（公信链）

GXChain WHITEPAPER 3.0

可信数据的价值网络

2018-10-10

引言

GXChain(公信链) 是一条为全球数据经济服务的基础链，旨在打造可信数据的价值网络。

本项目自 2016 年正式成立以来，经历了快速的发展，已经从创立之初一个基于区块链的去中心化数据交易所（已于 2017 年正式上线且商用），进化成为一个服务着数百万用户和开发者的基础链，从服务于一个具体的数据业务场景进化到服务于全球数据经济。

为了适应项目的不断进化，让关注本项目的社区用户、开发者和同业研究者对 GXChain 有全貌式的理解，我们在不断升级更新项目的白皮书，力求对项目的发展现状和未来方向有及时且客观的呈现。

本次 3.0 版本的 GXChain (公信链) 白皮书，在以下几个方面有重要更新：

◇ 明确了 GXChain 的治理架构，推进主链治理的民主、透明和去中心化，这标志着 GXChain 已经度过了早期的团队运营阶段，逐渐向社区化治理过渡，有助于进一步扩大和凝聚共识。

◇ 公布了 GXChain 的节点竞选规则和收益方案，竞选机制将带来节点的分散，提升主网出块的稳定和安全，后续节点竞选正式启动，也将引入全球有技术和社区号召力的团队融入 GXChain 生态参与竞争和治理，提升 GXChain 的全球影响力。

◇ 以更清晰的方式梳理和呈现了 GXChain 的系统层次结构和技术方案，重点阐述了智能合约 2.0、预言机、跨链等合约层设计和实现，介绍了可信数据组件多个组成部分的技术方案，对 GXChain 可信数据价值网络的业务场景进行了举例说明，为开发者提供了落地应用开发的场景指导。

◇ 将原有基于 GXChain 发行的 Token — GXS，1:1 自动替换为 GXC，GXC 将作为 GXChain 的主链核心资产 (Core Asset)，成为 GXChain 最重要的治理和应用通证，后续 GXChain 生态中治理、开发、应用、支付流通场景均以核心资产 GXC 为媒介。

◇ 系统阐述了 GXC 的经济模型、价值、产出及分发机制，明确了 GXC 的价值内涵和成长空间。

◇ 公布了 GXChain 后续的技术开发路线图，聚焦主线任务提升 GXChain 在技术上的竞争力，同时便于社区监督开发进度和开发者加入协作。

目录

序章

数据经济之困

大数据时代已经来临，随着 5G、AI、IOT 等技术的逐步成熟，人类社会产生、获得和处理数据的量级和能力将迎来全新的跃升，数据经济也会来到一个全新的发展阶段。通过对数据的合理应用，我们对世界的认知水平、对需求的响应速度、对商业和社会活动的规划能力，人与人的协作效率都将提升到一个新的高度。

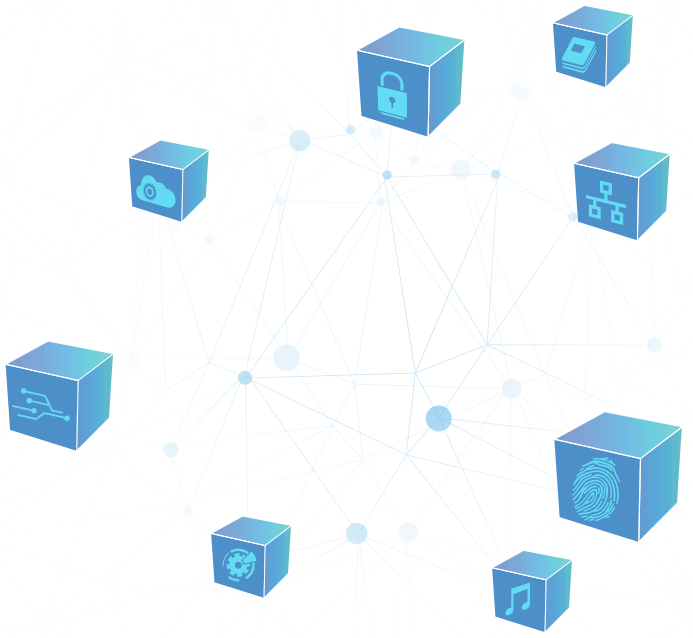
数据经济的快速发展过程，是围绕着计算机技术和互联网为基石演进的，而互联网公司作为其中的关键角色，则在不断地拓展着数据获取、分析和运用的疆域，实现了数据在众多场景中更高效的应用。可以说，传统的互联网模式，为数据的海量获取、便捷储存、分析运用和交换流转打下了坚实的地基。整个世界都在数据化，整个世界的数据都在联网化，但随着数据经济向纵深处发展和演化，数据经济也面临着几大挑战。

首先是数据所有权的挑战。随着个人数据在更多商业场景中的应用，数据价值巨大已成为全社会的共识，也成为商业竞争的重要资源。尽管在全球范围内，将个人数据的所有权归属于产生数据的个人，已经是大势所趋（如 2018 欧洲 GDPR 法规的颁布和执行），但是由于个人缺少管理自己数据的便捷手段和有效激励方案，在目前的传统互联网生态下，要做到“个人数据由个人管理”的大众化，依旧困难重重。此外，从全社会的经济效用来看，严控商业公司对个人数据的使用和开发，也造成了数据资源的浪费，妨碍了数据这一重要资源在全社会范围内有效配置。数据经济生态亟需一个既能保障用户数据所有权（意味着能使用自己的数据、分享自己的数据、从自己的数据分享中获得价值），又能让数据资源被有效应用的两全方案。

其次，是数据处理和交换中的泄露问题。从 facebook 用户数据被盗用，到华住酒店集团 5 亿条数据被窃取后在暗网甩卖，互联网商业机构中心化的数据储存和使用方案，始终逃脱不了数据被滥用的道德风险和被攻击的安全风险。这不但给个人隐私带来了极大危险，让我们稍有不慎就变成了“网络透明人”，也给企业造成了高昂的安全成本。数据安全事件的一再爆发，也令公众对大数据从趋之若鹜变为谈虎色变。

其三，数据的真伪和质量问题。大数据时代的阳光背后，是垃圾数据泛滥的行业阴影。由于现有数据的中心化管理模式，使得无论是企业还是个人，验证数据真实性都需要极高的成本，可达的渠道非常少。数据作为重要生产资料的鉴真困难所带来的成本，极大地拖累数据经济的协作效率。

其四，数据激励问题。个人数据未来仍将是数据的主要来源，目前大部分公众对个人数据的搜集、管理的动机不足，核心在于激励不足，感受不到数据的价值。单体的个人数据虽然微小，但就像数据经济的毛细血管，占据了人体血管的 97%，只有激活个人对数据的搜集、管理和应用意识，数据经济才能获得更多新鲜的血液。目前的数据生态里，个人是数据的产生和贡献方，但是互联网公司却切走了数据经济中的大部分蛋糕，如果有更好的、能获得多方共识的数据利益分配方案，不但个人能从数据的生产和分享中获得激励，企业也将合法地获得更多维度的数据，做大数据经济的整体规模。



GXChain 的实践与愿景

要解决这些在数据经济中普遍存在的核心问题，需要重构传统互联网机构对于数据搜集、储存、计算和交换的方式，需要新一代的数据经济基础设施。 更具体来说，解决数据经济面临的困境，我们需要一个透明、去中心、高效、能达成共识的数据基础服务和网络。

GXChain 就是这样一条面向未来的数据经济基础链，基于区块链的分布式特性、密码学等技术手段和通证设计，为数据经济的发展提供了全新的区块链解决思路，引领了数据服务的新变革。在项目成立的 2 年多来，围绕现有数据经济中的数据所有权分配、数据泄露、数据真伪和数据激励等问题，GXChain 团队开发了丰富的可信数据组件，逐渐打通数据上链、数据储存、数据计算、数据交换的各个环节，并且已经有了众多落地的应用和实践。

也正是基于数据经济必将整体改造人类社会效率、构建信任社会的信念，GXChain 团队在两年间根据路线图逐一兑现了自己的承诺，完成了底层基础链、去中心化数据交易所、布洛克城等众多产品和服务于开发者的数据组件。未来，GXChain 也将继续专注于服务数据经济发展的创新与实践，为人类未来千万亿级的数据经济市场提供共享、共治、透明、安全的底层服务，成为人类全民数字化时代的公共设施。

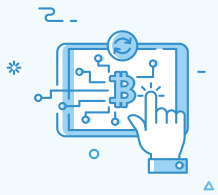
1. 治理架构

1.1. 治理架构与机制

“治理”是公链的核心命题，一个去中心化治理的公链才会有最长久的生命力。GXChain 通过链上与链下治理的结合将人与代码同时引入到公链的复杂治理体系中去，从而在实现治理的去中心化的同时保证治理的有效性。每一位 GXChain 资产持有者都有参与去中心化治理的权利。公链生态中的运营和发展方向，都会由全体 GXC 持有者以协商投票的方式来决定。

GXChain 的链上治理结构由理事会 (Committee) 和公信节点 (TrustNode) 构成。链上理事会由 11 名成员组成，可以提议修改 GXChain 的动态全局参数。公信节点由 21 名节点成员组成，负责 GXChain 网络的交易记账、交易验证、区块打包和确认等工作。

链上治理



理事会 Committee

- 相当于链上的董事会，负责 GXChain 区块、交易、手续费等全局参数的提案发起和投票
- 由 11 名成员组成，每名成员必须是公信节点之一

公信节点 TrustNode

- 矿工，负责 GXChain 的交易记账、交易验证、区块打包和确认等工作
- 至少由 21 名节点成员组成，前 11 个公信节点自动成为理事会成员

链下治理

GXChain 基金会

- 注册于新加坡的非盈利性组织
- 由决策委员会，顾问委员会、执行委员会、生态建设委员会等 7 个部门组成
- 负责 GXChain 的重大决策、技术开发、全球推广、财务管理和会议组织

图 1.1GXChain 治理架构

1.2. 链上治理—GXChain 理事会和公信节点

GXChain 的链上治理是通过 GXChain 理事会和公信节点实现的。GXC 持币人可通过公信节点去方便、快捷地行使GXChain 的治理权。GXChain 的生态内有 21 个公信节点，为 GXChain 提供网络、存储和计算等基础设施。GXChain 鼓励每一个公信节点构建自身的社区，使得每一个公信节点的社区都能在相互竞争中共同发展，壮大 GXChain 生态。公信节点按得票数的前 11 名当选为 GXChain 理事会成员，它是 GXChain 社区的核心链上治理组织。

1.2.1.GXChain 理事会和公信节点

在 GXChain 的治理生态中有如下三个角色：

1) 持币者：持有任意数量 GXC 的个体或机构。

2) 公信节点：由全体 GXC 持币者投票选举出的个体或机构，每 1 小时统计一次投票，共有 21 个公信节点。节点竞选投票中，得票数排名前 21 的成为公信节点。 公信节点负责 GXChain 网络的交易验证、交易记账、区块打包和确认等工作，成功打包区块将获得对应的奖励。公信节点接受 GXChain 社区的监督。

3) GXChain 理事会：公信节点按得票数的前 11 名当选为 GXChain 理事会成员。

GXChain 理事会是 GXChain 社区的核心链上治理组织，主要职责是设定合理的公链全局参数，以此促进 GXChain 长期的健康发展。其中包括：

1) 修改区块链的动态参数，比如区块大小、区块间隔等；

2) 公信节点出块奖励、公信节点数量和活跃理事会成员数量等；

3) 转账、发行资产及各类交易手续费；

4) 智能合约的创建和调用费率等。

1.2.2. 公信节点竞选规则

每一位 GXC 持币者都可成为公信节点的竞选者。竞选者需要向系统抵押 1 万 GXC(具体金额由理事会投票决定)，退出竞选时可在 30 天后 (系统动态参数，可由理事会投票调整) 取回。若节点作恶，其抵押的 GXC 可由理事会投票处理。为了保障节点竞选的高效进行，GXChain 针对公信节点候选人制定了一系列的标准和规则。由 GXChain 基金会的生态建设委员会 (GXChain-ECO) 根据标准和规则对候选节点进行审核。公信节点候选人必须符合以下基本条件：

1）具有合法设立的组织主体，且拥有官网及公共自媒体平台账号；

2）具有可供社区成员测试的节点；

3）拥有可运行节点的服务器和节点运维技术；

4）创建公信节点，需要抵押一定数量的 GXC，若取回抵押的 GXC，则视为退出竞选；

5）已制定未来三年的预算支持，技术方案，硬件扩容以及社区支持计划；

6）拥有一定规模的社区用户。

1.2.3. 节点收益

公信节点的收益主要来自出块奖励，由理事会投票决定出块奖励金额。在每一次区块打包完成之后，公信节点将获得相应的出块奖励。出块奖励池子由转账手续费以及基金会捐赠节点奖励两部分构成。为激励公信节点在 GXChain 生态中做出的积极贡献，GXChain 基金会将捐赠 400 万枚 GXC 注入系统资金池作为节点出块奖励，奖励分 8 年发放，每年释放 50 万枚。

1.2.4. 公信节点投票产生方式

每一个 GXC 视为一票，可为多个候选节点投票。参与公信节点投票的 GXC 将被质押在自己的钱包，如果资产转出，则视为撤票。累计票数排名前 20 名节点自动当选为公信节点，第 21 个节点从剩余的备选节点中随机产生。 投票途径主要有 3 种：

1) 布洛克城投票
在布洛克城钱包中的 GXC，可通过布洛克城的投票通道进行公信节点的投票。

2) 手机钱包和 PC 钱包投票
在 GXChain 手机钱包和 PC 钱包中的 GXC 可进行公信节点的投票。

3) 交易所投票
如果用户的 GXC 在交易所钱包里，且该交易所支持 GXChain 的公信节点投票，便可以采用此方式进行投票。

1.3. 链下治理—GXChain 基金会

1.3.1.GXChain 基金会的设立

GXChain 基金会于 2017 年 11 月在新加坡正式成立，全称为 GXChain foundation LTD.，旨在通过科学、合理、有效的治理机制推动并维系基金会及 GXChain 生态的建设和健康发展，为 GXC 持币者提供合适的保护和平等权利，构建 GXC 持币者、社区、节点、dApps 开发者等不同角色之间的高效沟通渠道。

GXChain 基金会每年将向社区披露 GXChain 的开发情况、运营情况、GXC 的使用情况等，并将引入第三方审计机构，监督项目的财务运作，审计报告将在年度信息披露中公告。

1.3.2.GXChain 基金会的组织架构

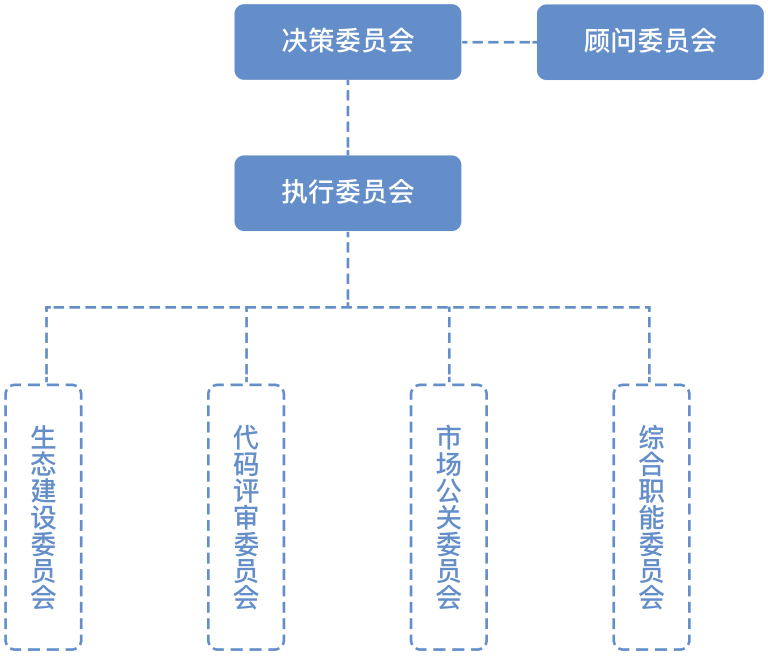


图 1.2 GXChain 基金会组织架构

1.3.3. 决策委员会

1.3.3.1. 简介

决策委员会是 GXChain 基金会的决策机构。

1.3.3.2. 人员组成

决策委员会由 11 名成员组成，包含主要发起人、开发者代表、投资者代表及社区代表，设主席、副主席、执行总裁各一人，从决策委员会成员中选举产生，其他代表名额不固定。

1.3.3.3. 人员介绍

决策委员会成员由选举产生，存在人员名单不确定性，具体名单请以 gxchain.org 官网公布的为准。

1.3.3.4. 议事规则

决策委员会至少每年召开一次会议，由决策委员会主席负责召集并主持，于会议召开 30 日前通知全体成员，决策委员会会议需由 1/2 以上的成员出席方可举行。决策委员会会议中，一般事项的决议须经出席成员 2/3 以上表决通过，特殊事项还须经决策委员会主席投赞成票方为有效。任何需决策委员会决议的事项，如决策委员会成员以书面形式一致表示同意的，可以不召开决策委员会会议，直接作出决定，并由全体成员在决定文件上签名。

1.3.3.5. 主要职权

决策委员会主要行使下列职权：

(1) 制定、修改基金会治理机制；
(2) 选举、罢免主席或副主席；
(3) 根据主席的提名选举执行总裁、副总裁和其他执行委员会成员；
(4) 决定基金会的经营计划和投资方案；
(5) 年度收支预算、决算及资金分配方案审定；
(6) 通过授予荣誉职务（包括聘请名誉主席和顾问），增减顾问委员会成员；
(7) 决定设立办事机构、分支机构、代表机构；
(8) 听取、审议主席所做的工作报告，检查执行总裁的工作；
(9) 决定基金会的分立、合并或终止；
(10) 决定其他重大事项。

其中，有关第 (1)、(4)、(5)、(9) 项的决议属于特殊事项。

1.3.3.6. 任职资格

决策委员会成员需具备下列条件：

(1) 有加入基金会的较强意愿，认同基金会的宗旨；
(2) 在基金会的业务领域或社区内，具有一定影响力；
(3) 对基金会的发展壮大，有所帮助或有所贡献者；
(4) 无任何违法犯罪记录。

1.3.3.7. 人员的产生和罢免

(1) 第一届决策委员会成员由主要发起人、开发者代表、投资者代表分别提名并共同协商确定；
(2) 决策委员会换届改选时，由决策委员会提前 60 日发布公告公布成员资格条件及改选规则等事项，面向全体 GXC 持有人征集候选人，最终由 GXC 持有人进行投票，选举产生新一届决策委员会成员；
(3) 决策委员会成员需在任职期间接受授信调查，并公开薪酬情况；
(4) 任何成员因违反基金会制度、损害基金会声誉或给基金会事业造成损失等，经决策委员会审议后终止任职；
(5) 任何成员因违法、违纪受到处理，职务即时终止；任何成员因涉嫌犯罪被起诉或接受调查，决策委员会合理地认为该成员继续担任职务可能影响基金会声誉或形象的，经决策委员会审议后终止任职；
(6) 任何成员自动请辞，死亡或因疾病、意外事故等丧失工作能力的，经决策委员会审议后终止任职。

1.3.3.8. 任期

决策委员会成员每届任期为 2 年，任期届满，连选可以连任。

1.3.3.9. 主席、副主席主要职权

决策委员会主席主要行使下列职权：

(1) 召集和主持决策委员会会议并组织实施；
(2) 提议召开临时决策委员会会议；
(3) 代表基金会签署重要文件，检查决策委员会决议的落实情况；
(4) 对重大突发事件进行紧急决策；
(5) 提名执行总裁、副总裁和其他执行委员会成员的候选人，各项职务应至少提名 2 位候选人供决策委员会选定。

副主席在主席领导下开展工作，经主席书面授权可代主席行使相关职权。

1.3.4. 顾问委员会

1.3.4.1. 简介

顾问委员会是 GXChain 基金会的专家顾问团，由决策委员会挑选业务相关专业领域内较具有影响力的人员组成，包括但不限于技术专家、资深投资人、资深律师等，为基金会运营管理事务提供咨询与指导。

1.3.4.2. 人员组成

不超过 7 名，由决策委员会选定。

1.3.4.3. 人员介绍

顾问委员会存在人员名单不确定性，具体名单请以 gxchain.org 官网公布的为准。

1.3.4.4. 主要职权

顾问委员会主要行使下列职权：

> (1) 为基金会运营管理事务提供咨询与指导；
> (2) 受决策委员会邀请可列席决策委员会会议，但不具备投票权。

1.3.4.5. 任职资格

顾问委员会人员需具备下列条件：

> (1) 在基金会的业务相关专业领域内，具有一定影响力；
> (2) 无任何违法犯罪记录。

1.3.4.6. 人员的产生和罢免

(1) 由决策委员会挑选并授予荣誉职务，包括聘请名誉主席、顾问等；
(2) 因违反基金会制度、损害基金会声誉或给基金会事业造成损失等，经决策委员会审议后终止任职；
(3) 因违法、违纪受到处理，职务即时终止；因涉嫌犯罪被起诉或接受调查，决策委员会合理地认为该人员继续担任职务可能影响基金会声誉或形象的，经决策委员会审议后终止任职；
(4) 自动请辞，死亡或因疾病、意外事故等丧失工作能力的，经决策委员会审议后终止任职。

1.3.5. 执行委员会

1.3.5.1. 简介

执行委员会是 GXChain 基金会的执行机构，负责基金会日常运营管理事务的具体执行，设执行总裁一人，其他执行委员会成员在执行总裁领导下开展工作，指导并管理下属专门委员会工作。

1.3.5.2. 人员组成

执行总裁、副总裁、秘书及各专门委员会负责人

1.3.5.3. 人员介绍

执行委员会存在人员名单不确定性，具体名单请以 gxchain.org 官网公布的为准。

1.3.5.4. 主要职权

执行委员会主要行使下列职权：

(1) 执行决策委员会的各项决议；
(2) 指导下属专门委员会开展工作；
(3) 决定下属专门委员会人员的聘用与解聘，包括决定其报酬事项；

应对基金会紧急事件，拟定应对方案供决策委员会主席决策。

1.3.5.5. 人员的产生和罢免

(1) 由决策委员会主席提名，经决策委员会审议后选定；

(2) 因违反基金会制度、损害基金会声誉或给基金会事业造成损失等，经决策委员会审议后终止任职；

(3) 因违法、违纪受到处理，职务即时终止；因涉嫌犯罪被起诉或接受调查，决策委员会合理地认为该人员继续担任职务可能影响基金会声誉或形象的，经决策委员会审议后终止任职；

(4) 自动请辞，死亡或因疾病、意外事故等丧失工作能力的，经决策委员会审议后终止任职。

1.3.5.6. 任期

每届任期为 2 年，任期届满，连选可以连任。

1.3.5.7. 执行总裁主要职权

执行总裁主要行使下列职权：

(1) 主持开展基金会日常工作，组织实施年度运营计划，并向决策委员会汇报工作情况；
(2) 拟订基金会的内部管理规章制度，报决策委员会审批；
(3) 协调各下属专门委员会、分支机构开展工作。

1.3.6. 下属专门委员会

1.3.6.1. 生态建设委员会

生态建设委员会负责 GXChain 生态建设相关事宜，包括对 GXChain 上开发者项目的投资、孵化，为构建 GXChain 生态筛选合作伙伴，进行尽职调查并负责后续合作对接工作。

1.3.6.2. 代码评审委员会

代码评审委员会负责 GXChain 底层技术构建、API 服务开发、开发者代码评审、代码合并与 Github 发布等工作。同时，代码评审委员会人员通过定期分享会、不定期交流会等形式保持技术团队紧跟行业趋势，积极研究最新区块链技术。

Github 地址 https://www.github.com/gxchain

1.3.6.3. 市场公关委员会

市场公关委员会负责基金会形象的建立与维护及社区的运营与推广，以及危机公关等工作。

1.3.6.4. 综合职能委员会

综合职能委员会负责基金会日常资金使用的审核与管理、基金会内部人事管理、行政事务管理及法律事务管理等事项。

2. 技术架构

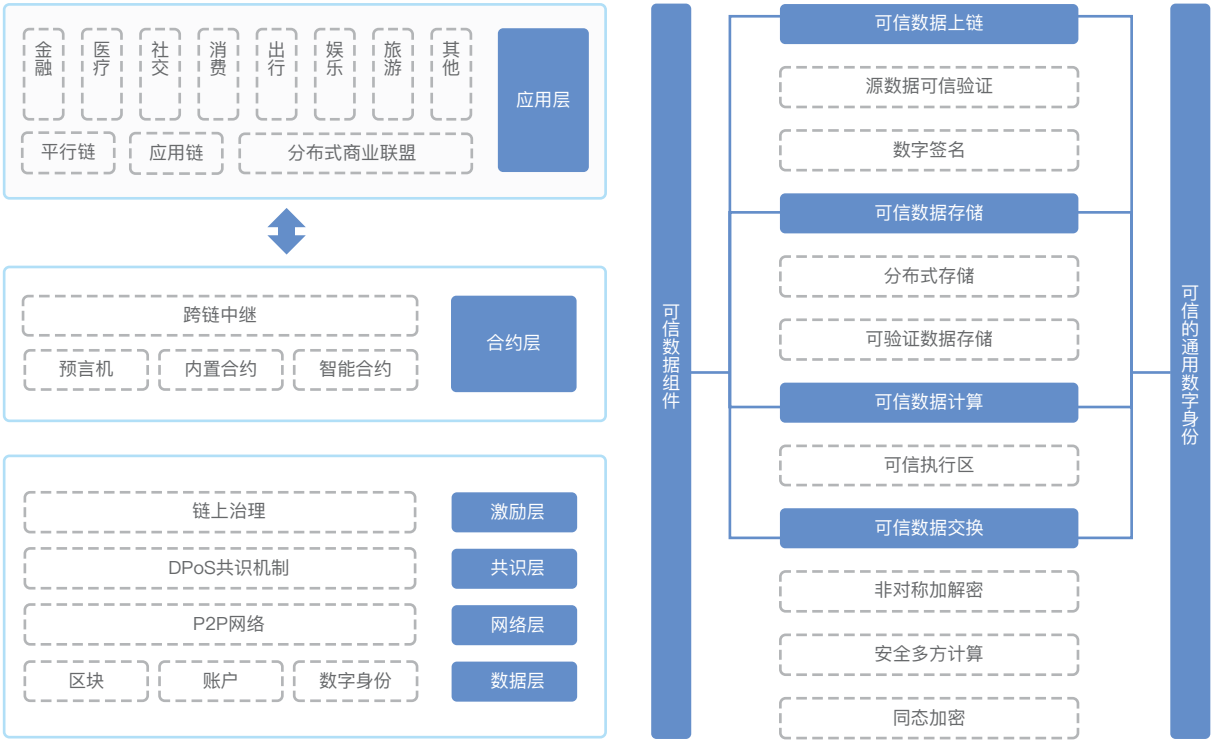


图 2.1 GXChain 技术架构

2.1. 数据层

数据层是区块链模型的最底层，数据层描述了区块的链式结构。在此之外 Graphene 引入了多重签名账户模型的设计，以对象的方式存储在内存中，而 GXChain 在账户模型的基础上，引入数字身份的概念，即 GXChain 上的每个账户，都可以映射到一个唯一的数字身份 (我们称为 G-ID) 上；**区块**、**账户**和**数字身份**，构成了 GXChain 的数据层。

2.2. 网络层

GXChain 的网络是一个由全节点组成的分布式的拓扑网络，网络上的每个节点以点对点的方式相互连接，节点之间彼此对等，每一个节点都可以独立自主的验证所有的区块和交易，不存在特殊节点。P2P 网络是区块链数据层上的重要基础设施；网络层实现了节点在网络中**相互发现、相互连接、相互通信**的底层机制，支撑着 GXChain 区块链系统高效稳定的运转。

2.3. 共识层

GXChain 使用 DPoS 来实现区块链记账和数据交换的共识机制。DPoS(Delegated Proof of Stake) 机制源自于 Graphene，中文名叫做股份授权证明机制 (又称受托人机制)， 它的原理是让全网代币持有人进行投票，由此产生至少 21 位代表作为系统的区块生产者，我们可以将其理解为 21 个 (可无限扩展) 超级节点或者矿池，而这 21 个超级节点彼此的权利是完全相等的。从某种角度来看，DPoS 有点像是议会制度或人民代表大会制度。GXChain 任一出块时间仅有一个代表有权生产区块，如果代表不能履行他们的职责 (在预定一段时间内未能生成区块)，他们会被除名，网络会选出新的公信节点来取代他们。

现有区块链项目的主要共识机制为 PoW(Proof Of Work，工作量证明机制) 和 PoS(Proof of Stake，股份证明机制)，少部分项目采用修改后的 BFT(拜占庭容错) 的共识机制，比特币就是 PoW 机制下最成功的加密货币，PoW 机制虽然已经成功证明了其长期稳定和相对公平，但效率相对低下，以比特币为例，每秒只能处理约 6 笔交易而且还需要消耗大量的能源，不太满足成为基础链的高性能要求；而 PoS 机制下较为成熟的数字货币是 Peercoin(点点币)，相对于 PoW，引入了“币天”这个概念来参与随机运算，由于可能会存在少量大户持有整个网络中大多数代币的情况，整个网络有可能会随着运行时间的增长而越来越趋向于中心化，PoS 机制虽然节省了能源，却也没有很好提升性能和安全性。

为了在保障安全性、去中心化的基础上实现性能的提升，DPoS 机制应声而出。DPoS 机制要求在产生下一个区块之前，必须验证上一个区块已经被受信任节点所签署。相比于 PoS 的“全民挖矿”，DPoS 则是利用类似“代表大会”的制度来直接选取可信任节点，由这些可信任节点 (即见证人) 来代替其他持币人行使权力，见证人节点要求长期在线，从而解决了因为 PoS 签署区块人不是经常在线而可能导致的产块延误等一系列问题。DPoS 机制通常能达到万次每秒的交易速度，在网络延迟低的情况下可以达到十万次每秒级别，非常适合企业级的应用。因为 GXChain 要服务于数据经济，对于可信环境下的数据交换和计算要求非常高，更要求长期稳定性，因此 DPoS 是非常不错的选择。

2.4. 激励层

激励层是公链生态非常重要的一个设定，主要负责激励的发行制度和分配制度，相比于全民挖矿，DPoS 共识机制更注重的是出块节点之间的相互协作和相互监督，这样的机制使得激励层能更高效地发挥作用。

GXChain 的激励层实现了独特的链上治理和激励分配制度：

> a. 基金会将一笔预算托管在一个全局的合约中，通过线性的算法来控制对预算的分配；
> b. 第一阶段，一次性投入了 8 年的预算 (4,000,000GXC)，公信节点每正确地产出一个区块，则可以从这笔预算中领得一笔收入；
> c. 每个公信节点参与的机会是平等的，公信节点需要做的是诚实并高效地推进网络的运行。

2.5. 合约层

GXChain 的合约层由 70 多个**内置合约，智能合约**和**预言机**构成，并在此基础上**实现跨链中继**，从而使得 GXChain 能够和同构和异构链之间实现可信的跨链交互。

2.5.1. 智能合约

GVM 使用 WebAssembly(WASM) 执行智能合约。借助 WebAssembly，开发者可以运用自己熟悉的编程语言编写智能合约，目前支持 C++。为了降低开发者编写智能合约的门槛，GXChain 将在未来支持更多的编程语言。

使用 GXChain 提供的编译工具，可以把 C++ 等高级语言代码编译成 WASM 格式的字节码，然后调用合约部署接口将代码部署在链上。成功部署的智能合约会在区块链上会创建一个智能合约账户，账户中存储了合约的字节码和对应的 ABI(Application Binary Interface)。不同于普通 GXChain 账户，合约账户和资产由合约代码控制，没有私钥。用户调用智能合约，需要指定合约账户名以及合约方法，利用 ABI 和智能合约交互。ABI 是由 GXChain 编译工具生成，包含合约接口、接口参数和持久化存储结构等信息。智能合约的持久化存储，以对象的形式顺序存储在内存中，对象的存储字段及类型由开发者根据业务需要自定义。

为了合理利用区块链资源，每次调用智能合约都需要燃烧一定的矿工费，费用由 3 部分组成：基础费用 (固定)，内存费用 (根据持久存储使用量计费)，CPU 费用 (根据本次调用占用的 CPU 时间计费)，3 种费用的价格和调用合约的 CPU 上限均可通过理事会动态调整。智能合约费用计算规则:

合约部署手续费：基准手续费 + 交易消息体大小 * 单位 KB 费用

```
deploy_fee = basic_fee+transaction_size*price_per_kb
```

合约调用手续费： 基准手续费 + 内存使用量 + cpu 使用量

```
transaction_fee = basic_fee + ram_usage * price_per_kb + cpu_usage * price_per_ms
```

2.5.2. 内置合约

GXChain 将协议层和通用性较强的 70 多种合约都写成了内置合约，非常丰富，这些合约都是 HardCode(硬编码) 在链上的，开发者可以按照合约的接口参数进行调用，对于不符合接口要求的请求会直接拒绝调用，这样的 HardCode 合约虽然失去了一些灵活性，但是却也提升了安全性和稳定性。

2.5.3. 预言机

预言机 (Oracle Machine) 将链外数据可靠、安全的输入到 GXChain，为智能合约和 DApps 的计算提供了极大的便利。

预言机将由 GXChain 系统内置合约和 GXChain 公信节点共同实现。同时 GXChain 有一个 有效的奖惩机制，鼓励公信节点提供真实可靠的外部数据输入 (data feed) 的服务。

2.5.4. 跨链中继层

跨链中继层通过智能合约来实现资产托管和链间交互的基本逻辑，公信节点通过预言机来实现链外状态的输入；通过中继层可以实现 GXChain 和平行链，应用链，去中心化商业联盟等同构和异构链之间的可信交互。

GXChain 的跨链中继层有以下特点：

1）公信节点即中继：GXChain 的公信节点作为全网公平选举的可信节点，除了负责整个网络的交易验证和区块生产之外，还可参与中继层的 data feed 服务，通过预言机来实现外部状态的输入；

2）保证金 / 奖惩机制：GXChain 的公信节点将抵押一定的资产在中继合约中，来提供保证金和兑换服务，所有的其他参与方都可以共同作为监督方来对公信节点的行为进行监督，一旦发现公信节点作恶并且举证成功，则监督方将获得一定份额的举证奖励；

3）预言机多方数据验证：除了保证金和奖惩机制外，为了进一步提高预言机外部参数输入的可信度，GXChain 通过多方参与的方式来实现多重数据的验证；

4）公信节点无手续费：传统的中继模式需要在链上发起大量的广播，从而消耗大量的手续费，而 GXChain 设计了独特的方案来保证公信节点在调用预言机来输入外部参数的时候，无需支付手续费，这样的方案是由**公信节点即中继，保证金 / 奖惩机制**和**多方数据验证**的方式共同保证的。

2.6. 应用层

和传统 OSI 模型中的应用层一样，GXChain 的应用层提供了为应用软件而设的接口，同时提供多种语言的客户端封装，简化调用过程，应用层主要包含以下几个部分：

1) GXClient: 内置合约、智能合约、预言机和跨链交互组件，供应用程序调用
2) DES-SDK: 可信数据交换交互组件，供应用程序调用
3) BaaS-SDK: 可信数据存储交互组件，供应用程序调用
4) CLI_Wallet: 命令行钱包，封装了主链交互 API
5) GXX: GXChain 的智能合约编译工具，可以将智能合约编译成 Webassembly 字节码 (wasm)

通过应用层提供的简化跨链交互组件，可以实现 GXChain 和平行链 (Para-chain)，应用链 (App-chain) 和分布式商业 (Distributed Business) 联盟链 (Consortium Chain) 之间的链间通讯。

2.7. 可信数据组件

2.7.1. 可信的通用数字身份

可信的通用数字身份将是区块链世界的通行证，打通所有区块链的应用，让用户在区块链的世界畅通无阻。去中心化不可篡改的区块链是强化身份之间信任的最好解决方案。数字身份的影响力是巨大的，它不仅能波及到货币所能覆盖的人口范畴，还能涉及到全球每一个人的协作共识。数字身份的背后锚定的是资产所有权、个人信息、个人背景、信用记录以及社会关系等，它和货币一样是需要强信任的。

图 2.2 GXChain G-ID 应用

G-ID(General Identity) 是 GXChain 上可信的通用数字身份，每一位用户在通过 KYC 之后都将在链上获得一个唯一的 G-ID，拥有 G-ID 包括但不限于以下功能：

- ◇ G-ID 将帮助用户记录自己上链的个人数据；
- ◇ G-ID 将帮助用户记录自己在链上的行为和信用；
- ◇ G-ID 将帮助用户打通可跨链的数据和资产交换；
- ◇ G-ID 可以帮助用户实现各个 dApp 之间的快捷登录。

2.7.2. 可信数据上链

区块链作为分布式不可篡改的可信账本，提供了很好的价值存储手段，然而区块链技术本身只是提供了链上数据的不可篡改性，忽略了数据从链下到链上的过程。如何保证这一过程的可信，是 GXChain 可信数据组件要去研究和解决的重要课题之一。

当我们讨论数据本身的可信度的时候，我们会想到通过一些可信的验证方来实现，如在中国个人身份的验证，我们可能会使用公安提供的二要素（姓名 + 身份证号）验证接口；或者说我们的银行卡信息，需要通过银行的接口来进行验证。所以我们认识到，银行和公安这样的中心化信任机构，在某种程度上是不可替代的存在，区块链技术的出现，不是去颠覆这样的信任机制，而是给这样的机制补充更安全和高效的解决方案：

1) 数字签名技术：
如果一个第三方的身份是可信的，那么我们认为他们是可信第三方，通过数字签名技术，可信第三方可以将验证过的数据进行签名，签名既保证了数据被验证后的不可篡改性，同时也包含了可信第三方的身份信息，允许所有的人对这个公开的签名进行身份校验。

2) 源数据可信验证：
GXChain 会提供标准的数据上链组件，数据交换协议，代理记账合约。源数据在数据所有方（个人，企业）确认通过后，用本人私钥对数据加密并签名 dataSign（本人确认），应用方使用数据并对内容生成 checksum（数据验证），调用代理记账合约并把数据绑定到数据所有方的 G-ID。链上数据使用需要数据所有方授权，通过验证 dataSign 和 checksum 校验数据有效性。

2.7.3. 可信数据存储

看到这个标题，也许你会产生疑问，区块链作为天然的分布式的可信账本，为何还要可信数据存储？这里并不是引出一个矛盾，而是试图去提出一个切实的痛点：区块链的冗余式存储是非常昂贵的。因此我们可以引入两种方案来解决这样的痛点：

1) 分布式存储：

分布式存储并不是一个新鲜的概念，HDFS 和 IPFS 这样的私有和公开存储方案，为我们在不同场景下的需求提供了非常好的选择，通过把数据在链外进行分布式存储的方式，既能做到主链存储资源的合理利用，也能让数据在隐私存储和公开访问上有所选择。

2) 可验证数据存储：

基于区块链的可信数据存储最重要的是继承区块链分布式账本的优势，保证数据的不可篡改性，因此可验证的数据存储是必不可少的，通过**数字签名**或者**文件哈希**等密码学的方式，我们可以实现在链外存储数据，并在主链账本上记录数据的可验证文件索引和哈希。

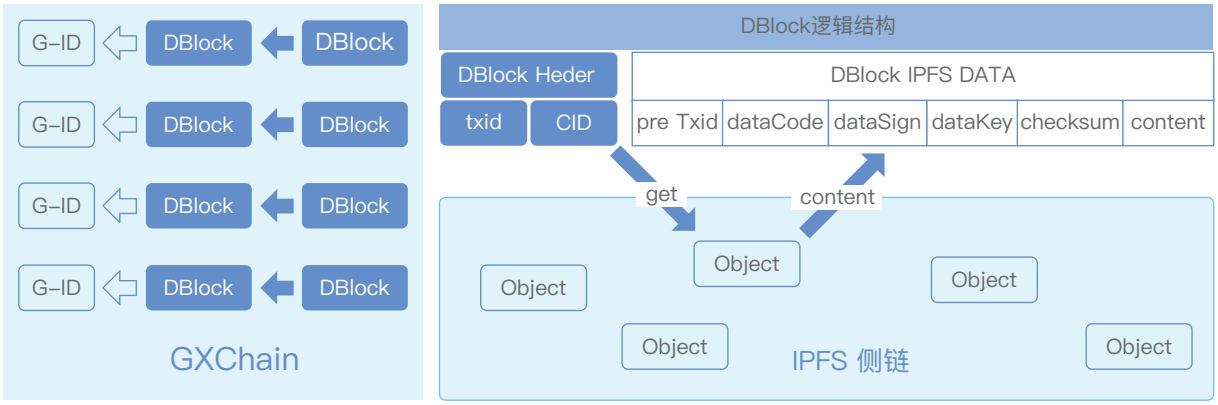


图 2.3 GXChain 可信数据存储设计

图 2.3 描述了 GXChain 中的可信数据存储设计。用户的 DBlock(个人数据块) 会被映射绑定到 G-ID 上，每个 DBlock 之间按数据版本串联。其中 DBlock 的主要数据结构包含 txid(记账的交易 id)，CID(IPFS 文档 Hash)。IPFS 根据 multiformats 保证每个文档能生成唯一的 CID，而 CID 又被不可逆的存储在 GXChain 上，确保已经被写入链上 (主链和侧链) 的数据无法被篡改。存储在 IPFS 侧链上的 DBlock DATA 包含 dataSign，checksum，可确保 DBlock 数据的真实可验证。

2.7.4. 可信数据交换

数据，是未来最重要的生产资源，也是每个人和企业未来最重要的隐性资产 (Hidden Assets)，这是每个人和企业从出生开始就积累的巨大财富。如何让这样的隐性资产高效、合理、安全地流通起来，也是可信数据组件重点要解决的问题之一。上述的内容中，我们探讨了一些方案，解决数据上链过程的可信和数据存储的可信，在此基础上，我们需要去思考，如何让数据流通过程可信，也就是如何实现可信的数据交换。在我们看来，可信的数据交换的重点在于解决数据**传输**和**存储**过程中的**隐私泄露问题**。

业务角度，我们可以通过链外计算的方式，来隔离数据被使用的环境，或者通过数据脱敏等手段，来保证数据在不涉及隐私的前提下被合理利用；技术角度，我们可以在不同场景下考虑以下几种方案：

1) 非对称加解密：
非对称加解密技术保证了数据在传输过程中，只有持有私钥的双方才能对内容进行解密，从而保证第三方无法对内容进行截取和爆破。GXChain 采用了 ECC 公私钥算法，通过 ECDH 可以计算两对公私钥之间共享密钥，从而实现两个账户间的隐私数据传输。

2) 安全多方计算 (MPC)：
安全多方计算 (MPC) 由姚期智在 1982 年正式提出。它主要探讨的是，n 个参与方各自输入信息去计算一个既定的函数，在保证计算的正确性的同时，不泄露参与方输入数据的隐私。具体来说，对于 n 个参与方，每个参与方 i 均知道自己的输入 xi，他们想协同计算一个既定函数 f(x1， ...， xn) = y，使得所有参与方都能获得最终的结果 y，但无法获知其他参与方的输入数据。

3) 同态加密 (HE)：
同态加密是一种允许在密文上进行计算的加密方式。除了传统加密方案的原始组件之外，还有另一种计算算法，它将目标函数 F 和加密数据作为输入。同态加密会生成一个加密的结果，当解密此结果时，获得的消息就像是在加密数据的明文上执行 F。支持密文上的任意计算的密码系统称为全同态加密 (FHE)。

2.7.5. 可信数据计算

可信数据交换重点在于数据传输和存储过程的隐私保护，而可信数据计算则关注对数据的**使用**和**处理**过程安全。链外计算、数据脱敏、安全多方计算和同态加密等都是可信数据计算实现的重要技术手段。安全多方计算 (MPC) 和同态加密 (HE) 虽说理论上存在可行性，然而前者需要大量交互，后者需要大量的计算，因此在性能和效率上决定了这两种方案暂时没办法大规模应用。

从目前技术成熟角度来看，可信执行环境 (TEE) 是一个更可行的方案，TEE 技术提供了三个功能:

> **1) 安全性**：TEE 是一个隔离区域，非授权设备或操作系统都无法对其进行操作。
> **2) 机密性**：TEE 内运行的程序是处于加密状态的，非授权设备或操作系统无法查看 TEE 内运行的程序。
> **3) 可验证**：在保密的前提下，TEE 内运行的代码可以接收外界验证。

3. 应用场景

3.1. 商用特点

GXChain 是一条对开发者友好，自带数百万流量的基础链。GXChain 具有基于 DPoS 共识机制底层架构的性能优势，同时具备 G-ID、GVM、BaaS、Blockcity-Pay、TEE、Oracle Machine 等链上配套功能，方便开发者开发各类应用。

GXChain 的以下特点，为 GXChain 的商用价值提供了无限可能。

3.1.1. 高性能和可扩展性

GXChain 是一条高性能基础链，理论上拥有每秒高达 10 万笔交易的处理能力，考虑到今后链上业务不断增长的可能性，GXChain 会支持纵向和横向扩展，可以迅速提升每秒交易处理能力。

3.1.2. 海量数据提供

GXChain 的可信数据上链和可信数据交换组件支持全领域的数据上链和交换，开发者在可信执行环境 (TEE) 中得到数据源的授权后就可以交易和使用这些数据。在 GXChain 上开发的应用都可以在用户授权之后使用用户个人数据，基于此，开发者能提供“更懂用户”的产品和服务。

3.1.3. 开发者友好

GXChain 有丰富的 API 和 IDE 工具以及完善的多语言开发文档，更有集合所有资源的开发者门户，实现对开发者从入门、发布、商用的全流程支持。

3.1.4. 低成本、高可用的 BaaS 存储服务

GXChain 提供一些如存储和验证类 BaaS(区块链即服务: Blockchain as a Service) 接口的支持，基于 GXChain 上的多方记账合约，以及自主搭建的高可用 IPFS 服务开发的数据存储和存证服务，完美结合了 IPFS 的高效存取能力和 GXChain 的高效记帐能力，任何一次数据存储都能在链上永久溯源。开发者根据丰富的 BaaS–API、数据交易 API、原生 API 开发出充满实际价值的区块链应用。

3.1.5. 动态全局参数调整

GXChain 不需要分叉就可以动态调整系统全局参数，这个功能称之为 DGP(Dynamic Global Property)，链上治理的理事会可以发起提案投票决定区块大小、出块速度、转账手续费等全局参数的动态调整。例如：将出块速度从 3 秒调整到 1 秒；将区块大小从 2M 调整到 8M；将转账手续费从 0.05GXC 调整到 0.01GXC。

3.1.6. 极速便捷的数字资产发行

GXChain 上有极简的数字资产发行流程和标准 (GUIA，GXChain User Issued Assets)，允许开发者自由发行和流通基于 GXChain 的数字资产。

3.1.7. 智能合约 IDE

智能合约 IDE 是基于 GXChain 开发的一个为开发者提供快速编码、部署、调用 GXChain 合约的工具。

3.1.8. 任何资产都可作为转账手续费，降低用户使用门槛

GXChain 上发行的数字资产，由发行人维护对应的手续费资金池，便可实现用任何数字资产作为 GXChain 的手续费支付。也就是由发行人维护其和 GXC 的汇率关系，类似于发行人在用 GXC 回购自己发行的数字资产。这样用户可以直接使用该资产来支付区块链记帐手续费，这将极大程度的方便不同的持币用户进行链上转账支付。

3.2. 应用领域

GXChain 定位于可信数据的价值网络，服务于全球的数据经济市场。GXChain 的高性能、丰富的链上配套功能以及海量的链上数据都为其大规模商用打下了扎实的基础。 GXChain 为数据经济搭建了一系列完善的基础设施，使得很多商业应用都能基于 GXChain 为用户提供优质的产品和服务。GXChain 提供的区块链技术解决方案能在各个领域解决数据所有权、支配权、收益权归属问题， 数据泄露问题，数据真实性问题以及数据上链的激励问题等等。在不久的未来，数据经济大生态将在 GXChain 的基础上拔地而起，涵盖但不限于个人数据权益管理、金融服务、移动社交、娱乐游戏、医疗健康、衣食住行等等。

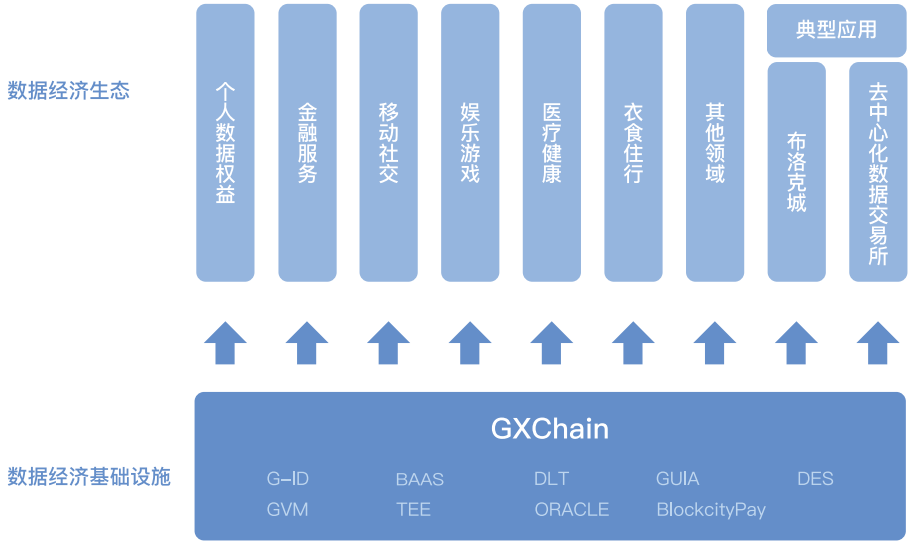


图 3.1 GXChain 应用领域

3.2.1. 典型应用

布洛克城

布洛克城是全球用户进入区块链世界的入口，是基于 GXChain 开发的大型个人移动端应用。布洛克城通过数据挖宝模式吸引了海量用户，并入驻了丰富的精品区块链应用，为全球用户提供多元化服务，帮助用户探索独特的区块链世界。布洛克城旨在打造流量最大最活跃的区块链应用平台，赋能区块链应用落地，并让区块链落地民生。在未来，布洛克城将致力于服务可信数据经济，让公民成为自己数据的主人，让数据为公民自己所用，在用户授权的情况下，充分激活数据潜力，丰富数据的应用场景。打造尊重用户隐私的区块链应用生态，用区块链重建可信的数据经济社会。

更多介绍请看详细的产品白皮书：
https://github.com/gxchain/whitepaper/blob/master/zh/gxbDapp-whitepaper.md

去中心化数据交易所

公信宝的去中心化数据交易所，为企业提供了与以往中心化数据交易（如数据中间商，数据黑市）全然不同的解决方案，基于区块链技术，数据交易双方可以直接进行点对点的数据交易和交换，拥有不缓存数据、保护隐私和数据版权、遏制造假等优点。面向的典型客户为互联网金融领域的网络贷款、汽车金融、消费金融、银行等企业以及有数据交换需求的政府部门、保险、医疗、物流等政企部门，以去中心化思维解决了各个行业的数据安全交换和流通等环节中一直没有解决的诸多核心问题。并可以为全社会所用，广泛使用于公民的学习、工作、生活等各种应用场景中，让数据释放应有价值，提升社会协作效率。

更多介绍请看详细的产品白皮书：
https://github.com/gxchain/whitepaper/blob/master/zh/dataExchange-whitepaper.md

3.2.2. 个人数据权益

通过数据上链可以实现将数据所有权、支配权以及收益权回归用户，让用户成为自己数据的主人，从而通过区块链去重构信用社会。在现有的互联网世界中，个人数据得不到很好的保护，如数据被盗，黑市泛滥，数据所有权错误归属等，个人数据安全问题频发，50% 以上的世界 500 强公司都出过数据泄露、黑客攻击等数据安全问题。各大互联网巨头以及数据黑市商通过数据的加工和交易将数据产生的价值占为己有。利用区块链技术，经过用户的授权，公信宝提供工具，让用户自助采集自己的互联网数据并通过非对称加密保存至 GXChain 之上，同时将能解开数据的唯一钥匙“Data-Key”交由用户本人管理，由用户完全掌握数据的所有权、支配权以及收益权。应用方想要获取或使用个人数据时，需要得到个人的授权，个人通过 Data-Key 将数据解锁后应用方才可以查看或使用个人数据。个人授权应用方使用其个人数据可以获得相应的 token 奖励。

互联网保管数据的痛点	区块链解决方案	区块链解决方案特点
数据滥用与被盗 在科技寡头的时代，在无授权的大数据滥用背景下，数据滥用与被盗的出现有其内在的必然性。	重获数据所有权 公信宝提供工具，让用户自助采集自己的互联网数据并通过非对称加密保存至链上，由用户保管。	区块链身份(G-ID) G-ID一旦创建，身份信息独一无二、不可篡改。G-ID将会成为未来区块链世界的通行证。
收益权被剥削 底下黑市数据交易产生巨额收益，却落入了数据交易贩子囊中，用户的数据收益权被剥夺。	赢得数据支配权 通过数据密钥Data-Key，用户掌握着数据的支配权。用户可以决定谁可以使用自己的个人数据。	数据加密存储不缓存 用户授权导入的数据，通过非对称加密，上传到侧链，并形成数据索引，公信宝本身不缓存任何数据。
所有权错误归属 占有大量用户数据的互联网巨头，往往自己牢牢掌握数据所有权，不愿意与民共享。	拿回数据收益权 用户每一次授权使用后产生的价值，都将归用户本人所有。	去中心化数据管理 用户的Data-key保存在本地客户端，没有任何中心化数据库存储用户的Data-Key和个人数据。

图 3.2 个人数据管理方案对比

3.2.3. 金融服务

金融领域是区块链技术最早落地的领域，比特币的出现就是为了解决传统货币体系的一些顽疾。随后，区块链技术在跨境支付、结算等领域也有着持续性的落地。目前，区块链技术正服务着越来越广泛的金融领域，包括银行、保险、股权交易、金融衍生品和支付等。从多家银行披露的 2017 年年报来看，“区块链”技术这个数年前被众多银行等金融机构竞相布局的金融新科技，正逐步从“概念式验证”阶段走向“应用成果”阶段。GXChain 可以通过可信数据上链，分布式数据存储、可验证数据存储等技术突破此前金融交易中信用校验复杂、流程长、成本高、数据传输误差等问题。

数据是金融应用的核心，大部分的金融产品都是围绕数据进行的。风险和收益一样，都是金融的核心内容，而风险的控制依赖于海量的数据。GXChain 是一条可信数据基础链，其上海量的可信数据可以为金融应用场景提供最好的风控支撑。例如，将企业的 ERP 数据，库存数据，现金流数据，物流数据，商流数据等进行可信上链，再基于链上数据进行可信数据计算与交换，能为供应链金融提供真实有效的风控服务。链上数据的不可篡改与公开透明更好的保证了金融风控模型中输入数据的真实性与一致性。

3.2.4. 移动社交

社交对用户有着强大的吸引力，也是绝大部分用户的刚需，这促使社交网络成为了互联网时代最基础和最重要的应用之一。2017 年全球社交网络用户占互联网用户的 73.9%，这是一个巨大的群体。至今，区块链仍然没有一个覆盖大规模主流人群的应用，社交无疑是区块链快速切入主流人群的一个好方向。目前基于互联网的社交网络存在非常多的痛点，比如信息造假、安全性不足、低质量内容泛滥、内容输出者得不到应有的收益权等。

基于 GXChain 的区块链社交应用，能较好的解决现有基于互联网的社交网络的一些痛点。数据的上链保管与非对称加密能够保证用户信息的真实性以及安全性。可信数据交换能让用户安心进行信息的交换，减少社交中的信息不对称。去中心化的社交平台能够让用户远离互联网平台的强制分发，将内容的审核权回归用户，从而提升平台的内容质量。此外，Token 经济的引入能够更好的去激励优质的内容输出。

基于 GXChain 的社交应用还能通过链上的海量数据为用户提供更为便捷与精准的社交服务。举个例子，GXChain 内的征信功能能够非常便捷地让两个陌生人了解彼此最真实的信息。GXChain 上目前有非常丰富的个人信息数据，这些数据都是与链上身份 G-ID 绑定的，比如信用卡账单、电商、社保公积金、学籍、年龄、通讯等等。这些信息都是通过可信数据存储在 GXChain 上的，这很好地保证了这些关键数据的真实性与安全性。当两个陌生人在社交软件上认识时，A 可以申请查看 B 的数据，B 同意后便可使用 Data-Key 解锁数据，授权 A 查看他的个人数据。我们相信区块链技术与 GXChain 上的海量数据能很好的赋能社交应用，助力区块链社交应用的快速落地。

3.2.5. 娱乐游戏

游戏行业市场规模巨大并且与区块链以及 Token 经济有着天然的结合。游戏行业过去 20 年作为一个朝阳行业保持了高速增长。全球范围内目前游戏用户共 5.8 亿，其中手游用户 5.5 亿，页游用户 2.6 亿，端游用户 1.6 亿。整个市场规模在 2017 年超过了 2500 亿元。

但是目前的游戏行业从业者也面对了重重的困境。游戏用户红利衰减，游戏生命周期短，除少数头部游戏外，付费率和 ARPU 的提升空间很小。此外，寡头集中度持续提高，中小游戏厂商生存困难。而区块链的发展，则给了游戏行业从业者一个机会去突破困境。一方面，区块链形成了全球分布的高净值用户群体，为游戏 ARPU 提供了更多的挖掘空间。另一方面，区块链行业发展尚处于初期，对于新进入者是一个机会更加公平的市场。同时，Token 经济能给游戏参与者更强的激励和项目参与感。区块链游戏将是一个全球化的新市场，有着优质的用户群，给新进入的游戏厂商一个公平的起点。GXChain 自带的数百万高净值用户以及极度便捷的 token 发行和流转体验，都是区块链游戏最好的催化剂。

GXChain 生态内的两款火爆游戏万利马和链与飞车已经充分证明了以上三点，也展示了 GXChain 能给予游戏的强大赋能。万利马上线 3 个月，便有了 24 万区块链用户，收入超过 600 万元。链与飞车上线当日充值超 13 万枚 GXC，ARPU 高达 135 枚 GXC(按当日价格为等值超 1000 元人民币)， 远超游戏行业的平均值 300 元人民币的 ARPU。在未来，GXChain 生态内将会为用户提供更多更好玩的游戏，助力中小游戏厂商在区块链领域的起飞。

3.2.6. 医疗健康

医疗行业是个关乎民生的重要行业，且行业规模巨大。区块链在医疗行业也有着巨大的发挥空间。区块链可以追溯药物生产商、批发商、制药公司和患者之间的每一次交易，验证和保护对于跟踪假药等问题来说很重要的药品信息。此外还可以避免一些潜在药物未受监管的分销。

GXChain 在欧洲正在孵化一个医疗领域的去中心化数据交易所。该项目致力于解决医疗数据在各个领域的高效与安全流通问题，并用 Token 经济充分激励用户进行医疗数据的上链。例如，个人的医疗数据可向特定商业公司授权查看，由此个人可得到 Token 的奖励。此外，该项目还可以解决海外就医时遇到的医疗数据隔断问题，通过区块链应用，个人可以把医疗数据安全、快速地共享给海外医院。

3.2.7. 衣食住行

除了以上领域，GXChain 生态在未来还将出现数以万计的应用，服务于全世界消费者的衣食住行。GXChain 的高性能、丰富的链上配套功能以及海量的链上可信数据能够赋能各个领域的区块链应用逐步落地，包括零售、餐饮、食品追溯、短租、长租、楼市、打车、租车等等。衣食住行都是围绕信用去实现的，所有涉及信用的使用场景都可以基于 GXChain 去开发应用。可信数据是信用社会的基石，GXChain 丰富个人可信数据的过程也是建立身份档案，建造信用社会的过程。

GXChain 上的海量可信数据可以为衣食住行应用提供评价信用的基石。企业和机构的数据，更像是一个集合体，单体体量大但总体数量小。而个人数据更像是人体中的毛细血管，细而杂，单体体量小但总体数量多。最终数据要回归个体，这些数据取之于个体，用之于个体。我们认为随着个人数据维度的不断扩大，C 端市场的价值，远大于 B 端市场的价值。这些用户数据，在经过清洗和加工后，可以有非常广阔的使用范围。

举个例子，在长租领域，已上线落地应用的 Lucia 便是基于 GXChain 的诚信租住社区。通过区块链网络链接全球有租住需求的用户，围绕 GXChain 信用数据网络，在共享生态的激励机制下，建立一个以信任为基石、高效自治的租住生态。让每位用户都有数，走过的每一步都算数。

4. 经济模型

4.1.GXC 经济模型和价值场景介绍

GXC(原 GXS 更名为 GXC) 是 GXChain 的核心资产，中文名为公信币，总量 1 亿。GXC 类似 Ethereum 主链的 ETH 以太币，EOS 主链的 EOS。GXC 作为 GXChain 非常重要的治理和应用核心资产，具体的经济模型和价值场景图如下：

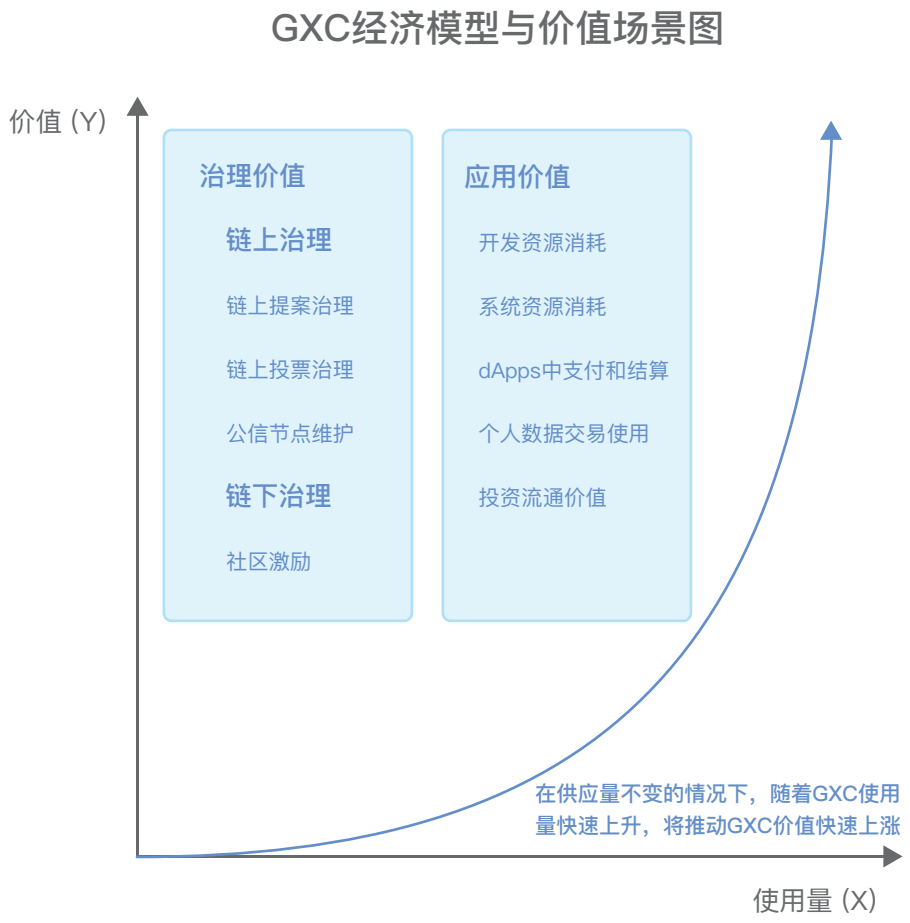


图 4.1 GXC 经济模型和价值场景图

4.2. 治理价值

GXC 在 GXChain 的链上及链下治理中都发挥着重要的价值，用于促进更大范围参与更有效的治理。

在链上治理中，GXC 主要扮演着表达介质与激励机制的角色；在链下治理中，GXC 主要用于激励更多的社群用户参与 GXChain 的治理。

在链上治理中，GXC 主要有以下几点用途：

1) 链上提案治理：理事会成员发起提案需要消耗 GXC，提案的通过与执行也需要理事会支付相应的 GXC；

2) 链上投票治理：在选举公信节点与治理委员会时，用户持有的 GXC 作为唯一选票使用；

3) 公信节点维护：创建与修改公信节点都需要消耗 GXC。

在链下治理中，GXC 主要用于激励开发者以及社区用户参与治理。GXChain 基金会对开发者以及社区用户积极参与 GXChain 治理、推动 GXChain 发展的行为会给予一定的 GXC 奖励。

4.3. 应用价值

除了治理价值，GXC 在数据经济中还有更为广泛的应用价值，为区块链在数据经济的落地与大规模商业应用提供了重要价值介质。GXC 的应用价值主要有以下几个方面：GXChain 开发资源的使用、GXChain 上各类系统资源的消耗、dApp 中的支付与结算、个人数据交易使用、投资价值流通等。

GXChain开发资源的消耗	创建dApp 部署智能合约 调用BaaS服务 发行资产 注册成为开发者
GXChain上各类系统资源的消耗	创建账户 升级账户 发起转账交易 调用dApps 调用智能合约 使用GXChain生态内的各类基础设施
dApps中的支付与结算	基于GXChain的dApps，都支持GXC的支付与结算 使用GXC在dApps中购买需要的产品与服务 各领域dApps体系内价值流通的最大载体
个人数据交易使用	当dApps需要使用个人数据时，个人授权给dApps使用其个人数据可以获得GXC的奖励 当个人需要查看其他人数据时，需要得到当事人的授权并需要支付GXC
投资价值流通	GXC本身的稀缺性以及强应用需求支撑了其巨大的流通价值 用户可以再全球各大交易所中交易GXC，共享GXChain生态成长带来的价值

4.4. 用户获得 GXC 的途径

用户可由以下途径获得 GXC：

1) 参与公信节点出块，获得出块奖励 GXC
2) 通过布洛克城挖宝获得 GXC
3) 通过完成活动或任务获得 GXC
4) 对社区贡献获得 GXC 奖励
5) 通过开发应用赚取服务费 GXC
6) 数据交易收入 GXC

4.5.GXC 分发机制

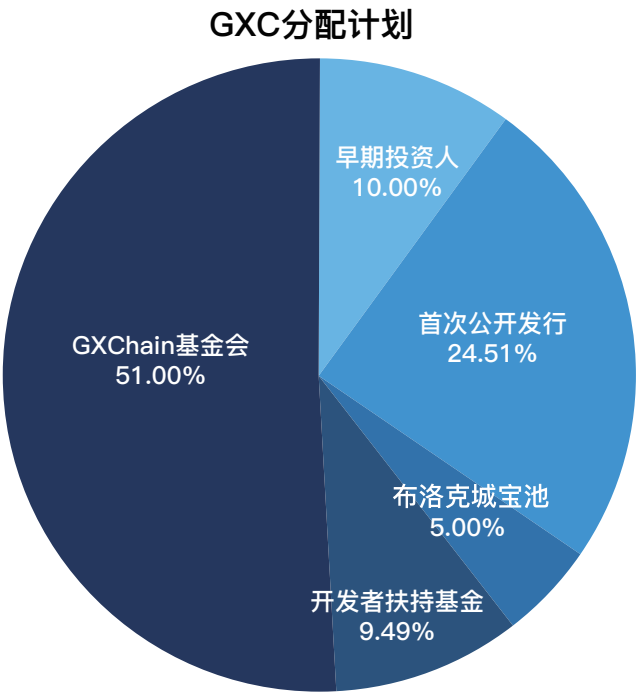


图 4.2 GXC 分配计划

比例		分配方案	详细说明
10%		早期投资人	用于发放给最早期的投资人
24.51%		首次公开发行	用于发放首次公开发行的投资人
5%		布洛克城宝池	作为布洛克城挖宝奖励投放至布洛克城宝池，激励用户进行可信数据上链
9.49%		开发者扶持基金	作为开发者扶持基金，用于扶持基于GXChain开发的dApps
51%	21%	创始团队	发放GXC以回报创始团队在GXChain筹备期、开发初期投入的大量的人力、资源、物力，以及为GXChain的技术和运营等各个方面都做出了重大的贡献，同时激励其之后在GXChain发展过程中继续发力
	10%	GXChain公链生态建设	用于公链生态建设、公链开发与开发者社区培育，用于支付合作费用、扶持开发者项目、举办技术竞赛等，推动GXChain技术的应用与生态的建设，展现并提升商业价值
	6%	市场公关	用于GXChain全球性的市场宣传、品牌营销及社区运营等工作
	4%	公信节点	公信节点出块奖励，共21个节点
	10%	日常经营	作为GXChain基金会的日常经营资金，用于支付员工工资、行政采购费用、外聘会计师服务费用等日常经营性开支

5. 实施和迭代

5.1.Timeline

2016 年 8 月 – 项目成立

2016 年 10 月 – 数据采集模块 Metrix 1.0 产品发布

2017 年 2 月 – GXChain 白皮书发布

2017 年 6 月 – GXChain 和去中心化数据交易所 DES 1.0 版本上线

2017 年 6 月 – GXC(原名 GXS) 在云币网开始交易

2017 年 8 月 – 主链代码开源

2017 年 9 月 – 去中心化数据交易所 DES 1.0 正式商业化

2017 年 10 月 – GXChain 的手机钱包 1.0 发布

2017 年 11 月 – 白皮书 2.0， 主打 ”CBD” 生态， GXChain 定位下一代大数据公链

2018 年 1 月 – GXChain 首款面向个人的 dApp 布洛克城上线， 24 小时用户突破 10 万

2018 年 3 月 – 布洛克城突破 100 万区块链用户

2018 年 5 月 – 基于 GXChain 的存储 + 存证服务 BaaS–Storage 上线

2018 年 6 月 – 去中心化数据交易所升级 DES， 服务全国百家互金企业

2018 年 7 月 – 布洛克城突破 200 万区块链用户

2018 年 8 月 – 智能合约 2.0 测试网络发布，支持 WebAssembly

2018 年 9 月 — GXChain 主链账户地址突破 100 万

5.2.Roadmap

2018. Q4 – 白皮书 3.0 面世， 定位升级成为一条为全球数据经济服务的基础链，旨在打造可信数据的价值网络

2018. Q4 – 智能合约 2.0 主网上线

2018. Q4 – 主网升级，将原有基于 GXChain 发行的 Token — GXS，1:1 替换为 GXC，中文名为公信币，GXC 将作为 GXChain 的主链核心资产 (Core Asset)，成为 GXChain 最重要的治理和应用通证，后续 GXChain 生态中治理、开发、应用、支付流通场景均以核心资产 GXC 为媒介

2018. Q4 – 2019.Q1 开发 TEE 可信数据合约执行容器，进一步提升数据隐私安全

2019. Q1 – 2019.Q2 开发 GXChain 的预言机 (Oracle Machine)，扩展 GVM 应用计算范围

2019. Q2 – 2020.Q2 GXChain2.0 计划启动，在保障安全性、去中心化的基础上进行横向纵向可扩展领域的探索，进一步升级友好开发环境；同时输出一个解耦且高度标准化的区块链基础框架，为全行业做出技术贡献

6. 总结

这是一次从应用型公链到基础型公链的技术跃迁，

这是一次治理结构的彻底变革，

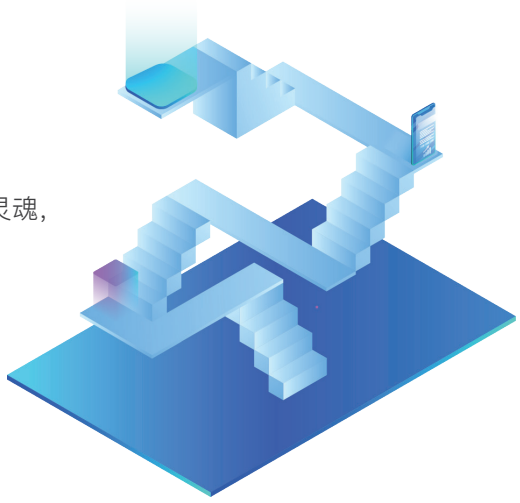
这是一次共识的全面升级。

全新的 GXChain，将以“用区块链重构信用社会”的愿景为灵魂，

以民主，透明，去中心化的治理架构为骨架，

以更广泛领域的社群以及开发者参与为血肉，

搭建服务于全球的可信数据的价值网络。



术语表

英文	中文	缩写	描述
Digital Identity	数字身份	DI	**数字身份**是身份标识方式的一种，是一对“钥匙”，其中一个只有她 / 他本人知道 (即密钥)，另一个是公开的 (公钥)
General Identity	通用数字身份	GID	**GID** 是 GXChain 生态的通用数字身份，GID 授权服务是一种在服务提供方为用户和应用方提供可信和高效授权的机制，这种机制允许用户授权第三方网站或应用访问他们存储在服务提供者方的信息，而不需要分享他们的访问许可或他们数据的所有内容。GXChain 的数据授权场景在 OAuth2.0 的基础上，对数据授权进行了分类和不同权限的划分，涉及个人隐私的数据，需要通过用户在本地用 DataKey 解密并授权，授权的数据通过第三方的 DataKey 公钥加密，整个过程安全、透明，保证传输过程不会造成数据泄露
Peer–to–Peer	对等式网络	P2P	**对等式网络** (peer–to–peer)， 简称 P2P，又称点对点技术，是无中心服务器、依靠用户群 (peers) 交换信息的互联网体系，它的作用在于，减低以往网路传输中的节点，以降低资料遗失的风险
Delegated Proof of Stake	股份授权证明机制	DPoS	**股份授权证明机制**的原理是让每一个持有 Token 的人进行投票，由此产生 11 到 101 位代表，我们可以将其理解为 11 到 101 个超级节点或者矿池，而这 11 到 101 个超级节点彼此的权利是完全相等的。从某种角度来看，DPoS 有点像是议会制度或人民代表大会制度
Smart Contract	智能合约	–	**智能合约**是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值

Oracle Machine	预言机	–	**预言机**，又称**谕示机**，是一种抽象电脑，用来研究决定型问题，如 x 是否可以整除 y，就是一个决定性问题
Relay	中继	–	区块链中的**中继模式**是指通过智能合约、预言机等技术实现跨链交互的技术方案
Para–chain	平行链	–	**平行链**采用和主链相同的区块链架构，通过跨链机制和主链串联
App–chain	应用链	–	**应用链**定位是垂直领域的区块链应用
Distributed Business	分布式商业	–	**分布式商业**是一种多方平等参与、智能协同、专业分工、价值分享、模式透明的全新的商业模式，而区块链技术是实现分布式商业的重要技术手段
Homomorphic Encryption	同态加密	HE	**同态加密**指在密文上进行计算，既能保证隐私又能提供可操作性的一种加密方式。而**全同态加密 (FHE)** 是支持所有操作的计算
Secure Multi–Party Computation	安全多方计算	MPC	**安全多方计算**指 n 个参与方各自输入信息去计算一个既定的函数，在保证计算的正确性的同时，不泄露参与方输入数据的隐私的计算方式
Blockchain as a Service	区块链即服务	BaaS	**区块链即服务**指通过对区块链底层技术的封装，对外提供一系列区块链特性的服务
Data Exchange Service	数据交换服务	DES	**数据交换服务**是基于 GXChain 多方记账合约实现的数据交换和数据存证服务