



白皮书

健康链

健康链·开启全球健康产业大数据时代

2018 年 06 月

健康链构建与区块链融合的全球健康产业生态圈

目录

摘要.....	1
第一章 项目背景.....	1
第二章 项目介绍.....	2
第三章 行业分析.....	3
3.1 行业现状.....	3
3.2 行业痛点.....	5
第四章健康链—开启全球健康产业大数据时代.....	6
4.1 什么是健康链.....	7
4.2 健康链的特点.....	8
4.3 开启全球健康产业大数据时代.....	10
第五章 健康链整体平台架构.....	10
5.1 健康链数字资产平台.....	10
5.2 健康链运行系统.....	12
第六章 健康链区块链技术应用.....	14
6.1 分布式结构.....	14
6.2 数据区块结构.....	18
6.3 共识机制.....	19
6.4 安全加密算法.....	19
6.5 智能合约协议.....	21
6.6 去中心化自治.....	22
6.7 可追溯性.....	23

6.8 不可篡改.....	23
第七章 健康链未来应用价值分析.....	24
7.1 健康链主要应用场景.....	24
7.2 健康链项目未来价值分析.....	26
第八章 健康链发展规划.....	27
8.1 初期规划.....	27
8.2 中期规划.....	27
8.3 未来规划.....	27
第九章 健康链盈利模式.....	28
9.1 经营盈利.....	28
9.2 交易盈利.....	29
第十章 运营团队介绍.....	29
10.1 团队成员.....	29
10.2 专家顾问.....	29
第十一章 发行计划.....	29
11.1 发行方案.....	29
11.2 发行细则.....	30
第十二章 风险提示.....	31
12.1 政策性风险.....	31
12.2 市场风险.....	31
12.3 技术风险.....	31
12.4 资金风险.....	32

第十三章 免责声明.....	32
----------------	----

摘要

健康链构建与区块链融合的全球健康产业生态圈，就是为了服务当今日益扩大的健康产业市场，使人们的健康养生可以全面系统化。面对当前美容、医疗、养老、保险等健康体系存在的行业痛点，以及由这些痛点导致健康体系信息被篡改、医疗信息不完善、用户个人信息被窃取、社会健康资源不平衡等问题，健康链利用区块链技术构建了一个生态化共享健康服务平台。

健康链借用区块链分布式、可信任、不可篡改性来记录所有相关数据，形成完整轨迹，让用户的医疗健康等信息能够完整记录，保障个人权益。健康链平台联合医疗、健康管理、美容等机构为用户打造了一个完善、公平的保障体系，用户可以在平台上享受到量身定制的医疗健康养生服务。

第一章 项目背景

由于工业、农业污染、空气污染、水污染等环境问题恶化。繁重的工作压力，健康严重透支，夜以继日的投入在工作当中，忽视了自身的健康。在全世界真正健康的人仅占 5%，经医生检查、诊断有病的人也只占 20%，75%的人处于亚健康状态，为疾病埋下了隐患。健康养生产业发展潜力巨大，随着经济的快速发展，健康的消费需求由简单、单一的医疗治疗型，向疾病预防型、保健型和健康促进型发生转变。随着全球经济快速发展和居民生活水平的提高，健

康成为了焦点话题，而当前由于工业、农业污染的严重，人类对健康营养的诉求已转移到功能食品、养生食品、绿色食品、美容、健康养生等。

据《医药项目可行性研究报告》数据显示，美国的医疗服务、医药生产、健康管理等大健康产业增加值占 GDP 比重超过 19.5%，是仅次于制造业、服务业、金融保险业、房地产的第五大产业。加拿大、日本等国大健康产业增加值占 GDP 比重也超过 10%。

健康链，一个致力于为全球范围内的大健康产业提供一个去中心化运作的健康资源平台，构建与区块链融合的系统化的健康资源智能化平台。健康链平台基于区块链技术的建立，以智能合约作为支付技术，充分发挥区块链去中心化、信息公正透明化特点，使平台信息共享化。

第二章 项目介绍

本项目在政策利好和区块链和大健康市场迅速发展以及成熟的背景下创建一个以“区块链+健康行业”为主营业务的项目，将区块链和健康产业完美结合，致力于构建新一代具备自优化能力的智能共享数据网络。区块链+健康产业项目主要目的在于解决传统中心化健康产业的信任问题、时效问题以及规模化发展问题，利用区块链的防伪、防篡改属性来记录每一笔交易和用户点击，让所有健康系统产业行业的上下游链条实现透明、高效，让全球美容，养老，医疗，健康领域市场最大化提高效率，降低成本，让人们的身体全面系统的进行健康养生，享受生命长寿。

一方面，健康链平台在底层技术的支撑下开发面向用户的客户服务端，并且为了保证能够兼容各个版本，开发出 iOS 版，安卓版以及 VIP 官网服务。另

一方面，吸引合作伙伴形成供应伙伴联盟进入该平台为用户提供服务，包括企业、养老机构、医院、政府机构、健康行为，实现生命一体化系统服务，该平台主要提供美容服务、养老机构筛选、医院挂号就诊、健康行为数据、交易服务系统等，通过提供这些服务平台可以获得用户的相关数据，由于是整合性平台，对于个人来说，可以就一个人的所有轨迹形成健康征信。而对于健康领域、保险业、养老业以及医药行业等相关利益者来说，形成的医疗健康数据、养老数据、交易数据以及结算数据可以为其提供营销建议，更为综合可靠的用戶信息为精准化营销作出贡献。相比于现有的区块链，通过健康产业技术的引入以及底层架构创新，健康链具备更易用、更安全、更快捷、更灵活四大优势。

第三章 行业分析

3.1 行业现状

随着社会的不断进步，国民生活水平的不断提高，美容、健康养生已经成为人们生活息息相关的产业。美容、健康养生行业迅猛发展,已成为人们生活中的日常不可或缺消费行为。生活节奏加快和压力的加大，让处于亚健康状态的人群不断增加。据世界卫生组织一项全球性调查结果表明，全世界真正健康的人仅占 5%，经医生检查、诊断有病的人也只占 20%，75%的人处于亚健康状态。有关资料显示，在美国每年有 600 万人处在亚健康状态，成年人中占 25%-48%。在亚洲地区，处于亚健康状态的比例更高，不久前日本公共卫生研究所

的一项新调研发现，接受调查的数以千计员工中，有 35% 的人正忍受着慢性疲劳综合征的困扰。

在中国约有 70% 的人呈亚健康状态，亚健康人数超过 10 亿，为疾病埋下了隐患。据统计，2002 年时中国 65 岁以上的人口占总人口比率只有 7.7%，到 2014 年，该年龄段的老年人口占比超过 10.00%，2015 年 60 岁及以上人口达到 2.22 亿，占总人口的 16.15%。2016 年中国人口老龄化加速，中国成世界老年人口最多国家，预计到 2020 年，老年人口达到 2.48 亿，老龄化水平达到 17.17%，2025 年，六十岁以上人口将达到 3 亿，成为超老年型国家。

中国经济增长的速度超越了世界上所有国家，但中国消费者平均用于养生用品方面的花费，只占其总支出的 0.07%，而欧美国家消费者平均用于养生用品方面的花费，占其总支出的 25%，相差甚远，这充分说明中国养生保健用品市场的发展潜力巨大。在中国，健康养生产业仅占中国国民生产总值的 4% ~ 5%，低于许多发展中国家。而在发达国家，这一比例普遍超过 15%，健康养生产业正逐渐成为带动整国民经济发展的巨大动力。

21 世纪健康养生产业已经成为全球热点，健康养生产业也将成为继 IT 互联网产业之后的全球财富集中产业。随着中国居民收入水平不断提高，消费结构升级不断加快，人们对生活质量的要求日益提高，健康养生产业面临着广阔的发展前景。

3.2 行业痛点



- 医疗供应链的集成化程度低导致信息传递扭曲失真，效率低下。

在医疗健康领域，存在大量高价值的敏感数据，比如患者病历，由于数据主权和缺乏可信交换和共享机制等原因，不同的医疗机构之间、医疗机构和其他相关机构之间，例如政府、保险、药业、医疗设备供应商等，无法进行有效的数据交换和共享来提高治愈率，各自系统分别形成一个个独立的信息孤岛，导致价值极大丢失和医疗资源的严重浪费。

- 假冒伪劣充斥医疗供应链，市场秩序被破坏。

充斥在市场中的假冒伪劣药品、保健品等医疗健康商品层出不穷，制假售假现象屡禁不止。不但严重扰乱了正常市场秩序，也埋下了使用假冒伪劣商品的隐患，甚至损耗消费者的健康，危及生命。

据世界卫生组织报告称，过去4年，该机构收到15万起假药案例，42%来自非洲，美洲和欧洲均占21%。假药泛滥威胁全球医疗安全和生命健康，许多

国家备受困扰。2017年上半年中国受理“医药及医疗用品类”投诉共1954件，其中涉及虚假宣传的有485件，占24.82%。

- 上下游行业壁垒降低医疗供应链整体效率。

供应链成员之间存在严重的信任危机，主要体现在上下游节点信任不对称、信任的易毁性和恶性循环以及供应链规范信任机制的缺失，如医院收取高昂的医药品佣金，从而压榨患者。

- 受众认知误区。

1、认知不多：在缺乏正确的认知引导后，他们的知识获取来源，很大一部分来自于广告，广告的花而不实，就导致了对产品的不信任。

2、认知错误：健康的人不用补，不健康的人不敢乱补，现阶段的认知都这样。

3、信任危机：从最初的信赖，到半信半疑，到最后的信任危机。

- 消费场景受限。

保健品本身带有一定的口味，很难勾起多数人的喜欢;再者面对强大的竞争对手，很难营造出能够替代的气氛。

第四章健康链—开启全球健康产业大数据时代

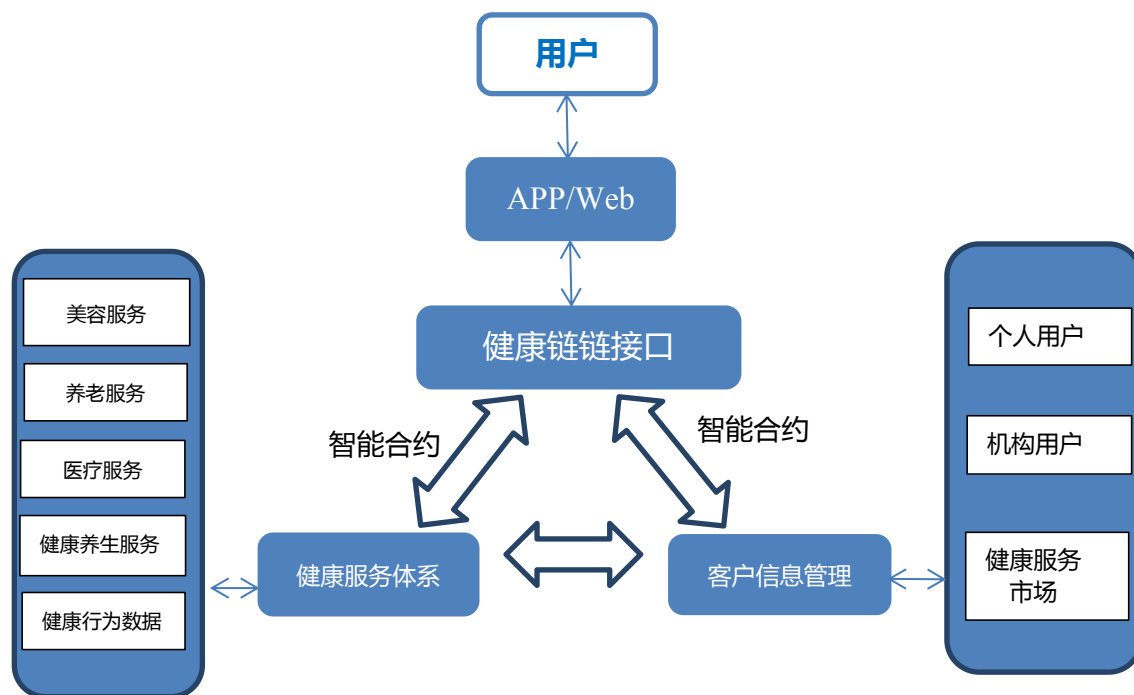
4.1 什么是健康链

健康链基于区块链的智能合约、去中心化、不可篡改、可追溯的特性，打造基于区块链技术的一个去中心化的全球健康产业交易平台，创建一个更加高效、透明、可信、且具备自我维护的生态系统，成为一个应用于全球健康产业市场的商用区块链。健康链利用区块链分布式记账技术提供一个安全的、防篡改的账本，以高防伪技术解决线下难题。让全球健康系统产业能够在健康链平台上快捷的开发自己的区块链应用，并根据智能合约自由交换数据，利用区块链的防伪、防篡改属性来记录每一笔交易和用户点击，让所有健康系统产业行业的上下游链条实现透明、高效，让全球美容，养老，医疗，健康领域市场最大化提高效率，降低成本，让人们的身体全面系统的进行健康养生，享受生命长寿。

区块链技术建立一种基于技术而不是基于约定规则的信任体系，智能合约、分布式数据库等技术特点构成的“去中心化”特点让医疗数据共享更加透明、权威和公平。充分利用区块链高可信共识、低成本安全、分布式账本和高效链接多中心的特点，采用全新的智能合约架构设计，整合先进的物联网技术，以数据交换和加快医疗健康知识流动为核心任务，创新性实现了医疗健康产业各方在不影响数据所有权的情况下实现数据的可信交换和验证，从医疗记录到医药供应链，再到用于医药费支付的智能合约，重塑严谨完善的医疗健康体系，让敏感数据在得到严格保护的情况下充分地流动起来，同时实现数据价值最大化。

健康链是在信息安全以及保密的前提下，实现业务和数据的共享，避免因数据不共享，互不信任而造成的严重经济损失的问题，从根本上解决了健康产

业行业的信任问题。可以说，区块链是具有不可篡改、去中心化、分布式账本和智能合约四大特性的，以去中心、去信任的方式集体维护一个可靠数据库的技术方案。



4.2 健康链的特点

去中心化结构消除数据孤岛，跨行业数据融合共享



1) 去中心化结构消除数据孤岛，跨行业数据融合共享。平台提供统一的数

据市场平台，打破各个行业间数据交互分享的壁垒，支撑跨行业数据应用开发的门槛。让数据易采集、易存储、易理解、易处理、有价值。针对逻辑性的信息孤岛，我们可以采用制定数据规范、定义数据标准、建设维护元数据的方式。针对物理性的信息孤岛，我们可以在合适的时机，对健康养生的主要业务流程进行整合，根据这样的流程，结合战略，把不同的业务系统串接起来，使数据相互之间形成联系。

2) 降低成本，高效物联。平台提供完善的标准体系、用户知识库以及用户、开发者社区，助力物联网生态建设。区块链可以为这个健康养生行业生态圈网络提供容纳性的、可信任的基础设施。可以降低中心化设备的运营和信用成本，提高运营效率和行业资产利用率。

3) 更为安全可靠的数据，隐私完全归属于用户。数据通过区块链的加密方式、身份验证、授权机制等技术存储于去中心化资源上，除了用户本人任何机构和个人都无法接触用户的原始数据。数据只有在用户同意授权下能够被有限地开放。在密码学的差分隐私加密下，应用可以对用户的部分数据进行大数据等研究，但无法解析个人数据，更不能查看，复制，篡改数据。

4) 智能合约让信用体系更为坚固。在平台中所有行业契约型的约定都实现智能化，利用智能合约自动执行双方所达成的契约，排除了人为的干扰因素，从制度上防止任何一方的抵赖。健康链可以保障所有约定的可靠执行，避免篡改、抵赖和违约。将社会中的有形资产转变为数字智能资产进行确权、授权和实时监控。

5) 统一正向激励参与者，共赢生态繁荣。代币体制让个体行为价值化、货币化，可以有效地激励行业发展良性循环，凡是对这个健康养生行业生态圈做

出价值贡献的任何个体行为，即使是用户自发的、自愿的和小微的行为，都可以以Token的形式价值化和货币化，被激励。也即是通过基于Token激励模型设计，可以在一个统一维度上的正向激励所有产业参与者，从而所有人通力合作共创和共赢生态繁荣。健康链不需要用户提供电子邮件，名字，或其他任何信息，为消费者提供隐私。

4.3 开启全球健康产业大数据时代

从健康数据的逻辑来讲，健康链平台可以根据人类共享的各个生命健康周期的数据，保证其数据精准的情况下，为消费者最终提供一个在区块链里模拟的个人生命健康状态和规律，并且去通过理解它的规律来做自我健康管理。通过健康链平台，将一个人的生命健康状态从生到死通过区块链技术以及分布式账本进行记录，从出生之前所作的健康检测，出生以后的生命状态，人的成长过程中所遇到的各种疾病以及死亡时间、状态、原因等都会记录在个人电子档案里，这些信息会作为数据存储健康链上，这样就使得人的生命的一生变成了数据，使得生命数字化，开启全球健康产业大数据时代。

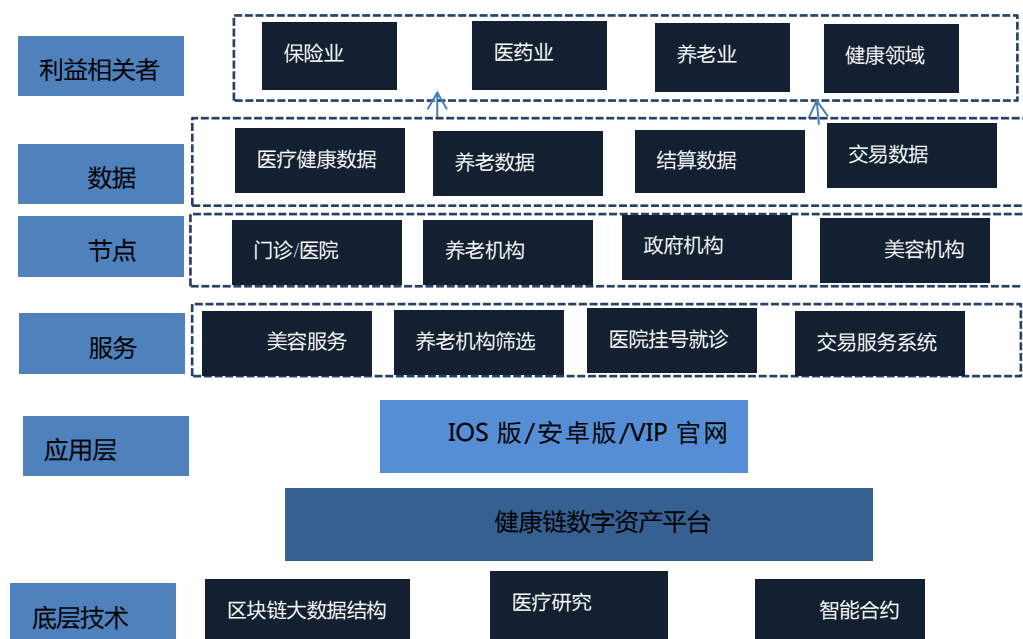
第五章 健康链整体平台架构

5.1 健康链数字资产平台

健康链数字资产平台旨在打通全球健康网络系统产业，成为数字行业价值互联网顶级去中心化公有链，搭建全球健康网络系统产业链行业底层区块链设施，让全球健康系统产业能够在健康链数字资产平台上快捷的开发自己的区块

链应用，并根据智能合约自由交换数据，利用区块链的防伪、防篡改属性来记录每一笔交易和用户点击，让所有健康系统产业行业的上下游链条实现透明、高效，让全球美容，养老，医疗，健康领域市场最大化提高效率，降低成本。

一方面，健康链数字资产平台在底层技术的支撑下开发面向用户的客户服务端，并且为了保证能够兼容各个版本，开发出 iOS 版，安卓版以及 VIP 官网服务。另一方面，吸引合作伙伴形成供应伙伴联盟进入该平台为用户提供服务，包括企业、养老机构、医院、政府机构、健康行为，实现生命一体化的系统服务，该平台主要提供美容服务、养老机构筛选、医院挂号就诊、健康行为数据、交易服务系统等，通过提供这些服务平台可以获得用户的相关数据，由于是整合性平台，对于个人来说，可以就一个人的所有轨迹形成健康征信。而对于健康领域、保险业、养老业以及医药行业等相关利益者来说，形成的医疗健康数据、养老数据、交易数据以及结算数据可以为其提供营销建议，更为综合可靠的个人信息为精准化营销做出贡献。



健康链整体系统结构

5.2 健康链运行系统

1) 生命数据模型

该生命数据模型对接各大医疗仪器厂商、医疗检查设备的厂商，让他们做一个专用的网关接口，授权给我们用户的检测信息，并且与各大医院进行对接，将用户的检测数据以及医疗记录对接到平台上，基于区块链技术的不可篡改性以及稳固性，保证了医疗数据的可靠性。

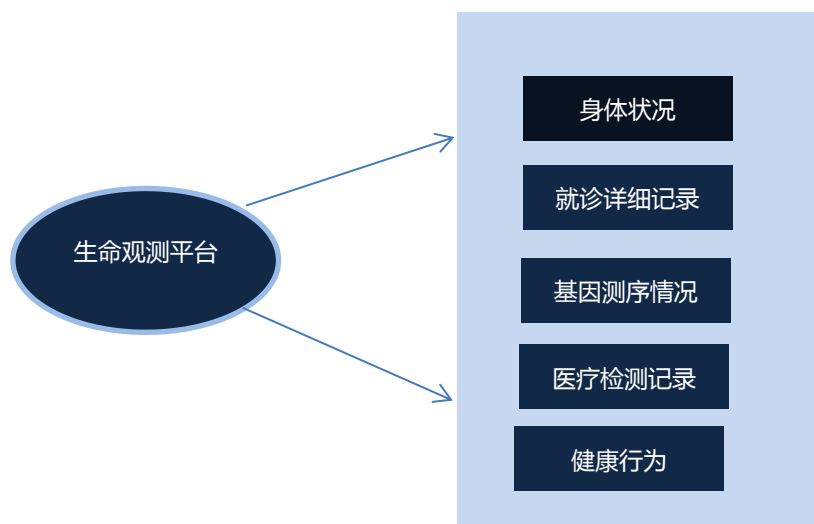
1.生态开放接口

疾病诊疗过程中形成的非病历医疗大数据，比如在 CT、MRI、血透、肾透、DSA 等检查、治疗过程中形成的相关参数，这些参数虽与人的身体健康相关，但却不为医生记入病历，仅在医疗设备中储存，不能归入病历。因此该平台对接医疗检测数据模型，该模型旨在获得在平台上的用户的医疗检测数据，一些通过医疗器械所检查出的用户的身体状况形成大数据在此模型上进行整合。

2) 生命大数据运行系统

1.用户生命观测系统

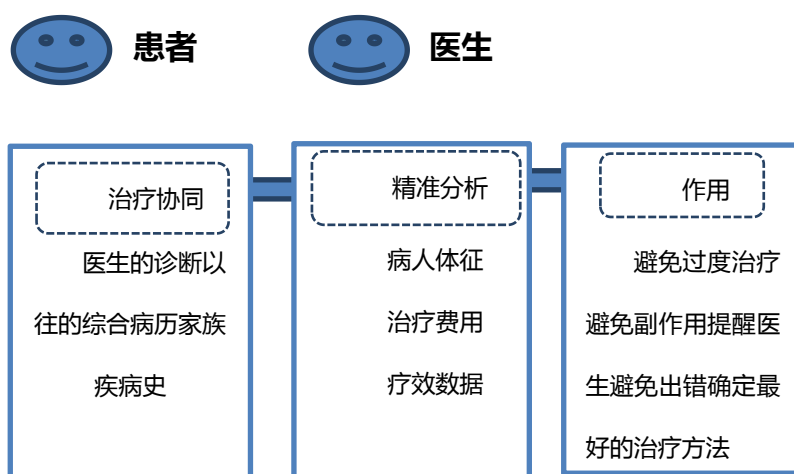
平台设置生命观测系统，通过该系统可以对用户的身体状态进行观测从而形成身体健康报告。生命观测系统主要观测用户从出生到死亡之前所有的就医记录以及身体各个指标值，通过对各个医院数据的整合可以综合观测用户的身体状况，并且对其进行分析出具健康报告。



生命观测系统

2. 治疗协同数据

通过对接治疗协同数据，可以将患者的病历以及在各大医院的就诊记录加以综合，精准地分析病人的体征、治疗费用和疗效数据，可避免过度治疗、避免副作用较为明显的治疗。并且通过进一步比较各种治疗措施的效果，医生可更好地确定临床最有效、效益最好的治疗方法。此外，通过将医生处方和医疗专家库医学指导比较，系统可提醒医生避免出错，如药品不良反应、过度使用抗生素等，帮助医生降低医疗风险。



图：治疗协同数据

第六章 健康链区块链技术应用

6.1 分布式结构

健康链的分布式控制区块头（Block header）结构如下，这一结构主要用于指定进行健康养生等服务参数列表，并内置添加用于健康链进行健康养生等服务的模型参数与更新健康链智能模型参数的功能。由于健康链支持多数据链结构，因此该控制区块头属于动态可变类型，通过内置的数据区块链健康养生等服务交易智能参数指示数量，健康养生等服务交易ChainNumber 来确认区块大小。

Bit 位宽	字段定义	字段说明
32	nVersion	健康链版本号
256	HashPrevBlock	前一个区块头的 Hash 值，目前基于 RNN 算法得到。
32	AIChainNumber	本区块包含的区块链数量，该数量将指定本区块头中包含有多少个区块链 AI 参数列表组。在健康链仅设定一条数据区块链时，AIChainNumber 为 1。当数据区块链包含多条时，则 AIChainNumber 设定为当前准备更新的参数链大小。因此区块头大小是动态可变的。从维护和实现角度，目前建议单个区块头中 AIChainNumber 不大于16。

32* AIChainNumber	AIChainSN[AIChainNumber]	用于指示后面对应的 AI 参数作用于哪一个数据链编号。目前存在 AIChainNumber 条需要指示的数据链
256* AIChainNumber	HashSystemAIParameterList [AIChainNumber]	用于指示对应数据链编号对应的本次标准 AI 参数更新列表 Hash 值
256* AIChainNumber	HashSystemTransModelList [AIChainNumber]	用于指示对应数据链编号对应的本次新增 AI 交易模型列表 Hash 值
256* AIChainNumber	HashUserAIParameterList [AIChainNumber]	用于指示对应数据链编号对应的新增用户定义 AI 参数列表 Hash 值
256* AIChainNumber	HashUserTransModelList [AIChainNumber]	用于指示对应数据链编号对应的新增用户定义 AI 交易模型列表 Hash 值
256	nNonce	随机数，健康链是 32 位，健康链为 256 位，用于保证整个区块满足 RNN 算法校验
32	nTime	更新时间，32 位
32	nBits	当前运算难度，32 位

参数的详细说明如下：

- nVersion，区块版本号，升级时改变。
- AIParameterVersion，本次区块定义的 AI 参数版本号，若当前没有更新系统 AI 参数或新增系统交易模型，则参数版本不变化。
- hashPrevBlock，从前一区块获得。

- AIChainNumber，数据区块链 AI 参数指示数量。
- HashSystemAIParameterList，本字段包含当前区块 AI 参数列表的 Merkle 树计算。通过该字段列表能够调整后续数据区块的字段配置与参数配置，是本区块链能够自主进化的典型标志。
- HashSystemTransModelList，本字段包含当前区块系统交易模型列表的 Merkle 树计算。通过该字段列表能够不断丰富系统的交易模型，并能完成各种交易缺陷弥补。
- HashUserAIParameterList，本字段包含当前区块用户进行健康养生等服务参数列表的 Merkle 树计算。通过该字段列表，单个用户能够自定义交易的进行健康养生等服务参数配置，从而保障用户交易的安全可靠性。此外，用户也可以通过该字段上报自身的能力，方便 AI 服务或其它节点调用。
- HashUserTransModelList，本字段包含当前区块用户自定义交易模型列表的 Merkle 树计算。通过该字段列表，单个用户能够发布自身的健康养生交易服务模型，并通过 AI 控制链发布，从而实现付费购买健康链其余用户的健康养生交易服务算力，或有偿开放自身业务服务算力。
- nNonce，健康链提供了 256 种可能取值，而健康链提供 232 种。
- nBits，由全网算力以及分配给 AI 的服务算力计算获得。目前，由 AI 参数决定如何动态调整难度，最小调整间隔为 16 个区块 1 次，最大为 2048 个区块调整一次。（健康链每 2016 个区块调整，以太坊每个区块调整一次）。
- nTime，基本取机器当前时间轴。

由于健康养生交易服务参数的重要性，系统通常需要最大限度的包含系统健康养生交易服务参数列表、系统健康养生交易服务交易模型列表、用户自定义健康养生交易服务参数列表、用户自定义交易模型列表，如果不能包含，则按照上述顺序，进行优先级排列。对于列表内部，系统则可以自由选择排布，并删减部分内容，从而形成最终的控制区块。

控制区块的头的构造过程如下：

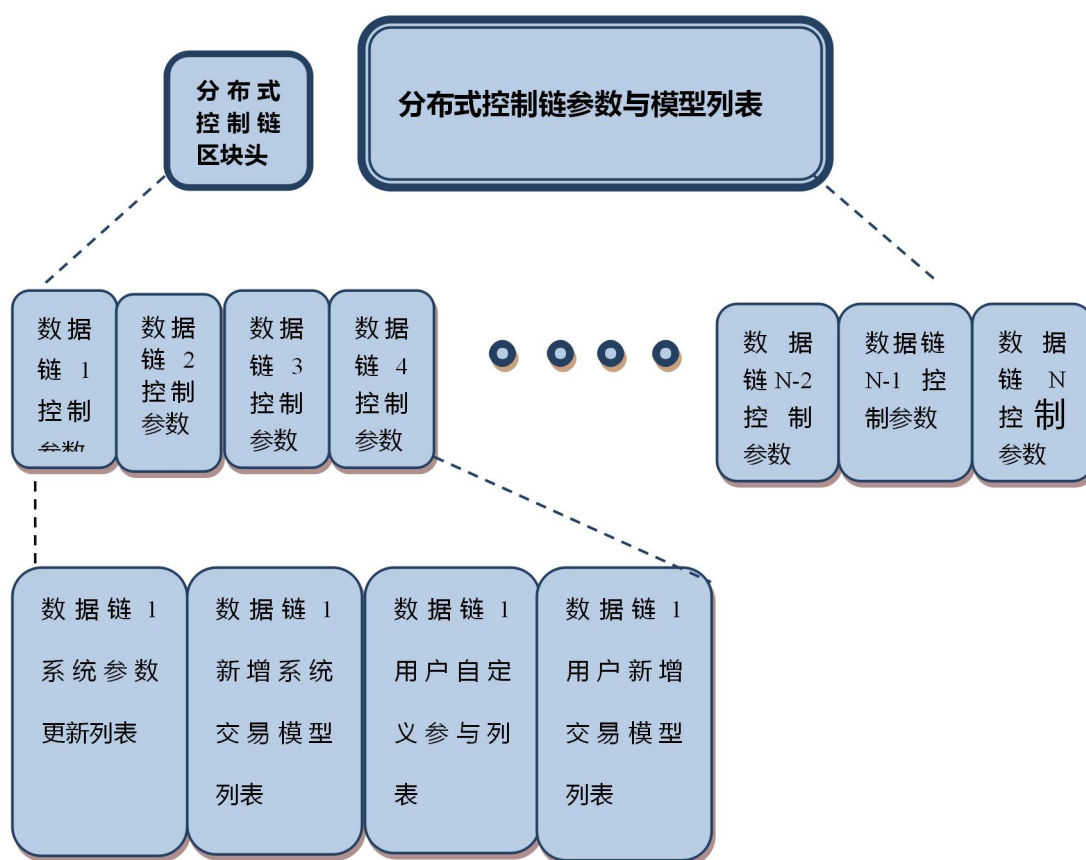
（1）选择待确认各个健康养生交易服务参数列表，因为系统可以从交易中获得手续费，所以一般构建区块时会选择尽可能多的交易，但是不能超过当前控制区块设定的容量上限。

（2）确定 Coinbase，这里记录假如该区块构建成功，系统将获得的收益（手续费+奖励）。控制区块不支持幽灵协议。

（3）构造各个集合参数列表信息的 Merkle 树，然后根据 DNN 算法生成随机数 nNonce，写入其他参数。

（4）最终构造健康链控制区块头。

6.2 数据区块结构



健康链控制区块内部结构图

其中：

目前的参数配置方式如下：**Data Chain Parameter_list = [Data ChAI
AInParameter 1,Data ChAIParameter 2,...]**

而对应的每条数据链的参数配置，则采用如下方式定义：**Data ChAIParameter=[System AInParameter List System TransModel List User
AI Parameter List User TransModel List]**

另外，考虑减少数据链的参数解析运算量，在更短时间内达成共识，安全性更有保障，健康链将周期性的提供每一条数据链的完整参数，并设定对应的标志。

6.3 共识机制

区块链的价值锚点在于链条自身的消耗与产出。当区块链选择 PoW 作为共识机制时，每一次区块的生成消耗的算力都将成为其价值的基石。另外，在健康链上，每个节点都具备解决现实中健康养生交易问题的能力。如果健康链上的节点能够参与实际问题的解算，整个区块链就具备了现实的产出价值。因此，为保证区块链自身价值最大化，健康链控制链与每一条数据链将默认选择基于 PoW 的共识机制。

但由于 PoW 容易产生分叉，需要等待多个确认等显性缺陷，因此在健康链中，除初始的数据链与控制链强制采用 PoW 外，后续的数据链，其共识机制将被设计成模块化的，可以通过控制链参数进行配置，能够动态适用公链和私链的不同应用场景。目前，健康链对后续数据链共识机制，支持 POW、DPOS、BFT 等。

健康链的健康养生交易等服务优化系统将针对数据链本身的应用场景和交易情况，选择合适的共识机制，确保各个分布式节点通过算法取得数据的一致性。

6.4 安全加密算法

健康链的安全加密算法，是基于采用传统的健康链加密方式上的改进。

健康链涉及的安全加密算法及相关定义如下：

对称加密：对称加密是最快速、最简单的一种加密方式，加密（ encryption ）与解密（ decryption ）用的是同样的密钥（ secret key ）。对称加密通常使用的是相对较小的密钥，一般小于 256 bit。密钥的大小既要照顾到安全性，也要照顾到效率，是一个trade-off。

非对称加密：非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，公钥（ public key ）和私钥（ private key ）。私钥只能由一方安全保管，不能外泄，而公钥则可以发给任何请求它的人。非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。

私钥（ private key ）：非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

公钥（ public key ）：可公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，目前常用的方案包括：secp256r1（国际通用标准）、secp256k1（健康链标准）和 SM2（中国国标）。健康链控制链与初始数据链选择 secp256r1 作为密钥方案。

Hash 算法：通常 Hash 算法是指安全散列算法 SHA（Secure Hash Algorithm），该算法是美国国家安全局（NSA）设计，美国国家标准与技术研究院（NIST）发布的一系列密码散列函数，包括SHA-1、SHA-224、SHA-256、SHA-384和SHA-512等变体。目前健康链采用SHA-256 算法。健康链除 PoW 外，其余 Hash 算法均指SHA-256。

6.5 智能合约协议

智能合约是区块链 3.0 产品，通过三个主要步骤，建立智能合约交易机制，实现从制定到自动执行全过程：

（1）多方用户共同参与制定一份智能合约。多方用户根据需要共同商定一份承诺，包含了双方的权利和义务；承诺进行数字化处理，用户获得区块链给予的一对公钥和私钥，公钥是用户在区块链上的账户地址，私钥是操作该账户的唯一钥匙。用户用私钥签名，可保证合约有效性。

（2）合约通过 P2P 网络扩散并存入区块链。区块链是 P2P 的端对端网络，合约通过 P2P 方式在区块链全网中扩散，每个用户都会收到一份合约。区块链中会将收到的合约暂时保存，经过共识时间的多轮发送和比较验证，最终达成一致的合约集合，以区块的形式扩散到全网。

（3）区块链构建的智能合约自动执行。区块链自带的共识算法将构建出一套状态机系统，智能合约会定期检查状态机状态，将条件满足的事务推送到待验证的队列中，等待共识；验证通过的事务会进入待共识集合，等大多数验证节点达成共识后，事务会成功执行并通知用户。

智能合约应用于实际交易具有以下优点：

（1）自动化执行，提高交易效率。智能合约由代码定义，同时也由代码执行，完全自动且无法干预。当一些预设的条件发生时，智能合约就一定会按照预先设定的代码来执行，对区块链上的各种数字资产进行复杂的操作，从而自动完成智能合约的内容。合约约定的行为无需透过人的控制执行，而是仅通过计算机自动执行，可以避免各种因人为因素而起的纠纷，也比人来执行合约内容更有效率。

(2) 智能合约是否执行不再依赖于交易双方的一致信任，而是抛开参与方信任的前提，仅依靠代码强制执行即可。如果当交易双方中有任何一方没有按照协议的合约条款来执行，那么就不会触发合约自动执行，从而使得遵循协议的另一方的权益得到应有的保护。最小化信任能够让事情变得更加便捷，因为通过全自动执行来替代人的判断和执行。



健康链智能合约协议执行

6.6 去中心化自治

区块链技术建立一种基于技术而不是基于约定规则的信任体系，智能合约、分布式数据库等技术特点构成的“去中心化”特点让消费大数据的使用通过加密算法确保安全，并且将每一次交易记录都完整记录，形成使用轨迹。

6.7 可追溯性

健康链就是利用区块链独特的不可篡改的分布式账本记录特性，构建正品溯源服务系统，实现商品生产、入库、出库、门店、上架盘点、销售、用户购买、售后服务等流程区块链化，实现用户、店家、合作伙伴、第三方、政府等相关方的共赢利益，保证项目管理的有效性、可持续性和安全性。健康链通过对应的 DAPP 应用来解决企业在商品生产、流转、分销、终端消费过程中的信息溯源、防伪鉴真、精准营销难题，为品牌企业和消费者解决“可信任”的难题。在健康链上，用户可通过健康链的查询服务平台作为入口进行溯源查询，因为产品的所有者在我们平台上都是有记录的，用户只需要在平台上输入产品信息和生产商或者分销商的名字便可以查询，追踪到商品的生产、储存、出仓等信息。

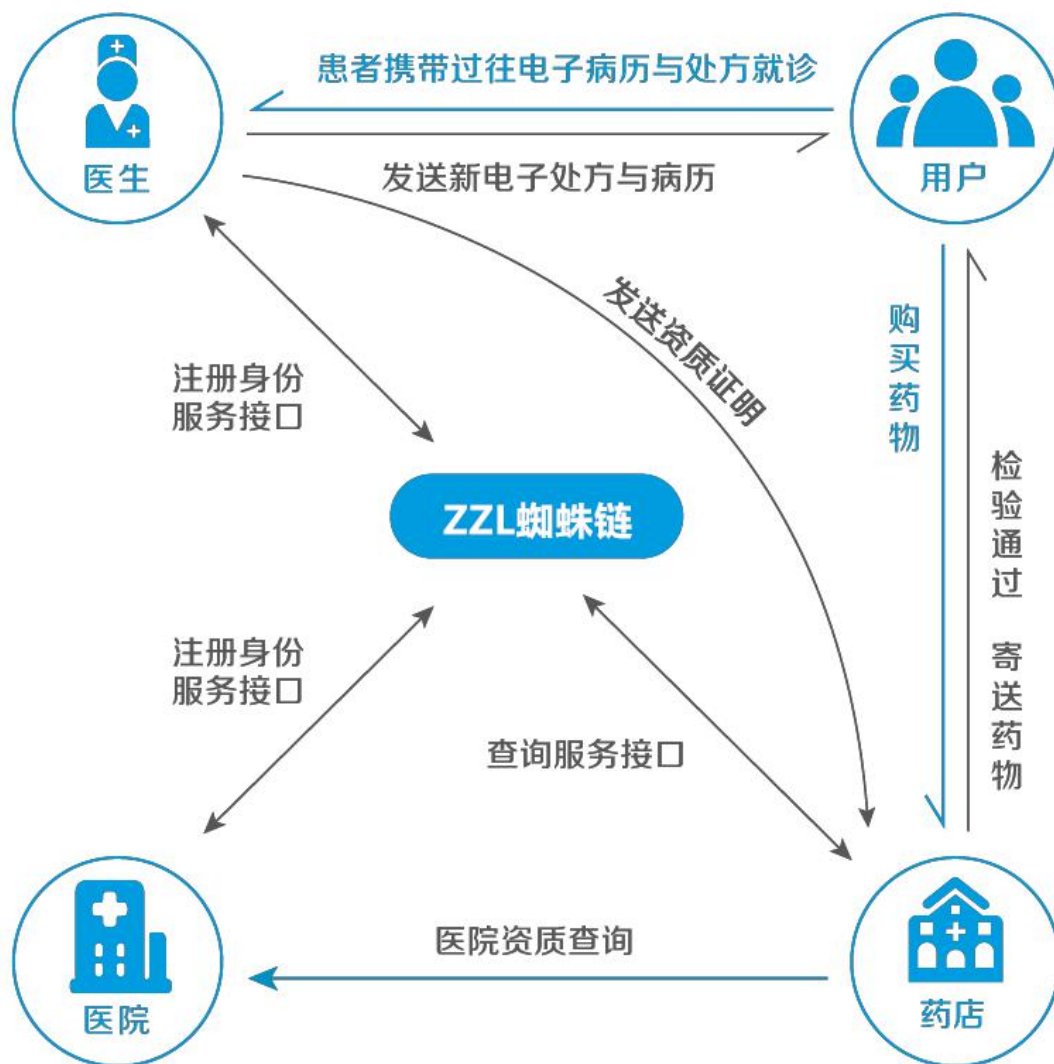
6.8 不可篡改

健康链利用区块链的不可篡改机制，采用了带有时间戳的链式区块结构存储数据，为数据的记录增加了时间维度，具有可验证性和可追溯性。当改变其中一个区块中的任何一个信息，都会导致从该区块往后所有区块数据的内容修改，从而极大增加数据篡改的难度。

第七章 健康链未来应用价值分析

7.1 健康链主要应用场景

➤ 个人医疗数据体系



当医院、药店、医生、用户都在区块链上注册身份后，云医链作为关键信息的存储和中转平台，解决了多方之间的信任问题。医生通过用户授权对其过往电子病历和处方进行查询与溯源，可为用户提供更优质的医疗服务。药店通过云医链查询医院资质，确认医生处方，就可将处方药卖给用户。健康链实时

追踪和记录患者个人的病例、患病情况、拿药记录等情况，形成患者个人的医疗数据体系。

➤ 医疗信用体系

健康链利用区块链的可追踪、可追溯的特性，对药品进行防伪查询，杜绝了假冒伪劣药品，为医疗健康供应链增加信用保障，并深层次挖掘信息价值。

➤ 健康养生管理

（1）养生餐厅

健康链提供的健康养生管理是全方位的，俗话说病从口入，同样的病除也是从口入，养生餐厅便是健康链提供服务的一种养生方法，各种养生餐厅可加盟健康链，养生餐厅作为一种全新的主题餐厅，采用非常生态的环境来打造，食物、烹饪方式、进食方式都以健康、绿色为主。目前的养生餐厅种类繁多，比如轻食餐厅、五谷餐厅、素食餐厅、养生粥餐厅、中医药膳餐厅等。

（2）养生会所

养生会所是为人们提供经络养生、经道养生健康保养、香熏 SPA、美容美体、驭经之术、按摩养生，中医预防养生，减压放松等服务项目的休闲养生场所。

（3）养生运动

健康链提供的养生运动，运动是形式，养生是目的。几乎所有的运动形式都能达到养生健身的效果，而健身方式也是多种多样，健身房、舞蹈室、瑜伽馆、攀岩馆、射击馆、真冰馆、卡丁车馆、风洞馆、击剑馆、保龄球馆、潜水馆……任何一种运动形式，都能独立出来作为单一场馆，这些都是受到 80 后、90 后喜爱的运动方式。

➤ 健康食品、用品

健康链在后期的发展建立健康食品、用品商城，在商城里，健康食品、用品的厂家、供应商可在商城入驻，并针对每个季节搭配不同的健康养生的食谱推出给用户参考，给用户一个全方位的养生方式。

健康养生的产业链很长，在医药、养老、体育、美容、旅游、地产等领域都有发展空间，上述所述仅是一小部分。

7.2 健康链项目未来价值分析

健康链能够提供一个去中心化的、权威的健康行业信息分享和管理平台，让整个健康服务行业更加规范。健康链致力于为用户提供一站式的新生态全球化健康生态圈，致力于打造安全、可靠、快捷、贴心的区块链健康养生服务生态圈。健康链不但为消费者构建了点对点支付、商品追溯的生态平台，从而减少了假冒伪劣健康养生产品，同时，健康链通过构建基于技术的信任体系，有助于加强行业监管，助力健康养生行业的健康发展。另一方面，健康链开启全球化健康养生数字经济时代，实现线上与线下的互通，促进健康养生行业的发展。打造成公众信任的健康养生消费交易支付真伪辨识系统和安全支付体系，形成商品根源信息大数据平台，有利于进一步完善物联网技术，提升数据采集和分析能力。

第八章 健康链发展规划

8.1 初期规划

通过前期会议、展览、政府介入等渠道，吸引、接触更多的传媒企业和有需求的企业深入了解健康链，并开展试点合作等。达成合作后和合作伙伴之间基于公共云平台的信息共享，为其提供基于精准的目标客户关系推送智能服务。有稳定的客户后，可以推广发展更多的客户，并定期做市场调研，通过公司官网和大数据平台开展业务。

8.2 中期规划

项目发展到中期，已有稳定客户，同样通过官网和健康链平台，保持与老客户紧密联系。进一步拓展业务，在官网和健康链平台建立数据加工中心，除了服务于现有客户，吸引更多相关行业客户，为更多行业提供服务。后期可参与面向市场的融合创新智能研发设计。与此同时，随着计算机技术的成熟，建立多领域产品数据模型，使个性化的订制越来越简单。中期将在初期已有的市场上进一步拓展，通过官网和健康链平台以及合作企业合作链接渠道等进入市场。

8.3 未来规划

项目发展到后期，总体运营趋于成熟，未来设备数据量势必空前巨大，建立标准化数据工厂，为客户提供更优质的服务，业务再拓展。此外，基于以市场链为纽带的供应链优化、用户精准识别的智能营销模式来打造新的商业模

式。前中期的积累和业务的拓展，将使健康链平台在行内具有一定品牌影响力，进入市场更容易。

第九章 健康链盈利模式

9.1 经营盈利

健康链发行以后，所有在以区块链技术上的经营活动，经营主体均要消耗数字资产来支撑平台节点运作。使用数字资产的组织或个人都需要以挖矿或买币的形式得到数字资产。

服务盈利主要从三个途径获得：

1) 第三方应用平台要加入健康链一站式健康服务平台，要收取一定的加盟费，必然消耗一定的数字资产；同时第三方应用平台无论是读链还是写链，都要消耗数字资产。

2) 第三方应用平台如果要获得本平台的用户的数据，必须要消耗一定量的数字资产。

3) 当用户在一站式健康服务平台上使用第三方应用平台获取信息产生行为数据，而健康链一站式健康服务平台会为用户的贡献付出数字资产。并且如果用户需要使用交易系统提供的增值服务比如加入会员等也需要消耗一定的数字资产。当有更多的用户使用一站式健康服务平台中的第三方应用则可以推动数字资产价格上涨时，平台将会获得更多的盈利增值。

9.2 交易盈利

交易盈利是健康链一项主要盈利来源。健康链上线以后，交易的各方参与者将会进行各种交易，在交易过程中，会产生一定的盈利，这个盈利来自于健康链交易过程产生的手续费。每笔交易都被赋予了一个优先级，由“输入”的历史时间、金额和笔数来决定。手续费多的交易请求会被优先处理。

第十章 运营团队介绍

10.1 团队成员

健康链的团队，来自中国、美国、日本、台湾，具有丰富的区块链、软件、医疗、健康管理、媒体和广告等行业的优秀人才，技术功底深厚、对未来各个行业的落地有着深刻的理解和广泛的资源，是健康链未来落地有力保障。

10.2 专家顾问

健康链专家顾问团具有丰富经验的区块链高级技术人才、全球顶尖专业的律师、健康管理专家、管理英才、商业顾问具有庞大行业顶尖的专家和顾问。

第十一章 发行计划

11.1 发行方案

(1) 项目名称：健康链

代币简称：HTC

(2) HTC 总量：100 亿枚

(3) 市值管理：200 亿—3000 亿

(4) 钱包机制：累积、复利计算、持币分红

(5) 发行周期：一周

11.2 发行细则

健康链代币发行细则如下：

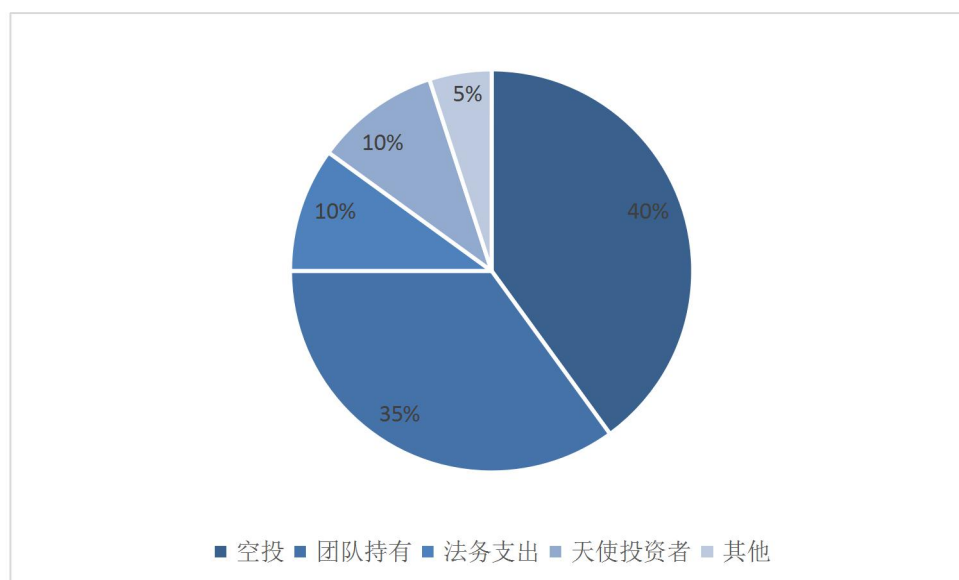
40%空投（通过注册赠送方式空投）；

35%团队持有锁仓 24 个月（其中包含开发费用）；

10%法务支出；

10%天使投资者；

5%其他。



第十二章 风险提示

12.1 政策性风险

目前虽然政府对区块链相关产业态度明朗并持积极鼓励政策，但公有区块链天生的去中心化属性在与现有的中心化政府的法律法规下依然面临政府政策层面的很多不稳定性。针对政策性风险将会采取如下措施：

在团队单独设立公共关系部门，积极与政府及业内从业人员保持沟通协作，在法律框架下设计数字资产发行 / 交易 / 区块链金融 / 区块链应用等方面业务。项目运营不涉及法定货币交易，但并不干涉第三方交易所开展交易业务，我们只专注技术。

12.2 市场风险

我们的终极目标是实现区块链技术真实落地应用，然而区块链产业刚刚兴起，项目的未来会面临各种各样的市场考验。针对市场风险运营团队采取的应对

方式为：

运营团队将定期的参与业内会议，并定期或不定期举行项目进展与发布会，与相关开发者沟通与交流目前的市场需求与前景预测，确保项目能够回应社区与市场的声音。

12.3 技术风险

我们要建联盟链的新技术标准，这其中的技术开发难度是非常巨大的，这

对于顶尖技术人才的需求以及科研的投入力度要求都是非常高的，如果把控不好，会影响项目进度甚至最终导致项目的失败。针对技术风险运营团队采取的应对式为：

紧紧依托国内外顶尖著名高校与区块链社区，与顶尖高校共建区块链技术创新实验室。基金会定期拨款，支持社区建设并与其他区块链社区开展深度合作，确保项目的技术风险可控。

12.4 资金风险

资金风险是指项目资金出现重大损失，例如：资金被盗，在预定时间内因为人员与资金问题无法完成开发进度等等问题。针对资金风险运营团队采取的避险方式为：

所有大额数字货币存储采取多重签名钱包+冷存储方式由基金会理事共同掌管。在 3/5 多重签名方式下，可以有效降低资金被盗以及被私自挪用风险。

第十三章 免责声明

该文档只用于传达信息之途，并不构成本项目买卖的相关意见。以上信息或分析不构成投资决策。本文档不构成任何投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖的行为，也不是任何形式上的合约或者承诺。

相关意向用户明确了解本项目的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。运营团队不承担任何参与本项目造成的直接或间接的损失。