MEDICAYUNLINK

技术白皮书V.01

[前言 3](#_Toc512436775)

[MCL链业务架构 4](#_Toc512436776)

[患者隐私处理 4](#_Toc512436777)

[数据的索引链 5](#_Toc512436778)

[数据的交易链 5](#_Toc512436779)

[授权节点 5](#_Toc512436780)

[备选节点 6](#_Toc512436781)

[参与节点 6](#_Toc512436782)

[数据交换 6](#_Toc512436783)

[MCL链医疗业务流程 6](#_Toc512436784)

[MCL区块链技术架构 9](#_Toc512436785)

[设计原则 9](#_Toc512436786)

[帐户 10](#_Toc512436787)

[共识算法（双链结构） 11](#_Toc512436788)

[MBFT算法 12](#_Toc512436789)

[MDAG算法 13](#_Toc512436790)

[交易过程 15](#_Toc512436791)

[交易确认 15](#_Toc512436792)

[默尔克树 16](#_Toc512436793)

[MCL链存储 17](#_Toc512436794)

[MCL链数据的检索 17](#_Toc512436795)

[MCL链数据授权 17](#_Toc512436796)

[MCL链医疗文件数据处理 18](#_Toc512436797)

[MCL链的激励机制 18](#_Toc512436798)

[积分使用 19](#_Toc512436799)

[MCL开发路线图 19](#_Toc512436800)

[MCL算法介绍 20](#_Toc512436801)

[总结 20](#_Toc512436802)

# 前言

区块链一种P2P的网络技术，推动着新的商业，技术，产业模式的转型，现阶段的互联网的价值主要体现在信息数据的传递。而区块链技术的产生，将在信息传递的基础上，实现了价值传递，其中的价值就是数字货币，从而使的互联网具备的货币金融的功能。这仅是对经济层面的改变，但对于其它行业呢？区块链技术也推动着相应产业模式的改变。

由于医疗行业的特殊性，利用区块链技术能够解决目前医疗领域中存在的各个问题。但是现有的公链或联盟链又很难满足业务需要，即使目前运行比较好的以太坊或者比特币因其结构上比较成熟，但是很难应用于医疗行业。其医疗数据隐私处理，患者数据的授权，医疗数据共享，医疗数据的存储以及医疗数据格式的复杂性，是无法用以太坊或比特币等框架。

梅地卡尔科技有限公司从事多年的医疗数据管理以及收集工作，结合医疗特殊情况建立的医疗数据链，称为:Medicayunlink链，（简称：MCL链）。

# MCL链业务架构

区块链中心化的架构，各个参与的节点能够在MCL的区块链生态环境中进行患者多种类型的数据收集，患者与医生交互、患者身份真实性验证与授权、各医疗机构之间可管理的数据交换共享以及多中心医疗医疗机构科研工作。



业务架构图

## 患者隐私处理

患者的数据上链之后会进行隐私化处理，患者的个人信息，过往的病历记录都会进行HASH处理。在链上的数据只显示相关的病种信息，患者可以授权自己的数据，提供给自己的主治医生查看。通过MCL链将医疗数据归还予患者，患者可以把自己的内容提供给医疗服务者。

## 数据的索引链

各级医疗机构之间的数据格式无统一的标准，造成了数据无法进行有效的共享与利用。MCL链依照不同的医疗数据类型，建立了标准化的区块链数据结构，各级医疗机构能够通过MCL链，向数据所有者申请数据的访问权。

## 数据的交易链

MCL的交易链主要用于存储患者与医疗机构之间的数据交易，医疗机构与医疗机构之间的数据交易，医疗机构与医疗企业之间的数据交易。交易不仅仅局限于数据之间，也可以存在患者与医疗机构之间的请求服务，通过交易链能够确保了患者身份的真实有效。

## 授权节点

在MCL区块链网络中，最重要的就是授权节点，授权节点主要的任务就是验证各个节点之间的交易，以及打包出块。出块是将在达到固定时间段内或者固定交易数量后，将交易数据进行打包处理，并生成区块。授权节点的生成采用申请机制，默认授权节点的个数应为奇数。MCL链在固定的时间段内，会对授权节点进行审核，对于长期不出块或者高于平均出块时间的节点会进行剔除，以维护区块链结构的稳定性。

## 备选节点

在相对于复杂的网络环境中，授权节点会发生各种问题，比如收到DDOS攻击，或者系统无法启动等。备选节点就会启动升级为授权节点，原先的授权节点则调整为备选节点。备选节点无须申请，系统配置初期交给用户选择，由用户判断此节点为备选节点还是仅作为客户端的参与节点。

## 参与节点

参与节点相当于web客户端，参与节点主要的功能进行模板数据的提交工作，完成患者与医疗机构的交易，各个节点之间的数据交易等。参与节点还有一个作用就是管理用户的帐户，以及管理用户积分等。

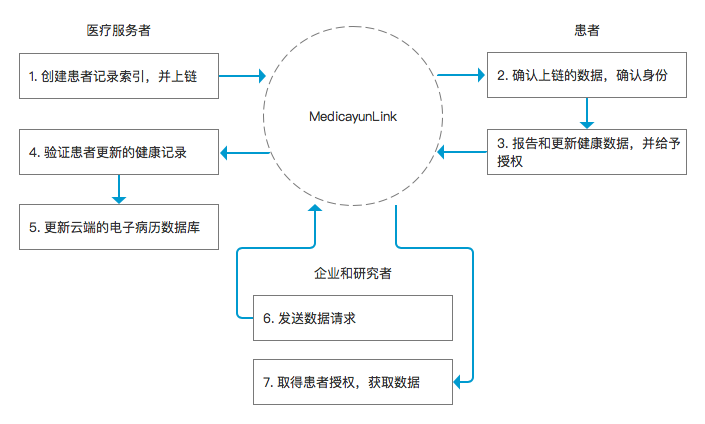
## 数据交换

MCL链会利用P2P的技术来解决医疗数据中“化验单”，“医疗影像”，“基因数据”等数据的共享与安全传输。首先这样级别的数据是无法用区块链技术进行上链存储以及共享。MCL提供了P2P点对点的方式进行数据传输下载。（注意：化验单，影像数据以及基因数据，都经过隐私化处理。）

# MCL链医疗业务流程

在MCL网络中，主要有三种角色：

* 患者：提供个人疾病以及健康数据和信息，向数据的使用方提供数据授权。
* 医疗服务者：包括各级诊所和医院等医疗机构，负责创建患者记录，验证患者身份，和收集医疗和健康数据。
* 企业或者其他研究者：包括制药和保险企业，基因等生命科学企业，或公共卫生的研究者以及数据的需求方或使用方。



在MCL区块链网络中，患者将分配一个具有全球唯一性识别码，UPI（Unique Patient Identifier）。UPI由医疗服务者负责创建和维护，而在确认了患者身份后，患者报告的健康数据就会被不端更新到MCL网络中。

确认患者的身份和其唯一性，可以将患者在任何医疗机构就诊的记录整合成为一个单一视图的数据集，而连续性医疗记录意味着可以更加全面地医疗方案进行评价。

在技术架构中，加入MCL的医疗服务者和企业等组织负责建立受信的服务器节点，为整个网路提供服务验证，出块支持。而患者可以通过PC客户端、移动端加入到网路中，APP用于确认和更新个人数据，接收数据请求和发送授权。

医疗机构在对患者进行身份确认和要求更新数据时，通过EHR（Electronic Health Record，电子病历）应用服务器的API接口：1）向授信节点发送请求和公钥；2）由授信节点向患者APP转发请求和公钥；3）患者端接受请求，返回更新的数据、公钥和授权访问的私钥；4）数据的交换在通过授信节点验证后，HER服务器得到患者的数据和对于数据访问的权限；最后5）受信任节点将此次数据交换做一个交易，打包到区块中。

MCL开发和提供公共接口、第三方应用通过调用接口，在授信节点上建立智能合约满足业务需要。

在进行跨机构间的数据交换时；6）医疗机构的EHR 应用服务器铜通过受信任节点向患者发送请求和公钥；7）患者端返回公钥和授权的私钥给受信任节点；8）受信任节点验证数据交换成功后，通知HER服务器，进行数据交换；9）受信任节点将交易打包到区块中。

患者的身份识别码UPI，每次更新的数据记录摘要，数据存储位置，数据交换记录等信息保存在基于区块链的统一帐本结构中，完整的医疗记录则保存在由受信任节点管理的分布式存储系统中。

MCL是一个去中化的网路架构，其特点是安全、透明和高效。它在各成员间建立了一种信任关系，可以有效地保护患者隐私，并且，数据的使用具有明确的授权记录，可以追溯和审计，符合法律监管要求。

# MCL区块链技术架构



## 设计原则

MedicayunLink链在技术架构上遵循如下准则：

* 全面符合医疗业务场景

MCL区块链架构主要应用于医疗产业服务，医疗产业尤其特殊性，MCL链会建立一套通用的医疗区块链平台，在通用的平台基础之上完成不同病种，不同科室以及不同的业务之间的数据整合与流转。

* 数据加密

MCL对于上链的数据除病种摘要信息以外，与患者等相关的信息全部加密处理。（MCL链对于PC客户端采用传统的对称加密算法。如：aes。另外MCL链会对手持移动端的加密算法进行优化，目前会次采用chacha20算法，此算法优化了移动端的加密机制，完全适应ARM平台）

* 模块化结构

MCL链采用模块化设计，并定义结构清晰的接口，以实现各个模块之间的松耦合，提高链的扩展性。用户可以根据不同的医疗业务场景，指定自己的模块化组件。

* 开源协议

MCL链采用MIT开源协议，具体协议请参见国内[百度百科](https://baike.baidu.com/item/MIT%E8%AE%B8%E5%8F%AF%E8%AF%81/6671281?fr=aladdin)，国外参见[wikipedia](https://en.wikipedia.org/wiki/MIT_License)

* 安全效率

MCL链在编码基础上遵守安全性，高效率系统设计原则，采用性能与安全性高的C/C++语言编码，以及简洁的算法来实现。

## 帐户

MCL链的帐户生成是有一定区分的，通过审核节点，备选节点生成的帐户在业务上为医生帐户，医生审核病历并提示患者下载应用节点的帐户为患者帐户。医生帐户的和患者帐户的生成规则全部都依照身份ID，根据身份证ID采用ECC算法生成公钥和私钥，其公钥可以作为各个用户的唯一标识，在MCL链中可称之为MECID，MECID=public key。

医生帐户在创建患者的时候，需要几点审核1）内容审核，2）是否已经存在，未存在表示尚未注册用户，需要让患者用户下载上链，生成MECID并建立关联。

MCL链虽然在业务层面分为医生，患者，医疗机构企业，但是在系统帐户层面不会进行区分，都为根据身份ID生成的公钥信息。各个节点的帐户信息将存储在本地的数据库系统中。

帐户信息的安全处理：MCL链为用户提供一套帐户信息找回机制，在帐户找回中，我们的采集用户帐户的基本信息，采集信息主要有身份证ID，用户的手机号，在注册帐户的时候，要求你保存的12字符编码。MCL链会根据你提供的这些 信息帮你恢复帐户。注意：MCL链也会不定期的提示你保存帐户信息以及更改帐户密码，尽量将风险降到最低。

## 共识算法（双链结构）

目前共识算法有“PAXOS”，“PBFT”，“Raft”，“POW”，“POS”等，通过对比发现，这些算法运行过程分为几个阶段：

* 交易扩散；
* 交易排序；
* 调用交易的执行顺序；
* 对交易执行结果进行共识；
* 提交共识结果；

各种共识算法的差异体现在不同的阶段采取了不同的实现策咯。

* POW，POS算法在交易扩散和排序时，不采用原子广播协议，同时以随机化的方式选择出Leader节点执行排序，因此会导致交易可能被随机丢弃。
* Raft，Paxos算法对全部交易进行原子广播和排序，但是共识的过程并不处理拜占庭错误。
* PBFT算法对全部交易进行原子广播和排序，同时在共识阶段处理拜占庭错误，但是不支持动态节点调整。

MCL链是主要面向医疗企业市场，在企业级市场应用比较好的就是Hyperlegeer，而的共识算法就是采用PBFT共识协议。MCL链会在PBFT的基础上对算法进行优化，能够实现动态的节点调整特性的MBFT。

还有一种共识算法结构在区块链中逐渐流行起来，就是DAG（有项无环图），DAG不同于以上所说的共识算法，在区块链结构中有一定的创新，因为在DAG算法不需要出块，具有高并发特性，把原先的同步记账方式升级成为异步记账，MCL会对DAG算法进行优化，使其达到能够处理患者模板摘要上链的MDAG算法。

### MBFT算法

MBFT算法是在BFT基础之上，能够实现动态节点的调整。MCL的节点是会随着参与的医疗机构是不断调整的。但采用BFT算法如果需要调整节点需要将各个节点的设备停机，之后修改配置文件等步骤后才可以完成节点的添加。这样的灵活性大大降低了，而且也不适用MCL的推广，因此MCL在BFT基础之上采取节点认证方式动态添加节点。

### MDAG算法

全称（Directed acyclic graph），有向无环图，DAG属于计算机算法中图论，是一种数据结构，在图论中为了简化结构，分为有向图和无向图两大类，在无向图中进一步约束形成了DAG，无环图是指它是由集合的顶点和有向边构成，每条边连接一个顶点到另一个，这样，在一些顶点V开始，沿着有序列的边，最终循坏回再次到V顶点是不可能的，其实DAG也是树的一种泛化处理，真正在用的时候一般会通过深度优先或者广度优先规则把图拆成森林，也就是“树”形结构。而DAG图由于规则的定义更容易形成一颗“树”。



应用到区块链的架构中是由Sergio Demian Lerner提出的，具体请参见DAGCoin Draft论文。在目前的大数据分布式处理的系统中，计算框架也采用了DAG算法结构，但是区块链这样的链式存储还是需要一定的考证。目前MCL的数据存储链按照医疗数据的不同类型，设计中不同的类型结构，每个结构存储格式固定的数据，每个数据结构可以标识成为一个数据点。比如（患者病例摘要数据点，化验单数据结构点，患者影像数据结构集合数据点）。下面会通过图例给与说明：



P1~PN为患者数量，PN-N为患者连续性数据，比如P1为患者1的摘要数据，P1-2为患者1的检验数据等。（每个数据点由各个节点提交，由于医疗数据的严谨性，提交后的数据需要进行审核，当然审核过程是通过MCL链的应用平台完成的，具体内容可以详见MCL链接应用层介绍。）由于提交上的数据都是审核后的数据，验证过程比较简单，一个节点必须被其它的节点引用，引用数为N>=1，被引用后才为有效的数据点，如图:



其中绿色的为顶点，在顶点中不会存储数据，类似于区块链的创始区块，蓝色为批准后的节点，而红色表示未进行引用的节点，未被引用的数据也为无效节点。

## 交易过程

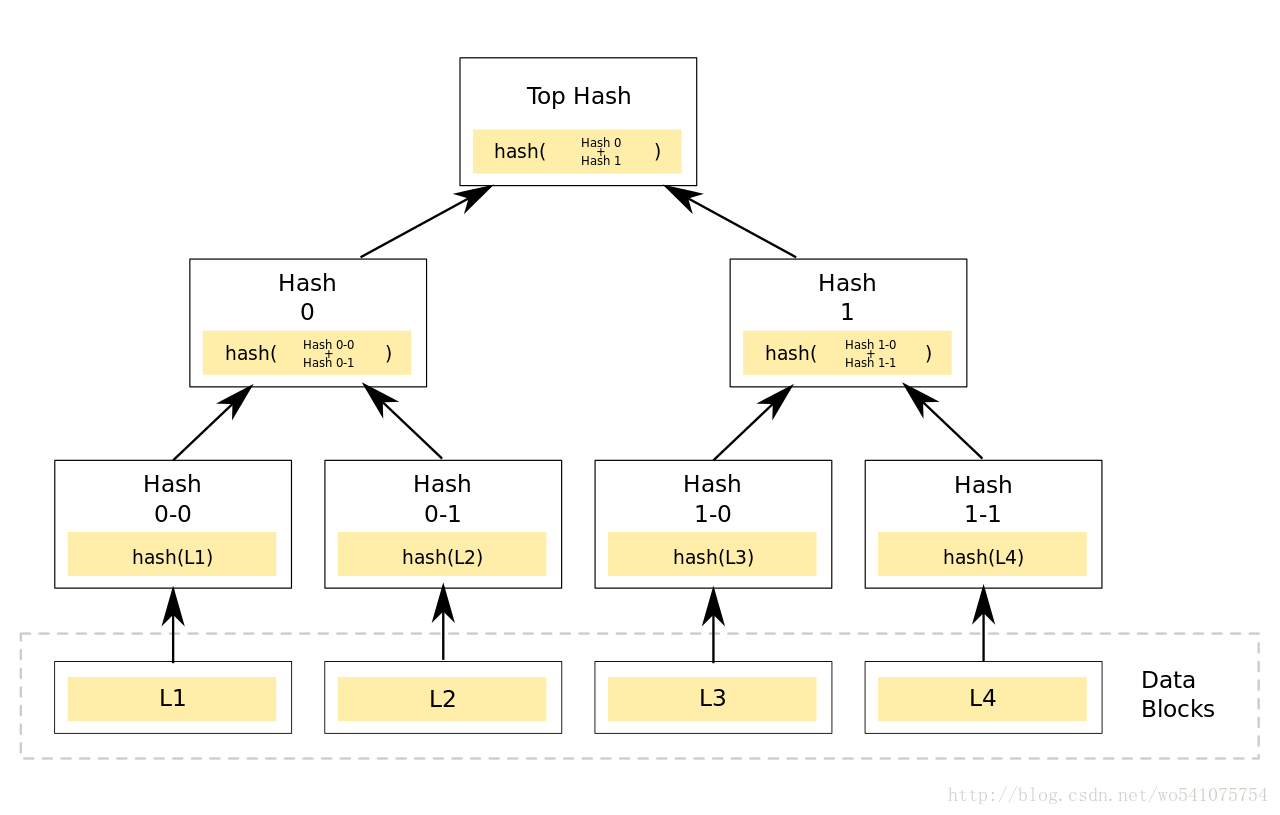
首先说明一下MCL链的交易类型，由于MCL链主要用于为患者，医疗机构提供服务，其交易类型大致分为两类：

* 各个节点的积分交易，此交易需要存储到MCL链的交易链（MBFT）。
* 各个节点的数据授权以及数据交换，这些内容不同于传统区块链的“货币”类型交易，此交易记录类似于数据的授权访问，但是访问的权限列表会存储到MCL的数据链，数据链会详细记录每个数据点由那个节点访问、更新等。

## 交易确认

MCL链的交易链采用的是MBFT算法，交易发起后进行全网广播进行确认，出块后会把交易打包到去区块中，并根据根据共识协议进行同步处理。MCL数据链接内容确认，MCL数据链就是患者摘要信息，确认过程需要有医生进行前期审核，审核患者提交的数据真实性，审核完毕后患者会接收到一个确认消息（确认消息会随着网路的阻塞会有一定的延迟），确认完毕后才为一个真实数据，之后会形成一个数据点，数据点会根据最短路径算法，引用上一个数据点，从而形成一个数据链。（注意：相关的算法为DAG，更详细的算法内容会在MCL黑皮书中介绍，另外DAG处理双花交易有点复杂，也会在黑皮书中一一介绍）。

## 默尔克树



比特币与ETH都利用了Merkle Proof，MCL的交易链会采用Merkle Prool的机制来存储每个区块的交易。为了尽量是交易简化，需要让区块头包含的内容尽量少，仅仅需要3个元素“上一个区块的HASH”，“时间戳”，“包含该区块交易的Merkle Tree的根HASH”，client如发起一个交易状态，只需要一个简单的Merkle proof请求，MCL交易与比特币类似，可以使用请客户端完成，比如需要发起支付或者查询

可以通过协议查询各个节点，至少大于1个的节点会进行反馈。

注意：MCL链不适合高并发的数据交易，主要针对于医疗领域中所产生的问题而设计（关于默尔克树具体算法，可以参考http://www.cnblogs.com/fengzhiwu/p/5524324.html）

## MCL链存储

MCL链分为交易存储，数据存储，本地存储。交易信息的存储和数据内容的存储都在上面章节都介绍过了，但是还有一部分内容需要进行存储，也就是区块的元数据信息和数据点的元数据。MCL采用的是LEVELDB进行本地化存储，存储的内容public key为固定标准，其余的存储内容采用（K,V）来进行定制。本地化的数据存储主要用于进行建立索引信息。

## MCL链数据的检索

MCL的数据存储链，对于医疗项目会有数据的检索与处理，MCL提供的搜索算法，能够快速检索数据存储的内容。数据点不仅可以存储医疗数据，其存储的内容范围很广，P1点可以存储患者相关的模板内容，但P2可以存储文本文件的内容，对于存储的内容MCL链接可以利用搜索算法处理，目前采用的图的深度优先搜索（DFS）。（关于具体的算法实现会在MCL链的黑皮书介绍）

## MCL链数据授权

医疗数据的授权是一个非常严谨的过程，MCL链要保证数据在提交初期都会有专业的人士进行审核，尽最大努力保证数据为患者本人。完毕后需要进行上链，上链的数据都是进行隐私化处理，采用（HIPAA）管理方法进行处理。但是对于需要服务的患者，患者可以将自己的个人数据进行有条件的授权。首先数据的需求者通过系统检索需要的数据，系统会向数据的拥有者发起一条交易信息，收到交易申请后，数据所者会利用private-key来进行批准。整个交易的过程会完全记录在数据存储点中。

## MCL链医疗文件数据处理

针对医疗数据的文件，MCL链接采用了点对点技术（peer-to-peer，简称：p2p）来实现医疗数据（化验单，医疗影像等）传输。P2P的数据传输依赖MCL联盟中网路参与的计算能力和带宽，并不是通过集中在少数服务器上。而且P2P技术使用已经非常成熟，而且传输机制也相对可靠。

## MCL链的激励机制

激励机制是维护MCL链共识联盟的一种机制，在MCL链中每个参与者都有平等获取激励的机会，使其共同维护整个网路的稳定性。MCL链不同于BTC或者ETH通过挖矿的形式来获得应有的激励，而是通过数据的贡献度，为节点用户（患者）的服务度，为MCL网络提供资源的程度来统一进行分配。MCL链提供总量为100000000的积分，每一个积分都由32为的MD5算法生成，每一个积分都有唯一标识，以统一结构存储在各个节点上，并可以通过客户端浏览器进行查看积分是否被分配，以及由那些帐户所持有。MCL的分配策咯分为几种：

* 当一个帐户向另一个帐户提供数据，数据审核有效则进行一个积分激励。
* 授权节点验证交易出块则进行一个积分激励。

积分使用：

* 各个帐户有余额的情况下可以进行各个帐户之间的转账。
* 各个帐户之间的医疗服务，如：在线问诊，患者随访调查。卖方可以对提供的服务进行定价，买方可以根据价格进行支付。
* 帐户请求数据的访问权等。

为了MCL链系统运行稳定会收取一定的服务手续费，手续费会继续进入到MCL资金池中。（注意：对于所发生的积分交易会存放到交易链）

MCL链的激励机制开放接口，调用者可以通过我们的积分与自己产品的激励机制相结合。

# MCL开发路线图



# MCL算法介绍

目前MCL链的算法大致分为两部分，1）数据信息安全加密算法，2）分布式算法。

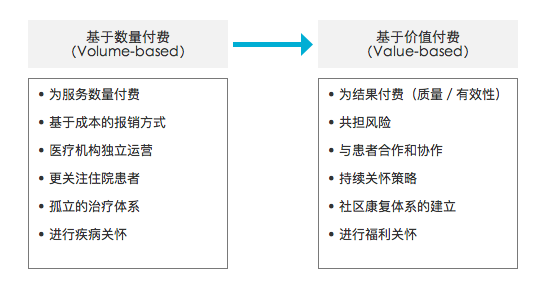
1）数据信息安全算法：AES，chacha20， SHA256，SHA512，SHA1，RIPEMD160，HMAC\_SHA512/256，ECC等

2）共识算法：PBFT=>MBFT，DAG。

以上的算法都经过时间考验安全稳定。

# 总结

人口老龄化和快速增长的医疗成本给社会福利体系造成了沉重的负担，这些因素迫使医疗服务体系开始进行转型，从事基于数量的付费转向基于价值的付费。

****

医疗服务机构同患者紧密连接、开展合作和协作成为了新模式下的一个显著特征。普华永道公司在2016年发表的研究报告也表明“在2017年，与患者互动将成为FDA监督（医疗机构）执行‘处方药用户付费法案’中的核心部分”[[1]](#footnote-1)。

MedicayunLink项目就是为了在患者、医疗服务者、以及制药等商业机构之间创造一种新的合作模式，通过区块链技术的应用解决困扰开展协作的隐私保护、数据安全等问题。并且，通过引入Token作为激励机制，充分实现各参与方利益的一致性和明确性。

MedicayunLink致力于维护一个去中心化、透明、高效的网络和协作社区，协助医疗卫生及生命科学行业加快转型，并帮助改善医疗资源的使用效率和促进群体健康水平的提升。

1. [↑](#footnote-ref-1)