# 一 医疗区块链介绍

1. 区块链的应用场景

传统的医疗模式主要提供基础设施的使用，在医护人员的帮助下完成诊断。这样的卫生服务的质量既取决于基础设备的完整，也与医护人员的水平有关。虽然各国的医疗制度或有不同，但核心原则基本是一样的，都是通过基础设备来支持各种医疗服务。随着技术的快速发展和人民对医疗水平需求的提高，传统的医疗平台面临着严峻的挑战。与此同时，各种新兴技术尤其是区块链的发展有可能为医疗行业带来新的解决问题的思路方法。

区块链作为一种去中心化的技术，提供了更加安全的信息存储机制。这使得信息可以由多人一起维护，不再受中央机构控制。每个人都可以在开放的分布式网络中共享和使用这些数据。因此，拥有去中心化、透明、匿名性、可追溯等特性的区块链技术在健康医疗领域有了越来越多的应用场景。据IBM称，70%的医疗领导者预测，区块链将在改善临床试验管理、法规遵从性以及共享电子病历的分布式结构这些方面产生巨大影响。到2022年，医疗区块链技术的全球市场预计将超过5亿美元 [1]。

在中国，传统的看病流程是拿着个人的病例记录本去到医院挂号就医，然后由医生在病历本上记录此次就医的各种信息，但是有一个很广泛的问题就是这个病历本很容易丢失，且丢失后难以找回特别是记录在本子上的就医信息。尽管各国的方式会有不同，但本质上传统的医疗诊断服务在当前电子信息时代已经暴露了与许多问题。医疗服务记录的丢失导致了患者每次去找新的医生就医时，都要花费大量的财力和时间去重新做医疗检查，这严重拖慢了患者的治疗进度，甚至会延误珍贵的治疗时间。所以，医疗服务的记录无论是对医生还是病人都至关重要，这甚至可以代表一个人的健康状况，就更需要好好的保存。在这个电子信息技术高速发展的时代，互联网无疑是保存病例记录的最好方式，但是病例涉及到个人隐私问题，不能轻易的放到网络中，就需要使用到区块链技术来提供安全的存储。区块链具有匿名隐私性，既可以保护患者的病例记录不会被暴露，也可以让医生等医疗服务提供者可以得到患者的过往就医记录。仅这一点就可以大大的提高就医的效率，方便患者对个人信息的管理。更有利于医生对不同的病人提供更加具体有针对性的医疗服务。

对个人而言，区块链可以有效地帮助他们自己保存个人的病例，而对医院这种医疗服务的提供者来说，无论是药品的供应链管理，还是不同医院之间安全的共享病人信息，亦或是医疗研究方面临床试验的记录和医疗教育的管理，在多方面都可以明显的看到区块链的用武之地。就比如药品的供应链，通过区块链可追溯、防篡改的特性，可以提供对药品无论是出厂阶段还是物流阶段的实时监控，保证药品及时、安全的送达一线，供患者购买使用。特别是在新型冠状病毒肺炎（COVID-19）泛滥的当下，导致全球的供应链出现了严重的中断，这是由两方面导致的。一是许多的工厂，由于安全的考虑而关闭，在这个对医疗用品需求空前大的情况下，严重影响了患者和医院的正常交流。从而迫使许多人盲目的去抢购一些来源不明，质量不确定的医疗物品，从而面临更多潜在的危害。另一方面，由于药品和医疗用品的需求增多，难免需要从世界各地进行采购，这无疑使得供应链延长，漫长的供应链难免会导致不透明，就更加难以相应的预测和规划供应。供应链需要透明性和可追溯性，而区块链特别适合应用于供应链，因为区块链可以连接供应链中的所有参与者，从出厂到运输再到销售，每一环都可以记录保存，从而提供透明唯一的真实情况，并且保证这些数据的安全性。

在新型冠状病毒肺炎蔓延的这一特殊时期，需要在必要的信息收集和保护隐私之间达成合适的平衡。在中国，面对新冠肺炎的疑似病例会将其安排到隔离点集中隔离待确诊后进行治疗，而在其他地区，并没有相关政策集中隔离这些疑似患者，这就可能导致个人在携带新冠肺炎病毒的情况下，与他人密切接触导致病毒的扩散甚至大范围的传播。因此需要对患者的数据和行程进行严密的监控管理，而区块链可以更加有效的收集和整理患者的数据，监控患者的行程，从而保证其与社会的距离，同时也可以保证患者的身份信息不被暴露。区块链没有中央权威，不受中央的控制，用户可以自主的控制其个人数据，有选择的共享新冠肺炎的相关信息，同时保护用户身份和其他的敏感信息。

## 健康医疗领域存在的问题

目前，医疗机构需要大量研究组织提供真实的数据，同时，黑客行为的广泛宣传还有对机密数据的抢劫等行为都大大破坏了公众对医疗行业的信任。另外在医疗保健系统中的各种破坏行为比如假医假药、程序不合规、医生腐败等都是棘手的问题。这些问题都阻碍了健康医疗行业的发展。就中国来说，健康医疗领域仍然存在这许多阻碍发展的问题。

1.医疗卫生资源总量不足，服务质量有待提高。与经济社会发展和人民群众日益增长的服务需求相比，我们的医疗卫生资源总量相对不足。在欧美发达国家，看病实行预约制。“预约”保证医护人员有充足的时间为患者提供个体化的服务。医生可以耐心地问诊、检查，每位患者都可以享受到完善的诊断和治疗，这在我国的公立医院中是难以想象的。17年丁香调查报道，我国公立医院的医生超负荷工作。在门诊工作强度项目中，59.7%的医生每半日需要看超过30例患者。按大多数从8点出诊至12点结束来算，平均每位患者就诊时间不足8分钟。为了节约时间,医生甚至少喝水以便少去厕所。在这种情况下谈要重视与患者沟通，要有同理心和合作精神简直是强人所难。

2.公共卫生服务体系不健全，医疗资源分配不均，布局结构不合理，影响医疗卫生服务的公平和效率，同时也使重大疾病预防控制任务艰巨和对突发公共卫生事件难以应付先进的医疗设备和资源多集中在一线城市，造成全国的病人蜂拥至北上广的三甲医院。不管大病小病，大家都往大医院跑，使得医院人满为患、拥挤不堪，服务效率和质量自然难以提高，有限的医疗资源也难以集中在最需要的患者身上。

3.医疗体制内的腐败现象，会使得医疗服务的公平性下降，卫生投入的效率低下，同时也会导致出现公众不满情绪增加、群体间关系失衡等一系列社会问题。目前医疗卫生领域时常会受到各种腐败势力的干扰和影响，比如官商勾结，在医药生产和流通环节谋取私利，假医假药，医生收红包现象等等。产生这些腐败的原因是相当复杂的，不过其中之一，是由于医疗卫生管理体制的非市场化因素和垄断过多导致的，过多的行政干预导致权力寻租。

4. 缺乏以人为本的患者关怀。医院文化中的人文关怀应该是指尊重患者的生命价值、人格尊严，以患者的利益和需求为中心，在医疗和护理服务的全过程中体现为使患者得到最佳的治疗和护理，实现医疗服务水平明显提升，让人民群众看病就医感受明显改善，社会满意度明显提高，努力构建和谐的医患关系。

然而，国内医疗服务存在一种十分普遍且“历史悠久”的“托熟人”现象,这种现象长期存在的原因大致有三种:1、医院对患者有意无意中表现出的“生、冷、硬”现象时有存在,没熟人介绍患者常感到害怕、不放心；2，为减少漫长的排队挂号和等候；3，为避免一些不合理的检查、用药费用。不难发现，患者普遍对本身疾病的发生、发展、预后存在焦虑和恐惧，对就医环境和过程还缺乏信任。“托熟人”现象长期存在体现了患者对高质量、多层次医疗服务的需求，同时也反映出了一些医院缺乏足够的人文关怀。决定患者体验的绝不仅仅是一场手术的成败或效果那么简单，真正的高品质医疗服务是渗透在每个细节的人文关怀。在医疗机构的硬件设施建设方面，参考新加坡医疗服务。新加坡的多数医院，其空间利用、光线色彩、采光通风、绿植景观、动线设计、香氛气味都经过精心设计，医院和社区服务融为一体，医院将美食广场、咖啡厅、面包房、书店、24小时便利店、药房等配套纳入整体布局，立体绿化覆盖到下沉庭院、露台、屋顶花园，给患者和亲朋陪护、探访提供便利的同时，也能在一定程度上缓解医院常有的压抑、紧张的氛围。

医疗健康领域要提升的不仅包括先进的医疗技术，还应包括贴心的高品质医疗服务。当今科学技术日新月异，为医生和患者都带来了极大便利，但过度依赖技术、“看病不见人”往往阻碍了人文关怀的实现，而人文关怀和技术深度结合才是当今时代的主流。

## 如何使用区块链技术

区块链的去中心化、隐私、安全等特性可以帮助当前的健康医疗领域解决许多问题。比如，在收集，存储和交换医疗数据方面，基于区块链实现的电子病历系统既可以确保数据的安全共享以及真实性，同时也大大加快了患者医生和医院之间的交流效率。对病人而言，看病的时间和流程节约下来对财力和人力都是一种节约，从而降低了看病的成本。对医生来说，仅需要病人的同意，信息就可以及时的从区块链上获取，这样医生就可以在面对患者的时候做出更加有针对性的诊断。而对医院来说，信息的获取效率变高就相当于节约了这方面的成本，更有利于将资源投入到医疗研究、临床试验等其他的方面，从而加快医疗技术的进步。

确保重要医疗数据的安全是目前区块链的主要应用。数据安全是一个重大的公共卫生问题。在2009年至2017年期间，超过1.76亿的患者记录受到数据泄漏（包括医疗和基因组信息)的影响。区块链提供所有患者数据的分布式存储的能力，使数据具有安全性。此外，区块链还可以保护患者身份，确保其数据的隐私。分布式的存储还可以让患者、医生和医院快速安全的[2]共享信息。另一个区块链应用的领域是医学教育[3]。区块链技术的去中心化，可以帮助确保保存有关医疗和教育许可的认证信息。基于区块链的教育平台可以帮助解决管理和教育的相关问题。 例如，大学的区块链系统可能安全地保存有关学术人员、教学内容、考试结果、工作人员和学生表现以及授予的学位的信息，这些信息确保了学习过程的完整性。此外，区块链还可以优化医疗教育的基础设施，保存文件来源、日期和作者的信息。可以改善师生互动，加快反馈，从而改善整个教育体系。这对于解决腐败问题也很重要，有助于提高管理效率。此外，不仅仅是数据方面，将区块链融入至健康医疗领域意味着可以在药品供应链，远程诊断和病人检测、灾害和检疫援助、促进生物医疗保健数据分布式存储等众多方面改善当前健康医疗领域的现状。

## 区块链给医疗行业带来的好处

通过使用区块链技术，健康医疗领域的众多方面都可以得到改善和提升。特别是在新冠肺炎大流行的形势下，区块链可以有效的帮助疫情防控的方方面面。

1.数据共享。为了有效的防控新冠肺炎的影响，必须对感染者进行追踪、分类以便为疫情的研究提供信息。将区块链其数据的真实准确等特性作为基础，同时利用区块链平台的可审计和数据安全实现数据在各方之间灵活的共享。MiPasa是基于区块链的全球控制和通信系统，它协助收集、整理和研究关于病毒传播和遏制的数据，由世界卫生组织发起，同时与创新组织和政府合作[4]。

2.医疗供应链。新冠肺炎的流行导致了全球范围内的供应链中断。许多工厂因为安全和卫生问题而关闭，使得对特定的医疗用品和药物需求供不应求。患者被迫购买使用来源不明或质量不明的产品。供应链的延长导致沟通效率低下，使得规划变得更加困难。区块链可以将所有的利益相关者连接在一个供应链网络中，同时保证链的透明性，且能够安全效率的分配数据，因此，在新冠肺炎流行的环境下，有大量的区块链被应用于供应链管理中[5]。区块链不适用第三方的机构，所以可以加速验证过程，同时还有着处理时间快、成本低、操作风险低和对各方结算快的优点。

3.接触者追踪。监控密切接触者可以有效的避免病毒的大范围扩散，但需要解决隐私等问题。区块链可以增加数据的准确性和可靠性，实时监控患者的行动，提供相关地区的最新情况并及时确定隔离人群等，并且严格遵守相关法律法规。同时还可以明确的标识出无病毒区域，方便公众安全的行动。

4.用户隐私保护。在这样一个特殊的时期，即要及时地收集数据，有需要保护个人的隐私，这就要求必须达成二者之间的平衡。区块链可以有效的收集病人的数据，并监控其行为，确保进行安全的社交活动，同时保护个人隐私。在没有中心化的系统中，用户可以自主的控制个人的信息，他们可以把重要的有意义的信息分享给专业的新冠肺炎工作人员，同时明确知道自己的隐私和身份会被保护。同时政府和医疗组织可以通过对新冠肺炎追踪收集更多的数据，并保证用户的数据不会被暴露和共享。一些欧洲的隐私专家设计了一个基于区块链的框架，使用蓝牙进行新冠肺炎患者的接触跟踪。 此外，德国的技术公司MYNXG已经提出了一个移动端的区块链计划，同时保护用户的安全[5]。

# 二 医疗行业现状

## 医疗行业分类

数据安全方面，当前有很多区块链的应用已经面向市场，在患者数据安全方面，美国的BURSTIQ医疗保健公司安全地管理大量患者数据。其区块链技术支持数据的保管、销售、共享或许可，同时严格遵守 HIPAA 规则。该公司使用区块链改进医疗数据的共享和使用方式。由于 BURSTIQ的平台包含有关患者健康和医疗保健活动的完整和最新信息，因此它将有助于根除鸦片类药物或其他处方药的滥用。Factom创建的产品可帮助医疗保健行业安全地将数字记录存储在公司的区块链平台上，只有医院和医疗保健管理员才能访问。物理文件可以配备特殊的 Factom 安全芯片，用于保存有关患者的信息，并存储为私人数据，只有授权人员才能访问这些数据。Factom 采用区块链技术安全地存储数字健康记录。

在共享数据方面，区块链可以简化交互的流程，让共享更加的方便。SimplyVital Health正在给医疗保健行业提供分布式技术。Nexus Health 平台是一个开源数据库，允许患者区块链上的医疗保健提供商访问相关信息。开放访问重要的医疗信息有助于医疗保健专业人员比传统方法更快地协调医疗工作。SimplyVital 使用区块链创建开源数据库，以便医疗保健提供商可以访问患者信息并协调护理。SimplyVital 最近与基因和精密医学公司 Shivom 合作，组成全球医疗保健区块链联盟，利用区块链安全性来保护DNA测序数据。Coral Health使用区块链来加速护理过程，自动化管理过程和改善健康结果。通过分布式分类账技术，公司比以往更快地将医生、科学家、实验室技术人员和公共卫生部门连接在一起。Coral Health还实施患者和医疗保健专业人员之间的智能合同，以确保数据和治疗准确无误。Coral Health的区块链技术可加速护理、自动化管理流程，并采用患者和医生之间的智能合约。Robomed结合了 AI 和区块链，为患者提供单点护理。该公司部署聊天机器人、可穿戴诊断工具和远程医疗会话，以收集患者信息并与患者的医疗团队共享这些信息。Robomeds Panacea平台让患者参与智能合约，激励并引导他们走上更好的健康之路。Robomed使用区块链安全地收集患者信息并与患者的医疗保健提供商共享这些信息。

区块链的防篡改、可追溯等特性帮助医疗供应链方面更加安全可靠，Chronicled构建区块链网络，展示监管链。这些网络帮助制药公司确保其药品高效到达，并且使执法部门能够审查任何可疑活动，如毒品贩运。2017年，Chronicled公司创建了Mediledger项目，这是一个致力于医疗供应链安全、隐私和效率的分类账系统。Chronicled区块链网络用于确保安全到达和详细审查药物运输。据该公司说，Chronicled公司最近的MediLedger项目的结果证明，其基于区块链的系统"能够作为药品供应链的可互操作系统"，"能够满足制药行业本身的数据隐私要求"。Blockpharma 提供了药物可追溯性和假冒的解决方案。通过扫描供应链并验证所有货点，该公司借助基于区块链的 SCM 系统的应用程序让患者知道他们是否正在服用假药，Blockpharma剔除了世界上15% 的假药。通过它的应用程序，该公司的区块链系统可以帮助防止患者服用假药。

在基因组学中，区块链可以降低研究成本，帮助实验。Nebula Genomics是使用分布式分类账技术，以消除不必要的支出和中间商在基因研究过程中。制药和生物技术公司每年花费数十亿美元从第三方获取基因数据。Nebula Genomics正在通过消除昂贵的中间商和激励用户安全地出售其加密的基因数据，帮助建立一个巨大的基因数据库。该公司使用区块链来简化遗传学的研究并降低成本。EncrypGen基因链是一个区块链支持的平台，可促进遗传信息的搜索、共享、存储、购买和销售。该公司仅允许同行成员使用安全、可追踪的DNA令牌购买遗传信息，从而保护用户的隐私。成员公司可以使用遗传信息来积累他们的遗传知识，并推进行业发展。该公司的区块链平台使搜索、共享、存储和购买遗传信息更加容易。EncrypGen 计划扩展其用户配置文件，以包括自报的医疗和行为数据。据公司联合创始人兼首席执行官大卫·科普塞尔博士说，该公司还致力于整合区块链支付和审计平台，以及与测试公司、分析软件开发人员和其他公司建立合作伙伴关系。

1. 医疗行业当前面临的主要挑战和发展趋势

在医疗行业中，数字技术的发展和应用可以为公众带来更好的医疗服务，即使在低收入的国家中，公众的医疗质量和体验也越来越好。但是，仍然存在许多的问题，比如安全性、成本、法律法规和道德层面等。在新冠肺炎流行的环境下，医疗行业更是面临这前所未有的挑战，这不仅仅是某一个国家地区的问题，是世界范围的挑战。

在技术方面，医疗行业的发展必然要走互联网+医疗的路线，通过与人工智能、物联网、区块链等技术的结合发展，促使医疗行业进一步的提升服务水平和质量，保证公众可以得到更好的就医体验。

在快速发展的同时，由于医疗行业必然掌握着众多患者的信息，信息安全方面也必须加以保护的提升，无论是小型的诊所还是大医院都不可以轻易的泄露病人的隐私，也不能因为安全性不足，导致信息被窃取，所以在信息安全的保护上也必须做到协同发展。

医疗行业一直是一个有国家监管执行关乎民生的重要领域，随着科学技术的发展，医疗卫生相关的法律法规、规章制度也需要与时俱进，仅仅切合行业的发展做出相应的调整，保证医疗服务和各种健康医疗研究可以有序的进行，及时提出问题反馈解决等。

未来医疗的发展趋势除了要与人工智能、物联网、区块链等技术结合外，还需要加强体系的晚上、隐私保护和人文关怀的方面的发展，在新的环境下，建立标准规范体系有助于整个行业在面对未知的风险和挑战时能够有效及时的做出应对，也可以防止不法行为的出现。在信息安全与隐私保护方面：需要制定专项政策法规，明确健康信息的隐私范围及使用条件，明细数据所有方、数据采集方、数据持有方等相关主体的责任与义务，并制定信息泄露事件的处罚与整改办法，以保证健康医疗领域未来的规范化发展。人文关怀是医疗行业一直需要面对的问题，随着公众对医疗行业的期望越来越高，无论是平时的治病，还是临终关怀，安乐死这些政策都需要与时俱进。面对公众各种心理层面的需求，及时的解决也同样是健康医疗领域需要面对的问题。

据IBM称，70%的医疗领导者预测，区块链将在改善临床试验管理、法规遵从性以及共享电子病历的分布式结构这些方面产生巨大影响。到2022年，医疗区块链技术的全球市场预计将超过5亿美元 [1]。总而言之，医疗行业的发展要考虑多方面的因素，不仅仅是技术，更重要的是制度规范和道德伦理，只有做好各方的平衡，才能保证整个行业想着正确的方向有序发展。

当前电子病历系统的主要缺点是数据都存储在集中式数据库中，医疗数据的安全性很差，很容易受到攻击。集中化需要对单一的权威机构的信任，而且增加了安全风险。最近的Ransomware攻击[6]和Equifax攻击[7]都对电子病历的隐私和安全造成影响。另一个问题是数据缺乏互操作性，数据很难共享给相关机构。而且数据无法做到防篡改，这导致一旦医院数据库中的数倍被删除时会永久丢失。此外，患者无法完全控制自己的信息，现阶段还是由医院等组织管理，考虑到医疗数据的庞大和安全问题，现有的系统还没有一种有效的方式存储、共享这些数据。现有的系统也难以确保云中的电子病历是安全的[8]。

1. 医疗行业软件的特点

对于医疗行业的软件来说，数据共享是很重要的一点，尤其是医疗组织内部使用的软件，数据共享可以大大减轻收集数据的困难，更加有效的进行医疗工作。其次可扩展性也是影响软件寿命的关键，扩展性差的软件很难升级，容易被时代淘汰。

医疗组织使用的软件需要共享数据、可扩展、隐私安全性好，但面向市场的尤其是移动端医疗APP，这基本上是一个商业化的行为，目前来看，大部分的医疗APP除了资讯的推送外，基本就是在线问答。好一些的软件有医疗网络咨询、挂号服务，有医生量和质的基础，可以向专家咨询，他们的优势就是医生资源好，请的到专家。也有专门查资料的那种软件，供专业医护人员使用的软件，这类的优势就是他们拥有强大的数据支撑。

但对于这些软件来说，因为面向市场和公众，那么商业化的行为就必不可少，一旦涉及到推广，成本必然会增加，那么面向用户收取的费用也会影响到用户的体验。对于传统的医生来说，看病诊断没有切实的“望闻问切”会对诊断的正确性造成影响，严重的还会出现误诊等情况，所以这类软件的特点就是基本上只是一个工具，小病可以节约时间不用去跑医院，面对大一点的病，这类软件只能起到在线挂号，预约医生的作用了。

精神和心里层面的诊断和就医，或许真正的需要在线来完成。精神与心理的不适症状似乎已成为现代人的文明病，而针对当代民众对于心理咨询和精神科问题的治疗还存在某些刻板印象和障碍，这导致在线的心理咨询发展缓慢。

# 三 现有医疗区块链分析

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。[9]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。

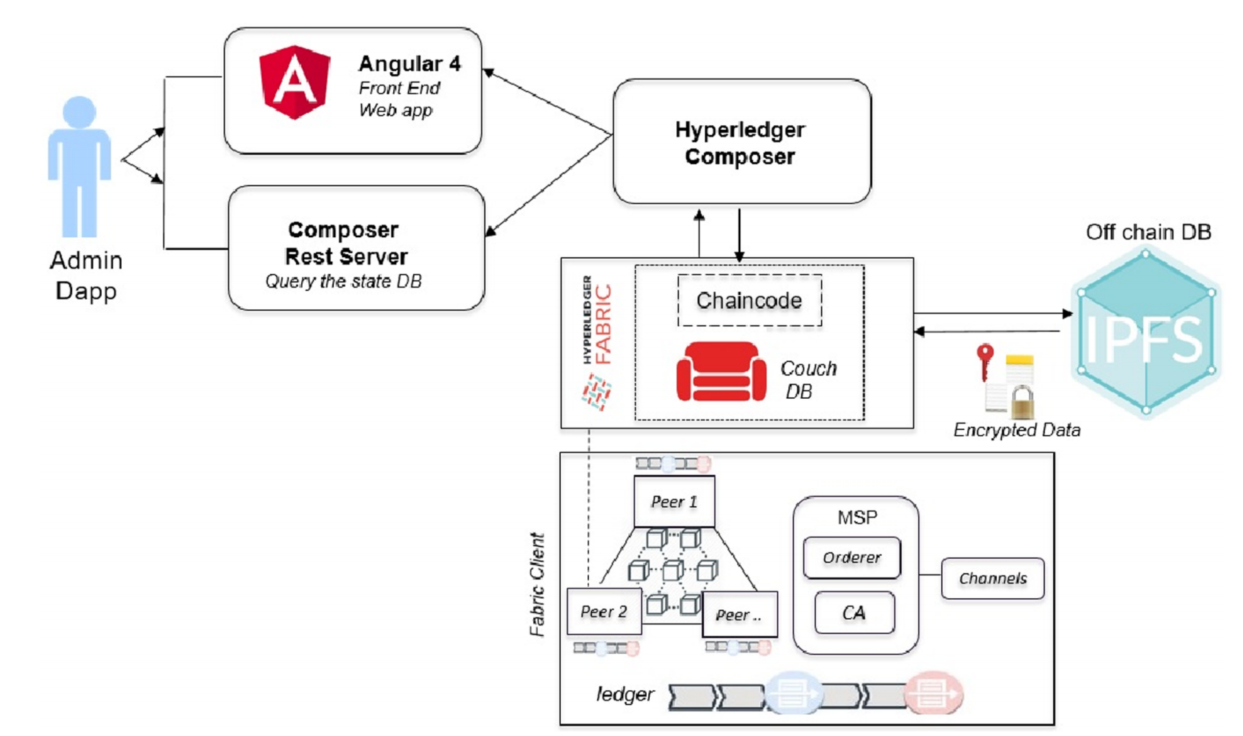
这个药物供应链系统的交易过程如下：首先，用户通过前端应用程序注册身份信息，连接到区块链系统，并完成交易请求。然后，将交易发送到所有对等节点。 这些对等节点分为两类：提交者或背书者。 背书者执行或签署过渡提议，并给予批准，如果是有效的，就履行智能合同标准，否则拒绝它。另一方面，提交者的对等节点验证交易结果，然后写入交易块中。背书者是有预定义智能合约的提交者的特殊对等节点。背书者在自己的虚拟环境中模拟智能合约然后更新账本。背书者读取所有历史记录，然后在自己的虚拟环境中将数据写入。完成后把签名返回给客户端应用程序，客户端再把所有的背书者的签名通过共识算法交付给提交节点，把数据排序放入块中。然后提交节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

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[11]。 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。

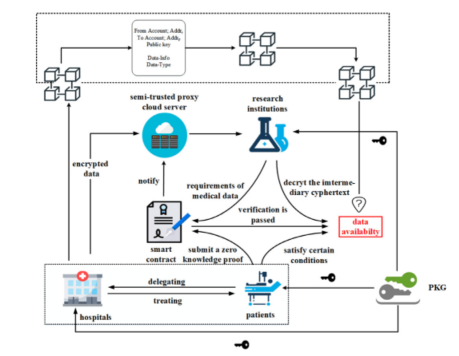
下图是Healthchain的架构，Angular4是DApp的前端框架，连接着Composer Rest Server，Composer Rest Server将CouchDB数据库可视化并公开。DApp通过Angular框架与用户界面交互，通过Composer Rest Server的REST API处理用户对Fabric的请求。REST API用于检索链上数据库CouchDB的当前状态，其中Angular框架通过对Composer Rest API的GET调用检索数据。Hyperledger Composer构建区块链网络，为应用程序创建智能合约。Healthchain的框架在Hyperledger 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。



[12]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。

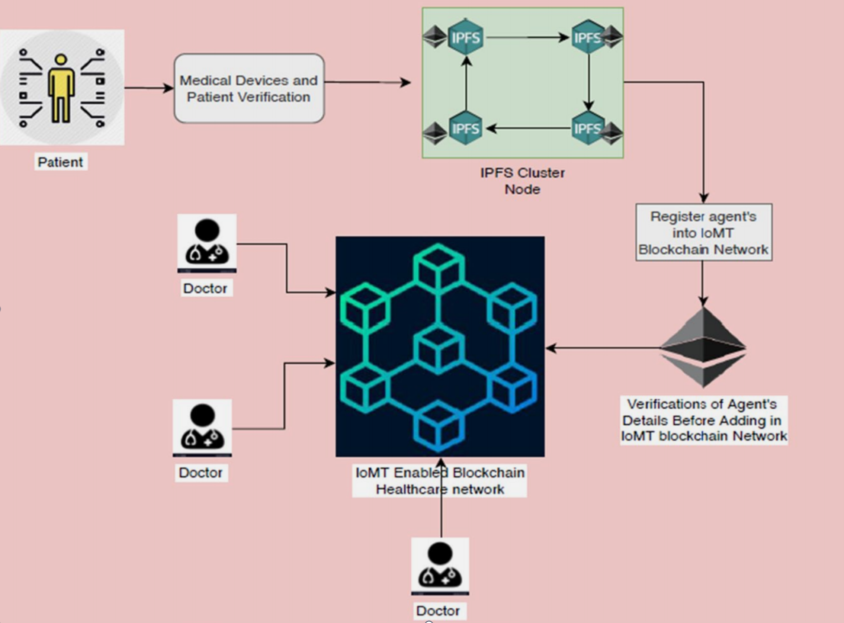
只有授权的实体才能使用他们的私钥来解密病人的医疗数据。此外，患者可以根据自己的医疗数据生成完全可信的零知识证明，并将其提交给区块链上的智能合同。零知识证明可以用来验证患者的医疗数据是否符合研究机构建议的某些条件。这一特性确保了具有供需匹配的数据可用性。

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。

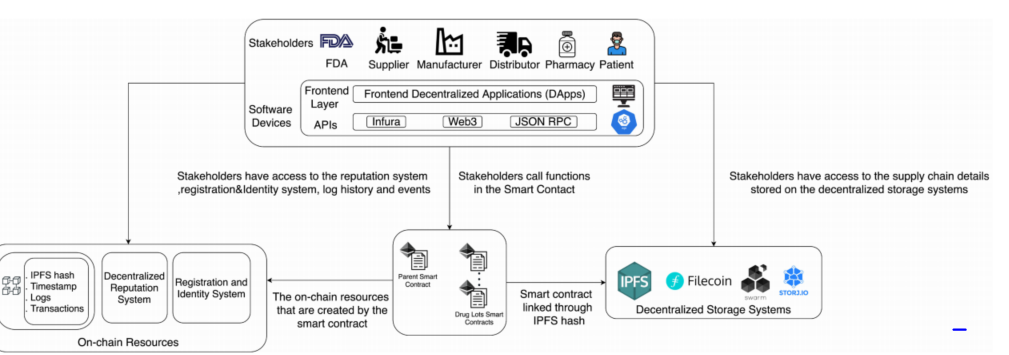
医疗物联网（IoMT）是数字革命的下一个前沿，它利用物联网在医疗领域。底层技术通过收集病人的实时数据和提供病人运动系统改变了目前的医疗系统。但是，由于基于云的存储，物联网也对数据存储管理、安全和隐私提出了巨大的挑战。今天，大量IoMT生成的医疗数据被存储在集中存储系统中。于是[13]提出了一个基于区块链和IPFS技术的增强IoMT的安全和隐私性的框架，因为物联网医疗网络比传统的医疗更加需要注重安全和隐私。该框架将IPFS集群节点和智能合约的去中心化框架用于医疗物联网，设计了一个医疗保健系统的认证和访问控制，确保了系统的安全性。还设计实现了身份的认证安全模型，用来满足医疗物联网的安全需求。还提出了一种IPFS集群节点的数据存储层，该集群节点在IoMT启用医疗保健系统中分布，缓解了单点故障。与智能合约共同验证医疗物联网系统中的安全问题。还在以太坊的Ropsten网络中部署了一个联盟链，用来保护患者数据隐私。

该模型设计为两个不同的部分，一部分是患者注册和医疗设备的认证和授权，另一部分是在区块链网络中的部署。下图是区块链的模型。Medical device这一部分负责在医疗物联网中部署不同的医疗设备，以便通过感知和驱动来实现医疗保健（单个病人的医疗设备）的通信。这些医疗设备产生的数据会在区块链网络中传输。IPFScluster 是负责病人及其医疗设备的认证及安全存储。此外，这一部分还与智能合约交互，在IoMT区块链网络中执行共识协议、交易映射验证和块的创建。

在通信框架中，包括医疗设备到IPFS的通信，IPFS到智能合约的通信和智能合约到区块链网络的通信三部分。第一部分负责登记病人及其医疗设备，和IoMT区块链网络中通信前的医疗设备认证。第二部分负责同步医疗设备数据的认证和授权及其映射，以确保医疗物联网区块链网络中的隐私。第三部分负责在成功的身份验证和授权后将信息传到区块链网络中，确保在医疗物联网区块链网络中不同代理（患者和医生）之间安全地传输数据。 这保证了医疗物联网区块链网络的隐私。所有的物联网设备都必须在IPFS集群节点上进行认证，没有认证过的设备是不能与IoMT网络进行连接的。该模型利用椭圆曲线数字签名算法(ECDSA)为医疗设备创建私钥和公钥。

此模型在使用时主要有两部分，第一部分是病人和医疗设备的注册和初始化，第二部分是病人相关医疗设备的认证。第一部分中，病人注册时，首先智能合约会创建一个唯一ID，是由用户名和时间戳前5位的哈希组成，ID通过公钥加密存储到IPFS中，注册成功后信息会存到IPFS中，并在区块链的块中存入哈希值然后发布。IPFS会给新注册的病人用私钥创建一个认证，这个认证也会发布在区块链上。设备注册时会根据设备ID、设备IP和病人的ID生成一个令牌，通过私钥加密和病人的证书一起发送到IPFS，然后转发到区块链网络。通过智能合约的验证后，就可以发布在区块链上。最后，为新注册的设备创建有效的通行证证书。此证书在IoMT区块链网络中分发，也会存储到IPFS中，以便将来对新注册的医疗设备进行身份验证。设备的认证过程是IPFS中的智能合约检查相关的病人ID设备ID和设备IP都匹配即可通过。

[14][15]提出了一种基于区块链的药物供应链解决方案，特别是针对假药的情况。为药物提供安全、可追溯性、不可变性和数据来源的可访问性，设计并实现了一个智能合同，能够处理制药供应链利益相关者之间的各种交易。系统架构如下图所示。



Stakeholders包括FDA、制造商、分销商、药店和病人等监管机构。这些利益相关者作为智能合约的参与者，根据其在供应链中的作用被分配特定的功能。 他们还可以访问链上资源，如历史和日志信息，以跟踪供应链中的交易。他们还有权访问存储在IPFS上的信息。系统使用IPFS作为分布式存储系统，IPFS的特点是低成本离线存储，确保数据安全完整，通过哈希确保文件不被篡改，将哈希值存储在区块链上，用智能合约控制访问。智能合约可以控制访问权限，只有满足要求的访问者才可以访问相关内容。此框架使用的区块链是以太坊。供应链的追踪不需要实时跟踪，通过追踪药物历史验证相关信息即可确定药物的真实性。在系统中，制造商向FDA发送请求，申请启动药品的制造，得到允许后即会向所有参与者宣布此事，并且药品批次的图像会上传到IPFS，IPFS向智能合约发送哈希值，这样授权者就可以访问这些图像，完成制造后将药品交付给经销商包装。然后经销商开始分销过程，他们将药品打包，并把打包图像上传至IPFS，IPFS同样将哈希值发给智能合约，完成打包后将药品交给药房。药房得到药品后开始销售，然后在供应链上发布信息，并上传药品图像至IPFS，IPFS再把哈希值发给智能合约。药品出售给病人，就结束了药品销售阶段。这一过程确保所有交易都存储记录，并且可以由所有供应链参与者之后访问，以交易序列的形式检查供应链中产品的真实性和有效性。

这一方案的优势是去中心化的系统，消除了单点故障，利用区块链确保了数据的完整和安全。分布式的存储也确保了数据的安全。在访问数据时，只要是参与者都可以访问药品的交易信息，但没有提到药品相关信息是否加密，即会不会泄露病人的隐私。IPFS离链的存储方式降低了区块链的存储压力，使用以太坊的货币作为支付方式或许会增加相应的门槛。这个区块链供应链系统的主要目标是跟踪医疗保健供应链中的所有交易，确保批次、所有权转移及其相应历史的可追溯性。通过区块链不可变的特点和IPFS存储图像的方式确保每笔交易都能被追踪。然后每次操作都会留存访问者的信息，所以在供应链中谁干了什么是公开的，这可能会影响到用户隐私，但保证了药品供应链绝对的透明。当然关键的操作都由智能合约监控，只能由授权的参与者执行。由于区块链的特性，链上的信息不可篡改且可以被所有参与者访问，交易信息一旦存储到链上，便永久也可见，不能删除。区块链上的交易在被私钥加密后上传，一旦信息上传便不能销毁，使得任何人不能否定他们的行为，他们需要对各自的行为负责。该框架还提出了一些区块链应用于医疗供应链的不足，一是区块链不能修改，这保证了信息的完整性，但对于链上的错误不能改正，尤其是人工难免造成一些错误。二是隐私问题，虽然不可变性是区块链的主要优点之一，但它可能与解决信息存储问题的新兴法律相冲突。 例如，欧洲的一般数据保护条例(GDPR)要求各组织准确地控制数据存储的地点和方式，因为收集数据的人有权随时修改或删除数据，如果不按照他们的要求采取行动，该组织可能会受到严重的罚款。在医疗供应链中，患者可能拒绝将他们的数据永久存储在区块链上，他们可以合法地起诉医疗中心。另外，对于医疗供应链来说，如果某种药品进行大规模的生产制造，就会导致其在区块链上占用很大的存储空间，但区块链的存储空间有限，这就会造成影响。区块链的互操性也被提到，不同的区块链无法相互通信。还有就是效率的问题，在区块链中，智能合约决定着实施和决定过程的成本，共识协议决定了资源的消耗水平，医疗供应链会涉及众多交易，如果智能合约代码不是那么有效率，会大大降低供应链的效率。

参考文献

[1] J. Fu, N. Wang, and Y. Cai, “Privacy-preserving in healthcare blockchain systems based on lightweight message sharing,” Sensors, vol. 20, no. 7, p. 1898, 2020.

[2] S. Daley, 15 Examples of How Blockchain Is Reviving Healthcare, 2020, https://builtin.com/blockchain/blockchain-healthcare-applications-companies.

[3] C. C. Agbo and Q. H. Mahmoud, “Blockchain in healthcare,” International Journal of Healthcare Information Systems and Informatics, vol. 15, no. 3, pp. 82–97, 2020.

[4] Singh, G.; Levi, J.: MiPasa project and IBM Blockchain team on open data platform to support Covid-19 response. IBM, 27 March 2020. https://www.ibm.com/blogs/blockchain/2020/03/mipasa-project-and-ibm-blockchain-team-on-open-data-platform-to-support-covid-19-response/. Accessed 27 May 2020

[5] Dragov, R.; Croce, C.L.; Hefny, M.: How Blockchain Can Help in the COVID-19 Crisis and Recovery. IDC-Analyze the Future, 4 May 2020. https://blog-idcuk.com/blockchain-help-in-the-covid-19-and-recovery/. Accessed 27 May 2020

[6] Mohurle S, Patil M. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science. 2017; 8(5).

[7] Berghel H. Equifax and the latest round of identity theft roulette. Computer. 2017; 50(12):72–76. <https://doi.org/10.1109/MC.2017.4451227>

[8] Shu J, Jia X, Yang K, Wang H. Privacy-preserving task recommendation services for crowdsourcing.IEEE Transactions on Services Computing. 2018.

[9] Khizar Abbas,A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry

[10] Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology

[11] 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.

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

[13] Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology

[14] A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain

[15] <https://github.com/DrugTraceability/DrugTraceability/blob/master/Code>