

版本 1.0 2017年10月 MEDIBLOC 团队 WWW.MEDIBLOC.ORG

本白皮书介绍了当前MediBloc公司关于MediBloc平台及相关事项。MediBloc公司可能会随时部分修改本白皮书，恕不另行通知。本白皮书中提供的信息仅供参考，对MediBloc公司或任何其他方不具有法律约束力。本文档的目的在于提供信息参考，文档本身不构成也无意成为出售要约、招揽购买要约或推荐：
(i) MED币，(ii) MediBloc平台投资或MediBloc公司的任何项目或资产，或(iii) MediBloc公司和其任何关联或附属公司的股份或其他有价证券。请阅读本白皮书末尾的重要法律免责声明。

目录

摘要(Abstract)

1. 导论(Introduction)

- 1.1 当前医疗信息系统问题概述(Problem Overview)
- 1.2 MediBloc的团队使命(Mission statement of MediBloc Team)

2. 新型医疗信息系统-MediBloc(New Medical Information System)

- 2.1 最高级别的安全性(Maximum Security)
- 2.2 极强的可靠性(High Reliability)
- 2.3 高度的透明性(High level of Transparency)
- 2.4 强大的互操作性(High Interoperability)
- 2.5 便捷的可访问性(High Accessibility)
- 2.6 以患者为导向的理想型综合医疗信息系统；个人健康管理记录(PHR)

3. MediBloc技术细节(Technical Detail)

- 3.1 MediBloc平台构架(Platform Structure)
- 3.2 MediBloc平台构成要素(Platform Components)

4. 代币模型(Token Model)

- 4.1 MP积分(Medi Point, MP)
- 4.2 MED币(Medi Token, MED)
- 4.3 代币生成活动(Token Generation Event)

5. MediBloc服务示例(Use cases)

- 5.1 个人健康记录(Personal Health Report)
- 5.2 自动保险理赔(Automated Insurance Claims)
- 5.3 医疗信息交易(Healthcare Data Trading)
- 5.4 人工智能医疗对话机器人(AI-powered Medical Chatbot)
- 5.5 临床研究(Clinical Trials)
- 5.6 远程医疗(Telemedicine)
- 5.7 社交网络服务(SNS)

6. 开发规划(Roadmap)

- 6.1 平台开发规划(Platform Roadmap)
- 6.2 基本应用开发规划(Basic App Roadmap)

7. 其它 (法律事项等)

参考文献(Reference)

MediBloc：基于区块链的医疗护理生态系统

摘要(Abstract)

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。

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诊疗记录输入MediBloc。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来创建各种基于医疗信息的服务。

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贡献的大小来获得相应的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。

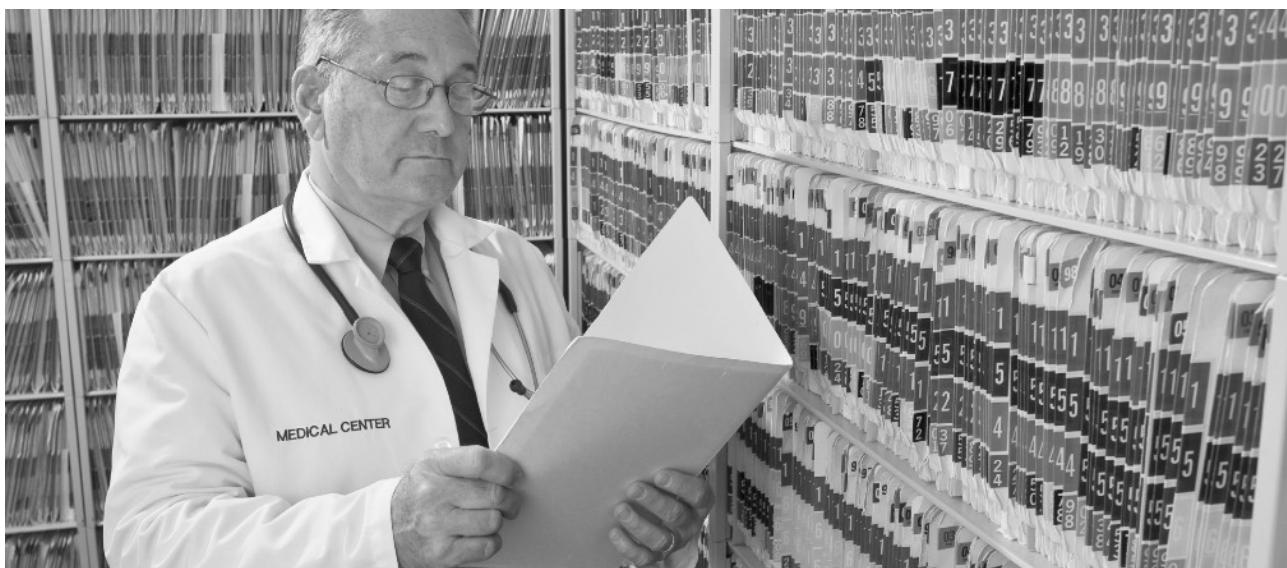
MediBloc为医疗服务消费者、医疗服务提供者和研究机构等单位和个人提供了一个可以自由参与的医疗信息平台。MediBloc团队坚信，MediBloc平台通过重新分配医疗信息的所有权，将为医疗护理领域带来一场创新发展浪潮。

1. 导论(Introduction)

目前，在大多数医疗信息系统中，医疗数据是由患者就医的医疗机构集中进行管理，除非患者本人同意，在医院外部进行的一切有关患者的医疗信息的交换是被禁止的。这种以个体医疗机构为导向进行的医疗信息管理，不仅导致医疗数据的分散，还严重阻碍了医疗数据的有效利用。医学届、患者和医疗产业界对医疗信息交换的需求与日俱增。虽然人们已经为解决医疗数据交换开展了各项工作，但至今也没有提出一套明确有效的解决方案。其中，美国政府主导的蓝纽连接器[1]、苹果公司的移动健康应用程序[2]以及三星电子的健康应用程序[3]等，可以看作是在这方面努力的代表。除此之外，相关医疗服务虽然层出不穷，但都没有从根本上解决构建理想型医疗信息管理系统时最为重要的安全性、可靠性以及开放性的要求。因此导致这些服务难以切实地吸引医疗消费者、医疗服务提供者¹以及医疗护理相关的机构或企业的积极参与[4]。然而，MediBloc团队坚信，通过金融领域为中心快速发展的区块链技术，我们可以构建一个能满足用户对医疗数据管理需求的理想型医疗信息管理系统。我们将进一步利用这些医疗数据创建一个可以提供各种健康/医疗护理相关应用和服务的平台，使之成为一个可以真正支持个性化健康管理和以患者为导向的医疗护理体系。MediBloc必将为整个医疗护理行业带来一场创新发展浪潮。

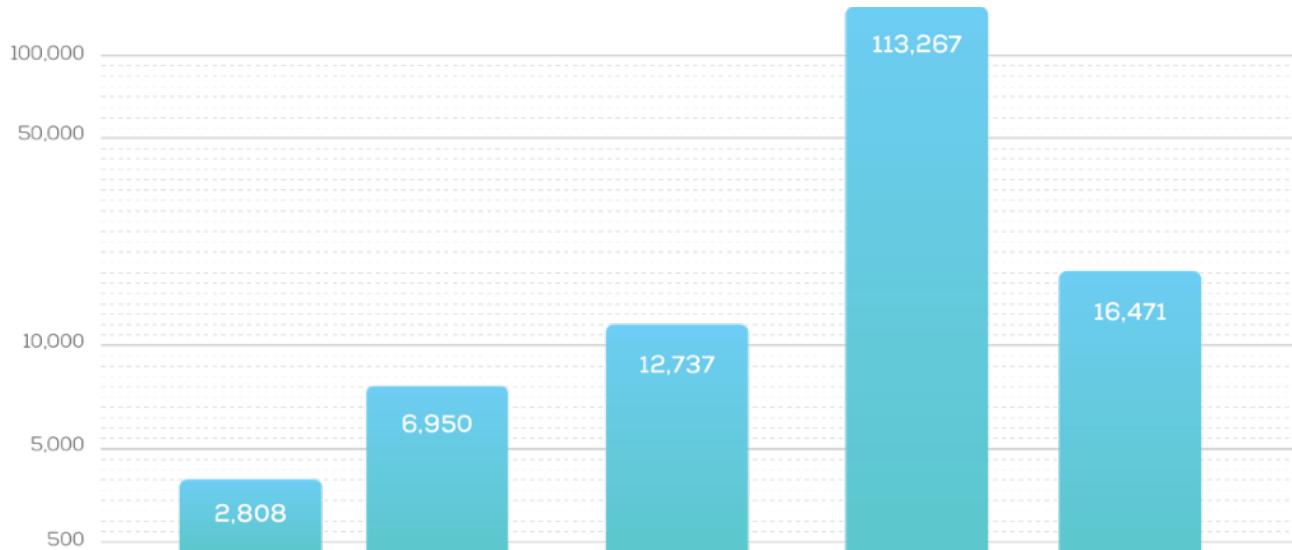
1.1 当前医疗信息系统问题概述(Problem Overview)

有过就医经验的人肯定也有过这样的经历：当我们在某家医院接受治疗，出于一些原因又转到另一家医院时，经常会被要求重做一次已经做过的医学检查和成像。重做检查和成像主要是因为之前一家医院生成的医疗信息没有跟着转到新的医院。医疗信息没有得到有效的交换是因为目前医疗信息是以医疗机构为导向进行管理的。政府法规对医疗信息这种重要的个人信息的转移和共享作了许多限制规定。其中最著名和被广泛引用的是美国HIPAA法案（健康保险流通与责任法案）[5]，其中详细规定了处理医疗信息的所有医疗服务提供者和机构必须遵守的规则，以确保医疗信息安全。根据HIPAA法案，可以处理医疗信息的主体非常有限，仅允许医疗信息的共享在必要的最小程度上进行，这使得患者的医疗信息只能由就诊医院和保险公司来进行管理。包括美国在内的大多数国家都有和HIPAA类似的规定，不难想象，在这些国家医疗信息的交换和共享并不容易。在某些情况下，许多医疗数据仍未被数字化，这也使医疗信息交换变得困难。据美国疾病预防控制中心的调查显示，只有约一半的医疗机构具有全功能的电子病历/健康系统[6]。



在医疗机构为导向的现行管理体系下，并不能保证医疗数据的可靠性和数据使用的透明性，甚至会有数据丢失和遭受黑客入侵的风险。同时，个人难以使用自己的医疗信息，导致数据可靠性降低，还要一直担心个人信息泄露。事实上，每年医疗数据遭到黑客入侵的案件都在迅速增加。仅2015年一年，在美国遭受到黑客入侵的医疗记录的数量就高达1.12亿条。据报告，美国每年因此造成的经济损失超过62亿美金[7,8]。

- Number of records exposed (1000 records)



[Source: Department of Health and Human Services' Office for Civil Rights]

医护人员由于缺乏医疗信息交换而无法轻易获得患者的过往医疗信息，导致难以以为患者提供最佳的医疗服务，还要进行不必要的重复检查和医学成像，增加医疗费用负担。研究报告指出，如果医疗信息可以被有效地交换，那么在急诊室进行的临床检查和放射学检查将会减少50%以上[9]。在目前的医疗信息管理系统下，医疗信息的可靠性不能得到保障、信息交换困难，每年在保险领域也造成巨额的损失。报告称，全球范围内每年因为虚假索赔造成的保险损失高达4870亿美元，占美国年度总医疗费用的1/5 [10]。此外，医疗机构有时任意歪曲或更改医疗记录也已经成了一个严重的社会问题，现存的医疗信息系统无法系统的解决这个问题。

目前医疗信息管理系统的问题并非只有这些。现在，医疗数据越来越多地被机构和企业要求用于医学研究和医疗护理项目的开发 [11]。大多数医疗数据被隐去患者个人识别信息通过医院分享到研究机构和企业，这种情况也引来越来越多的社会关注。此外，对数据所有权的争议仍在继续[12]。在以美国为首的一些国家允许将不具有个人识别性的医疗信息对外分享使用，但是由于不难通过社交网络服务等各种方法进行个人信息再识别，这也意味着这种数据分享方式有待改善[13,14]。

1.2 MediBloc的团队使命(Mission statement of MediBloc Team)

“重新分配个人医疗信息的价值，提高医疗访问和服务的质量，
加快个人医疗信息的去中心化。”

MediBloc团队旨在根据医疗领域的专业知识，实现个人医疗信息去中心化的目标。MediBloc将医疗信息管理系统实现以医疗机构为导向到为以患者为导向的转变，以此来达到现有医疗信息系统不具备的信息交换的可靠性、透明性和安全性。MediBloc将以平台上存储的医疗信息为基础，进行各种优质的健康护理相关服务的开发。它还将为平台上的所有参与者提供一个独特的获取奖励的机会。

2. 新型医疗信息系统, MediBloc(New Medical Information System)

已经有很多尝试来克服当前医疗信息系统中存在的问题，但是至今仍没有一个完美的解决方案。在不同利益主体共同存在且以一个主体为导向的集中医疗环境中解决问题，必然会受到限制。为了解决这些问题，进一步实现医疗领域的发展，我们必须探索开发一个全新的医疗信息管理系统。



MediBloc运用区块链技术来实现现有医疗信息系统无法实现的以患者导向的综合医疗信息管理系统。换句话说，通过建立一个理想型个人健康记录平台[15]，满足医疗护理信息系统可靠性、透明性和安全性等所有要求，实现可靠医疗信息的安全交换。MediBloc不是一个单一的服务，而是一个医疗信息平台。平台提供的API和SDK便于各种应用程序和服务可以轻松访问平台上的医疗信息，并以此进行新服务的开发。另外，平台还将发行一种名为“MED币”的加密货币，并通过货币的流通来形成一个以患者为导向的医疗信息经济生态系统。这就为平台的所有参与者提供了一个独特的可以根据贡献度获得相应经济奖励的机会。

MediBloc的优点如下。

2.1 最高级别的安全性(Maximum Security)

根据HIPAA法案的规定，所有的医疗信息均应加密保管。在现行的医疗体系中，对医疗信息进行管理并加密的主体是医疗服务的提供者，医疗机构一般由一群人组成，因此即使医疗信息被加密存储，也可能存在一些人可以解密医疗信息。事实上，根据最近的一项调查，医疗信息泄露的最主要的原因并不是因为黑客的入侵而是因为内部人员故意或错误造成的[16]。MediBloc为了最大限度地降低个人信息泄露的可能性，将访问医疗信息的权限由医疗服务提供者移交给患者本人。使得只有患者本人才可以解密自己的数据，自由地设置医疗信息的访问权限并记录在区块链上。这样不仅可以最大限度地降低医

疗信息泄露的途径，也极大地减少了他人干涉的空间。同时消除了通过一个医疗机构泄露大量患者个人信息的可能，也从根本上杜绝了大规模医疗信息泄露事件的发生 [17]。

2.2 极强的可靠性(High Reliability)

MediBloc将医疗信息存储在分布式数据存储空间中。MediBloc为了防止数据的丢失，连续生成和维护备份数据，对于被记录的数据，其哈希值将被记录在区块链中以验证数据的完整性，当数据被强行变更或伪造时，将使用备份数据来恢复原始数据。这就使连拥有信息所有权和管理权的本人也无法随意更改已保存的医疗信息，极大的保证了医疗信息的完整性和可靠性。只有通过MediBloc平台上“医疗服务提供者资质认证系统”认证的医护人员才有权限生成他人的医疗记录，通过将记录中的创建者指定在一起并用区块链验证，进一步提升生成的医疗数据的可靠性。医疗服务提供者若想要查看他人的医疗信息，则也需要完成一定的认证流程，并在获得信息所有者本人同意后才可查看。

2.3 高度的透明性(High level of Transparency)

MediBloc平台上所有医疗记录和他人查看信息的过程都会被记载在区块链上。现行的以医疗机构为导向的医疗信息系统，无法追踪个人医疗信息在何时、被以何种目的使用，但MediBloc则会完全透明地管理和控制个人信息在何时、何地、被以何种目的使用。MediBloc上所有医疗记录的访问权限都由本人记录在区块链上并由亲自进行管理，这就从源头上阻止了他人对医疗信息的恶意访问。

2.4 强大的互操作性(High Interoperability)

MediBloc倡导开放式平台，以平台上存储的数据和信息为媒介可以和各种应用程序自由连接。医学图像信息和遗传信息已经拥有统一的标准，因此它们可以方便地相互转换并通过MediBloc轻松的交换和交易。由于医务记录、院务纪录以及检查结果记录并没有一个统一的标准，MediBloc采用了一种增强互操作性的方法，支持多种格式并实现各种支持格式之间的相互转换，而不是制定自己的标准并指定一种格式。为此，MediBloc不仅支持HL7 CDA构架[18]等被广泛使用的标准，还将提供符合多种标准的API和SDK,如有必要，甚至还会针对个别医疗机构或个人提供个性化解决方案和数据格式所需的API和SDK或可能的开发环境。凭借这样高的自由度和可扩展性，MediBloc医疗信息系统将具备现有医疗信息系统无法媲美的强大的互操作性。

2.5 便捷的可访问性(High Accessibility)

通过将所有的医疗信息存储在分布式数据库，MediBloc可以随时随地通过互联网连接为用户提供便利的访问。目前，大多数的医疗机构并不允许外网登陆访问医疗信息，仅有的少数提供这种服务的医疗机构也会根据情况的不同只提供限制性访问权限。通过推出不依赖于任何特定医疗机构的数据系统，MediBloc减少对单个医疗机构的依赖，从而使用户可以更加便捷地访问并管理本人的医疗信息。

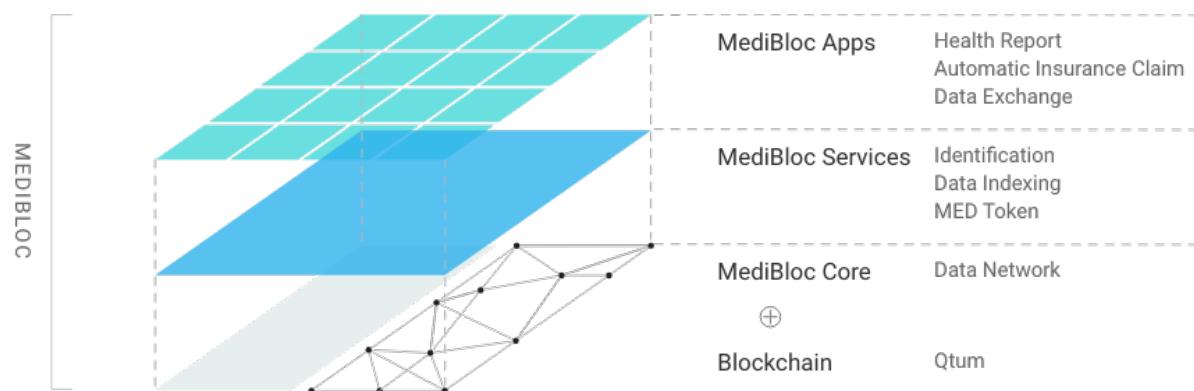
2.6 以患者为导向的理想型综合医疗信息系统；个人健康管理记录 (PHR)

MediBloc使用以分布式和去中心化为主要特点的区块链技术来进行数据管理和整合。MediBloc不仅整合、存储和管理医疗机构创建的医疗记录，还包括患者本人创建的医疗数据。不管用什么设备，在医疗机构外部由用户个人直接生成的医疗数据，都可以轻松的保存在MediBloc上。这些集成整合后的医疗护理信息将可广泛用于普通的医院护理和个性化移动医疗服务中。

3. MediBloc技术细节(Technical detail)

3.1 MediBloc平台构架(Platform Structure)

MediBloc由核心、服务和应用三层构架组成。



3.1.1 第一层：MediBloc核心层

核心层是一个分布式数据库，可以使用MediBloc医疗数据网络中的最新加密技术来保护数据。由于可以在存储在区块链上的数据量非常有限，所以需要单独的存储空间来有效地存储医疗数据，核心层则提供了此功能。在MediBloc应用中生成并传送的医疗数据通常会通过MediBloc SDK在应用层加密后再传送，这就使得除了可以解密数据的数据持有者本人外，任何他人将无法读取原始数据。核心层可以通过MediBloc的服务层进行访问。此外，MediBloc的核心层还为存储的数据提供备份和恢复系统，以便数据可以安全的存储而不会丢失。

3.1.2 第二层：MediBloc服务层

服务层提供包括连接MediBloc应用程序与核心层和管理用户信息在内的所有核心功能。服务层以区块链为动力，以区块链中存储的信息为基础，通过与MediBloc核心层的连接来执行数据的输入/输出功能。在内部，服务层可以分为以太坊虚拟机(EVM)为基础的智能合约和连接应用层与核心层的部分。智能合约包括含有MED币信息的账户信息以及核心层的医疗数据的链接等。在MediBloc中，通过最大限度地减少存储在包含智能合约的区块链中的数据量来降低可能发生的平台运营成本。

3.1.3 第三层：MediBloc应用层

MediBloc应用层指的是通过平台来进行医疗信息管理和利用的所有应用程序的统称，它包含移动和网页环境下的所有形态的应用程序。这些应用可以通过服务层访问平台中的数据。利用即将提供的SDK可以使应用程序的开发变得更加轻松快捷，这样可以方便地开发用以连接MediBloc平台的应用程序。即使不使用SDK，如果遵循即将发布的API和开发协议，也

可以开发连接到MediBloc平台的应用程序。基于MediBloc开发的一些实用的应用和服务示例将在下文第五章的服务示例中有更详细的说明。

3.2 MediBloc平台构成要素(Platform Components)

MediBloc平台是一个基于EVM的分布式应用程序。EVM并不完美，但是目前它正被广泛用于智能合约的开发。因此，从时间成本、金钱成本、通用性和可靠性等方面来看，基于EVM构建平台要比自己构建区块链网络和建立基于它的平台更有效率。另外，基于EVM的开发，理论上可以在诸如以太坊（ETH）[19]以及支持EVM的量子链(Qtum)[20]和EOS[21]等各类区块链平台上运行。因此，根据这些区块链平台的技术支持，MediBloc可以灵活选择运行平台,这也是MediBloc平台的一个优点。在这些区块链平台中，量子链的比特币平台和以太坊平台的优点是他们都是目前借用POS形式的协议算法支持EVM最快的可扩展平台。MediBloc使用量子链（Qtum）为主要平台。

MediBloc平台有三种主要信息类型：MED币信息，个人信息和医疗信息。虽然，将所有信息都存储在区块链上的方法最为理想，但是由于成本、存储空间和性能等现实因素的限制，将最大限度地减少直接存储在区块链上的信息量，占用较大存储空间的个人信息和医疗信息将以加密的形式存储在区块链外部，而只将对应于它们的哈希值存储在区块链上。数据存储使用基于IPFS文件系统[22]的分布式存储。

3.2.1 MediBloc账户(Account)

在MediBloc平台上可以创建的账户根据其使用目的可以分为普通用户账户、医疗服务提供者账户（医护人员，医疗机构，医疗护理应用等）和医学研究者账户。虽然这些账户是以相同的技术方式创建和运行的，但是根据他们在MediBloc生态系统中的实际角色的差异，它们需要不同的功能、权限和可靠性。下表简要介绍了三种账户之间的差异。

	普通用户账户	医疗服务提供者账户	医疗研究者
读／写本人医疗信息的权限	有权限	有权限	有权限
查看他人医疗信息的权限	默认没有权限。可在账户所有者同意的情况下获得权限（家庭账户设置）	<ul style="list-style-type: none"> 在紧急状况等特殊情况下，一些信息可以在未经授权的情况下查看 默认只有在账户所有者同意的情况下有权限，并被医疗服务提供者标记为“医疗服务提供者申请查看” 	<ul style="list-style-type: none"> 只有在账户所有者同意时有权限。申请其他人的记录时标记为“医学研究者申请查看”
填写他人医疗信息	<ul style="list-style-type: none"> 默认没有权限。在账户所有者同意后有权限（家庭账户设置） 标记为“非医疗记录填写” 	<ul style="list-style-type: none"> 只有在获得账户所有者的同意后有权限。标记为“医疗服务提供者申请填写” 	<ul style="list-style-type: none"> 默认没有权限。在获得账户所有者的同意后有权限 标记为“非医务人员申请填写”。

医疗服务提供者和医学研究者在进行账户注册时要分别进行资质认证。这么做是为了将医疗服务提供者填写的信息和普通账户中生成的信息有效地区别开来。原则上禁止普通用户账户访问另一人的账户。在账户所有者本人不能亲自管理账户的情况下可以由他人代为管理，但只有在获得本人同意的情况下才可以进行。医疗消费者因意外或疾病而丧失意识使其无法

进行本人身份认证的情况时有发生。为了应对这种情况，医疗消费者账户紧急状况下必须的血型等重要信息可单独记录，特殊情况下，医疗服务提供者在未经本人同意的情况下，也可以访问单独记录的信息。

想要查看他人医疗信息的情况大致可以分为两种：一种是医疗服务提供者为了提供医疗服务而提出的查看申请，另一种则是申请医疗信息用于进行医学研究和开发医疗护理服务的情况。后者的行为主体为医学研究者，这种情况下，他们需要独立的医学研究者身份认证并通过账户所有者身份认证。

3.2.2 MediBloc医疗服务提供者资质认证系统(Healthcare Provider Credential System)

MediBloc平台有一个医疗服务提供者资质认证系统，用来区分医疗服务提供者和普通用户。为了保证MediBloc平台上记录的医疗信息的价值，数据生成者必须被认证为医生。如果是医疗机构，还需要确认是否已通过资质认证。经过认证的医疗服务提供者填写的医疗记录也自然地具有更高的价值。

MediBloc采用混合认证体系，它结合了由受信任的权威机构直接认证的集中认证方法和来自已经通过认证的P2P的去中心化的认证方法。为了提高P2P认证的可信性，认证人在参与认证时需要交纳一定的MP积分作为押金，在认证过程中诚实地完成任务的用户将会获得奖励，否则会被没收押金的一部分作为罚金。P2P认证的结果最终将由认证参与者的投票决定。这个过程中将不会公布个别评估者的投票结果，为此，将采取匿名认证协议[23]的方式进行评估。

3.2.3 MediBloc存储空间(Storage)

虽然电子文档形式的临床记录所占的存储空间一般很难超过几兆字节，但是医学图像资料却动辄数百兆字节甚至更大。遗传数据的大小虽然根据数据处理阶段的不同会发生变化，但所需容量很可能会超过几千兆字节。将这些数据全部存储在区块链上是不可取的。所以，MediBloc使用只能有用户本人解密的形式的私钥对数据进行加密并保存在区块链外的存储空间，而只把这些数据的哈希值存储在区块链中。如上所述，存储空间将使用基于IPFS的文件系统[22]和内部数据网络构建。

除了使用自己的个人设备（手机，电脑等）作为主要数据存储空间外，用户还可以将医疗信息存储在MediBloc核心层区块链外的存储空间里。基于这样存储的数据，用户可以轻易地获取多种个性化数字医疗护理服务。通过存储在区块链中的哈希值可以验证存储数据的完整性。

出于各种原因，用户可能会丢失其个人设备管理的数据。存储数据的智能手机和电脑可能会出故障或丢失，数据也可能会被删除或部分遗失。为了应对这些突发情况，MediBloc内部提供一套数据备份系统，并将向用户免费提供1GB的医疗信息存储空间。普通用户即使存储了自己所有的临床记录和医学图像资料也几乎用不完这些存储空间。但是，这些容量可能难以满足保存有遗传数据或者经常去医院就医的少数用户，以及通过各种服务产生更多医疗记录的用户的需求。这种情况下，MediBloc将以极低的价格提供额外的存储空间。对于所有这些存储空间，MediBloc将遵守HIPAA等法案规定的国际医疗信息管理标准。

3.2.4 MediBloc搜索系统(Search System)

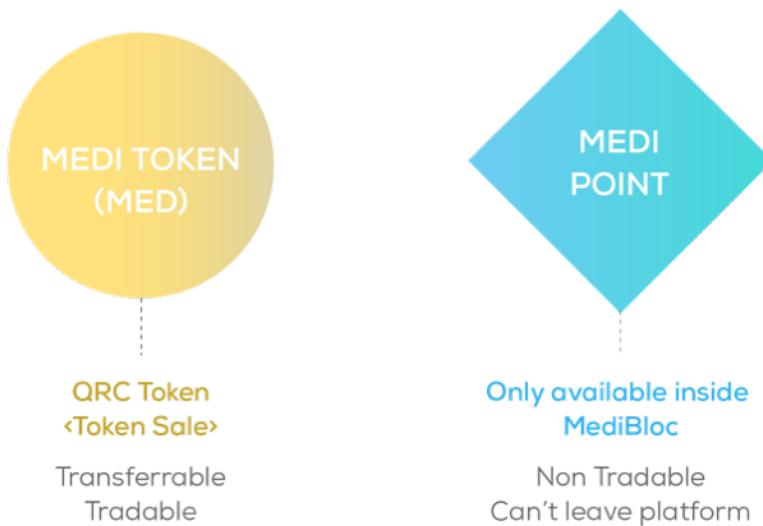
MediBloc通过服务层提供数据搜索功能,作为其核心功能之一,想要获取符合某些条件的人的医疗信息的用户,可以使用这一数据搜索功能。为此,MediBloc单独运营自己的搜索系统。所有用户都有可以管理个人信息,决定其是否能成为被公开搜索的对象。因此,该搜索系统基本上只针对那些允许被搜索的用户。

用户可以设置搜索条件,包括搜索许可和搜索许可选项。如果用户允许被搜索,MediBloc搜索系统则存储关于用户数据的索引信息。医学研究人员可以通过搜索系统检索他们想要的数据的用户,并通过数据所有者和智能合约以对等(P2P)的形式进行数据交易。

为了最大限度地减少对用户信息的暴露,MediBloc使用英特尔软件防护扩展系统(SGX)[24],这样即便是MediBloc搜索系统的管理员也无法了解在系统中注册用户的信息。通过在密封的空间存储和管理敏感的用户信息,可以最小化用户信息暴露的可能,从而使个人信息的存储更安全。

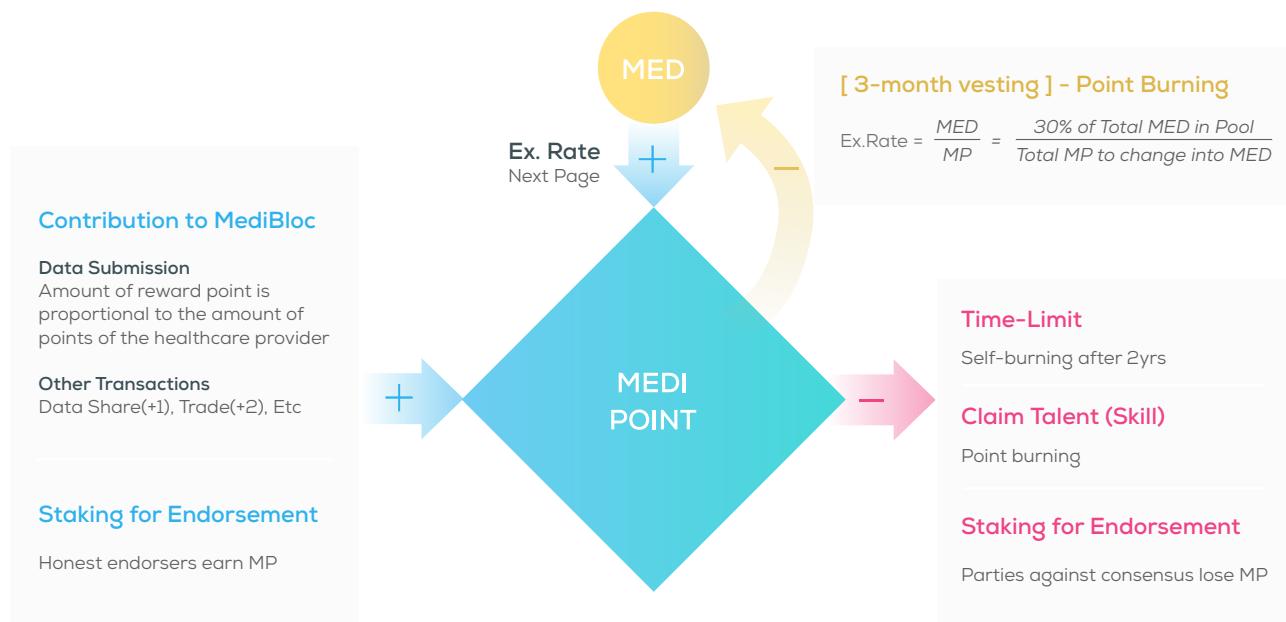
如果用户不希望数据被MediBloc搜索系统直接检索,但是符合条件的时候仍然愿意出售或者捐赠数据,则可以以稍微不同的方式参与数据的交易。想从其他人那里获取数据的用户,只需在MediBloc网络中输入所需数据的搜索条件和提供数据的报酬等信息,就可以通过MediBloc实时搜索系统找到数据。用户可以从个人设备确定他的数据是否满足该条件,并通过推送通知功能等参与数据的交易。用户甚至不用主动参与,所有这些功能也可以在后台自动完成。

4. 代币模型(Token Model)

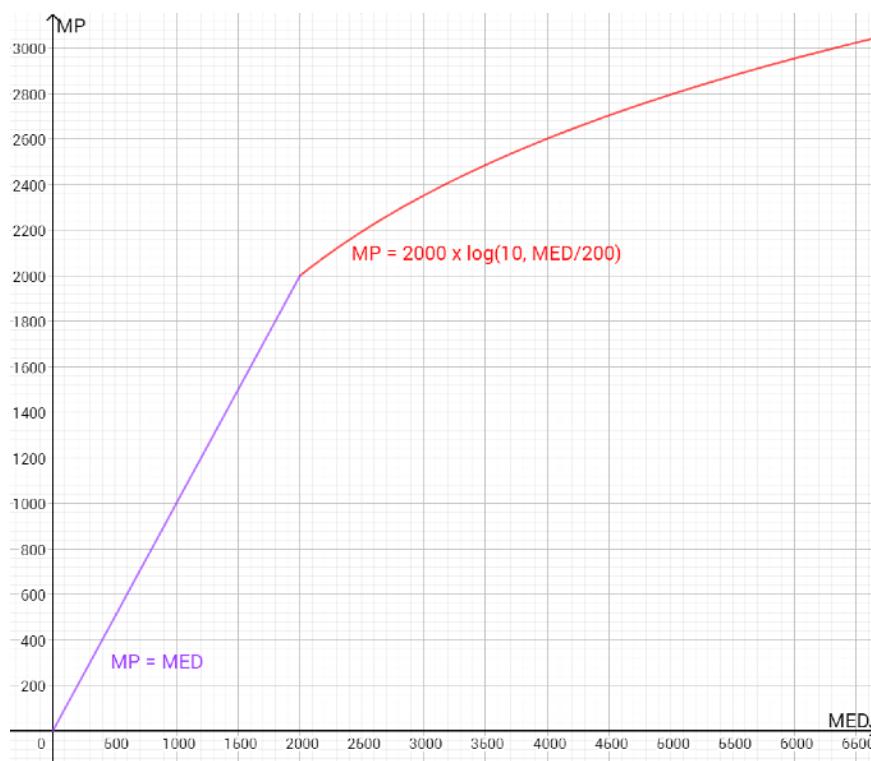


MediBloc根据QRC代币标准(属于以太坊的ERC20的量子链的代币标准) [25]发行新的代币MED币。虽然MediBloc基于量子链 (Qtum) 平台，但是由于Qtum和以太坊使用相同的协议，所以基于Qtum的MED币也符合ERC20标准。MED币是MediBloc平台内部一切交易活动的主要载体。MediBloc平台使用MED币和MP积分，MP积分用于衡量用户对平台的贡献度（平台生态系统内部评价）。MP积分不能转送给其他用户，也不能进行交易，只能在平台内部使用。MediBloc平台除了MED币还引入了MP积分，是因为为了处理包括医疗机构、医疗护理企业和个人等在内的医疗信息等敏感信息的交易，有必要建立一个用来判断交易双方信誉度的最低客观指标体系。因此，MP积分被设计为用于衡量用户为MediBloc平台生态系统所做的贡献。但是，MP积分并不代表医疗服务提供者的医学成就和技能水平。MP积分可以作为医疗消费者选择医疗护理时对医疗服务提供者评判的参考指标，但并不是绝对指标。

4.1 MP积分(Medi Point, MP)



MP积分是一种平台内部积分，用来衡量用户对平台的贡献，获取和使用MP积分的方法如上图所示。最简单的获取MP积分的方法是使用MED币购买，MED币购买MP积分时的汇率如下图所示。在一定的MP积分数量以内，二者之间的汇率保持恒定，超过这一数量后，汇率按照对数函数进行计算。虽然为了获得基础MP积分（下图中的2000MP积分），只需使用MED币购买即可。但是如果想要获得更多的MP积分，则意味着用户需要购买大量的MED币，因为购买多于2000MP积分所需的MED币数量将呈指数级增长。当然用户也可以通过在平台内进行有意义的活动来获得MP积分，比如数据的创建或者交易。基础MP积分可以视为医疗服务提供者或者医学研究者从其他用户获取数据所要求的对平台最小贡献。根据MED币的初始发行价计算，预计购买100MP积分所需的MED币价值约为10美元，这对于用户来说可以毫无负担的加入MediBloc平台进行交易。随着平台的发展，MED币的价值可能会随着变化，初始入场费可能会增加。所以早期加入MediBloc平台并尽早获取MED币可能对用户更有利。



MP积分基本上是与用户对平台的贡献值成比例的增加的。医疗服务提供者会在生成医疗信息的贡献做出后获得相应的MP积分奖励。医疗消费者使用MediBloc平台进行生成的个人的医疗信息的整合和管理本身就是对平台的贡献，因此将获得相应的MP积分奖励。奖励的额度取决于医疗信息的类型和生成医疗信息时持有MP积分的数量。此外，为了鼓励积极参与平台，平台上开展的所有活动都会有少量的MP积分奖励。

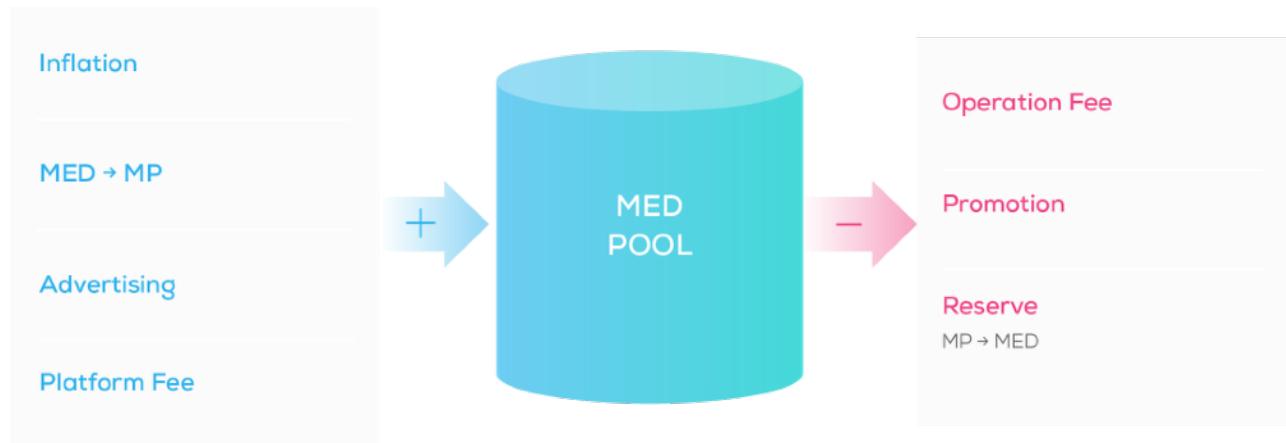
持有的MP积分三个月后可以兑换为MED币。用MP积分兑换MED币的汇率由用户要兑换的MP积分数量以及代币池中MED币总量的30%计算得出。也就是说，汇率会根据市场情况实时浮动，因此平台会实时提供有关预期汇率变化的信息。所有用于兑换MED币的MP积分，在兑换完成后将消除。

为了鼓励用户在平台上积极互动，MP积分设定了有效期。MP积分的结算以月为单位进行，从获得MP积分的当月开始后的24个月内MP积分有效，24个月后积分自动消除。通过这种设置，可以避免长期不动的MP积分导致平台经济生态系统的通货膨胀。

最后，MP积分可以用于P2P认证过程。它的工作方式类似于分布式空间里的LinkedIn这种理想化的匿名认证模式[23]。有人拥有一定的能力或技能，当他使用MP积分要求平台进行身份认证时，认证请求将被发送给网络中的其他参与者，并且接收到认证请求的参与者根据内容判断是否参与认证过程。为了参加身份认证过程，要求进行身份认证的用户必须用一部分MP积分做抵押。认证结果根据平台其他参与者的反馈，按照多数服从少数原则决定。根据结果得出一致结论的用户将获得额外的MP积分奖励，否则，用户将失去作为押金的MP积分。为了保证认证过程中不暴露用户的信息，认证采取与背面签名定义的零知识协议验证的匿名认证方法类似的方式完成。这种认证过程引导参与者进行诚实的评价，因此被认证的能力或技能可以认为是可靠的信息。

4.2 MED币(Medi Token, MED)

与MP积分不同，MED币可以在平台用户之间进行交易，并且可以移动到平台外部。MED币和MP积分一起构成了MediBloc平台社会经济生态系统的支柱，可以用于支付数据和信息的交换以及所有连接到平台的服务，也可以用来吸引尚未加入MediBloc平台的医疗消费者和医疗服务提供者参与进来。



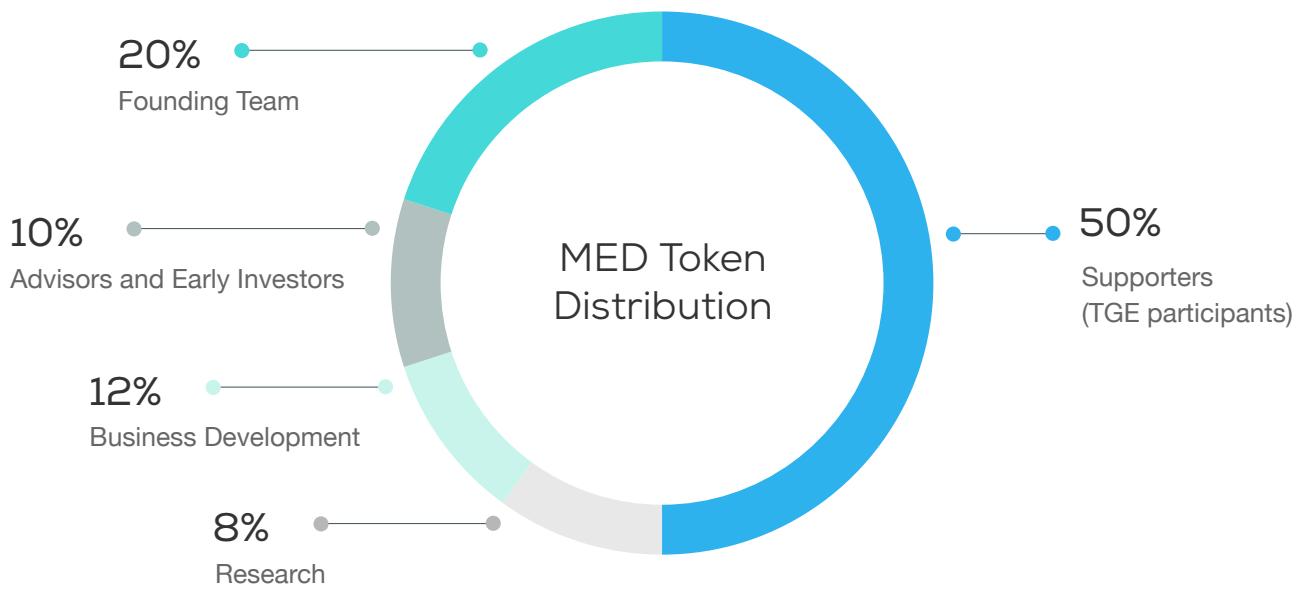
MediBloc平台拥有支持内部生态系统不断发展的MED币代币池。ICO后，设定MED币的额外发行使第一年的通货膨胀率在5%，计划以后每年通胀率降低30%，并将所有以这种方式创建的新MED币纳入MED币代币池中。平台用户可以通过MediBloc平台向其他用户推送广告，可以使用MED币支付广告费用，这些MED币也将纳入MED币代币池。平台使用基本上是免费的，但是如果通过MED币做数据交易，用户则需支付交易费的10%作为佣金，佣金纳入MED币代币池。MediBloc向每个用户免费分配1GB的容量（1GB的存储容量，1GB/月的带宽）用于存储数据，超过免费额度的容量需按比例支付费用。预计超过1GB数据[26]的用户仅占总用户数量的0.01%（基于医疗消费者），使用提供的每人1GB免费容量，用户的使用费基本可以忽略不计。最后，用于购买MP积分的MED币也将纳入MED币代币池。

这样，MED币代币池中收集的MED币的50%用于创建新账户时产生的区块链网络使用手续费（为账户创建智能合约的成本）和免费提供的存储容量成本，也将用于购买MP积分向用户支付参与活动的奖励。用MED币代币池中的MED币购买MP积分时采用固定汇率制（1MED币=10MP积分），这与一般用户购买MP积分的情况不同。其中一些MED币也可以用来支持生态系统扩展的相关服务和应用开发。其余30%用于用户的MP积分兑换MED币的储备金，由于数量不定，从MP积分兑换到MED币的汇率将会随时变动。最后的20%用于平台运营、维护和进一步的开发。

代币机制相关的数值信息可能根据后续的模拟过程而更改。

4.3 代币生成活动(Token Generation Event)

MED币的发行旨在支持MediBloc平台的开发和基于它的医疗信息生态系统的创建，默认情况下，也可以使用量子链(Quantum)参与平台。后续还将支持比特币(BTC)和以太坊(ETH)，各币种之间兑换的汇率将在MED币发行之前通过官方渠道(公司主页，Slack，脸书，推特)公布。用于支付MED币代币生成活动的MED币数量约占总初始发行量的50%。总发行量的20%用于MediBloc的开发，剩余20%资助MediBloc团队，最后10%归属咨询顾问和早期投资者。



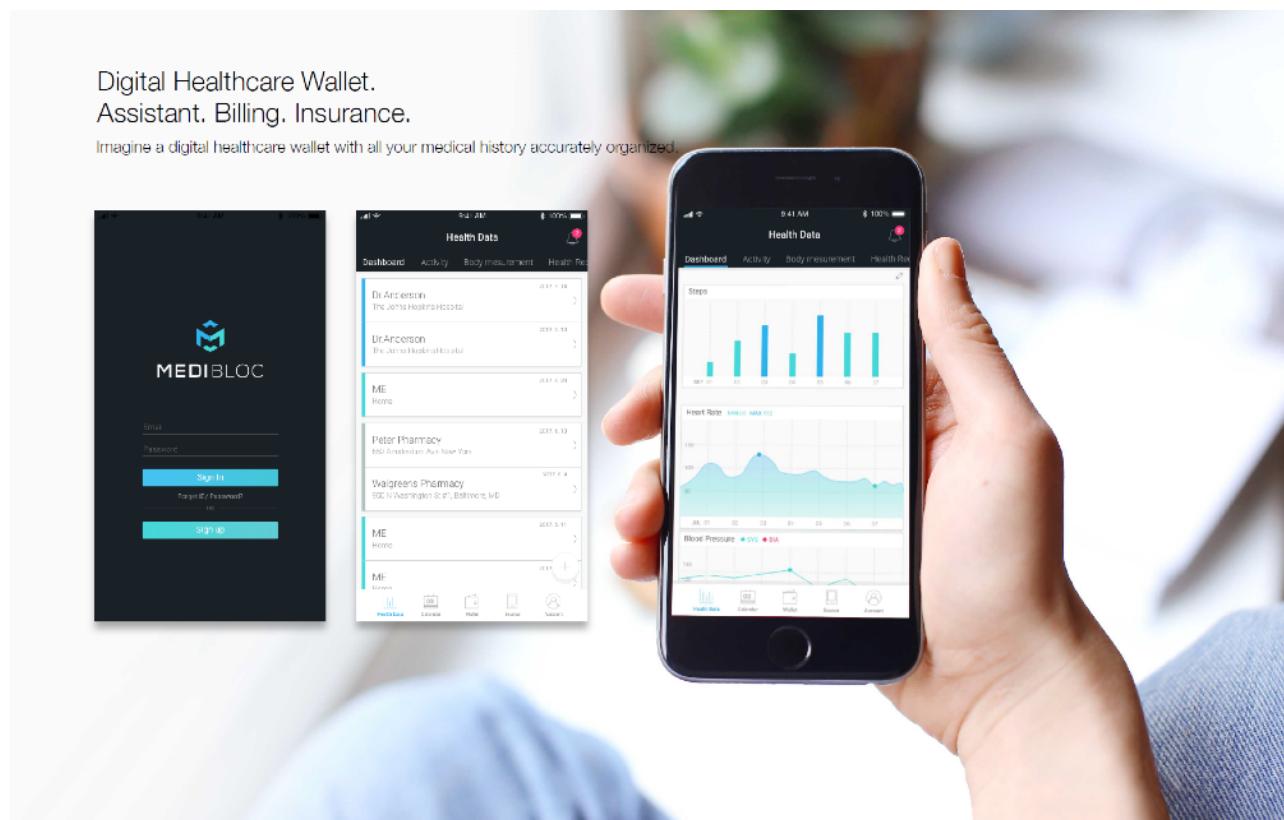
Please note, the percentages discussed above are indicative and may vary with the amount raised through the Token Sale.

与代币销售相关的准确信息将通过以下官方渠道发布。

- Website: <http://www.medibloc.org>
- Slack: <https://medibloc.slack.com>
- Facebook: <https://www.facebook.com/medibloc>
- Twitter: https://www.twitter.com/_MediBloc/

5. MediBloc服务示例(Use Cases)

5.1 个人健康报告 (Personal Health Report)



医疗消费者可以通过MediBloc平台整合分散在各个医疗提供者处的医疗记录和由可穿戴设备收集的信息。整合后的信息可以作为医疗消费者完整的健康记录进行管理和使用。医疗消费者在接受诊疗和享受个性化人工智能医疗护理服务时都可以使用收集到的医疗信息。所有这一切都是医疗界一直追求的理想型个人健康记录（PHR）的必要条件[27]。

通过这样的服务，医疗消费者不仅可以随时查看自己何时在医院接受过何种治疗、健康状况如何，还可以轻松了解自己在吃什么药物、药的成分如何、有何副作用等信息。并通过和过去医疗记录比较来把握自己健康状况的变化和现在的健康状态等相关信息。借此，用户可以进行更优质的健康管理。

5.2 自动保险理赔(Automatic Insurance Claim)

MediBloc可以根据收集的医疗记录，利用智能合约自动进行医疗保险的理赔和审核。医疗消费者不必再给保险公司打电话或者约见保险代理询问自己的保险可以报销何种疾病、检查和治疗手段，也完全不需要复印病历文件提交给保险公司做为理赔证明。根据治疗后提交到MediBloc上的医疗记录和医疗消费者加入的保险类型，智能合约将会自动进行保险理赔。在完成医疗记录和保险条款的对比之后，便会向投保人支付相应的保险赔偿金额。

还可以进一步按照整合后的个人医疗记录来选择符合自身情况的定制化保险产品。投保人可以用最经济的价格来买到最适合自己的保险产品，从而最大限度的减少医疗费的支出。

5.3 P2P医疗数据市场(P2P Healthcare Data Market)

MediBloc向用户提供了一个P2P医疗数据市场，医疗消费者可以直接与需要医疗数据的医学研究者、机构或企业建立联系。当前，医疗消费者的医疗信息被一些大型医疗机构和企业垄断，并以此来获得巨额经济利益，MediBloc平台将通过这样一个医疗数据交易体系将这些利益归还给医疗消费者本人。



仅在美国，医疗数据交易就已经有超过100亿美元市场规模，随着对医疗数据的需求不断增长，市场规模预计将继续增长。然而，医疗数据的供应有限，数据的质量也不能保证。MediBloc生态系统将不断产生优质的医疗数据，并通过建立以患者为导向的医疗数据交易市场，提高获取优质医疗数据的便利性。这样一来，曾经被一些大型医疗机构和企业垄断的巨额医疗数据收益将会归还给患者本人。

通过MediBloc，患者将意识到曾经被自己忽视的医疗信息的潜在价值，从而更加积极地参与到MediBloc平台当中。医疗研究者也可以获取更佳准确和完整的医疗信息，促进医疗事业的发展，这样就建立了患者又将从中获益的一个良性的循环结构。

5.4 人工智能 (Artificial Intelligence)

当前，所有行业都在尝试人工智能技术的创新，医疗领域也不例外。人工智能正在从复杂的、高维度的领域，如医疗诊断和新药开发，到简单的健康管理领域全面改变医学各个领域的发展。人工智能开发的核心最终取决于数据的数量和质量，想要开发人工智能服务的开发人员可以通过MediBloc来获取大量高质量的数据资源，进而实现基于更高级的进人工智能开发的服务。

通过MediBloc，患者可以根据整合的医疗数据来享受医疗聊天机器人等个性化服务。目前，基于智能手机等个人设备的个性化医疗服务很多，但是除了技术水平有限外，从用户获取输入信息仍然存在很多困难。MediBloc可以轻松解决这一难题。MediBloc平台可以实现向急需医疗服务的患者推荐医生、诊断估计、治疗建议、预后预测等服务。通过整合这些功能并创建医疗聊天机器人，可以为用户提供个性化的健康管理服务。

5.5 临床研究(Clinical Trial)

MediBloc可用作医疗机构和制药公司的临床研究平台，不仅可以用来筛选试验对象，还可用于辅助整个研究过程。

例如，在前瞻性研究中，被试验者将通过智能合约赋予研究者和研究指导员查看相关记录的权利，这就保障了整个研究过程公开透明。这样，研究过程的客观性也可以得到检验。在追溯性研究中，研究者则可以在MediBloc中找到符合研究条件的试验对象并获取所需数据来进行研究。



5.6 远程治疗(Telemedicine)

医疗消费者对医疗服务有着多样化的需求。但是，现在很多消费者由于地域和时间的限制而无法获得想要的医疗服务。MediBloc通过将平台连接的丰富医疗资源与消费者相连，打破了地域和时间的限制。消费者可以通过提供远程治疗的MediBloc平台来找到所需的医生和医疗机构，并可以全天候地接受世界各地的实时医疗服务。

5.7 社交网络服务(Social Networking Service, SNS)

MediBloc为医疗消费者，特别是一些相同疑难杂症的消费者创建一个可以相互交流的网络社区。在这里，他们可以和相同病患消费者分享有关疾病的信息，通过形成相同疾病患者之间的情感纽带，非常有助于相互鼓励并克服疾病。另外，平台也鼓励对某些疾病感兴趣的医疗服务提供者和研究人员加入该社区，使社区生活更加丰富。

6. 开发规划(Roadmap)



MediBloc的开发规划可以分为MediBloc平台和与之相关的应用程序的开发规划。

6.1 平台开发规划(Platform Roadmap)

MediBloc平台的主要开发规划如下。

MediBloc将于2017年10月发布白皮书，同时发布公开观点证据(PoC)，用于介绍MediBloc的未来蓝图。同年11月，将通过首次代币发行 (ICO) 发行MED币，与此同时也将进行平台和基础应用的开发。

2018年5月发布用于开发连接MediBloc平台的应用所需的API和SDK。2018年7月将发布平台内测版，10月发布平台公测版。在Alpha版本上，我们首先支持应用最广的HL7 [28] CDA临床文件构架标准[29]。同时，为了方便临床文件和医疗图像的交换，还将支持用于交换医疗图像的DICOM标准[30]。公测版还将发布基于IPFS文件系统的MediBloc核心数据网络，以便用户轻松备份数据。经过测试阶段后，MediBloc平台正式版将于2018年末正式上线。

2019年后，我们计划启动对HL7 CDA以外的标准的支持，并发布相应的SDK和API。2月，MediBloc核心层将配备符合HIPAA规范的存储空间，并公开相关软件和进行平台升级。这样，可以保证平台拥有足够的存储空间，以便满足平台在3月份对遗传数据的支持。此后的平台开发计划将在主页上公布。

2017年10月	White Paper Ver 1.0 Release
2017年10月	Proof of Concept (PoC) Application
2017年11月	Initial Coin Offering (ICO)
2018年5月	发布MediBloc平台API和SDK
	发布MediBloc平台内测版
2018年7月	-支持HL7 CDA®, DICOM文件标准
	发布MediBloc平台公测版
2018年10月	-上线MediBloc核心数据网络
2018年12月	发布MediBloc平台正式版
2019年1月	支持更多HL7 CDA® 以外的医疗记录文件标准，并发布其他API和SDK
2019年2月	支持第三方网络（符合HIPAA规范的存储）
2019年3月	支持遗传数据

6.2 基本应用程序开发规划(Basic App Roadmap)

MediBloc的生态系统是一个开放式生态系统，任何人都可以开发应用程序并与MediBloc平台进行连接。MediBloc正在策划一个旨在鼓励第三方参与丰富平台生态系统的奖励计划。另外，我们还将开发一些基本应用程序用来演示MediBloc平台的作用和价值。这些基本应用程序的开发规划如下。

	MediBloc 应用	MediBloc EHR	MediBloc 研究人员App
17年12月	开始应用设计和规划		开始应用设计和企划
18年01月		开始EHR设计和规划	
18年03月	开始MediBloc 应用开发		
18年04月		开始EHR开发	
18年05月			开始研究人员App开发
18年07月	内测MediBloc应用		内测研究人员App
18年08月		内测EHR	
18年09月	公测MediBloc应用	开始医院内部测试	公测研究人员App
18年10月		公测EHR	
18年11月			
18年12月	上线MediBloc应用		上线研究人员App
19年01月		上线EHR	

MediBloc计划同时开发三个在平台上运作的应用程序。这三种应用分别是1) 针对患者的医疗信息管理应用，2) 针对医疗机构和医护人员的EHR和3) 针对研究者的数据搜索应用。所有这些应用都将于2017年末或2018年初开始设计和规划，目标是在2018年末或2019年初推出。EHR不同于其他两个应用，需要进行以医护人员为对象的医院内部测试。

7. 其他（法律事项等） - TBD

This MediBloc white paper is for information purposes only, and does not constitute and is not intended to be an offer of securities or any other financial or investment instrument in any jurisdiction. MediBloc Inc. does not guarantee the accuracy of or the conclusions reached in this white paper, and this white paper is provided "as is." For the purpose of this disclaimer, the term, "MediBloc Inc.," includes its shareholders, directors, executives, employees and affiliates. With respect to this white paper or any of the content contained herein, MediBloc Inc. expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including without limitation, any representations or warranties of title, non-infringement, merchantability, usage, suitability or fitness for any particular purpose, or the absence of any error.

In no event shall MediBloc Inc. be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special, even if advised of the possibility of such damages, arising directly or indirectly from the use of, reference to, or reliance on this white paper or any of the content contained herein.

References

1. Blue Button Connector | Use Your Health Records [Internet]. [cited 13 Aug 2017]. Available: <http://bluebuttonconnector.healthit.gov/>
2. iOS - Health. In: Apple [Internet]. [cited 13 Aug 2017]. Available: <http://www.apple.com/ios/health/>
3. Samsung Health | Start a Health Challenge [Internet]. [cited 13 Aug 2017]. Available: <https://health.apps.samsung.com>
4. Krebs P, Duncan DT. Health App Use Among US Mobile Phone Owners: A National Survey. JMIR Mhealth Uhealth. 2015;3: e101.
5. Office For Civil. Summary of the HIPAA Security Rule. In: HHS.gov [Internet]. US Department of Health and Human Services; 26 Jul 2013 [cited 13 Aug 2017]. Available: <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>
6. National Electronic Health Records Survey: 2015 State and National Electronic Health Record Adoption Summary Tables. In: <https://www.cdc.gov> [Internet]. [cited 7 Sep 2017]. Available: https://www.cdc.gov/nchs/data/ahcd/nehrs/2015_nehrs_web_table.pdf
7. Munro D. Data Breaches In Healthcare Totaled Over 112 Million Records In 2015. In: Forbes [Internet]. Forbes; 1 Jan 2016 [cited 7 Sep 2017]. Available: <https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/>
8. Dietsche E. Healthcare breaches cost \$6.2B annually [Internet]. [cited 7 Sep 2017]. Available: <http://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html>
9. Wolters Kluwer Health [Internet]. [cited 7 Sep 2017]. Available: http://journals.lww.com/lww-medicalcare/Citation/2014/03000/Does_Health_Information_Exchange_Redundant.7.aspx
10. Llp B. The Financial Cost of Healthcare Fraud 2014. In: PR Newswire [Internet]. [cited 7 Sep 2017]. Available: <http://www.prnewswire.com/news-releases/the-financial-cost-of-healthcare-fraud-2014-252162971.html>
11. Who's Buying Medical Your Data. In: Bloomberg.com [Internet]. [cited 7 Sep 2017]. Available: <https://www.bloomberg.com/graphics/infographics/whos-buying-your-medical-records.html>
12. News B. Google DeepMind NHS app test broke UK privacy law - BBC News. In: BBC News [Internet]. BBC News; 3 Jul 2017 [cited 7 Sep 2017]. Available: <http://www.bbc.com/news/technology-40483202>
13. Re-Identifying Anonymous Medical Records. In: Bloomberg.com [Internet]. [cited 7 Sep 2017]. Available: <https://www.bloomberg.com/graphics/infographics/reidentifying-anonymous-medical-records.html>
14. Sweeney L. Only You, Your Doctor, and Many Others May Know. Technology Science. 2015; Available: <https://techscience.org/a/2015092903.pdf>
15. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc. 2006;13: 121–126.
16. Verizon. Data Breach Digest. In: <http://www.verizonenterprise.com/> [Internet]. [cited 13 Aug 2017]. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf

17. Thousands of patient records leaked in New York hospital data breach. In: NBC News [Internet]. 10 May 2017 [cited 13 Aug 2017]. Available: <http://www.nbcnews.com/news/us-news/thousands-patient-records-leaked-hospital-data-breach-n756981>
18. HL7 Standards Product Brief - HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, Release 1.1 - US Realm [Internet]. [cited 13 Aug 2017]. Available: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=258
19. Ethereum Project [Internet]. [cited 22 Aug 2017]. Available: <https://www.ethereum.org/>
20. Website [Internet]. [cited 22 Aug 2017]. Available: <http://www.qtum.org>
21. EOS - Decentralize Everything [Internet]. [cited 22 Aug 2017]. Available: <http://www.eos.io>
22. Labs P. IPFS is the Distributed Web. In: IPFS [Internet]. [cited 22 Aug 2017]. Available: <https://ipfs.io/>
23. Indorse - Ethereum based Decentralized Professional Network. In: Indorse - Decentralised Professional Network [Internet]. [cited 24 Aug 2017]. Available: <https://www.indorse.io/>
24. admin. Intel SGX Homepage | Intel® Software. In: Intel [Internet]. 28 Mar 2016 [cited 3 Sep 2017]. Available: <https://software.intel.com/en-us/sgx>
25. ERC20 Token Standard - The Ethereum Wiki [Internet]. [cited 8 Sep 2017]. Available: https://theethereum.wiki/w/index.php/ERC20_Token_Standard
26. Storj - Decentralized Cloud Storage. In: Storj - Decentralized Cloud Storage [Internet]. [cited 8 Sep 2017]. Available: <https://storj.io>
27. AHIMA e-HIM Personal Health Record Work Group. Practice brief. The role of the personal health record in the EHR. J AHIMA. 2005;76: 64A–64D.
28. Health Level Seven International - Homepage [Internet]. [cited 1 Sep 2017]. Available: <http://www.hl7.org/index.cfm>
29. HL7 Standards Product Brief - CDA® Release 2 [Internet]. [cited 1 Sep 2017]. Available: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
30. DICOM Homepage [Internet]. [cited 1 Sep 2017]. Available: <http://dicom.nema.org/>