



GenkiCell

可信大健康数据价值生态系统

www.Genkicell.io

目录

摘要	4
第一章 背景简介	5
1.1 世界大健康市场规模	5
1.2 大健康产业瓶颈概述	5
1.3 大健康产业机遇	8
1.4 Genkicell 的定义与愿景	13
第二章 应用理论	16
第三章 去中心化大健康技术生态	18
3.1 链上系统设计理念	18
3.2 技术生态架构	19
3.3 IPFS 大数据挂载	20
3.4 共识机制	21
3.5 智能合约	28
3.6 业务流程	28
第四章 区块链技术及通证生态	38
4.1 通证模型	39
4.2 基于 Genkicell 开发的生态产品	40
第五章 应用场景	42
5.1 数据授权	42
5.2 大健康服务	42
5.3 全球诊断	43
5.4 医疗保险	44



5.5 PHR.....	45
5.6 其他应用场景	46
第六章 总结	48
第七章 团队及顾问人士	49
第八章 GCL 分配细则	53
第九章 里程碑计划	55
第十章 免责声明	56
十一章 风险提示	57
参考文献	60



摘要

通常意义上，大健康是根据社会需求与疾病谱之改变，随着时代的发展进步，而提出的一种全局理念。其围绕着人类的生产生活场景，关注各类可能影响人类健康的危险因素和误区。同时也将健康的管理模式从现有的已病-治疗的模式逐渐引向至自诊断-预防的新自健康管理模式。其概念范畴内涉及与健康相关的概念也十分广泛，包含大数据、物联网、传感器、人工智能以及各类组织为了满足社会的健康需求所采取的行动等。我们一直致力并深耕于将这些技术和行动通过区块链这一核心技术串联起来，以物联网终端进行数据采集、到数据分类标记与数据可信化，再到数据价值变现与应用。大健康数据来源是极为广泛，但在我们在实际生产与服务过程当中，经常面对如何有效过滤非有效数据并使之标准化，如何调用敏感数据；如何能使大健康资源更合理分配，如何让研究及商业机构减少数据获得成本，以及如何让用户获得自我健康管理的最大便利。是否有一种足够革命性方法彻底解决问题痛点或者说提高大健康产业链中参与者的收益呢？

因此 Genkicell 应运而生，Genkicell 是全球性的，由区块链驱动的可信大健康数据价值生态系统。平台完全开放给所有大健康数据生态与相关物联网终端及传感器使用者，通过利用区块链技术，保护数据隐私的同时，奖励每位参与数据可信化过程的用户，而需求数据的用户则付出奖励，为每位参与者实现最大收益。



第一章 背景简介

1.1 世界大健康市场规模

作为全球最大的新兴产业，大健康产业仅在 2014 年就已经超过七万亿美元，其中美国约有三万亿美元，日本约五千亿美元（世界银行、WHO，2015），中国约六千亿美元（中国卫计委，2017）。这一数字在不断增长的同时，在消费比例上来看，各国在医院大健康费用支出上比例惊人(世界银行、WHO，2015)，同时在总体社会支出的占比也极为庞大，大健康支出费用极为高昂。根据美国医学研究院（Institute of Medicine, IOM）的一篇报告，如今大健康支出的 1/3 被浪费而没有被用于改善大健康。这些浪费包括不必要的服务、行政浪费、昂贵的大健康费用、大健康欺诈和错失预防的机会（IOM，2012）。可见大量社会人群在可能存在的医学知识缺乏或是大健康体系不了解的情况下，盲目的寻求大健康服务，在此过程当中占用大量大健康资源，或是遭遇欺诈，更严重的遭遇不匹配的大健康水平服务导致健康状况恶化，从而形成大健康资源不平衡。除此之外，我们也在关注着各国都在不断的进行大健康实验性改革，如英国的 NHS 体系，日本国民健康保险体系，或者中国的新医改政策，无一例外的都包含分级诊疗，医药分离等特点，以期达到大健康体系健全的目的。

1.2 大健康产业瓶颈概述

从我们可见可认知的物联网设备数据库到不可见的健康档案、公共卫生数据等，由于存在机构组织间的信任问题，极大的影响了数据的流转，以至于每一个数据库都形成相应的数据孤岛；同时，其所包含海量的、时间维度长的、非标准化的、复杂结构数据在实际应用上难以真正发挥作用。



1.2.1 非可靠的自诊断数据收集来源

通常情况下，我们不认同非专业用户通过自我感知对健康状况进行判断，无论是从医学知识储备还是从面对问题经验性而言。而想要培养人群对于医学的认知还是训练 AI 辅助人群认知都必须有较为严谨的数据采集源头，否则将会影响各类别数据与病征的关联性。

我们结合现有业务并在实践中总结性的认为，物联网终端及传感器是原始可信数据最优来源之一。由于每个人在基因、生活方式、身体特征等各项细节上不同。即使同一血压、血糖数据也未必含义相同。收集多态性、时效性的细节数据有助于优化整体体征数据。健康检测终端提供非聚集的体征信息，而其他智能设备则提供聚集化的信息可以更容易地提供准确、一致性的个人健康信息。

1.2.2 数据流转过程中的信任问题

在健康大数据背景下，将数据逐渐形成共享与开放的生态系统是建设大健康信息化并打破数据孤岛的基础。大健康数据将随着技术的发展变的日趋活跃，数据互操作形成的数据流转将更为频繁，在此过程中数据价值将逐渐被挖掘并应用改善目前的健康服务，如，分级诊疗，大健康管理，远程医疗，认知诊断辅助系统，药物副作用研究等，同时随着这些产业的发展，也必将产生对数据有序流转，安全分享，合理使用等迫切需求。

然而在数据的流转过程中，数据隐私问题，数据可信与完整性问题将尤为重要。在健康服务系统中，个体更加注重数据的隐私泄漏问题，然而对于机构与部门来说，数据的完整性，真实性，可信性，安全性变得极为重要。

然而区块链数据不可回滚的特性，将保证链上数据的不可修改。区块链的匿名性将保证数据的隐私，个体对数据泄漏暴露隐私的担忧。同时 Genkicell 依靠数据的分布式储存，和链上数据处理过程中的确权使用，则能达到数据真实完整。



1.2.3 海量复杂数据处理困难

通常情况下，社会群体数据分布在各个机构组织中，包含着数字信息和影像信息等各类大健康信息。而信息产生速度更是与日俱增，即使通过算法筛选大量碎片化信息，数据依旧是原始的、缺乏验证的、非标准化的，而真到了到用时，对个人还是区域层面而言，时间不够，信息复杂，只能将数据束之高阁。

因此，我们通过区块链技术在海量判断节点中通过日常分布式标准化判断进行数据标记分类 EMR 与 PHR 数据，筛选并优化数据，使得数据结构符合 EHR 适用标准，不断完善特征库。并在数据流转过程中，由生态体系进行自主筛选，逐渐舍弃可信度低与完整性低的数据，从而在数据变现使用中，在有效数据中减少初筛的各类成本，降低数据使用成本，用户与节点同时都能获得被使用收益，实现链内价值共享。

1.2.4 身份信息不通用及数据不连贯、非标准化

大健康服务提供者所带来的数据来源极多，即使是医院使用的 HIS 系统，都有数十套完全不同标准的格式。而跨地域、跨行业、跨层级的实际现象中，机构间的信任问题导致其数据流转性丧失、完整性缺失与连贯性断裂，故而目前大健康数据产业是由一个个中心化流转性差的数据孤岛组成，而最终受害的是用户群体。

区块链技术颠覆性的改变了这一问题，其分布式记录、不可篡改、共识机制等技术特性在不侵犯各方利益的基础上，实现数据互操作性、可调用性、标准化，完善了数据的连贯性。

1.2.5 敏感数据使用及隐私

对于个体而言，由于大健康数据的自有特性导致数据本身存在着高度敏感性。现有中心化的储存模式下，数据操作性、确权使用、隐私保护、数据安全等均无法做到切实保障。



这些情况造成的后果是可预计而又十分严重的。与此同时，各类企业机构自身在一定数据保有量的情况下进行研发、商业化推进等行为会产生出大量处理后的价值数据，这些数据对其他机构同样具有价值性，但又十分敏感。

在用户隐私保护方面，我们使用 IPFS 文件存储系统来对于用户数据的挂载的存储提供一层 Hash 加密，在记录区块信息的时候我们将采用一层额外的哈希加密方法来加密链上索引数据，从而保证了大健康数据的隐私绝对安全。

1.3 大健康产业机遇

1.3.1 人口老龄化带来的慢性疾病问题

人口老龄化是各国面临的普遍问题，由此带来的慢病管理与养老问题正成为愈加棘手的问题。随着年龄的增长而导致机能退化，慢病的控制愈加困难。而实际情况是，并没有足够多的人力资源能够承担这部分日常的护理需求。由于经济成本等问题，这一矛盾，十分难以缓解。

我们设想以智能物联网设备作为健康管理助手来缓解这一矛盾，将日常轻服务通过人工智能来提供认知辅助、风险预警等功能来完成。同时实现大健康提供者一对多的服务模式。通过区块链技术为技术底层，大数据作为 AI 训练基础，在区域用户的小数据基础上，精确的为老龄用户做出风险预警与诸多个人服务。

1.3.2 反医疗欺诈与追踪药品使用风险

全球的医疗资源分配不均衡是公认的。由于信息不对称而导致找不到合适的资源以及错误信息误导引起的健康问题比比皆是。而且，通过网络寻找健康服务提供者的信息不仅不全面甚至具有一定倾向性。同时，患者与健康服务提供商之间即便存在互评机制，双方往往都得不到对方公平的评价，故评价不具备参考价值。

而区块链所含的透明性、不可更改的技术特点使得每一个评价有所依据，有所分量，也为更多的患者提供了参考依据。确保能够获得更匹配的健康资源并避开劣



质资源，净化大健康服务体系。

每年，医院及其他医疗服务机构，处理的处方数量以千万计。在庞大的使用群体面前，医疗工作者很难做到精准开药及后期跟踪。面对可能发生的药品使用风险，如：药物高度依赖、药物过敏、药物副作用、用药剂量等问题。在现有的医疗机制下无法做到精准药品使用，对于医疗服务受众者而言，无疑是具有较大风险的。

通过区块链可将药品购买者的购买行为记录、社会心理信息、药品服用后的指标参数等其他可揭示药品使用者在使用某款药品的风险信息。归集并通过对大数据的高性能精细化分析，有效分析每位使用者的情况，帮助使用者更安全的使用药物，减少不必要的医疗开支。

1.3.3 大健康数据安全挑战

因为大健康行业中数据安全性与隐私性的需求，所以其有着严格的合规政策和监管，然而网络安全威胁逐年增加从而为医疗行业带了新的挑战。以至于目前的大健康数字化进程进入了两难的困境。目前的医疗系统、制药商、设备制造商都有着迫切的需求——安全可信赖的互联大健康 IT 生态，用于高效的管理各项大健康数据，从而推进真正意义上基于价值的服务。

2017 年 IBM Security 和 Ponemon Institute 研究发现，医疗卫生机构的数据泄露成本增加了，大约是每份病例 380 美元，而其他行业的相应成本却下降了 10%。因此网络安全已经成为医疗设备和技术公司的困扰。最近美国食品药品监督管理局（FDA）发布了 St. Jude Medical 心脏辅助装置的网络安全漏洞。随着可穿戴设备的进步与互联网医疗设备的发展，无论设备是否联网，医疗物联网设备遭到攻击的可能性逐渐引起了一些老设备原始设备制造商（OEM）的重视。

与传统中心化的系统不同的是，区块链构建的分布式网络共识体系中，利用加密技术和区块链的设计结构保证所有数据事件的记录不可篡改，利用分布式系统的优势大大提高了网络安全性。区块链技术的特性同时可以提供额外的信用层，将传统 HIT 系统，互连医疗设备和嵌入式 IT 系统的网络安全威胁最小化。这一项新



的区块链技术让医疗系统，医疗设备 OEM，医疗卫生技术公司可以增加可靠安全的设备身份管理战略，推广医疗物联网（IoMT，Internet of Medical Things）去中心化应用程序（Dapp），保证用户隐私，同时保证所有访问由用户授权下的行为。

1.3.4 医疗数据交换和可互操作性

目前医疗行业数字化趋势不断增长，其目的在于实现更高效的健康数据的互操作性，以便于各机构间的相互协作。然而互操作性的基础在于机构间的相互信任、共担责任、共享信息，而不是仅在于数据本身间的信息交换。可见机构间的去信任化，透明化，明确信息价值，实现对等与高效的数据流转是当下的主要问题。因此大健康产业中数据的互操作性的真正挑战应更着重于基础层面，是解决在缺乏受信框架的基础上与现有 HIT 系统的整体性间如何做到数据的互操作问题。因此 EMR / EHR 系统与数字化健康解决方案的应用不断增多，但是缺乏受信任的数字化工作流程带来了各种不同的 HIT 系统和中心化医疗数据管理模式。

目前缺乏受信任的数字化流程已经成为了新解决方案部署的重要一环，例如以区块链技术带来的可互操作性的方案实施可能。依赖于区块链本身独有的不可篡改的受信任工作流程，数据交换的完整性可由单一的信任来源来保证，同时减少网络安全隐患，并有效提高数据管理程序可靠性。由现有 HIT 基础上部署相应区块链技术作为额外的信任与安全层，从而建立一个去中心化的信息共享平台，保证数据流转时的访问控制、真实性和完整性，同时通过替代目前健康医疗系统中数据交换中受托于管理员或注册表所有者达到减少行政抵低效性的问题。同时随着物联网健康设备的发展，基于区块链技术架构的医疗大数据生态将可做到健康普适计算，从而给予个体可以在任何时间、地点，获取和处理任何健康信息的服务。



1.3.5 医疗卫生消费主义和健康自我量化需求

随着数字化的医疗健康服务于可穿戴设备的不断发展和进步，大量的个性化医疗和生活方式的数据被大量创造出来，飙升了随着技术进步医疗卫生消费主义逐渐被接受。目前不管是健康服务的消费者或是健康服务提供者，都想积极的参与到不同水平的健康服务之中。大约有近 69% 的美国消费者有追踪自己健康状况的行为，同时有研究标明有 74% 的消费者希望获得定制化的健康服务和后续的保健服务。此外 41% 的患者表示，如果无法访问自己的医疗记录，会选择更换自己的医师。然而传统的中心化健康服务平台导致的数据所有权、可信流转、隐私安全等问题阻碍了健康量化的发展进程。

目前大型健康服务机构或企业没有高效地在提供健康服务中于消费者产生互动与交流，从而导致消费者难以获得随时个性化的医疗保健服务，医嘱遵循警告，转诊支持。由此而产生了信息的不对称性问题，访问数据权问题，健康数据所有权问题，隐私问题等。此外，多纬度多层次的大健康消费者的数字化互动，可互操作性和可信的工作流程的需求逐渐凸显。

区块链技术的开源性质，点对点的信息传输模式，共识机制，零知识证明等特点，为健康服务产业中身份管理功能，用户访问规则，数据确权，医患互动提供了可能。同时在不可篡改的分布式账本中可以低成本储存用户健康信息，同时做到隐私保护。让用户个体有选择的进行自身健康数据的匿名共享，从而促进了研究与医疗技术发展，同时通证保证了整个健康产业中不同角色的机构或个体能积极地参与到数据共享中。

1.3.6 基于价值健康服务

健康服务的数字化和民主化是基于价值的健康服务模式，需要医疗卫生服务，健康保健服务提供者更高效的利用医疗数字化标准，提高健康服务的可互操作性。现在医疗卫生的前景不仅仅限于访问，质量与可负担性，同时还有着可预测性，基



于结果的服务模式，促进社会普惠。随着全球降低医疗成本的压力不断上升，产生新的经济模式，减少中介服务，将健康服务流程自动化已经成为了迫切需要。

基于区块链技术可以让高成本效益的商业关系建立地更加轻松，同时可以做到任何价值的追踪，在无中心化机构控制体系下进行交易。从而帮助大健康医疗服务产业基于结果的健康服务模式，为行业降低成本。

1.3.7 分级诊疗与精准医疗

当前医疗资源配置不合理与不均衡的问题日渐凸显，导致的医疗成本提高与医疗资源不合理浪费。从而促使分级诊疗逐步落实与发展，目前以英德日为代表的推行的社区首诊制与逐级转诊制以及美澳加代表的费用控制引导分级诊疗成为当下解决方案。目前分级诊疗的制度下暴露出了对全科医生的人才培养与管理问题，以及健康医疗数据的信息化问题。

随着药品价格调整的压力不断增加，药品无法提供预期药用效果，副作用的产生，耐药性的不断增加，医药行业逐渐从规模化转变成以用户为中心的药品开发模式，用于未来的靶向治疗，逐渐的将精密医学转变成精密医疗。其主要目的是整合个体的大健康数据，从而多方面的保护个人健康。精密医疗发展将有助于分级诊疗的落实，将加速双向转诊的效率与精准的就医方案配置。精密医学的基础是个性化医疗数据，同样的也相应面临特有数据可互操作性、隐私性、安全性和所有权的挑战。

区块链全面的安全基础设施，可以前所未有的为医疗保健从业者，学术机构，研究人员与病患提供最切实的帮助从而有效促进精密医疗的发展。区块链的不可回卷性，不可篡改性可以有效消除临床试验数据核对成本和负担，并为双向转诊提供基础。去信任化的数据流转可有效的优化现有体系下的分级诊疗制度，为个体提供高效低成本的就医方案并为机构提供高效的、精准的、可行的转诊方案建议。



1.3.8 健康数据产业链羸弱

优秀、可持续的商业模式可以促使数据更高效的流通。但在医疗数据领域，由于数据权属的问题，数据在流通中产生的收益被中心机构完全获取，而数据拥有者（患者或用户）反而没有获得收益。拥有者不获益的商业模式显然是缺乏合理性使之无法长期持续增长。对机构来说，为了防范法律、道德风险，保持数据垄断，许多中心化的数据存储机构选择将数据封存。对整个社会来说，在医疗设备重复投资、医疗数据重复收集上的花费惊人，造成巨大的医疗资源浪费。

从各项数据指标来看，医疗数据变现能力目前极弱，不论是数据孤岛问题，还是数据动态性问题。目前中心化医疗数据资源方存储着大量数据，然而本质上的数据所有权问题，中心化机构只是数据的存储方而非完全所有方。而数据的分析应用需求需要大量不同来源的数据及其使用权，但目前体制下合法的获得大量数据的使用权限将消耗惊人成本和面临相应的法律与道德风险且未必能找到合适的来源。

所以通过区块链技术可实现整体产业带动，数据提供方获得相应激励后将数据出让给数据处理方。处理方实现数据可信化并归类的同时亦能通过区块链将处理后的数据出让给需求方获得奖励。整个受让流程清晰可追溯，确保数据来源合法。

1.4 Genkicell 的定义与愿景

Genkicell 的直译是元气细胞，一种可以解决任何大健康问题的假想细胞。Genkicell 区块链技术的本质是一个大健康的数据交易平台，通过区块链技术将这个平台上的数据加密变得更可靠后，为医生，患者，智能设备使用者，研究机构以及医院提供多样的健康数据服务。

Genkicell 旨在为大健康产业提供一个开放的、低成本的、隐私的，可信的，安全的去中心化可信大健康数据应用与交易平台，为利益相关者之间提供共享业务资源。



1. Genkicell 通过区块链技术实现全数据库安全接入调用，无论是物联网终端还是现有客观数据资料，在不改变现阶段全球大健康数据存储体系情况下，授权调用各方数据库。

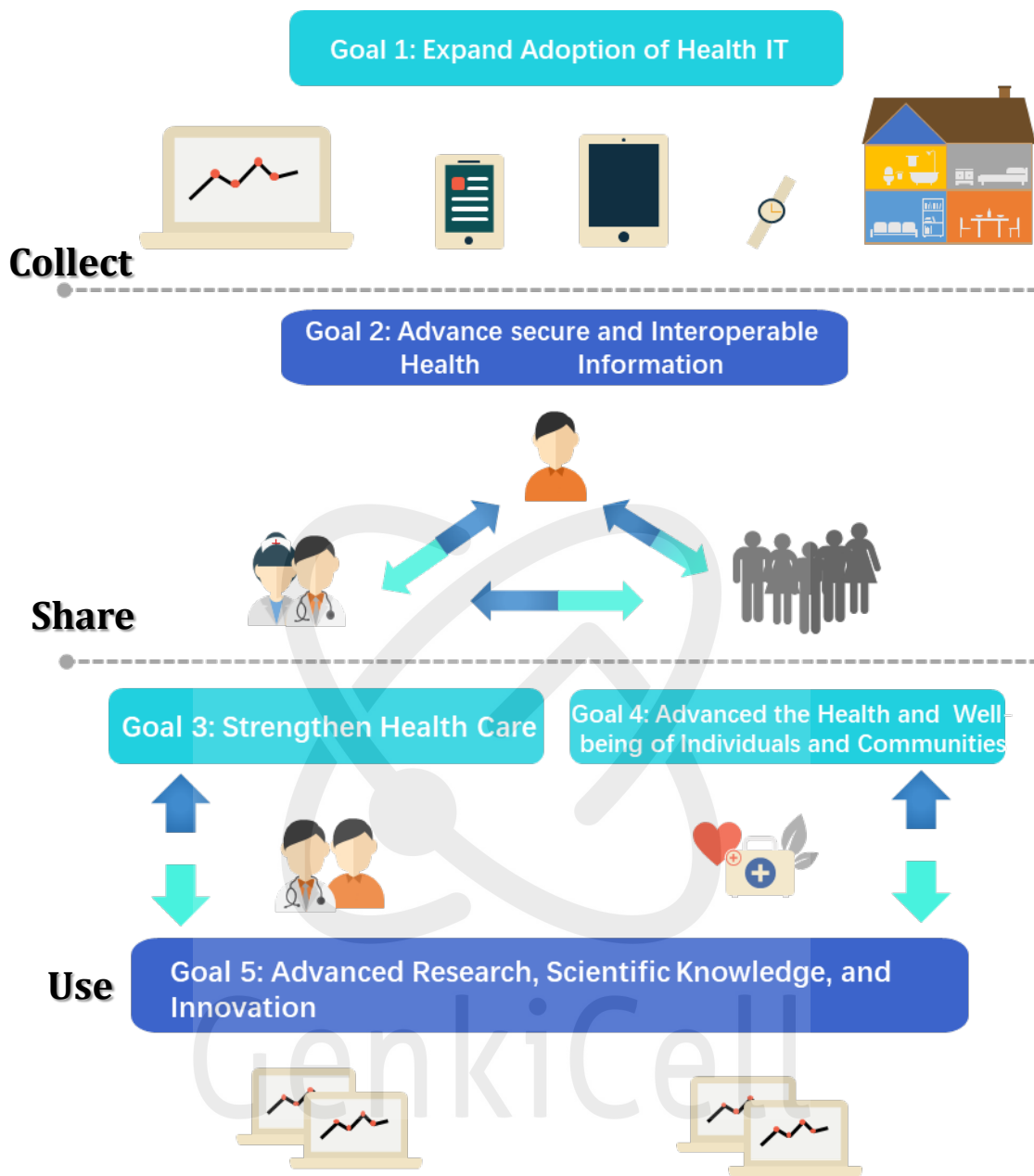
2. 用户可上传大健康数据或数据组，形成匿名化 PHR（Personal health records），这份 PHR 具有时间连贯性、来源可信性等特点，同时用户可在授权被使用数据后获得相应授权收益。

3. 用户基于 PHR 及相关授权发起诊断申请，分布式诊断服务提供者在独立诊断、权重模型引导下做出健康建议，每次交易都将形成标准化病例库，被标记的数据（标准化病例库）是监督学习基础。每位服务提供者都将获得数据可信化过程收益。

4. Genkicell 通过区块链技术优化医联体和医共体之服务效率，调动相关闲置资源优化当前分级诊疗方案。大健康服务提供者根据 PHR 快速精准的提供相应服务，甚至是跨境大健康服务。同时依赖于分布式账本记录形成地区性医疗资源网络并进行有效分级筛选配置，给个体提供最高效的转诊治疗方案，同时给予相应医疗机构双向转诊提供参考，并高效的控制住院时间与诊疗间平衡，大大降低核心医疗网络的资源浪费，提高首选医疗网络的资源利用。而大健康生态服务提供商都将在透明的区块链中获得权重评分，将有助于健康与医疗资源的动态化达到动态化的资源网络更新。

5. Genkicell 希望有更多的研究机构、商业组织通过智能合约使内容提供商获得授权收益的同时，低成本的获得大量匿名化的可信数据。同时可以通过数据交易平台快速获得大量可信数据访问授权。这些数据可帮助大健康型 AI 人工智能提升准确性，疾病源研究，药品副作用追踪等；也可用于如用户自诊断端使用的健康认知决策辅助系统，或是健康服务提供者使用的病例特征辅助识别系统，又或是公益性的大规模风险性疾病预警预测系统等先进分析技术。





Genkicell Chain 是一种通过区块链技术实现物联网硬件设备数据登入，通过日常体征、环境空间、医疗信息等数据流辅助医疗机构实现对用户身体状况的长期关注，及时有效的实施干预；数据日常化被标记的同时，可通过医疗联合体等形式实现数据流转，提高医疗机构固定客户率；而商业机构则可在授权情况下获得标记后的价值数据；因此，Genkicell 将致力实现个人、医疗机构、商业机构三者间被标记后价值数据的流转工作，实现链内用户共同收益。

第二章 应用理论

区块链是一种结合分布式数据存储、点对点传输、共识机制、加密算法等技术的新型应用模式。将区块链技术和大健康相结合，可以充分发挥其安全可靠、交易透明，确权使用等优点，同时也与去中心化的大健康数据构架相吻合。可以说把区块链技术作为底层技术，可以重塑大健康数据价值，并带来与生俱来的自治性。在传统的大健康数据体系中，医疗健康机构作为枢纽搜集并储存着大量的医疗数据信息，并形成中心化的网络，各机构间的互信问题致使产生一个个数据孤岛，同时数据的中心化储存，为了保证数据的安全，而花费大量数据安全服务费用；而在基于区块链的大健康数据的体系中，信息将安全地分布式储存在各网络节点中，同时数据的授权，传递，共享等将安全透明。

通常大数据具有 4V 的特性：数据体量巨大（Volume），增长与处理速度快（Velocity），数据结构多样（Variety），价值密度低应用价值高（Value）。此外，大健康数据同时具有：长期保存性，时空性，语义性，隐私性。同时因为这些特性，也面临了问题：数据真伪，隐私保护，授权使用，数据孤岛，体量大价值密度低，信任问题。

1. 大健康的数据分布式储存于各节点上，由一个加密散列指向内容本身。该加密散列将以交易单的形式，标明数据所有者，并不可篡改的储存在区块链上。从而解决了数据量庞大的高额储存成本，并解决传统中心化服务器的安全问题，与数据流转中的篡改问题。由于数据本身的分布式储存，我们将完整的数据分片至多个储存在各节点之中，从而做到了数据的明文脱敏，保证用户的隐私。同时由于分布式的文件储存，数据的交易单将作为数据使用的授权，储存着文件分片的节点将数据统一传输给被授权方，同时保证了数据的安全和防止盗用造假。基于应用层的统一形式和自然语言分析系统将有助于在当前医疗体系下不同系统中的快速访问和数据传输。



2.以数据可多方标记为基础，将确定数据真伪，同时将信息归类提高价值密度，数据查阅请求速度与标记方数量将决定数据价值。随着同一账户用户在平台上购买大健康服务的增加，相应的 PHR 将逐渐在分布式账本中生成。通过区块链内的共识机制形成各大健康网络主体间（e.g.:组织机构，个人，公司等。）的低成本信任传递，同时使用链内功能达到快速的授权使用，提高数据的流转性。通过 ECDSA 技术非对称加密对数据来源做出数据初步脱敏，从而保证数据提供者的隐私安全保护。区块链能够为大健康数据的交易提供成本低廉，公开透明，价值明确的系统平台。

3.根据 Genkicell 的设计,所有的医疗服务可以在 Genkicell 上的大健康服务平台购买(例如:医疗保险服务、医药服务、医疗服务、健康评估、医疗诊断、宠物疾病治疗,等等)因为 PHR 的存在,所有服务的购买时间和个人健康状况关系能够被追踪,这将有助于使医疗服务结果透明,服务价格合理化,减少服务代理。由于可以实现快速授权，区块链技术能够连接虚拟资源与现实资源，以高速、柔性的近邻、跨域交易方式，最大化能源资产活性与效益。

4.基于区块链部署的物联网大健康设备间分区局部共识、分区间共识，在实现分布式决策的同时兼顾效率，以区块链的低成本信任传递为手段，将不同主体和不同系统融合为一个大健康网络的主体，区块链能够为大健康系统提供一个去中心化的系统平台。同时被标记数据将有助于智能大健康的发展中人工智能医疗中监督学习的发展并产生高准确率算法。

大健康数据区块链未来将具备以下功能：同类数据下的多数据补充，数据可信确认，快速确权使用，可溯源追踪，数据匿名与去信任化互操作，数据透明，低成本。区块链技术使得传统大健康服务消费者转变为服务消费者与数据生产者的双重身份，依靠快速的点对点授权与非对称加密的隐私保障，以及大健康产业的发展成熟，将有大量的数据交易请求在数据的生产和消费者间产生。区块链技术除了可以执行数据交易以外，还可以作为技术水平，计费 and 结算流程的评估的基础。



第三章 去中心化大健康技术生态

3.1 链上系统设计理念

我们技术设计的原则主要有以下四点：

第一、数据真实可信

数据可信包含两个方面：首先，被标记的数据必须足够可信的；其次，来自数据提供方的数据必须满足发起方的各项需求。

第二、数据安全且可被标记

只有被正确标记的数据才有机会被记录进入主链，本身的机制会对主链内的数据进行有效的降噪。在被标记的过程中，数据会通过机制本身的限制来做到传输过程中的安全不被拦截。

第三、标记过程独立

在标记过程中，标记结果在各个标记工作单位之间不可见确保标记过程不会干扰以及作弊。同时为了进一步提高标记过程的可信程度，针对每个节点的行为评测的权重需要通过算法控制保证多方参与过程中的公平与效率平衡。（算法细节将在下文详细论述）

第四、节点价值体系

节点标记的准确性证明该节点的可信程度，将可提高该节点在系统内的权重，从而高可信度的节点将在未来标记活动中更具权威性，从而减少多数人作恶导致的标记错误入块的可能。同时系统将激励进行可信工作的节点，从而保证生态系统的健康发展。



3.2 技术生态架构

Genkicell 将由以下三层构成：业务层，BaaS 层，数据层。

首先，业务层上包含所有大健康有关的业务逻辑，针对大健康行业数据的细分行业领域的业务应用主要的目的是为了完成数据收集的流程，同时搭设自然语言处理技术平台，人工智能平台，可穿戴智能设备管理等以便数据的输入和输出。

第二，BaaS 层的任务主要是向下访问数据层的数据以及给应用层提供开放可用的接口。而为了让模块之间更加独立解耦，BaaS 层自身拆分为三个部分：

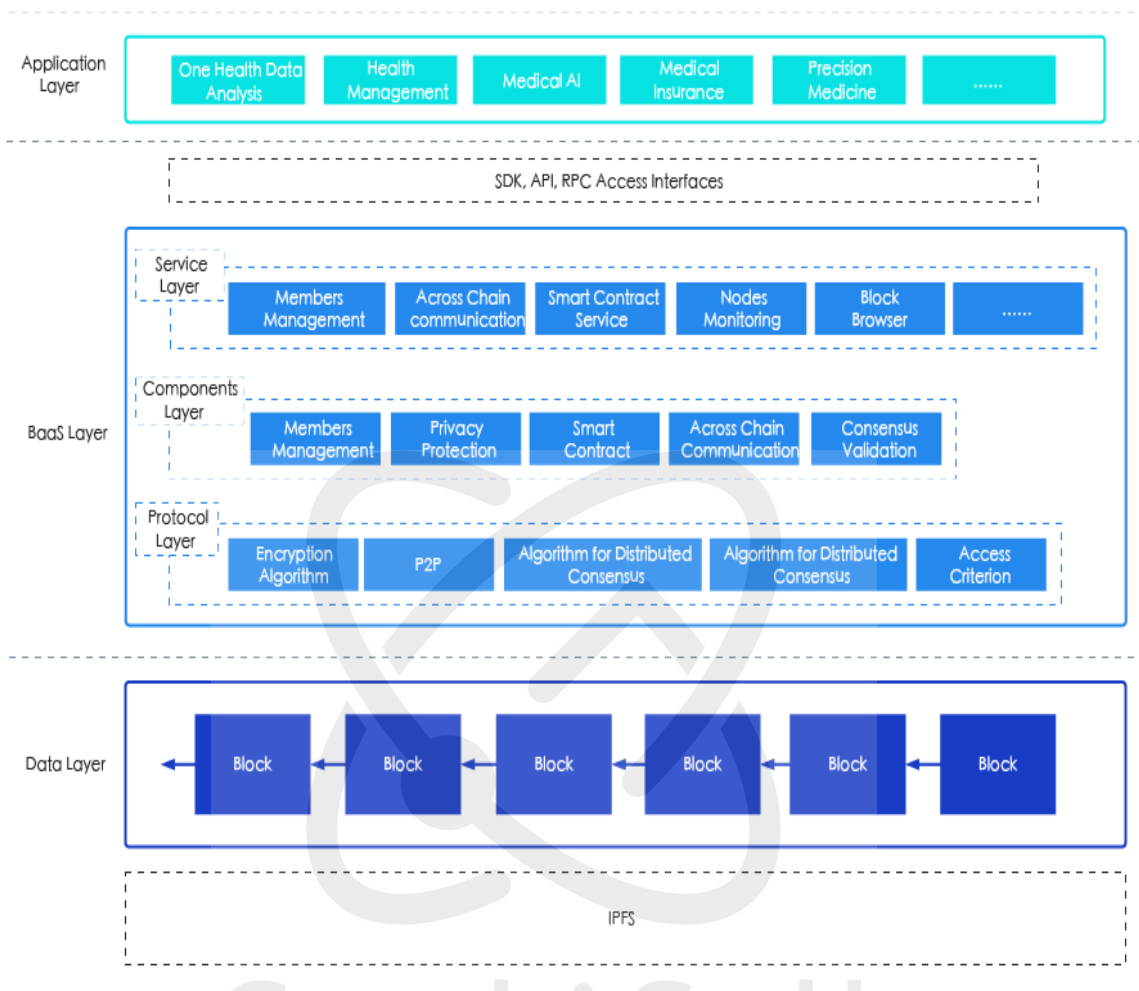
- 服务层：主要包含与业务密切相关的各个模块，直接服务于接口实现。
- 组件层：为服务层提供抽象的逻辑操作，供服务层调用。
- 协议层：实现基础的协议逻辑，与数据层交互并与业务细节解耦。

第三，数据层的任务主要在于对现有的数据进行保存。现有的数据包括用户本身测量的数据以及标记的结果，以及交易的数据。他们通过一种特殊的梅克尔树的机制。通过非对称加密的方式存储，保证了数据的安全。同时也保证侧链挂载的

GenkiCell



大数据能够迅速的被查询。



3.3 IPFS 大数据挂载

Genkicell 中将使用 IPFS 技术将已经标记的健康数据储存与分布式系统中，交易子单中的私钥将作为 IPFS 数据文件中被加密的相应数据的权限，从而保证医疗数据的安全性。因为 IPFS 具备高传输速度，高可靠性以及无存储上限的特性，所以 IPFS 本身极其适合存储大健康相关的大数据。在数据标记流程中，IPFS 的哈希地址机制保证了文件的可靠。

IPFS 星际文件系统（InterPlanetary File System）是一个点对点的分布式超媒体分发协议，旨在创建持久且分布式存储和共享文件的网络传输协议。为所有人

提供全球统一的可寻址空间，包括 Git、自证明文件系统 SFS、BitTorrent 和 DHT，同时也被认为是最有可能取代 HTTP 的新一代互联网协议。它是一种内容可寻址的对等超媒体分发协议，在 IPFS 网络中的节点将构成一个分布式文件系统。

IPFS 用基于内容的寻址替代传统的基于域名的寻址，用户不需要关心服务器的位置，不用考虑文件存储的名字和路径。我们将一个文件放到 IPFS 节点中，将会得到基于其内容计算出的唯一加密哈希值。哈希值直接反映文件的内容，哪怕只修改 1 比特，哈希值也会完全不同。当 IPFS 被请求一个文件哈希时，它会使用一个分布式哈希表找到文件所在的节点，取回文件并验证文件数据。

IPFS 是通用目的基础架构，基本没有存储上的限制。大文件会被切分成小的分块，下载的时候可以从多个服务器同时获取。IPFS 的网络是不固定的、细粒度的、分布式的网络，可以很好的适应内容分发网络的要求。

该文件系统可以通过多种方式访问，包括 FUSE 与 HTTP。将本地文件添加到 IPFS 文件系统可使其面向全世界可用。文件表示基于其哈希，因此有利于缓存，可以加大提高传输速度。

3.4 共识机制

因为 Genkicell 的一个完整的交易单由一个交易子单或多个交易子单组成的有限集合。我们决定使用创新的 WDPoS 共识机制来维护各个节点数据的统一。

3.4.1 DPoS 概述及改进思路

DPoS 算法中使用见证人机制 (Witness) 解决中心化问题。总共有 N 个见证人对区块进行签名，而这些见证人由使用区块链网络的主体投票产生。由于使用了去中心化的投票机制，DPoS 相比其他的系统更加民主化。DPoS 并没有完全去除对于信任的要求，代表整个网络对区块进行签名的被信任主体在保护机制下确保行为正确而没有偏见。另外，每个被签名的区块都有先前区块被可信任节点签名的



证明。通过减少确认的要求，DPoS 算法大大提高了交易的速度。通过信任少量的诚信节点，可以去除区块签名过程中不必要的步骤。

DPOS 算法被分为了两部分。选举一组区块生产者和调度生产。选举流程要尽量保证，权益所有者最终能控制整个网络，因为一旦网络出现问题，权益所有者损失的将会最大。如何选举恰当的人对共识能否最终达成几乎无影响。由此，本文着重介绍的是区块生产者选好后，如何达成共识。

为了说明算法，假设只有三个区块生产者，A，B，C。因为共识需要 $2/3 + 1$ 个成员来应对所有场景，在现在这个简化的模型中，我们将认为区块生产者 C 是那个破局者。当然在实际场景中，也许会有 21 个或更多的区块生产者。另外，如同 POW（工作量证明）共识一样，基本规则是我们总是应该选择最长的区块链。任何时候，一个诚实的节点看到另一个合法的且更长的区块链，它应该总是切换到那个更长的分支上。

下面将通过例子展示在各种各样网络情形下，DPOS 算法将如何工作。这些例子将解释为什么 DPOS 是鲁棒的，且是很难被攻破的。

正常情况：

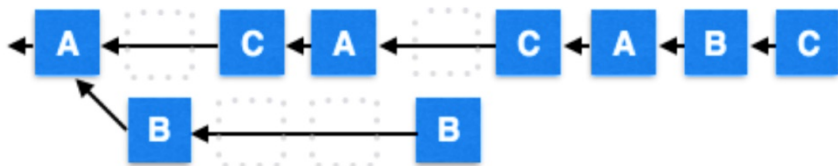
在正常情况下，记账节点轮流每隔三秒可以产生一个区块。假设没有生产节点错过自己顺序，那么他们生产的链条势必是最长的链条。记账节点在非指定时间生产的区块会被认为是规定时间之外生成的无效区块。



少数群体的分叉情况：

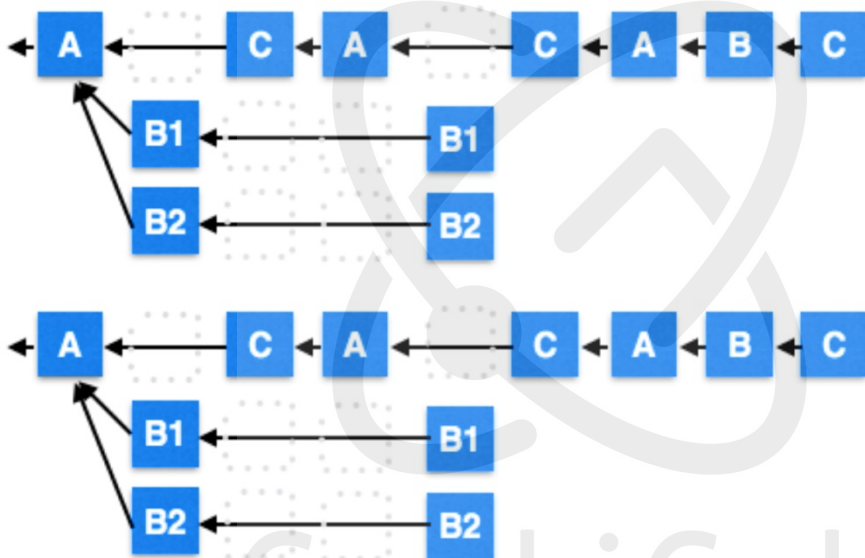
可以允许上限三分之一的节点是恶意或故障，从而导致出现分叉。在这种情形下，少数分支将只能在 9 秒内生产 1 个块，而大多数分支，由于数量多一倍，将预期能在 9 秒内生产 2 个块。所以诚实的 $2/3$ 的大多数节点可以比小的那一部分

创建一个更长的正确链条。



隔离环境下的重复区块生产情况：

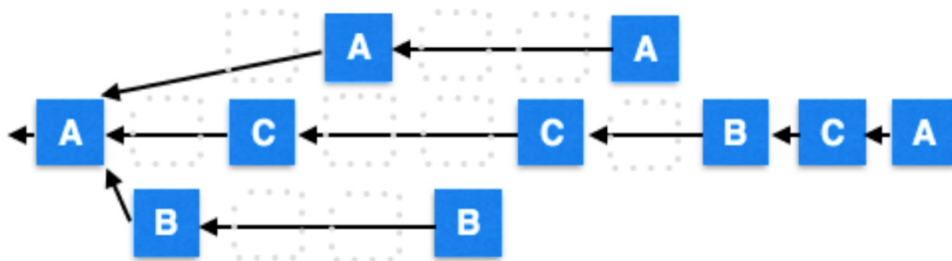
少数群体可能尝试创建一个无限数量的分叉，但所有分支都将比主链短，因为少数群体在链的成长上更慢。



网络不稳定时的碎片生成情况：

网络非常有可能碎片到，每一个链上的区块生产者都在各自生成不同的区块。在此情景下，最长的那个链将变成最大的一个少数群体。当网络连接恢复正常后，相对较小的那些群体将自然的切换到最长的正确的链，从而可以恢复明确的共识进

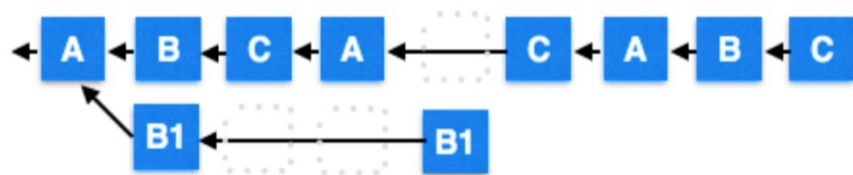
而保证了整个链条的完整。



还有一种可能性比较大的情况是，三个分支中，最大的两个分支一样大。此时，将由相对更小的第三个分支加入网络时来决定正确的链条是哪一个。存在奇数个区块生产者，所以僵局一般不会持续很久。下文还将介绍区块生产者的重新清洗过程，该过程会将生产者随机生成顺序来确保即使两个分支具有相同数量的生产者时，两个分支也将以不同的长度爆发增长最终导致一个分支最终接管另一个分支。

少数群体重复生产区块的情况：

在这种情景下，少数群体 B 在自己可以生产的时间节点，同时创建两条，或多条的区块链。下一个执行的生产者 C，将选择 B 创建的可选链中的任一条。C 选中的这条链将成为最长的链，当这发生是，所以如下图所示的 B1 链条上的结点都会转过来。所以，无论少数作恶结点制造多少的链，他们在下一轮中，肯定不是最长的那个链。



最后的不可逆区块生成：

在网络碎片的情况下，多个分叉可能持续较长时间的隔离。长远来看，最长的链将最终受到认可。但观察者需要一种手段来确定某个块是否是在最长链条的一部分（确认共识）。这可以通过 $2/3 + 1$ 个区块生产者是否对某个块有确认。

下图中，块 B 被 A、C 确认了，这意味着 $2/3 + 1$ 都已经确认了。由此我们可以为不可能存在更长的链了，因为 $2/3$ 的区块链是诚实的。



需要注意的是这个规则与比特币的 6 个区块确认类似。一些聪明的人可以设计一系列事件，其中两个节点可能会在不同的最后不可逆块上结束。这种极端情况需要一个攻击者，精确控制通信延迟的时间，并需要在几分钟内实施不止一次，而是二次攻击。如果发生这种情况，那么最长链条这一长期规则仍然适用。我们认为这种攻击的可能性足够接近 0，经济后果也几乎微不足道，所以不值得担心。

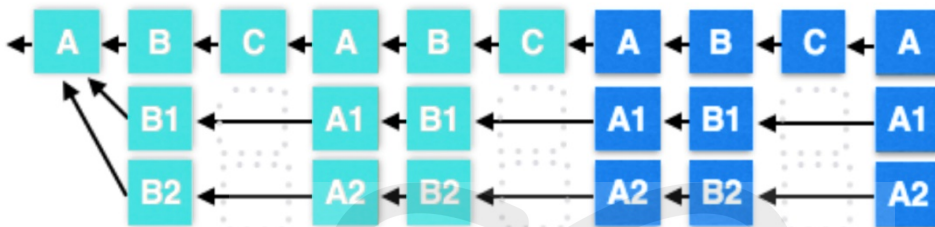
法定区块生产者数量不足的情况：

在一些极少数的情况下，区块生产者没能达到规定的人数，少数节点可能仍然在继续生产区块。在继续生产的区块当中，利益相关者可能会包含一些改变投票的交易。这些投票会选举一组新的区块生产者，并将区块生产参与度恢复到 100%。一旦发生这种情况，少数人链最终会超过其它低于 100% 参与链。当这个流程发生时，所有的观察者必须要知道整个网络处于不稳定的状态，直到多于 67% 的参与者出现后才会稳定下来。

那些选择在这种情景下发起交易的与那些在比特币中接受低于 6 块就确认交易成功那样，冒着类似的风险。作弊节点需要明白，存在一些共识最终会以另一个链为准的情况。在实践中这种情形相对于比特币中接受少于 3 个块就确认的机制则显得更加安全。

大多数区块生产者联合作弊的情况：

如果大多数区块生产者合谋作弊制造了无限数量的分支，每一个分支都有多于 $2/3$ 的大多数的签名。在这样的场景早，最后不可逆转块算法退化为最长链算法。此时最长的，获得了最大的群体认证的，将由少数的诚实节点的加入来确定。这样的情形不会持续很久，因为利益相关者会最终投票替换掉这些区块生产者。



基于历史行为权重的改进策略：

由于 DPoS 无法完全去除对选举信任的要求，并且在投票过程中并未有明确的选举规则设定，所以我们对 DPoS 做出如下改进。简称 WDPoS，旨在现有的股份授权证明机制（DPoS）上边进行改进，加入了权重（Weight 即 W）的因素考量，对于每一个见证人，对于之前的历史工作行为，会有一个权重系统进行权威认证，随着完成正确行为的增加，系统会给予相应的节点进行权重提升的奖励。在标记过程中的正确性激励方面，首先我们会对于整个标记中的各方给出的结果进行验证，只有标记正确的节点才会获得用户预付的费用奖励，同时正确的一方会获得相应的 Genkicell 信用增加，更高的信用在判定验证过程中将会获得更高的权重。在后续每次完成见证的过程中，权重越高的节点的意见将会通过加权的方式获得额外的优先受益。通过这种变相的工作可靠性证明的机制，将逐渐减少无事实基础的信任需求，从而减少 DPoS 的共识算法对信任的要求。

3.4.2 分布式一致性算法实现

比特币是通过计算机之算力来投票，算力高的自然得票较多，容易获胜。



DPOS 机制是通过资产占比（股权）来投票，更多的加入了社区人的力量，人们为了自身利益的最大化而投票选择相对可靠的节点，相比更加安全和去中心化。然而这种方式依然依赖其他人的选择，WDPoS 则会根据节点的历史可靠度来自动票选出诚实可靠的节点，进一步提高整个系统的稳定性。整个机制需要完成如下过程：

- (1) 注册受托人，开始记录节点行为
- (2) 维持循环，调整受托人权重
- (3) 循环产生新区块，向整个网络广播

1.注册受托人

注册受托人必须使用客户端软件(业内俗称钱包)，因此这项功能需要与节点进行交互，也就是说客户端要调用节点 Api。

2.评估节点

所有这类交易的逻辑都会影响到节点的可信度权重。这里要提示的是，该功能是普通用户具备的功能，任何普通用户都有投票权利，所以放在账号管理模块。

3.块周期

块周期，是其他周期的基础，但是这里的代码并不包含任何区块、交易等关键信息。这里隐含的关联关系，就是区块、交易等信息的时间戳。只要知道任何一个时间戳，其他信息就可以使用这里的方法简单计算出来。

4.循环周期

为了安全，GCL 规定受托人每隔固定的轮次之后都要变更，确保那些不稳定或者作恶节点被及时剔除出去，同时新加入的节点有机会可以证明自身的可靠。另外，尽管系统会随机找寻新的受托人产生新块，但是在一个轮次内，每个受托人都有机会产生一个新区块（并获得奖励）并广播，这一点与比特币每个节点都要通过工作量证明机制（PoW）竞争获得广播权相比，要简化很多。

同时，GCL 计划采用模块化设计，支持可插拔共识算法，根据具体的应用场景/类型可以方便、快速地 切换成其它的共识算法，包括 PoS、Raft、Pbft 等算法，使的共识机制本身在出现局限性时可以进一步的迭代升级。



3.5 智能合约

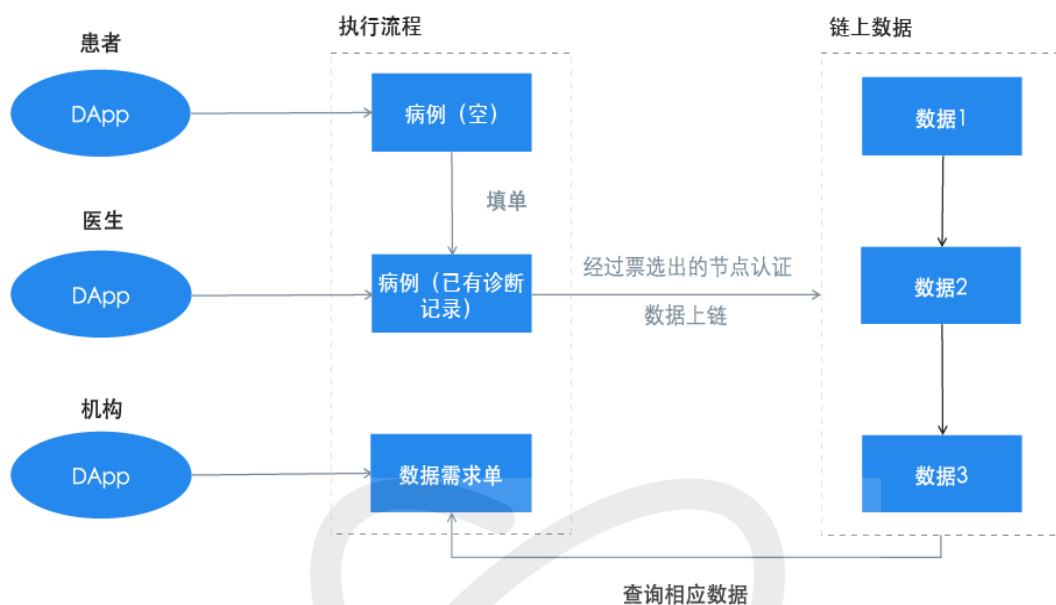
核心账本的实现过程中将搭建 GCL 虚拟机作为智能合约的执行环境，可以为网络应用层框架实现智能控制逻辑。GCL 虚拟机理论上应具备图灵完备性，可以实现任意逻辑，同时具有高度的确定性。非常适合用于对确定性要求很高的场景中。此外，虚拟机将 JS 字节码等中间语言编译为区块链虚拟机的指令。从而使智能合约的开发者不需要学习新的语言，就能使用熟悉的 JS 等编程语言编写智能合约，快速融入全球百万级的开发者社区。共享平台各参与方将容易上手操作和维护，为其提供进行智能合约编辑的可操作性，降低了其接入的门槛。

虚拟机将与上层高级语言解析转换相结合，灵活支持虚拟机的基础应用。通过定制化的 API 操作实现虚拟机的外置接口，可以灵活地与账本数据以及外部数据进行交互。这一机制实现了智能合约运行时达到原生代码执行的高性能。同时也实现了支持不同区块链的通用虚拟机机制。

3.6 业务流程

整个 GCL 流程的核心部分可归纳为数据标记流程以及数据采集流程，如下图所示，患者通过生态上的 DApp 可以进行就医环节的流程，在整个流程提出病例的申请，然后通过一个或者数个医生端的给出的结论集合通过认证节点判断出最后的结果，最后的诊断将通过共识机制的认证之后记录于链上并且完成通证的扣除与分发。而对于采集流程来讲则相对自动化程度高一些，机构可以直接发布交易单需求，链上数据通过智能合约直接定价采集，机构可以直接通过支付相应的通证直接完成数据采集的工作。





3.6.1 数据标记

为了方便解释，我们将发起标记需求，也是通证所有者与需求数据标记的一方称为 A。通证接收者，为数据进行标记的一方称为 B。负责进行传输信息与见证的一方成为 C。

子交易单由以下几个部分组成：A 的账户公钥地址，数据的 hash，这笔交易所包含价值，B 的账户公钥地址，对 A 数据的判定，该交易单 A 的数字签名，该交易单 B 的数字签名。

数据的 hash 将指明待标记数据在分布式储存网络的位置，与交易子单所属的交易有限集合。

A 的账户公钥地址标明了该数据的 hash 的所有权，与支付通证的地址。

B 的账户公钥地址标明了该数据的 hash 调取权限的指向，与接收通证的地址。

A 的签名保证了子单的信息完整性与对 B 在分布式储存网络下载待标记数据的权限

B 的签名保证了对待标记数据标记后的完整性。

交易单价值代表该交易单交易成功后 B 获得的通证数量。





A 填写的内容包括：

- A 的账户公钥地址
- 待标记数据的 hash
- 交易单价值
- 参与合约的信用
- 参与 B 的数量

这里根据 A 填写的参与交易的信用，系统根据公共账本将在线节点分为，A(交易发起方)，B(满足信用的参与方)，C（不满足信用，参与传输和见证的见证方），将符合条件的 B 的账户公钥填入子交易单。

A 发起一个数据标记请求后，系统根据 B 的数量（N）将形成 N 份交易子单。该交易子单上所包含信息：

- 待标记数据的 hash
- A 的账户公钥
- B 的账户公钥
- 交易单价值
- A 的签名

完成合约后 A 将 N 份子交易单（这时候 B 的签名和 B 对待标记数据的标记均为空白），通过 P2P 的方式传输给 B 与 C。C 获得该交易单将数据传送给 B，此时的交易子单可视为一份数据调取授权。B 收到待标记数据后填写对数据的判定，将完成交易单传给 C 和 A。当第 N 个 B 填完所有交易单后，所有 C 节点开始逐渐收到这次请求的所有完成的交易单。之后等待共识。A 的交易单集合（这次请求，发出的 N 个交易单），根据一套权重算法得出最终成功交易的结果。简单来说，标记相同答案的 B 的获得通证，信用加 1，标记不同答案的获得通证，信用减 1。如果有子单没有完成则进行等待并向相应的 B 进行索取，当等待时间超过其他子单（N 大于 51%）的平均完成时间，视 B 标记答案为错误，则 B 信用减 1。

3.6.2 数据采集

为了方便解释，我们将发起收集需求者，也是通证所有者与需求数据调取的一方称为 A。通证接收者，数据的所有者的一方称为 B。负责进行传输信息与见证的一方成为 C。

子交易单由以下几个部分组成：A 的账户公钥地址，数据类别，这笔交易所包含价值，B 的账户公钥地址，该交易单 A 的数字签名，该交易单 B 的数字签名。

数据类别将指明待调取数据在区块链上数据所在的交易单（同时依据 B 的账户公钥地址），与此次交易子单所属的交易有限集合。

A 的账户公钥地址标明了该数据的 hash 调取权限的指向，与支付通证的地址。

B 的账户公钥地址标明了该数据的 hash 由谁所有，与接收通证的地址。

A 的签名保证了子单的信息完整性。

B 的签名保证了对 B 在分布式储存网络下载待调取数据的权限。

交易单价值代表该交易单交易成功后 B 获得的通证数量。





具体流程如下：

A 填写的内容：

- A 的账户公钥地址
- 待调取数据类别
- 交易单价值
- 参与 B 的数量

这里根据 A 填写的待调取数据类别，系统根据公共账本将在线节点分为，A(交易发起方)，B(拥有数据的参与方)，C（不满足信用，参与传输和见证的见证方），将符合条件的 B 的账户公钥填入子交易单。

A 发起一个数据标记请求后，系统根据 B 的数量（N）将形成 N 份交易子单。该交易子单上所包含信息：

- 待调取数据类别
- A 的账户公钥
- B 的账户公钥
- 交易单价值
- A 的签名

完成合约后 A 将 N 份子交易单（这时候 B 的签名为空白），通过 P2P 的形式传输给 B 和 C。C 作为一个请求发起后的见证，B 则将交易单签名确定同意将数据调取权授予给 A。C 获得该交易单将数据传送给 B，此时的交易子单可视为一份数据调取授权。当第 N 个 B 填完所有交易单后，所有 C 节点开始逐渐收到这次请求的所有完成的交易单。然后等待共识完成，再然后将数据传输给 A。

普通交易转账：

为了方便解释，我们将发起交易者，也是通证所有者一方称为 A。通证接收者一方称为 B。负责进行传输信息与见证的一方成为 C。

交易单由以下几个部分组成：A 的账户公钥地址，这笔交易所包含价值，B 的账户公钥地址，该交易单 A 的数字签名。

A 的账户公钥地址标明支付通证的地址。

B 的账户公钥地址标明了接收通证的地址。

A 的签名保证了子单的信息完整性

交易单价值代表该交易单交易成功后 B 获得的通证数量

具体流程如下：

A 填写的内容：A 的账户公钥地址，与 B 的账户公钥地址。

此时 B，C 均成为了见证节点。

A 发起一个数据标记请求后，系统根据 B 的数量（N）将形成 N 份交易子单。

该交易子单上所包含信息：



交易单



- A 的账户公钥
- B 的账户公钥
- 交易单价值
- A 的签名

完成合约后 A 将交易单（这时候 B 的签名为空白），通过 P2P 的方式传输给 B 和 C 之后等待共识，交易单上块后交易达成。就是根据同类数据的数据标记本身的加权统计结果来判断诊断本身的正确性，由于在数据标记过程中会存在误诊以及故意作弊。所以在诊断流程里，Genkicell 引入了正确性数据标记机制，即统计所有的数据标记结果，并根据他们的权值系数分配非整数倍的票数，使得整个权重系统可以有效抵御女巫攻击，防止大量的伪造数据来影响数据的可信度。最后所有的数据标记结果中，只有存在了，诊断结果的概率超过 51% 的时候才会认为本次诊断切实有效，否则将认为本次诊断模糊不清，或者是属于难以标记的数据，则重新执行订单分配数据标记流程。直到用户放弃数据标记或者出现了正确的数据标记之后的标记数据才可以入块。

根据各节点对数据的标记答案（A1、A2……An），将各节点以往该答案的交易单调取，获得以下四类：

- 1) 节点标记为 A，判定后正确标记为 A，标记正确
- 2) 节点标记为 B，判定后正确标记为 A，标记错误
- 3) 节点标记为 A，判定后正确标记为 B，标记错误
- 4) 节点完成时间超过 51%，判定后正确标记为 A

针对于本次交易：

N1: 正确标记相同答案（A）的节点获得通过验证次数

* count of situation (1) above

N2: 等待时间超过 51% 的平均完成时间

* count of situation (4) above

N3: 节点标记错误的次数

* count of situation (2) + (3) above

每个节点在当前交易的信用的计算公式为：

$$\alpha_i = 1 * n_1 + (-1) * n_2 + (-1) * n_3$$

α : 各节点的信用.

n: 节点总数量.

计算出各节点的信用平均值：

$$\bar{\alpha} = \frac{\alpha_1 + \alpha_2 + \dots + \alpha_n}{n}$$

因为反正切函数的导数为 $1/(1+x^2)$ ，所以曲线的增长率在前期会随意信用值的增大而增大，在信用值达到一定数值后，增长的幅度则会逐渐变小。这样可以将信用值偏低的机构的权重有效缩小，并且可以防止有过高信用值的机构主宰整个投票结果。

$$\beta_i = \frac{\arctan(\alpha_i - \bar{\alpha})}{\pi} + \frac{1}{2}$$

X:节点的结果。



因为有 n 个节点参与判定，那么我们将有 n 个结果： x_1, x_2, \dots, x_n 。之后将所有相同标记结果的 β 相加。

P 是经过合并同类项后所有结果的总数，即将所有节点给出标记结果归类后所有标记类别的数量。

$$\begin{aligned}
 & \begin{bmatrix} x_1 & x_2 & \dots & x_n \end{bmatrix}_{1 \times n} \begin{bmatrix} \beta_1 \\ \beta_2 \\ \dots \\ \beta_n \end{bmatrix}_{n \times 1} = \sum_{i=1}^n \beta_i x_i \\
 & = \sum \beta x_1 + \sum \beta x_2 + \dots + \sum \beta x_p \quad (p \leq n) \\
 & = \omega_1 x_1 + \omega_2 x_2 + \dots + \omega_p x_p
 \end{aligned}$$

对于每个标记，概率公式为：

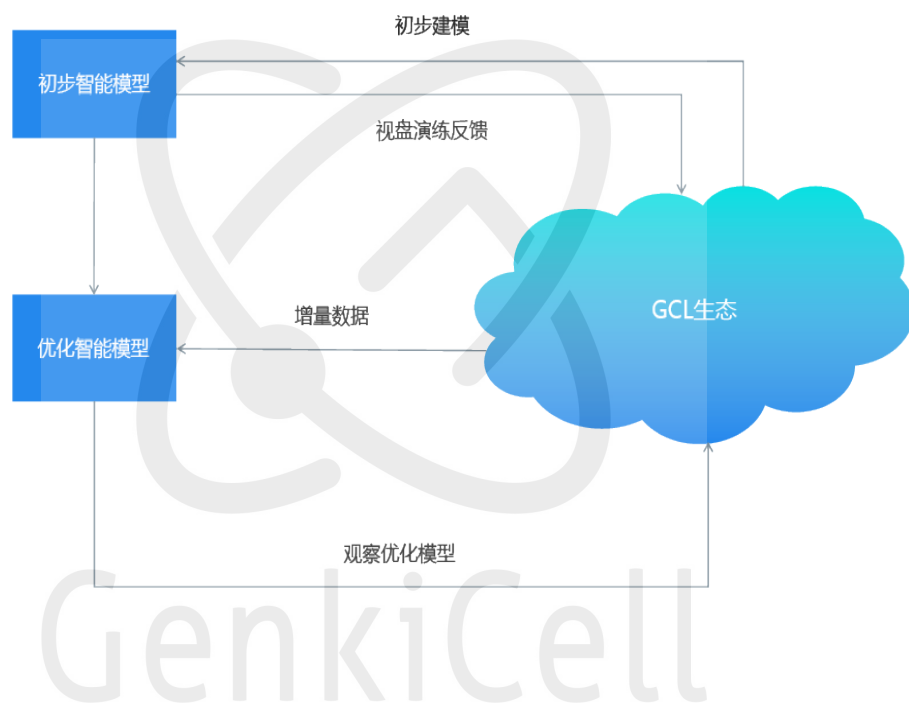
$$\begin{aligned}
 & \frac{\omega_i}{\sum_{i=1}^p \omega_i} = \frac{\sum_{x_i} \beta}{\sum_{i=1}^n \beta_i} \\
 & = \frac{\sum_{x_i} \left(\frac{\arctan(\alpha_i - \bar{\alpha})}{\pi} + \frac{1}{2} \right)}{\sum_{i=1}^n \left(\frac{\arctan(\alpha_i - \bar{\alpha})}{\pi} + \frac{1}{2} \right)}
 \end{aligned}$$

当节点对数据作出的标记概率高于 51% 时，作出该类标记答案的节点被视为进行了正确的标记工作。



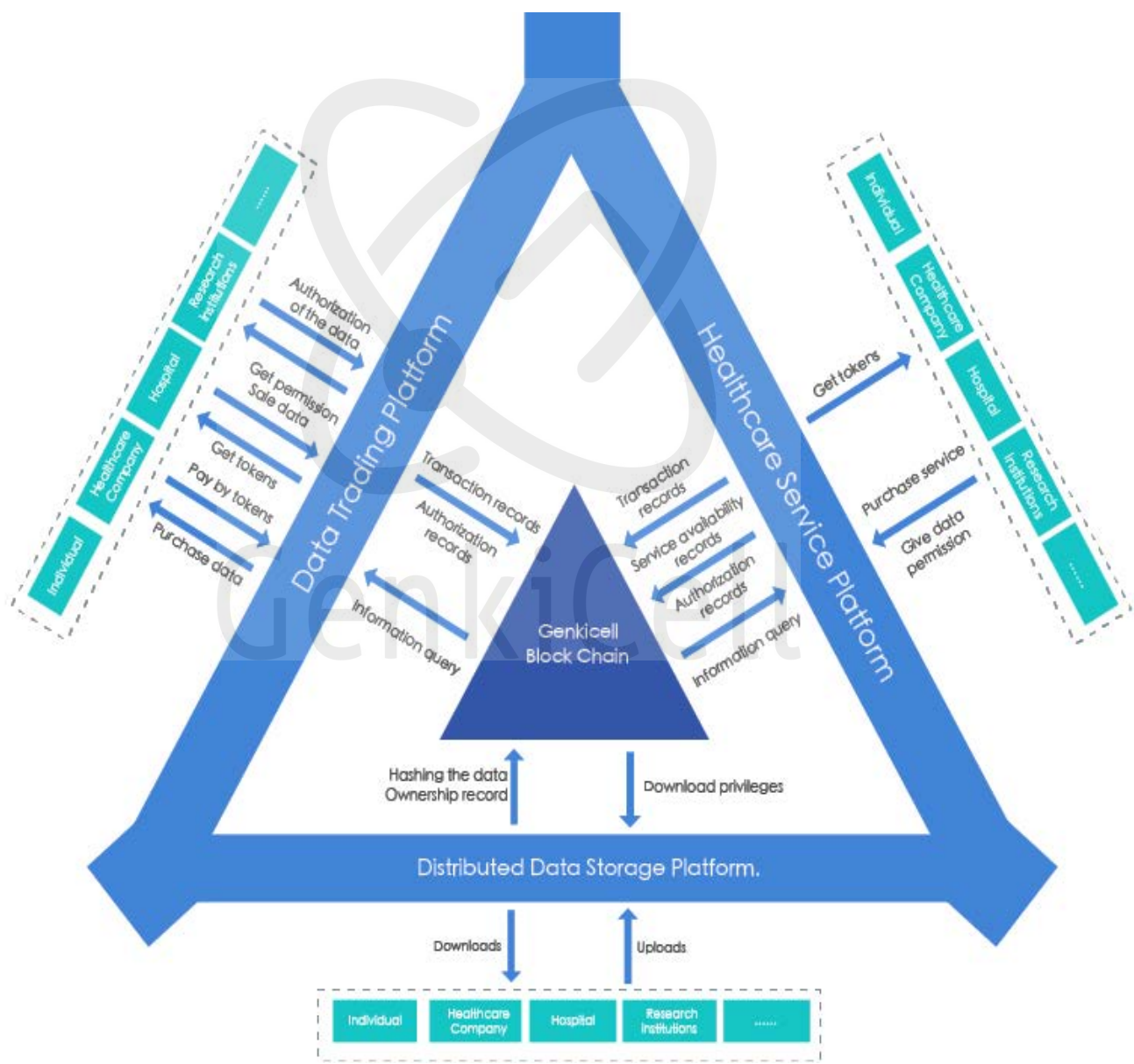
3.6.3 智能诊断机

基于如上的业务逻辑，具备相关人工智能技术实力的机构可以利用链上数据来训练自己的智能诊断模型来获得收益，通过链上不断增长的相关数据，可以不断训练更加精准的 AI 诊断模型，而一个更加精准的模型本身也可以为拥有模型的机构带来源源不断的收益。



第四章 区块链技术及应用生态

由于 Genkicell 在技术上属于大健康区块链范畴，整个生态系统由三大部分组成：数据共享平台，大健康服务平台，数据储存服务。该三部分将覆盖大健康产业的所有需求，如：保险机构对于病症研究的数据需求，个体对医疗保健的需求，疑难病症的联合诊断，自动化的保险理赔，研究机构对流行疾病的研究，人工智能对大量标记数据的需求，个体病例授权与查阅需求等。



4.1 通证模型

Genkicell 将基于 Genkicell 数字通证与 Genkicell 信用作为生态系统的价值传输中介与生态系统内部评价。Genkicell 信用将不具有流动性，将作为激励机制的价值因子，作为生态系统内部评价的一部分。Genkicell 数字通证是可流动性的，是生态系统中价值传输的纽带。

4.1.1 Genkicell 数字通证

我们拟发行总量恒定的数字通证 Genkicell token，简称同为 Genkicell。每一个 Genkicell 对应相应的大健康数字资产。

Genkicell 可以交易，根据用户对大健康服务需求的数量增长和研究机构等对数据的积累的总数增长所带来的交易需求增长而增值。

Genkicell Token 将会应用在三大基础场景：

1. 大健康服务的购买
2. 对于大健康数据的收集
3. 数据长期储存

GenkicellToken 是基于区块链技术的可溯源通证，所有数据基于分布式账本进行管理，数据真实、可靠、可以追溯。GCL 通证将作为 GenkiChain 链间各方参与者间的价值传输中介与生态系统支柱，矿前期（Pre-mainnet）总量为 36 亿枚，区块奖励（Block rewards）总量为 24 亿枚。

GCL 约定如此：在每个区块中将设定一个特殊化处理的交易，该交易产生一定量的新的通证用于节点激励，之后逐年减半直至区块奖励结束。此外随着区块奖励的减少，将产生支持内部生态系统的激励池，将在每个受托人周期结束后第一个区块产生时发放。激励池将依赖于用户储存数据费用与数据流转费用。激励池内 GCL 将按照参与者贡献比例进行配发，其中激励主要包含以下贡献：贡献储存空间与可信工作。贡献储存空间因子将由所储存数据占全网数据总量与带宽贡献决定，可信工作因子由完成打包入块的交易价值决定。



Genkicell 数字通证用途包括但不限于：

奖励和鼓励生态参与者提供运算能力，保证网络的正常运转。

制定智能合约、执行智能合约的费用。

交易双方的结算凭证。

数据储存消费

4.1.2 Genkicell 信用

Genkicell 信用是一种生态系统内部评价的基础，以一种激励机制下的价值因子所存在。是权重模型中的基础变量，也是体现节点工作信用程度与工作水平。其主要来源于在数据标记流程中，节点做出正确标记后的奖励。其主要拥有两种体现路径。总量的体现：代表该节点信用的总体能力水平与诚实程度。标记类目下的体现：代表该节点对于该类目的标记准确性或成功率，是类目下标记能力优势的体现。Genkicell 信用将影响生态系统中两个主要流程：

- 未来数据标记中结果判定的权重
- 共识过程中票选见证人的权重

随着 Genkicell 大健康价值生态系统的逐步完善与发展，该价值因子将给予生态系统中不同参与者提供便利并产生相应的服务场景。Genkicell 将形成不同机构或个人的大健康诊断服务的评价体系，间接体现了该单位卫生服务水平，同时根据各疾病下数据标记数据将产生国际疾病分类编码，有助于改良且规范疾病诊断标准与临床路径病案质量控制，帮助临床流行性病学的研究发展。此外可在此基础上形成疾病谱并追踪，为大健康企业与基金提供投资和发展导向。

4.2 基于 Genkicell 开发的生态产品

4.2.1 数据交易与管理 App

在 Genkicell 网络里，不同地域的用户，可以通过 APP 进行日常生活的大健康数据查询、交易与共享。同时还能用户个体身体状况进行统计与分析做到服药提



醒，跨境诊断，医患互动，保健服务预约，保险购买等服务。未来 APP 会支持各种智能家居，通过人工智能的方式进行控制以及毛细血管级的数据分析与管理。

4.2.2 钱包

Genkicell 钱包是帮助生态系统内用户管理通证资产的 APP。钱包可以创建新账户、实现 Genkicell 转账及其他未来 Genkicell 生态上的通证、导入导出私钥，也可以查看 Genkicell 的使用情况和交易记录。

4.2.3 大健康服务

Genkicell 与合作伙伴提供丰富的大健康服务。无论是智能健康设备，慢性病护理，电子病例，食品安全等等。同时现有大健康服务也将支持接入 Genkicell 并支持 Genkicell 支付。

4.2.4 数据共享系统

Genkicell 平台与医疗，环境，食品，药品，科研等系统进行互联互通，建立完整大健康体系生态，并使用 Genkicell 实现各平台间的交易与结算。

4.2.5 交易所

由于 Genkicell Chain 之网络将会覆盖到全世界各地，位于不同国家的使用者皆可通过官方交易所进行不同法币和 GCL 间的交易，我们会首先在香港、新加坡、日本、马耳他与韩国开通交易所



第五章 应用场景

5.1 数据授权

依靠区块链技术搭建的健康数据交易平台，依赖于非对称加密技术，将全交易过程透明化的同时保证数据的隐私。由于链上数据的难可回滚性，保证了数据流动中被篡改问题。GCL 独有的结构保证了数据所有者对数据需求方的快速授权，同时依赖于共识体系，将有效解决当前缺乏受信任的数字化工作流程带来了各种不同的 HIT 系统和中心化医疗数据管理模式，从而解决了目前大健康医疗数据流转中的信任问题，打破数据孤岛。从而实现目前大健康生态系统中数据数字化与数据互操作性，产生真正意义上的价值服务体系。



5.2 大健康服务

依赖于区块链技术，服务的需求方（匿名）与服务提供方将的服务购买行为将

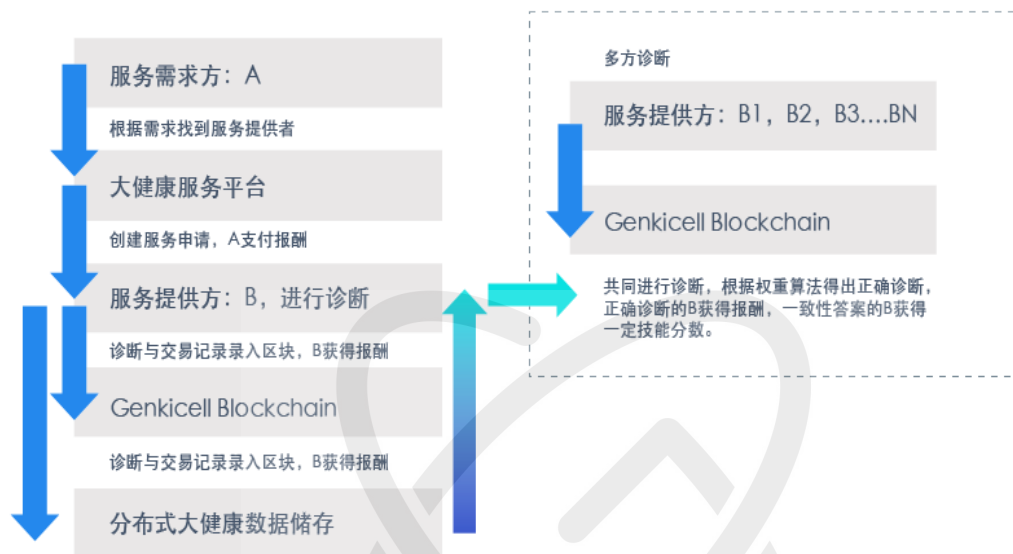
记录在区块中，整个医疗交易过程将透明化的同时保证需求方的隐私。服务期间的健康数据变化将保证服务中的需求方的权益，减少信息不对称，减少医患纠纷与医疗事故。该功能将有效提高数据在普通用户与大健康服务商间的数据流转与互性，而服务后一定时间内的健康数据可视为该治疗效果的评估，形成服务方的技能水平目录。同时此过程中优质的服务方的技能评分将增加。这将有力促进健康服务的数字化与民主化进程，支撑基于价值的健康服务模式，同时将利用形成的数字化医疗标准建立，为精密医疗提供基础。以便于在确诊后给予患者个性化医疗提供路径，构建分级医疗网络，加速双向转诊的效率的服务。



5.3 全球诊断

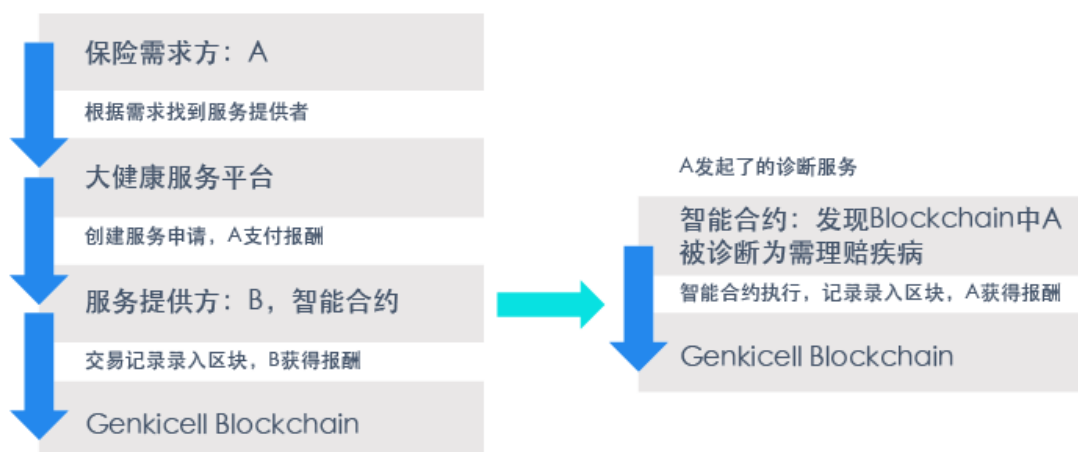
Genkicell 通过区块链技术优化医联体和医共体服务效率，调动相关闲置资源，甚至是跨境诊疗服务。在降低大健康成本的同时，收益到最为匹配的健康服务。通过多方诊断同时可以形成疑难问题下的服务方的诊断水平目录。Genkicell 将邀请更多医疗机构参与，随着跨国界多领域大健康机构的增加，对于疑难病症的高效治

疗和准确诊断将在 Genkicell 上实现，需要进行诊断或治疗建议的机构将可以发起一笔或多笔的数据标记请求，根据发起者的需求，世界范围内的机构都将可以给予建议和治疗方案。



5.4 医疗保险

通过智能合约，Genkicell 可以根据医疗大数据自动进行医疗保险的审核和理赔。保险理赔的审核过程将由去信任化的区块链技术替代。保险服务商可以依照提交到链上的医疗数据（医疗记录、保险消费记录）使用智能合约自动进行保险理赔。此外，个人医疗“大数据”还可以实现个人化定制的精准投保。



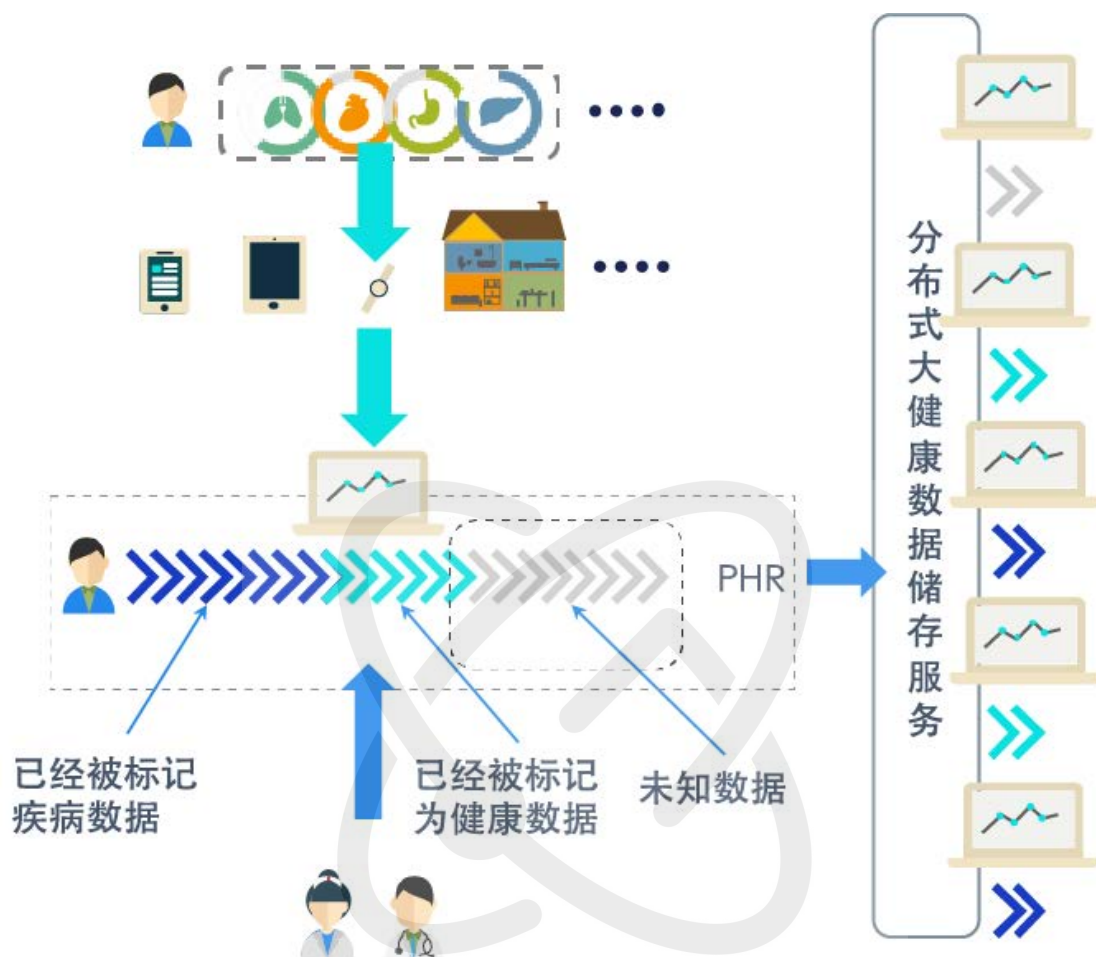
5.5 PHR

依赖于 IPFS 的分布式数据储存技术，将数据分片储存在各个节点。相比现有的中心化储存机制，降低了数据储存成本的同时，保证了数据安全。此外依赖于数据的分片化处理，各储存节点无法得知数据内容，保证数据隐私。同时 GCL 特有的结构保证数据只有数据所有人授权的情况下才可以查阅。

用户可以通过物联网设备上传大健康数据或数据组，此外在获得大健康服务后，所有数据也将被记录于用户名下并储存至分布式大健康数据服务中从而形成匿名化的 PHR，这份 PHR 将具有时间连贯性，价值密度高，数据完整性强的特点。这将有效满足当下健康自我量化的需求，有助与个体与健康服务商间形成高效及时互动。就研究机构而言，数据的完整性与连贯性的大大增加，将大力促进健康领域中横断研究与追踪研究，例如：药物临床研究，疾病相关性研究，亚健康研究，流行病学现状研究等。

未来 PHR 记录将是一个人从出生起，所有健康情况、患病情况、诊疗情况、服药情况，以及反馈情况变动的轨迹和趋势。通过 PHR 可以对患者的耐药情况、病史、药物反应等做出更清晰的判断，同时，也可以对患者的健康状况、疾病的产生

和发展做出预测，预防可能发生的疾病。



5.6 其他应用场景

AI 的发展让我们的数据处理能力得到了极大地提升。在医疗数据社区不断健壮的条件下，医药研究公司的 AI 将可以得到和处理跨国、跨行业的医疗大数据。更广阔的样本可以使新药的研发大大加速，从而造福更多生命。当下智能大健康概念及其火爆，加上大健康资源供需严重不平衡的现状，智能大健康作为一种在轻量病症状况下的补充，可以很好地解决大健康资源供需不平衡与供应分配不均的问题。

而智能大健康依赖的是人工智能技术，如果要达到一定的准确度，需要的是人工智能中的机器学习技术方法，机器学习目前最主流同时也是应用最广泛的方式是监督学习，而监督学习目前最大的瓶颈则需要大量的训练数据才能得到非常好的效果，而中心化的人工标记不但费时费力，同时还会包含大量的噪音数据，影响最终的智能模型的训练结果。为了提高可用于研究数据的准确性，我们通过类似于囚徒困境的博弈数学模型的设计，利用个体逐利的本能作为驱动力，最大可能的提高数据的精准度，相信随着区块链技术赋能下的大数据基础建设越来越完善之后，我们的有效数据会带着智能大健康本身上升到一个新的台阶。

精准医疗是医疗观念和技术的革命。未来医疗服务将更多地运用 PHR 从而选择对个体最有效的治疗解决方案，而非粗略的使用一般性方法进行诊治。随着 Genkicell 链上数据真实可信数据的不断增加，PHR 的丰富性和数据价值将逐级倍增。我们甚至可能勾画出每个人的健康图谱，并在疾病发生前做到有效预测进行及时预防。

GenkiCell



第六章 总结

我们已经提出了一个不需要第三方信任的诊断数据标记以及统计数据收集的
系统，我们通过加密机制的设计以及诊断过程中的独立标记流程设计，可以有效地
避免诊断过程中对于结果的互相影响，从而保证了数据标记的正确性。又通过标记
正确性的奖惩机制的设计，来激励各方节点来尽最大努力提供更多的正确和大量的
标记结果。通过上述标记生成的正确的数据，又可以通过系统被各个需要收集数据
的机构购买。整个系统的定价支付与奖励数额通过算法定义并被自动执行，对于系
统的各方努力都提供奖励，从而保证了整个经济体系的有序流转。



第七章 团队及顾问人士



栗田 翔太 Shota Awada

CEO 立命馆大学硕士

东利多财团少东家。2009 加入 Synergy Marketing, , 从事云服务业务企业客户管理系统和网络营销推广销售工作, 为多家日本及海外医院客户提供数据存储、管理与分析服务。

2013 年成立安达株式会社并进入中国市场, 期间担任董事一职, 负责公司整体商务、营销工作, 并参与了城市政策论坛, 任内积极拓展了跨国商业合作, 在 To B、C 端业务精湛, 同时在日本拥有极大合作资源。

2017 年 与日本乐天股份有限公司合作共同参与跨境医疗业务, 同时与日本相关公司合作, 拓展物联网健康设备研发生产业务。

同年, 与原日本厚生劳动省老健局局长中村秀一、原内阁参事官、厚生劳动省大臣官房长大谷泰夫及原日本 NTT 集团前副社长宇治则孝等人共同创立 JCDA (日本高龄社会预防医疗研究协会), 并担任理事一职, 全面负责并管理社团机构工作。



四条 能伸 Yoshinobu Shijo

CTO 大阪大学硕士

原软银（Softbank）旗下金融财团 SBI 虚拟货币公司 LastRoots CTO。

自主设计，研发，并发行上市了数字货币 c0ban，同时为其打造了专属的日元 / c0ban 交易平台，日本天才技术协会会员。



吉田 圭一郎 Keichiro Yoshida

COO 北京大学 MBA

北京大学日本人留学生会第 7 代会长，原职野村证券高级分析师，曾在日本风险基金负责日本医疗项目的 M&A，对医疗健康类项目有着丰富的管理经验，并精通中日英三国语言，在中日两国政界有着极强的人脉关系。



佐々木 太裕 Sasaki Daisuke

CRO

原日本三大银行之一的瑞穗银行融资部经理，后进入瑞穗证券风控部门，主管上市公司的资金审查等业务。2011 年获瑞穗银行营业部最优秀奖，2012 年获瑞穗银行法人部门最优秀奖，2013 年担任瑞穗银行对软银集团债券顾问，同年度调度资金 2000 亿日元，2015 年后获瑞穗证券社长奖后独立出来，成立自己的投资顾问公司，年间调度资金 100 亿日元的同时为客户提供优质的风控服务。

**柴田 諭 Shinada Satohe****日本政策研究咨询顾问**

曾担任原自治大臣佐藤观树的秘书，成为政治家，在政界积攒了一系列的人脉，2006 年后，独立成立了咨询公司，为东急集团、Cyber agent 集团等知名企业提供各类资讯服务。

**藤井 伸一 Shinichi Fujii****媒体运营特聘专员**

1992 年创立株式会社 DR 后，多年从事广告代理，广告企划业务与日本大型的艺人事务所，电视台，出版社有着很深的联系。公司平均年收 75 亿日元。于 2017 年卸任所有职务加入团队。

**Charles Li****市场运营顾问**

日本著名私立大学早稻田大学政治经济系毕业，原日本烟草（Corporate Venture Capital）大中华地区、美国地区负责人。主要负责于区块链，人工智能，大健康等项目的投资运营。同时，负责执行并管理日本烟草与 NASA 合作的健康项目。



JCDA

日本高龄社会预防医疗研究协会

理事长：中村 秀一

理事成员（部分）：栗田 翔太、大谷 泰夫、宇治 则孝、
一般社団法人医疗看护政策研究中心等。

主要是构思研究针对于高龄社会带来的慢性病的解决方案，运用人工智能和 IOE（internet of everything）的手段来预防和检测疾病的机构。

理事长中村秀一先生曾担任厚生劳动省老健局长一职，常年工作于医疗健康行业，致力于推动健康行业的进步与发展。

大谷泰夫先生曾担任国立研究开发法人，日本医疗研究机构理事，其早年曾在政界担任内阁参事官、厚生劳动省雇用均等-儿童家庭局长、厚生劳动省大臣官房长、厚生劳动省医政局长等职务。

宇治则孝先生长期担任 NTT 集团前副社长，现任企业情报推进协会会长，在信息科技业内具有极强影响力。

GenkiCell



第八章 GCL 分配细则

经过我们团队讨论，确定如下分配方案：

公开兑换：30%

本次通证将有 30%比例的 Token 在公开市场上以 ETH 兑换 GCL 的形式发行。

早期天使：10%

10%比例的通证将向全球顶级投资机构进行 ETH 兑换 GCL 发行。

基金会社区发展：10%

本次通证有 10%将作为 Genkicell Chain 基金会的社区建设，将用于进行商务拓展、媒体报道、技术社区建设、教育合作等。

团队持有：10%

初始团队将有 10%的通证奖励，冻结及解冻方案见下文。

挖矿生成：40%

本次将保留 40%的通证作为挖矿奖励。

比例	数量	分配方案
30%	18 亿	Token 公开兑换发行
10%	6 亿	全球顶级投资机构兑换
10%	6 亿	基金会社区发展预留
10%	6 亿	创始团队成员早期持有
40%	24 亿	挖矿生成
Total：	60 亿	



团队的 GCL 按照如下计划释放

阶段	释放比例
2019/1/1	2%, 12,000 万枚 GCL 通证
2020/1/1	2%, 12,000 万枚 GCL 通证
2021/1/1	2%, 12,000 万枚 GCL 通证
2022/1/1	2%, 12,000 万枚 GCL 通证
2023/1/1	2%, 12,000 万枚 GCL 通证



第九章 里程碑计划

2017.02	1.Genkicell Chain 项目计划启动
2017.06	1.与日本各医疗机构、健康协会达成意向，启动医疗健康大数据收集共享计划
2017.10	1.初版 Genkicell Chain 完成，并启动日本金融厅登入计划
2018.01	1.与日本 JCDA 开始合作，启动基于区块链及大数据技术的预防医疗联合实验计划
2018.03	1.Genkicell 白皮书 v1.3 版发布 2.启动 Pre 轮通证兑换
2018.04	1.完成 Pre 轮通证路演 2.完成官方网站建设
2018.05	1.路演以及相关宣传完成 2.启动公开通证兑换计划
2018.06	1.完成公开兑换计划 2.选择相关交易所登录
2018.Q3	1. 进一步引进人才 2.组织并召开一系列学术闭门会议（大健康+区块链） 3.组织研发社区 4.开始初步研发 5.项目季度相关信息公布
2018.Q4	1.初步架构设计搭建 2.搭建业务逻辑相关代码 3.GCL 推广与医疗机构以及研究机构洽谈 4.钱包的研发启动 5.项目季度相关信息公布 6.与日本一流大学合作建立区块链研究实验室
2019.Q1	1.与相关的人工智能结构洽谈合作 2.搭建相关智能医疗的模块 3.主链开发完成，进入测试 4.项目季度相关信息公布
2019.Q2	1.修复相关问题 2.预计主链开发完成上线并公开源代码



第十章 免责声明

本文档只用于传达信息之用途，并不构成买卖项目股份或证券的相关意见。任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其他相关法律允许下进行，以上信息或分析不构成投资决策或具体建议。

本文档不构成任何关于证券形式的投资建议，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行为，或任何邀请买卖、任何形式证券的行为，也不是任何形式上的合约或者承诺。

本文档中所有的收益和利润举例仅为展示目的，或代表行业平均值，并不构成对用户参与结果的保证。

Genkicell Chain 明确表示相关意向用户明确了解 Genkicell Chain 平台的风险，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。

Genkicell Chain 明确表示不承担任何参与 Genkicell Chain 项目造成的直接或间接的损失包括：

- 1) 本文档提供所有信息的可靠性
- 2) 由此产生的任何错误，疏忽或者不准确信息
- 3) 或由此导致的任何行为。

GCL 是以 Genkicell Chain 平台为其使用场景之一的数字通证。GCL 不是一种投资。我们无法保证 GCL 将会增值，其也有可能某种情况下出现价值下降。鉴于不可预知的情况，本白皮书列出的目标可能发生变化。虽然团队会尽力实现本白皮书的所有目标，但所有购买 GCL 的个人和团体将自担风险。

GCL 是以 Genkicell Chain 平台为其使用场景之一的数字通证，通证兑换之行为将遵循各国法律法规，所有兑换本通证的个人和团体需知悉其当地法律法规，目前暂不接受中国大陆籍、美国国籍、在日本及日本国籍个人投资人士兑换。

本文档以最终版本为准，根据市场和项目进程，不定期会有更新版本出现。



第十一章 风险提示

数字资产投资作为一种新的投资模式，存在各种不同的风险，潜在投资者需谨慎评估投资风险及自身风险的承受能力：

1. 通证销售市场风险

由于通证销售市场环境是整个数字货币市场形势密不可分，如市场行情整体低迷，或存在其他不可控因素的影响，则可能造成通证本身即使具备良好的前景，但价格依然长期处于被低估的状态。

2. 监管风险

由于区块链的发展尚处早期，并且目前政策会如何实施尚不明朗，这些因素均可能对项目的投资与流动性产生不确定影响。而区块链技术已经 成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则 GCL 链应用或 Genkicell Chain 可能受到其影响，例如法令限制使用、销售通证诸如 Genkicell Chain 有可能受到限制、阻碍甚至直接终止 Genkicell Chain 应用和 Genkicell Chain 的发展。

3. 竞争风险

随着信息技术和移动互联网的发展，以“比特币”为代表的数字资产逐渐兴起，各类去中心化的应用持续涌现，行业内竞争日趋激烈。但随着其他应用平台的层出不穷和不断扩张，社区将面临持续的运营压力和一定的市场竞争风险。

4. 私钥丢失风险

购买者的通证在提取到自己的数字钱包地址后，操作地址内所包含内容的唯一方式就是购买者相关密钥(即私钥或是钱包密码)。用户个人负责保护相关密钥，用于签署证明资产所有权的交易。用户理解并接受，如果他的私钥文件或密码分别丢失或被盗，则获得的与用户账户 (地址) 或密码相关的 GCL 将不可恢复，并将永久丢失。最好的安全储存登录凭证的方式是购买者将密钥分开到一个或数个地方安全储存，且最好不要储存在公用电脑。



5. 黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 Genkicell Chain 应用或 Genkicell Chain 功能的可能性，包括但不限于拒绝服务攻击、Sybil 攻击、游袭、恶意软件攻击或一致性攻击等。

6. 未保险损失的风险

不像银行账户或其它金融机构的账户，存储在 GCL 账户或相关区块链网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保。

7. 系统性风险

开源软件中被忽视的致命缺陷或全球网络基础设施大规模故障造成的风险。虽然其中部分风险将随着时间的推移大幅度减轻，比如修复漏洞和突破计算瓶颈，但其他部分风险依然不可预测，比如可能导致部分或全球互联网中断的政治因素或自然灾害。

8. 不被认可或缺乏使用者的风险

首先，GCL 不应该被当作一种投资，虽然 GCL 在一定的时间后可能会有一定的价值，但如果 GCL 链不被市场所认可从而缺乏使用者的话，这种价值可能非常小。有可能发生的是，由于任何可能的原因，包括但不限于商业关系或营销战略的失败，GCL 链平台和所有的众售资金支持的后续营销将不能取得成功。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对本项目而言是非常不利的。

9. 应用存在的故障风险

GCL 链平台可能因各方面可知或不可知的原因故障(如大规模节点宕机)，无法正常提供服务，严重时可能导致用户 GCL 的丢失。

10. 应用或产品达不到自身或购买者的预期的风险

Genkicell Chain 应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何 Genkicell Chain 自身或购买者对 GCL 链应用或 Genkicell Chain



的功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，一个设计的改变等均有可能导致这种情况的发生。

11. 无法预料的其它风险

基于密码学的通证是一种全新且未经测试的技术，除了本白皮书内提及的风险外，此外还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其它风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。



参考文献

- Agorise. (2018). *c-ipfs : IPFS implementation in C. Why C? Think Bitshares Stealth backups, OpenWrt routers (decentralize the internet), Android TV, decentralized Media, decentralized websites, decent..* *GitHub*. Retrieved 5 October 2017, from <https://github.com/Agorise/c-ipfs>
- Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., & Accenture, L. (2016). Blockchain: Securing a New Health Interoperability Experience.
- Buterin, V. (2018). *Slasher: A Punitive Proof-of-Stake Algorithm - Ethereum Blog. Ethereum Blog*. Retrieved 19 October 2017, from <https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/>
- Culver, K. (2016). Blockchain Technologies: A whitepaper discussing how the claims process can be improved. In *In ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST.
- Ekblaw, A., Azaria, A., Halamka, J., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data (p. 13).
- Finley, K. (2016). *The Inventors of the Internet Are Trying to Build a Truly Permanent Web. WIRED*. Retrieved 19 February 2018, from <https://www.wired.com/2016/06/inventors-internet-trying-build-truly-permanent-web/>



- Hazard, J., & Hardjono, T. (2016). *CommonAccord: Towards a Foundation for Smart Contracts in Future Blockchains*. W3.org. Retrieved 19 February 2017, from <https://www.w3.org/2016/04/blockchain-workshop/interest/hazard-hardjono.html>
- Ivan, D. (2016). Moving toward a blockchain-based method for the secure storage of patient records. In *In ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST.
- Kobayashi, D., Otsubo, T., & Imanaka, Y. (2015). The effect of centralization of health care services on travel time and its equality. *Health Policy*, 119(3), 298-306. <http://dx.doi.org/10.1016/j.healthpol.2014.11.008>
- Koo, Charles, C., & Yuh-Ming Shyy. (2005). Medical records data security system. U.S.
- Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *In Security and Privacy (SP)* (pp. 839-858).
- Kuo, T., & Ohno-Machado, L. (2018). *ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks*.
- Lamport, L. (1979). Constructing digital signatures from a one-way function. In *Technical Report SRI-CSL-98*. SRI International Computer Science Laboratory.
- Leftwich, R. (2016). *The Path to Deriving Clinical Value from FHIR | InterSystems Corporation*. InterSystems Corporation. Retrieved 19 September 2017,



from <http://www.intersystems.com/library/library-item/path-deriving-clinical-value-fhir/>

Linn, L., & Koo, M. (2016). Blockchain for health data and its potential use in health IT and health care related research. In *In ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST.

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. (pp. 1-10). In Proc. NIST Workshop Blockchain Healthcare.

Price, M., Bellwood, P., Kitson, N., Davies, I., Weber, J., & Lau, F. (2015). Conditions potentially sensitive to a Personal Health Record (PHR) intervention, a systematic review. *BMC Medical Informatics And Decision Making*, 15(1). <http://dx.doi.org/10.1186/s12911-015-0159-1>

Raval, S. (2016). *Decentralized applications: Harnessing Bitcoin's Blockchain Technology*. Sebastopol: O'Reilly.

Rawat, A., Papailiopoulos, D., Dimakis, A., & Vishwanath, S. (2016). Locality and Availability in Distributed Storage. *IEEE Transactions On Information Theory*, 62(8), 4481-4493. <http://dx.doi.org/10.1109/tit.2016.2524510>

Satoshi Nakamoto. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Shrier, A., Chang, A., Diakun-thibault, N., Forni, L., Landa, F., Mayo, J., & Hardjono, T. (2016). Blockchain and Health IT: Algorithms, Privacy, and Data. In *In ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST.



- Underwood, S. (2016). Blockchain beyond bitcoin. *Communications Of The ACM*, 59(11), 15-17. <http://dx.doi.org/10.1145/2994581>
- Van Panhuis, W., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., & Herbst, A. et al. (2014). A systematic review of barriers to data sharing in public health. *BMC Public Health*, 14(1). <http://dx.doi.org/10.1186/1471-2458-14-1144>
- Yang, J., Li, J., & Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems*, 43-44, 74-86. <http://dx.doi.org/10.1016/j.future.2014.06.004>

