感病历的准确性、完整性，并且让这些病历信息只有获得授权的人员才能得到，这将使患者获得更高质量的医疗服务。

使用区块链技术构建的电子病历和疾病数据，能完整记录包含生命体征、记录服药、诊断结果、病史手术等健康数据，以及医护人员、地点、器械相关等涉医数据。各医疗机构根据收集的完整数据链，再提取各自所需信息，克服了收集与数据处理没有统一标准的弊端。

当前医疗信息大道交通严重堵塞主要源于数据收集不统一与信息被盗取的风险极高两大痛点。对此，区块链的治愈之道可从目前已处于风口中的数字病历应用窥知一二。区块链技术可提供统一的数据存储结构，每一笔医疗交易所经过的客户端都成为数据服务器，病人的生命体征、体检记录、诊断结果，以及医护地点、人员、科室、器械等涉医数据都将完整地纳入区块链，以节点数据存在。各医疗机构在收集了完整的数据链之后，可提取所需信息，可以突破收集与处理数据缺乏统一标准的局限，从而更好地了解患者的生理信息，以采取更准确的治疗方案。在分布式查看共享的机制下，可以通过区块链的身份识别技术和治理规则，预先定义用户的访问权和身份匹配机制，保证只有授权的参与方才能接触信息，从而确保数据准确透明。如果出现患者基本信息填写错误，只需获得链上参与者的一致共识，或者一半以上网络参与者的更改批准，就可以更改历史数据区块，这可以兼顾信息安全与灵活度。在整个过程中，病历的所有权掌控在患者手中，患者可根据自己的就医路径自行决定数据共享的对象，实现历史信息的共享，便于精准治疗和疾病的预防，重现就医本身所需的人性化。微信智慧医院当前已基于区块链技术更新了智慧医院3.0版本，除涵盖1.0版本和2.0版本的所有功能之外，还增添了处方流转、药品配送等功能，确保所有参与方的数据上链保存，实现链上实时监管以保护个人信息。

当前，在对信息数据的分类和处理上，医疗行业仍显粗糙模糊。其实，医疗数据的细分领域极多，需要制定数据价值标准，形成数据等级划分。除基本病历信息之外，区块链可为医疗信息大道开拓信息来源，提升数据价值的整体深度。首先，患者的授权信息也会上链形成对照，简化医疗审批流程。其次，区块链还可作为平台型工具，用于集成其他设备，如可穿戴设备、专业医疗设备等的数据，提供患者的服药量、临床数据、影像资料等有价值的信息，进而提供基于个体差异的个性化护理。篡改手术记录以粉饰医疗事故的案件并不鲜见，因此手术记录也是未来数据上链的重点对象。区块链可以记录存储完整的手术过程，以确认医疗事故的真实责任人。链上了解医疗事件事实的可信方还可以将信息添加到系统中，从而提高记录的准确性和可信度。此外，由于涉及重大的财务利益，临床试验数据被篡改的可能性也很高，再加上患者生物学测试包含大量的统计数据和大量的研究人员，临床数据跟踪的难度很大。区块链在这个场景中便可大显身手，即使大多数人的动机不纯，急于公布具有结论性的试验结果，也很难逃离哈希值强大的可验证特性。因此，区块链可降低利用临床数据欺诈的风险，推动科研界多方可信赖的协作进展，降低研发成本，加速为更多的患者提供有效的治疗方案。

区块链具备的身份识别特性与智能合约自动执行功能在未来的医疗行业中也有很大的应用空间。基于数据实时集合并经过身份验证之后，医疗保健服务者在访问数据之前也需要“过安检”，身份核查无误后才能对数据进行监测和分析，以此保障患者所接收的私人化建议和定制化保健计划的可靠性。不仅如此，过了“安检”的临床主治医生还可以跟患者一起制定合同条款与授权文件，设定疗程的目标与流程。患者的病史和影像资料将作为科研

学习的参考资料，利于医生建模，寻找病理规律。在监测患者医疗数据的过程中，可深度挖掘区块链的智能合约功能，预置各种响应条件以探索智能护理的不同可能性。比如，链上可设置一次性阅读机制，如果在医生阅读后数据可以被销毁，便可保证患者健康数据的隐私性。又或者设置监测指令，一旦某个指标超出标准，会自动完成挂号，就医诊断的流程便可更为顺畅。对于患者而言，可以利用智能合约实现对数据访问的商业化。其中的一个可能性是，患者向制药公司收费，授权公司在药物研究过程中访问或使用有关他们的数据。医疗保险一开始就像一支镇静剂或强心针，给予患者与家属希望之光。然而在进入冗杂的保险报销流程之后，这根救命稻草就变得越来越沉。大多数患者心里对“如何报销”与“何时报销”的疑问与恐慌一直得不到回应，很多时候医疗保险反倒沦落成患者的心理负担。当前医疗信息主要掌握在医院手中，医院数据保护与防泄露机制的存在使得各个医疗机构之间存在很高的访问壁垒，保险公司因而无法立即获得医疗数据，需要参保人提供各种相关证明。也就是说，在获得理赔之前，投保人需要先向医院支付医疗费用，然后再用从医院获得的相关费用文件向保险公司申请理赔，这会耽误将救命稻草及时送到患者手中。对于保险公司而言，管理成本也很高，无论是合同签订、数据库维护、款项收支，还是理赔检查、资料审定，都面临耗时耗力的痛点问题。同时，医保监管体系水平不高，没有针对不同地区之间的政策差异及时调整，滞后性较严重，且国内各地区之间均存在医保目录范围和报销比例失衡的现象。

在区块链系统的运作下，索赔支付和保险裁决可以在一个相对简单的逻辑下自动化处理。相关数据以区块链要求的格式存储上链，节省了在信息纠正和信息索取等方面的时间滞留。医院数据的确权则保证了数据不可篡改、安全共享，有效避免了在解决合同争议上耗费时间。即使投保人没有申请理赔，医院与保险公司的账本联动也可以进行自动化的验证，理赔流程依然可以自动执行。在保险公司接收到医院自动发送的相关文件后，赔偿金

会自动支付给投保人，减轻患者和家属的心理负担，也推动流程高效运转。由于这种就诊数据的实时动态参访，医保机构还可以展开对数据的预测工作，推动高级分析基础上的顶层保险精算决策和规划。区块链全流程的数据留痕也将大幅度减少医保中心的监控负担，赋能医保支付资格的审查工作。

现阶段，在发展中国家出售的药品10%～30%是假冒的。欧洲也是重灾区，假药制品每年会给医疗行业带来1020万欧元左右的损失。生产环节长期存在制造商伪造数据、篡改产品检验记录、变更工艺参数等问题，流通环节的封闭失控，以及供应商之间的信息不对称，都提供了无数造假机会，网购的发展进一步模糊了医疗产品的来源，给患者的身心健康带来不少潜在风险。区块链的出现则可以排除制造商、批发商、终端药房对药品信

息的干预，实现生产、流通全周期公开透明。

基于区块链的溯源系统并不是由一个实体或组织运作，而是由多家实体，包括开发商、分销商和医院这些上下游单位共建数据库。具体而言，制药公司将具有唯一性的RFID标签贴到药品上，用于监控药品的身份动态。在供应链全链条中，药品从生产、质检、入库、出库、流通的各节点都留有RFID识别码的痕迹，作为交易过程统一协议的标准，在交易结束时以数字方式签名。在高效的区块链中，上链标准可以完全确保假冒产品无法渗透，一旦被发现，假冒产品也会被精确召回。如果有药品失踪导致传输中断，那么各方也可以通过区块链账本上的数据快速追踪定位其最终位置并及时找回。

在消费端的使用上，区块链将增强患者对制药行业的信心。医生在开处方时，将相关信息上链，确保药物开得准、价格开得合理。消费者将配备数字证书，即密钥，用以查询详细信息。具体来说，消费者在购买过程中将个人数据上传至区块链，使得购买信息透明化，通过与区块链上的信息相互对照确保药品的合法性，同时满足监管要求。一旦消费者或机构在供应链终端发现假药，区块链的优势便显现出来，因为每个节点的信息都不可篡

改，且具有身份存取的权限机制，经过信息比对，可迅速查明药品问题出现在哪个具体环节。

天津市于2019年12月1日正式开放了疫苗追溯监管平台，实现疫苗生产、运输、仓储、配送、接种全部环节相结合，以及生产企业、流通企业、疾控机构、医生、受种者、监管人员全覆盖。更重要的是，它实现了平台与国家疫苗追溯协同服务平台的连通。该实践的交付包括面向公众的疫苗查询系统、面向疫苗生产企业的企业服务系统、面向监管人员的监管系统。公众可通过三个官方App，扫描条形码或输入疫苗批号以查询相关信息。监管人员也可提供预警、召回及销毁相关药品。

在药品溯源领域，区块链的智能合约在未来也有施展拳脚之地。国家药监局会给每个药企发放一个GMP（生产质量管理规范证书），要求企业全面确立作业规范。如果GMP可以全面嵌入区块链溯源系统，一旦企业不符合要求，可设置扣分或吊销证书等惩罚，并将这些不可篡改的记录保存下来，提高作恶成本。反之，若企业稳定保持良好信誉，则可通过智能合约技术实现信誉积分，以激励药企合规作业。

然而，药品溯源不能仅仅依靠“术”，还需要“法”和“道”。国际上在药品溯源方面较为典型的区块链药品追踪项目Medi Ledger，目前已成长为医疗界的区块链联盟典范，收纳了25名成员，其中包括辉瑞、基因泰克等制药商，以及三大制药批发商—麦克森、美源伯根和嘉德诺，最近也吸引了零售业巨头沃尔玛加入。然而，联盟的壮大还需各方克服在透明度上的意愿障碍。数据要上链，就需要有分享精神和节奏相当的行动配合。在药品溯源层面上，由于所有上链的数据具有互操作性，各利益相关方需愿意同行，在多技术的集体支持下齐头进入透明系统，推动链上数据的有效多方交叉验证，形成更有约束力的监督机制。

4、区块链医疗的亮点

1.分布式账本，去中心化

分布式账本指的是交易记账由分布在不同地方的多个节点共同完成，而且每一个节点记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证。

跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：

一是区块链每个节点都按照块链式结构存储完整的数据，通过“时间戳”技术和链式结构实现数据信息可追溯，每个事件和交易都有时间戳记，成为一条长链或永久性记录的一部分。

二是没有任何一个节点可以单独记录账本数据，从而避免了单一记账人被控制或者被贿赂而记假账的可能性。也由于记账节点足够多，理论上讲除非所有的节点被破坏，否则账目就不会丢失，从而保证了账目数据的安全性。

2. 非对称加密，数据不可篡改

非对称加密指用一个密钥对来进行加密和解密。加密和解密使用不同的密钥，通过公钥加密的信息，在网上即使被截获也无法解密，因为公钥加密后的信息不能再通过公钥解密，而必须使用私钥来解密，而私钥只有自己有，就可以保证信息的安全性。

所以，存储在区块链上的交易信息是公开的，但是账户身份信息是高度加密的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。此外，区块链上的数据无法被篡改，而且在区块链上的任何篡改都会留下密码学上的证据从而被快速发现。

5、区块链医疗的挑战

医疗机构信息化覆盖程度参差不齐

医疗大数据的主要来源是医院，而医院医疗大数据的汇集主要依赖于院内信息化建设的程度。由于医疗机构的信息化发展时间较短，从总体上看信息化覆盖程度不够。以中国为例，三级医院和三级以下医院、经济发达地区和经济欠发达地区还具有一定差别，特别是高集中度、高共享度的医疗信息化解决方案覆盖还不够。中国医院协会信息管理专业委员会(CHIMA)发布的2015~2016年度中国医院信息化状况调研报告统计报告显示，在342家三级医院、194家三级以下医院样本医院中，电子病历系统(EMR)实施比例为71.05%，而区域卫生信息系统实施比例仅为8.77%。从全国范围看，医疗软件信息化市场远未饱和。

医疗数据来源可靠性问题

孕育期的区块链药品溯源，同样需要跨越三大障碍：生产源头作假与掉包问题，即区块链只能提供信息化的技术，并不能解决造假和掉包的问题；数据来源可靠性问题，即能保证上传数据不被篡改，但不能保证数据本身不因人为因素导致数据不真实；利益相关方的参与问题，也就是区块链应用的前提是各利益相关方的分享意愿，引导企业上链还需要一定的教育工作。

区块链技术发展瓶颈

区块链的tps，智能合约的安全性，目前还存在不小的瓶颈制约，有赖于高性能公链的出现。区块链目前的主要缺点是延时高、交易速率慢，目前区块链应用尚在初创开发阶段。比之于互联网技术，人们可以用浏览器、APP等具体应用程序，实现信息的浏览、传递、交换和应用，但区块链明显缺乏这类高效的应用程序，在技术层面尚需突破性进展。

通证的法律风险

由于各国的文化、认知、经济等差异，势必造就了对新生技术的态度与政策差异。鉴于对新生科技的风险未知性，目前全球各国对于区块链项目的发展均没有相对统一的市场管理原则与法律监管环境。这其中以区块链项目通证表现最为突出，比如有些地区合规、有些地区禁止等。比较混乱的全球政策环境，也是融合扩大发展的重要制约因素之一。

3.智能合约

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。基于这些可信的不可篡改的数据，能够采用完全自动化的流程，不需要任何人为参与，只要满足智能合约代码所列出的要求即可自动化地执行一些预先定义好的规则和条款，这些交易可追踪且不可逆转。优势是更高效率、降低成本、交易更准确，且无法更改，此外，智能合约去除任何第三方干扰，进一步增强了网络的去中心化。

4.通证生态激励

区块链的通证经济想要把本来免费的社会行为变成被金钱衍生品激励的市场行为，并想象这样可以精准量化，定向生产有价值的行为结果。通证除了承担支付或价值贮藏的角色，还被设计为如股权、金融资产、奖励积分等更复杂、多元的功能。在去中心化的区块链世界里，激励机制是利益分配和使用的核心点，通过激励机制达成网络共识，从而使得区块链每个环节的参与者都能获得相应的回报，进而分工明确、积极的完成各项工作，让系统在很大程度上免受了各种威胁和攻击。这相当于参与者们共同维护了系统安全性，推动了系统的生态发展。

综上所述，区块链是一种多方维护、全量备份、信息安全的分布式记账技术，具有去中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明、等特点。这些特点保证了区块链的“诚实”与“透明”，为区块链创造信任奠定基础。而区块链丰富的应用场景，在于解决信息不透明、各环节参与者激励不足、系统整体运转效率低下等问题，实现多个主体之间的协作信任与一致行动。

区块链对医疗的赋能点

通过区块链技术进行医疗历史数据记录，实现共享数据的防篡改、可追溯。区块链具备高冗余性，分布式存储使得每个节点都有备份，杜绝由于单点故障导致的数据库崩溃情况。通过共识机制来共同记录和维护数据，防止某参与者单方面修改或删除数据，保证信息在区块链上的不可篡改。以此保证了数据的安全性。

区块链技术可以将各机构与患者置于一个受保护的环境中共享敏感信息。通过区块链的密码学技术在隐私保护层面将医疗数据经过加密处理，用户信息具有匿名特性。区块链上的智能合约和非对称加密算法，可生成访问控制机制，并实现多私钥的复杂权限保管。在有权限限制的区块链上，其他人员必须获得私钥授权才能够查看数据，从而维持数据隐私性。

利用通证激励机制，解决数据确权不明晰导致的传统参与者信息化的意愿低问题，最终推动医疗健康领域大数据的发展。

通过“时间戳”技术和链式结构实现数据信息可追溯，解决供应链防伪溯源难题。区块链也可用于监督药物分配，监管合规或管理医疗用品。

通过智能合约的流程自动化，可解决信任问题，降低协作成本并降低差错率。

区块链在数据保密、智能合约、生态激励等方面具有天然的优势，与医疗行业具有较高的契合度，能为医疗行业提供多环节BIS的一份研究报告显示，到2025年，全球医疗保健市场在区块链上的支出预计将达到56.1亿美元。到2025年，采用区块链技术每年可为医疗行业节省高达1000亿至1500亿美元的数据泄露相关成本、IT成本、运营成本、支持功能成本和人员成本，并可减少欺诈和假冒产品。

通过区块链技术进行医疗历史数据记录，实现共享数据的防篡改、可追溯。区块链具备高冗余性，分布式存储使得每个节点都有备份，杜绝由于单点故障导致的数据库崩溃情况。通过共识机制来共同记录和维护数据，防止某参与者单方面修改或删除数据，保证信息在区块链上的不可篡改。以此保证了数据的安全性。

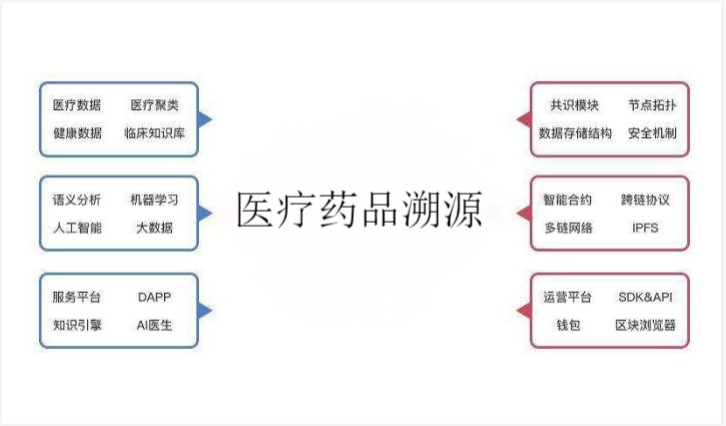
区块链技术可以将各机构与患者置于一个受保护的环境中共享敏感信息。通过区块链的密码学技术在隐私保护层面将医疗数据经过加密处理，用户信息具有匿名特性。区块链上的智能合约和非对称加密算法，可生成访问控制机制，并实现多私钥的复杂权限保管。在有权限限制的区块链上，其他人员必须获得私钥授权才能够查看数据，从而维持数据隐私性。

利用通证激励机制，解决数据确权不明晰导致的传统参与者信息化的意愿低问题，最终推动医疗健康领域大数据的发展。

通过“时间戳”技术和链式结构实现数据信息可追溯，解决供应链防伪溯源难题。区块链也可用于监督药物分配，监管合规或管理医疗用品。

通过智能合约的流程自动化，可解决信任问题，降低协作成本并降低差错率。

区块链在数据保密、智能合约、生态激励等方面具有天然的优势，与医疗行业具有较高的契合度，能为医疗行业提供多环节BIS的一份研究报告显示，到2025年，全球医疗保健市场在区块链上的支出预计将达到56.1亿美元。到2025年，采用区块链技术每年可为医疗行业节省高达1000亿至1500亿美元的数据泄露相关成本、IT成本、运营成本、支持功能成本和人员成本，并可减少欺诈和假冒产品。



6、区块链技术在医疗中应用场景

1.电子健康病例（EHR）

公认的区块链在医疗领域最主要的应用是：个人医疗记录的保存，可以理解为区块链上的电子病历。

如果把病历想象成一个账本，原本它是掌握在各个医院手上的，患者自己并不掌握，所以病人就没有办法获得自己的医疗记录和历史情况，这对患者就医会造成很大的困扰，因为医生无法详尽了解到你的病史记录。

但现在如果可以用区块链技术来进行保存，就有了个人医疗的完整历史数据，看病也好，对自己的健康做规划也好，就有历史数据可供使用，会对精准治疗和疾病预防有宝贵价值。

而且这个数据真正的掌握者是患者自己，并不是某个医院或第三方机构，这对于消除医疗信息摩擦，包括信息不完善、信息风险和信息无法访问等，以及保护数据的隐私性和安全性有重要意义。

2.DNA钱包

基因和医疗数据能够运用区块链技术进行安全存储并且通过使用私人秘钥来获得，这将形成一个DNA钱包。

这使得医疗健康服务商能够安全地分享和统计病人数据，帮助药企更有效率地研发药物。目前这种模式也正在逐步建立起来。

3.医疗支付与理赔

在支付和理赔方面，区块链技术不仅促进了加密货币的发展，还能有效阻止骗保等不当行为，减少医疗资源浪费。

全球每年的医疗总支出超过7万亿美元。其中，个人消费者每年直接自费支付近18％或1万亿美元。这在单一付费机制和商业保险国家都是如此。

尽管经济支出巨大，但医疗服务生态系统还不够完善，不能让消费者享有经济主体的主动权。消费者可能并不知道一些医疗服务的成本是多少，或者他们应该花费多少。

企业PokitDok、Capital One和Gem提出一种由区块链支持的平台，旨在帮助患者在接受治疗前，提前确定自付费用金额，也能提供预付款等服务，避免造成患者意料之外的成本，医疗机构也能减少未收款项。

4.药品的回溯与防伪

区块链的可追溯性，使其可用于药品的回溯、监管与防伪。比如建立药物一致性的物流配送与管理体系，对假冒药品构成致命打击。

因为区块链的数据是即时更新、广泛共享的，药店、厂商、买家、监管部门等多方都能实时观察数据流动，包括药品制造和分销信息，从而加强药品监管，阻止假药进入市场。

据悉，英国Blockverify就是开展药品来源试点项目的组织之一，帮医疗人员通过扫描药品验证真伪。

5.身份认证

在全球范围内，世界正面临着合格医疗从业人员短缺的情况。

一般情况下，医务工作者的身份是一个复杂的数据点组合，它包括了医学教育背景、国家认证的医疗人员从业证书等多个信息。

医务人员的身份和证书的可靠性是确保患者安全和高质量护理的首要因素。但是对医务人员身份和证书的验证牵涉到太多利益相关者，费时又费财，会给本就已经不堪重负的医疗系统带来成本压力。

而利用区块链技术，可以将搭建一个验证平台，允许医护人员、医疗系统和卫生计划，对医务人员的身份和证书进行验证，方便未来医生多点执业。

6.健康管理

大部分健康管理是在医疗体系之外的活动中实现的。特别是随着全球慢性疾病患者逐年增加，世界各地的医疗保健系统正面临成本上升的压力。

基于区块链技术搭建的健康管理平台，可在智能家居/办公环境中运作，让用户能够安全地跟踪并收集个人健康数据。

这些数据多来自联网的可穿戴设备和其它家庭监控设备。在该应用场景下，智能合约将被用于医疗健康识别中，如遇紧急情况，还能触发潜在紧急健康状况的警报，并将适当的信息传递给临床医生和家庭成员。

该智能合约还可以利用健康预防资源创建一个本地可访问的健康社区项目。这种项目会给参与者带来诸多好处，如：

组织对个人或团体健康有利的活动；

使用物联网追踪，制定个性化的预防性医疗护理计划；

管理急性和慢性病的护理计划；

提供针对老年人的监测方案；

处理紧急事项，完善急救护理等。

临床试验

研究表明，制药公司要上市一款新药，平均花费是26亿美元和15年。

由此可见，药物研发所需的成本、精力和时间很难估量。这些成本中的大部分是由于过度复杂的多机构行政和临床试验管理问题所造成的。

如果可以利用区块链帮助机构审查委员（IRB）实现“分散式 IRB”管理，同时对来源于多个试验场所、多个试验患者的实验结果进行评审及管理，就可以降低多中心试验（每个试验站点都有自己的标识码、进程和时间线）方式的试验成本。

关键技术及方法

从计算机科学的角度出发，以太坊可以看作是一个分布式状态机，其中交易区块等同于状态转换函数，新的交易区块由从状态A到状态B的状态转换记录构成。因此，以太坊就像一个巨大的虚拟状态引擎或去中心化的计算机，可供多方共享计算平台并基于此运行智能合约。以太坊有一种原生资产—以太币，它是以太坊生态系统中的价值基础。以太币用于调整运营智能合约的激励机制，同时提高网络的安全性。与比特币比较起来，以太坊是一个应用程序平台，而不仅是加密货币。比特币主要用于交易，而以太坊则可以执行更为复杂的规则，是一个用于构建分布式应用程序的平台。以太坊有一个图灵完备的脚本语言，利用程序代码将合约规则实例化成智能合约。智能合约是表达、验证并协商或强制执行数字合约的一段计算机代码，它可以在没有任何第三方的情况下被以太坊网络自动执行。以太坊的脚本语言比比特币的脚本语言要强大得多，可以实现复杂的智能合约规则。借助以太坊计算平台，开发人员可以用分布式应用程序（DApp）替代集中式应用程序。因为没有集中的数据库可以成为黑客的目标，DApp极大地增强了网络安全性。典型的DApp案例包括去中心化的内容发布平台Steemit、社交网络Synereo、去中心化的打车平台LaZooz、音乐版权平台Ujo Music和去中心化的就业市场Ethlance等。比特币和以太坊之间的另一个区别在于，比特币是基于UTXO（未花费的交易（tx）输出）的，而以太坊是基于账户体系的区块链。在比特币中，交易的所有输入必须在UTXO数据库中才有效。UTXO是先前交易中未支出的金额，需要确认为未花费用作为当前交易的输入，比特币用户的可用余额是由其私钥控制的UTXO总和。而以太坊使用基于账户的模型，用户的可用余额记录在用户的账户中，该账户具有用户的地址、余额以及可选代码字段中的任何数据。例如在比特币中，Alice拥有控制一组UTXO的私钥；在以太坊中，Carol拥有控制由地址、余额和代码字段组成的账户的私钥。通过账户模型，以太坊节点只需更新其账户余额而不是存储每个UTXO，因此更节省空间。同时，以太坊也更直观，因为智能合约是一种更有效的编程机制，其可以在账户之间转移余额，而不是不断更新UTXO集来计算用户的可用余额。以太坊有两种账户类型：外部账户（EOA）和合约账户，这两种账户都有用户地址和以太币余额。EOA通常被用于某种形式的外部实体（如个人或公司），这类用户在注册以太坊网络时都被分配为EOA账户。EOA具有加密地址，它可以发送交易（将以太币转移到其他账户或触发合约代码）。第二种账户类型是合约账户，这些账户具有地址、以太币余额以及任何关联的合约代码。代码执行由从其他合约或EOA中收到的交易或消息（函数调用）触发。这意味着合约是以太坊网络上的自主账户，其他账户（EOA或合约账户）可以与它们进行交互，但没有人控制它们（因为一旦启动，它们就是自治的）。由于其他程序可以调用合约上的函数，因此可以与合约账户交互或执行某些交易，但是不能直接控制合约账户。以太坊账户以交易为媒介，与以太坊网络上的其他账户、其他合约和合约状态进行交互。以太坊某一时刻的所有账户状态构成了整个以太坊的网络状态，它们需要就每个账户的当前余额、存储状态和合约代码达成共识。每个新的区块都需要获取前一个区块的信息并更新新的以太坊网络状态，每个网络节点都必须就新的网络状态达成一致。因此，交易区块是以太坊网络状态之间的状态转换函数。

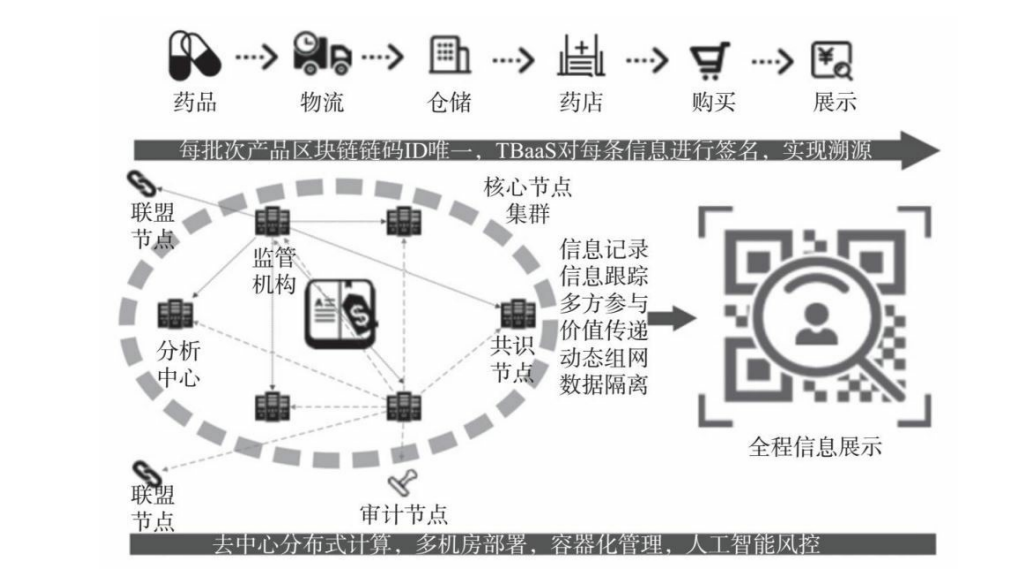
许可链的节点准入机制

目前有很多以太坊项目都是基于以太坊公链开发的，同时以太坊也可用于构建联盟链和私有链。公链的特征是任何人都可以加入、读取区块链数据和发送交易，一般需要激励机制来鼓励记账节点（挖矿）；联盟链是由若干个机构或组织共同参与管理的区块链，每个机构或组织都运行着一个或多个节点共同参与记账；私有链的写入权限由某一个组织或机构控制，参与节点的资格由该组织或机构严格限制。与公链的任何人都可以随时加入不同，未经许可的节点不可以加入到联盟链和私有链，因此联盟链和私有链又被称为许可链，需要进行权限设计。许可链拥有更高的共识效率、更好的隐私保护和更强的安全性，能被更好地应用于金融、政务等领域。考虑到电子证照数据共享业务的安全性需求，本章以许可链的方式设计和搭建区块链底层平台，并加入节点准入机制。任何参与区块链的网络节点都需要先完成身份注册，通过验证后，其数字身份才能被允许接入私有链网络中参与交易，形成自主可控的底层区块链平台。具体来说，以类似会员制的方式实现一种区块链节点的准入机制，通过会员制的注册服务对区块链参与者的身份和权限进行管理。区块链网络中的分布式记账节点、数据共享方节点、查验方节点、其他访问节点等，都需要事先完成节点注册，以使其数字身份合法。特别的，分布式记账节点作为区块链底层平台的核心节点，由政府部门统一部署和维护，并有这些节点执行整个区块链的共识记账功能，其他参与节点无权成为分布式记账节点。参与节点通过区块链客户端完成会员注册后，系统会自动完成注册节点公私钥的分配，并生产合法的数字身份即交易地址。

一、设计方案

基于区块链的医疗药品溯源，这个溯源系统并不是由一个实体或组织运作，而是由多家实体，包括开发商、分销商和医院这些上下游单位共建数据库。具体而言，制药公司将具有唯一性的RFID标签贴到药品上，用于监控药品的身份动态。在供应链全链条中，药品从生产、质检、入库、出库、流通的各节点都留有RFID识别码的痕迹，作为交易过程统一协议的标准，在交易结束时以数字方式签名。在高效的区块链中，上链标准可以完全确保假冒产品无法渗透，一旦被发现，假冒产品也会被精确召回。如果有药品失踪导致传输中断，那么各方也可以通过区块链账本上的数据快速追踪定位其最终位置并及时找回。

从业务功能上来说：医疗药品溯源包括药品的生产、质检、入库、出库、流通。



1. 药品生产：由监管机构对药品原材料的品质进行检查，确保生产源的安全。
2. 药品质检：对成品药进行检疫所检验合格。
3. 药品存储：应严格遵守药品外包装图式标志的要求，规范操作。怕压药品应控制堆放高度，防止造成包装箱挤压变形。药品应按品种、批号相对集中堆放，并分开堆码，不同品种或同品种不同批号药品不得混垛，防止发生错发混发事故。
4. 药品物流：依托一定的物流设备、技术和[物流管理信息系统](https://baike.baidu.com/item/%E7%89%A9%E6%B5%81%E7%AE%A1%E7%90%86%E4%BF%A1%E6%81%AF%E7%B3%BB%E7%BB%9F/3580170" \t "https://baike.baidu.com/item/%E5%8C%BB%E8%8D%AF%E7%89%A9%E6%B5%81/_blank)，有效整合营销渠道上下游资源，通过优化药品供销配运环节中的验收、存储、分拣、配送等作业过程，提高订单处理能力，降低货物分拣差错,库存及配送时间，减少物流成本，提高服务水平和资金使用效益，实现的自动化、信息化和效率化。
5. 药店要求：一、具有保证所经营药品质量的规章制度；二、具有依法经过资格认定的药学技术人员(药师)；三、具有与所经营药品相适应的营业场所、设备、仓储设施以及卫生环境；在超市等其他商业企业内设立零售药店的，必须具有独立的区域(城关地区营业场所、仓库面积要求分别不低于30㎡和10㎡，农村地区适当放宽)；四、具有能够配备满足当地消费者所需药品的能力。资格：要申办药品经营许可证、医疗器械经营许可证、然后还要去办营业执照，税务登记证，卫生许可证，健康证。新开的药店也要施行GSP认证，GSP就是指：药品经营质量管理，一切都要按药品售卖：每一个卖掉的药品都会有相应的记录，药品名称，买入（进货）时间，卖出时间，药店地址等信息都应记录。
6. 架构设计

功能需求包括：

1. 需要建立起高效的机制，对各类扶贫信息整合；要求方便系统的维护、升级和推广，对运行环境不断优化；
2. 需要系统在智能合约基础上将各类信息拆分规划，使其具有良好的人机交互能力，提高实用性；
3. 其次需要增强系统的实用性与美观度。

非功能需求包括：

1. 系统需要具有普适性、安全性，能保证数据的安全；
2. 系统的可维护性要好；

系统具有良好的交互性； 系统需要保持较低的故障率

为真正实现药品溯源，药品溯源区块链平台通过“静态数据展示、动态数据管理、 监督比对审查”三位一体的方式，为溯源工作的开展提供了重要抓手，为分辨真假的全面胜利保驾护航。

本系统是一套基于B/S架构、以区块链技术为依托的管理服务与辅助决策平台，按照信息的流转过程，该系统的总体结构从上到下主要拥有以下5个层次，依次为: 基础设施层—网络传输层—数据资源层—应用服务支撑层—应用服务层—用户接入层。

基础设施层：主要包括服务器、存储、网络设备、安全设备，有时也考虑跨平台的需要，对应的操作系统因情况而定，还有些中间件等等。

网络传输层：作用是为不同主机的不同应用提供通信服务。例如互联网、移动通信网、电子政务外网、vpn专用网和一些其他数据传输网。

数据资源层：用来存特效药库存，金额数据。通过对数据库逻辑的设计，对数据库进行操作，将需求用户主要信息模型化，使用户通过接口或 WEB 客户端对数据库进行一定规则的操作。通过对需求的分析，对于应用层的设计，通过前端界面对相关功能进行调用。

应用服务支撑层：具体包括数据交换服务、数据分析能力、网络化管理等。

应用服务层：分为四大模块，

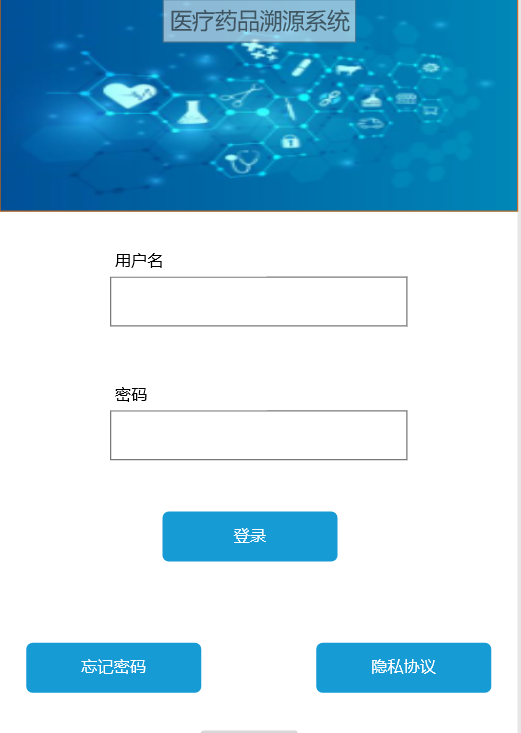
1. 基础数据管理平台，其中又划分为药品储存、项目计划管理和药品帮扶管理。
2. 日常工作管理平台，划分为重点工作管理、信息变更管理、工单管理和问题上报。
3. 药品监督比对平台，包含需求药品对象比对、综合分析、行业信息比对和帮扶计划比对。
4. 药品溯源移动应用平台，有药品监管、用户管理、个人资料中心及特殊需求人群帮扶。

用户接入层：指网络中直接面向用户连接或访问的部分。如web接入、手机APP、微信公众号等多媒体平台方式。

该平台支持云部署架构，平台建设模式采用统一部署，分散接入。 移动终端通过 3G/4G/5G 网络接入互联网实现与药品溯源区块链平台数据交互。外部数据通过防火墙等安全设备后接入药品溯源平台。

1. 系统前端表现层设计

前端表现应该有用户登录界面，用户管理界面，购买界面，及相关机构对药品的认证界面，和药品的详细信息介绍。





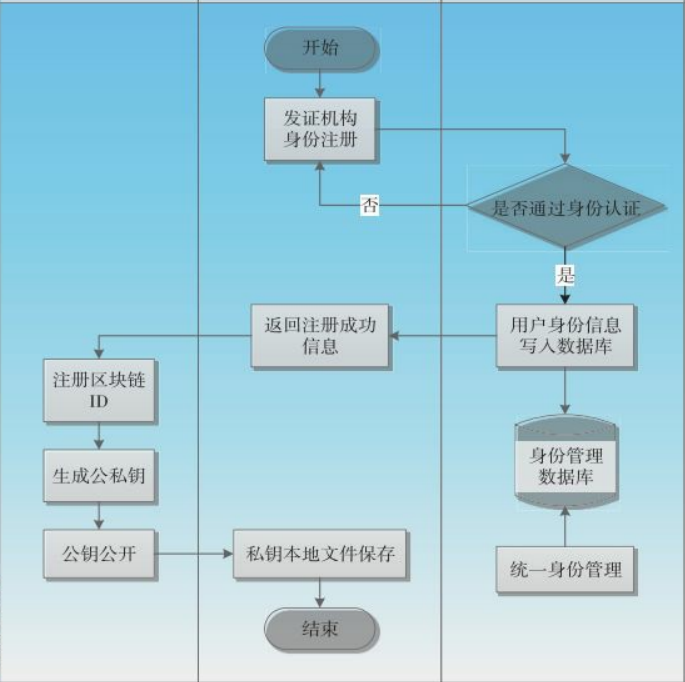
交互设计

1.身份认证阶段

身份认证系统主要涉及区块链平台、用户App和后台管理系统的交互。对于业务系统注册账号分3个不同的角色：普通用户、制证机关用户、查验机构用户。

普通用户身份认证：在app上身份注册，后台进行身份认证，确定成功，将用户数据写入数据库，并向用户返回成功信息。其次，注册区块链ID，由用户信息（姓名、单位、城市、国家及其

他代表用户身份的信息）生成全网唯一的身份标识，根据这一身份标识，判断用户是否为新用户。我们利用Hash算法生成全网唯一身份标识。原则上，同样的输入会产生同样的Hash输出，而不同的输入产生的输出肯定不同。这类的Hash算法有很多，我们主要采用SHA3、最大量2128算法。后台管理系统可以保存当前区块链中所有用户的全网唯一身份标识，可将认证机构根据用户信息生成的全网唯一身份标识与存储过的全网唯一身份标识进行对比，来判断该用户是新用户还是老用户：若未找到存储过的全网唯一身份标识则为新用户，否则为老用户。



各大医院机构认证：对患者信息接入数据库，并和系统连接检测注册用户的真实性。

药品监管机构：由国家专门机构对特效药进行监管并统一上链。

药品售卖：每个注册的用户都是由各个医院进行过身份认证的，对每个人的病史都有相应的记录，且平台会推荐相关药品，和健康保护方面的建议。

总结：经由国家相关机构，医院信息记录，用户身份认证，三者相结合的方式，向有相关需求的用户提供需要的药品和疗养建议，为看病难，买药难，和可能会被一些医疗保健品欺骗的人提供了可信任的平台，给病人安心和放心。