# ZitChain

全球开源应用 DAO 生态

白皮书 V4.2

# ZitChain 社区宣言

“计算机、软件、互联网、移动互联网、云计算、大数据、IOT 以及区块链….”，近 50 年来，信息科技革命让人类进入了生产力发展最迅猛的阶段，一次次历史罕见的技术创新爆发式涌现，使这个时代成为了文明史上当之无愧的巅峰。全球数以亿计的开发者们无疑是这一切最大的贡献者，正是他们用一行行源代码无时不刻地改变着世界。然而，开发者自己的世界却没有改变：由于工业化时代带来的市场信息不对称、中介化高度泛滥的社会现象继续蔓延，“企业”这种少数股东最大利益分享的组织形式也依然占据主流地位，使真正付出劳动的开发者群体长期身处利益链的最远端，没有获得相匹配的收益、权利，甚至尊严！

ZitChain 旨在通过构建一个可信的去中心化开发协作基础设施用以承载一个公平的开发者劳动成果市场并沉淀出一个透明的开发者征信体系，最终形成一个真正由开发者共建、共有、共享的共治社区。在这个又是家园又是舞台的社区生态环境里，数字货币体系激励了每个开发者用创新直接兑现现实价值，包括公正的货币回报（币值）和社区地位（币权）；共治规则体系则保障着每个社区开发者永远具有参与自己理想国建设的责任和权利。

我们是一群开发者，为了我们开发者这个群体共同的未来价值和公正权益，我们希望天下开发者联合起来，共同将上述的一切变成现实。唯有如此才将可以只靠代码说话，唯有如此被公司雇佣才将不是唯一选择，唯有如此才将可以早日拥有自由。

正是由于我们对于所有开发者无比的信心，我们创始团队在本白皮书出具的

技术方案、今后的实施成果和治理规则都只是用来抛砖引玉：一方面保证 ZitChain 的如期诞生和顺利成长；一方面用以吸引志同道合者立即参与。所以如果你是一名开发者，请马上加入 ZitChain，在这里尽情展现你的才智，获得你的收益，并实现你的意愿吧。

# 目 录

# 第一章 ZitChain 项目背景

## 1.1 开源生态的繁荣

开源生态是一种围绕开源软件开发、应用和商业推广形成的全球性合作网络，是当今科技创新和产品研发的重要驱动引擎。开源开发者是开源生态的主体，为全球软件技术和产品的创新做出了巨大贡献。

目前，全球最大开源开发平台 Github 汇聚了 2400 万开发者，托管了 6700 万个版本库，超过 500 万个开源项目；中国最大开源开发平台 OSChina 也聚集 200 万开发者、托管了 300 万个版本库、；2017 年全球开发者在 GitHub 上提交的 Issue 有 6880 万个，Commit 次数在 10 亿以上。除了 IBM、谷歌等老牌开源贡献者外，曾经封闭的微软也成为开源生态中最大的贡献组织之一，可见开源正在彻底改变软件产业的运作模式和开源开发者的生存方式。

## 1.2 开源生态的问题

开源开发者在持续贡献和创新的同时，其收益模式却一直没有升级，导致开发者的创新和创收存在矛盾和冲突，这些问题在开源力量储备不够发达的地区更加尖锐。主要表现在以下方面。

### 1.2.1 开发者尚处于科技产业价值链的远端

开源商业模式汇集了目前最为灵巧又最为复杂的开发与商业行为。但一个不可否认的事实是：开源生态的价值链顶端一直被商业和科技巨头占据，广大开发者长期贡献却不能及时获得收益，或者只获得极为间接的小部分收益。这对开源

生态的公平与效率都将产生根本性的不良影响。

### 1.2.2 开发者的知识产权难以得到有效保障

知识产权保护一直是科技创新领域的难题。很多科技巨头尚且常常被知识产权问题搞得焦头烂额，普通开发者群体更是无暇顾及，版权利益难以得到有效保护。特别是，目前开源代码主要托管在一个中心化平台 GitHub，其用于管理代码的 Git 协议本身并不能确保版本信息不被篡改，而版本信息是开发者的知识产权不被窃取的唯一证据，这种证据在技术和管理层面都面临巨大隐患。

### 1.2.3 开发者并非开源生态基础平台的主人

目前的开源生态为广大开源开发者提供了自由学习、协作开发的工具和社区平台。但是，比如以 GitHub 为首的大型开源平台往往本身并没有基于开源模式构建，开发者对开源社区基础设施的发展没有决定权，更没有拥有权。

## 1.3 ZitChain 的提出

目前，开源生态与理想的开发者家园还有巨大差距，开源生态的利益分配、产权保护、社区发展决策等基本权利并不属于开发者。

为此，我们提出 ZitChain 项目，旨在**联合全球开发者构建一个彻底由开发者缔造、被开发者共有、为开发者谋利的共治社区。**ZitChain 包含了两层含义：Zit 取自 Git，但希望超越 Git；Chain 取自区块链，希望利用区块链技术构建一种更有活力的开源生态系统。

## 1.4 专业术语

本文使用到的主要术语如下。

**Blockchain（区块链）**

区块链是一种去中心化的分布式账本系统，基于密码算法、共识机制、时序机制等，实现了系统中各节点的数据持续记录、即时验证、难以篡改、无法屏蔽等特性，从而可用于建立一套隐私、高效、安全的共享价值体系。

**ZitChain**

ZitChain 是一个彻底由开发者缔造、被开发者共有、为开发者谋利的基于区块链技术构建的全球性开发者共治社区。

**Zit 协议**

Zit 协议是 Git 协议与区块链技术的结合体，旨在解决 Git 协议在开发者价值度量与交换、代码仓库去中心化管理等方面的瓶颈问题。

**Git / GitHub**

Git 是目前开源开发者广泛使用的代码版本控制系统。GitHub 是基于 Git 的互联网代码托管平台，目前已发展为全球最大的社交化开源开发社区。

**IPFS**

InterPlanetary File System(星际文件系统),下一代分布式存储和分享的网络传输协议，目前成熟应用有分布式哈希表、Git 系统、比特币等。

**DAG**

Directed Acyclic Graph(有向无环图),下一代区块链技术区块结构。

**默克尔树**

Meekle Tree,存储一组 Hash 值的树结构，广泛应用在区块链和 IPFS 系统等。

# 第二章 ZitChain 愿景与目标

## 2.1 ZitChain 愿景

ZitChain 是面向开发者的开放型 DAO（Distributed Autonomous Organization，分布式共治组织），致力于构建一个全球化的开发者共建、共有、共享的共治社区。ZitChain 代表全球开发者的全体利益，将逐步解决现有开源生态在开发者产出物安全管理、能力合理度量、价值及时兑现、创意快速实现、权利真实拥有等挑战性问题。

这里特别说明，参与 ZitChain 的所有用户都称为开发者。虽然 ZitChain 中活跃的用户可能是技术产品的消费者，也有可能是企业和组织，他们也被视为广义上的开发者。

ZitChain 借鉴开源理念，**基于区块链技术打造一个去中心化的全球开源软件新型社区系统。**ZitChain 社区通过独创的核心底层架构技术和共识机制，由全世界开发者参与并完全共治，社区收益完全由社区用户共享。开发者劳动产出物通过 ZitChain 开源托管协议 Zit 协议实现共享存储、浏览、分发、有偿使用等。在 ZitChain 社区，每个开发者的劳动成果都将得到尊重并自动版权保护，通过数字货币得到量化回报。


图一 ZitChain 开发者愿景

ZitChain 创始团队均来自于知名技术公司和开源组织如 Redhat、Google、Apache 基金、Linux 基金及开源中国等核心专家，具备很强的相关技术实力和运营能力。

## 2.2 ZitChain 目标

### 2.2.1 世界上最大的软件开发协作平台

ZitChain 的一个首要目标是普惠全球软件开发者。ZitChain 致力于解决开发者最根本的生存和价值问题，将吸引更多的开发者参与其中。无论开发者来自何地、水平高低与否、职业目标如何，他们都可成为 ZitChain 的构建者和拥有者。

相对于 GitHub 等关注代码共享、协同编程、汇聚贡献等开源开发平台，ZitChain 则是激活全体开发者、服务全体开发者、保障全体开发者的精神和利益兼顾的理想家园。

### 2.2.2 劳动成果通过去中心化的形式被存储

目前 GitHub 是全球开源项目的主要代码托管平台，但其基本是由一家公司

独立运营和管理，在技术上存在单点故障、可扩展性等隐患，在服务上存在商业化和垄断化的隐患。

ZitChain 希望为全球开发者提供一个去中心化的开发成果存储和管理平台，以解决上述问题。在此基础上，ZitChain 为开发者提供一个安全、可扩展、去中心化的劳动成果（如源代码、开发文档、开发行为日志等）存储和管理平台。

### 2.2.3 开发产出物的知识产权自动被保护

目前开源社区基于版本管理系统、问题跟踪系统等进行开发过程和成果的管理。开发者的代码和文档等知识产权也主要基于这些系统中的数据进行确认。但是这些系统都不具备防篡改能力，在某些极端情况下开发者的成果原创性可能被恶意剥夺。

在 ZitChain 中，开发者劳动成果的原创性可以得到更好的保护，同时任何未经授权的直接使用都会被及时发现。这就要求开发者成果和过程数据存储在一个开发者共有的平台中，以得到安全存储和防篡改保护。因此，ZitChain 应当具有属于全体开发者的、非中心的代码变更数据存储和管理能力。

### 2.2.4 开发者综合能力的技术征信

开发者的技术能力是其在开源生态系统中的通行证，是协作开发与成果估值的重要依据。ZitChain 通过区块链技术对开发者的技术特征进行安全地提取和管理，可望建立权威、公认、透明的开发者能力信用体系。基于 ZitChain 构建的开发者技术征信库将极大降低开源生态中合作和交易的成本。

### 2.2.5 开发者的劳动成果货币化

目前，活跃在开源社区中的开发者的参与动力主要包括两方面：一是本人对开源项目具有浓厚的兴趣；二是直接受企业雇用参与开源软件的开发。由于开发者在开源活动中基本处于产业价值链的远端，个人能力不能直接变现，也缺乏更客观的量化标准。

为此，ZitChain 具有发行数字货币的能力，开发者的工作量和作品质量在一定条件的触发下能够直接量化为相应的数字货币，这些触发条件可以是重要开发过程的推进（如 PR 被接受、项目成熟度晋级等），也可以是大众的关注度（如点赞、fork、复用、订阅等）。

在 ZitChain 中，开源贡献的利益分配不应仅由商业组织决定，而应首先由开源项目的管理组织来决定。

### 2.2.6 交易历史透明且具有独立性

ZitChain 中的供求双方信息对称，价格公开透明，开发者之间的交易行为公开透明，任何发生争议和纠纷的交易都可追溯。ZitChain 中的交易结算不依赖于任何第三方交易系统，而是基于全体开发者共同建立的区块链完成。

以开源开发活动为例，每个开源项目都是一个潜在的创业项目的起点。因此，开源项目本身可以在开源生态中招募其他开发者为其提供临时编程支持或非编程支持。此类与开源项目发展直接相关的交易活动都应当方便的在开源生态中基于数字货币完成，并且交易可以独立结算，不依赖于任何第三方中心机构。

### 2.2.7 社区完全由开发者共治

ZitChain 是一个彻底由参与其中的开发者共同维护和升级的平台。ZitChain

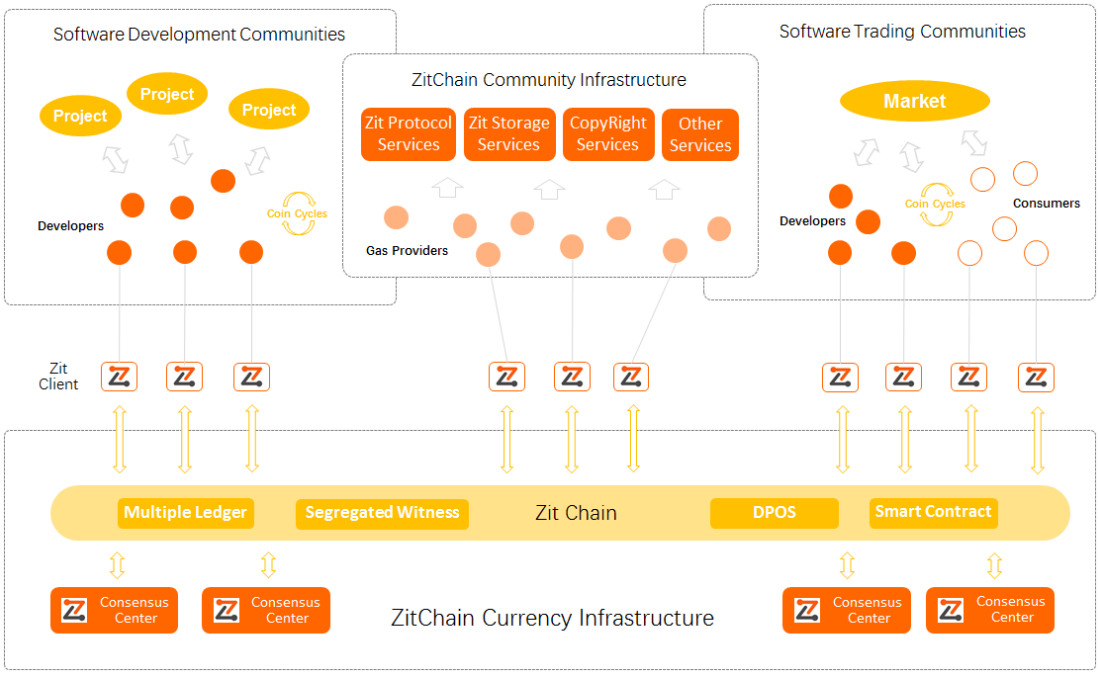
提供的开发工具、交易工具、运行规则、奖励机制、交易机制等技术和运营活动都由全体开发者共同决定。ZitChain 中任何事务的决策都是通过民主投票的形式进行，但是不同开发者的投票效力可能与其技术信用度相关。

# 第三章 ZitChain 技术方案

## 3.1 系统整体架构

为真正建立一个由开发者共建、被开发者共有、为开发者服务的社区，推动开发者价值实现，需要解决几个关键问题，即开发者自由高效的代码开发、开发者代码知识产权的保护与传播，以及开发者代码价值的度量与交换。

我们创新地提出了一种将 Git 协议与区块链技术相结合的新型代码管理协议和代码知识产权鉴定方法，并构建了一整套的解决方案，实现去中心化的代码托管、产权保护、价值度量、服务交付等，从而建立一个透明、公正的全球开源应用新生态 ZitChain。




ZitChain 生态系统结构图

ZitChain 整体架构主要包括运行基础设施、社区基础设施、ZitChain 开发与交易社区以及 ZitChain 应用软件等四个核心组成部分：

**ZitChain 货币基础设施（ZitChain Concurrency Infrastructure）**

主要基于区块链技术，为 ZitChain 生态系统的运行提供基础技术支撑，包括分类账本、隔离见证、共识机制以及智能合约等。

**ZitChain 社区基础设施（ZitChain Community Infrastructure）**

主要为 ZitChain 社区运转提供关键服务，包括 Zit 新型代码管理协议、分布式代码存储管理服务、代码鉴权服务等。

**ZitChain 社区**

包括 ZitChain 开发社区（ZitChain Development Community）和 ZitChain 交易社区（ZitChain Trading Community）基于社区基础设施构建和形成，主要包括软件开发社区和代码交易社区。其中，软件开发社区主要由开源开发者构成，借助 Zit 协议和分布式存储技术等完成代码的开发等；代码交易社区则由代码开发者和代码消费者构成，借助代码鉴权等服务进行代码的交易。

**ZitChain 应用软件**

为开发者和消费者等提供 ZitChain 生态接入服务，用户通过 ZitChain 应用软件来使用 ZitChain 提供的各项服务，完成代码开发、交易等。

## 3.2 ZitChain 区块链基础网络

Zit Chain 是基于区块链技术构建的面向软件代码开发、存储、交易活动等的

区块链，并为 ZitChain 社区提供运行时支撑。其中，主要涉及的组件和服务包括混合式分片链、分类账本、共识机制、隔离见证与智能合约等。

### 3.2.1 混合链基础架构

以比特币、以太坊为代表的区块链架构，在不断的应用实践中，暴露出了交易规模、响应速度和扩展性等一系列问题，这些问题阻碍着区块链商业应用的发展与落地。ZitChain 作为领先的区块链网络应用，需要建立在能使用高频次并发、亿万级用户、零延迟响应的区块链公有链上，结合 Zit 分布式托管系统，才能真正地归于成功。

ZitChain 采用混合式分片链技术，将公有链、分片链（逻辑子链）有机结合，形成混合链基础架构。ZitChain 将少量的交易记录核心内容保存于公链账本，而对于见证历史、共识记录、业务流转等交易，保存于独立的空间中。

通过标准化跨链通信协议，ZitChain 在公有链和分片链中无缝对接交换数据。哈希索引技术可有效保证同一数据的有效映射和唯一权威性。

### 3.2.2 DAG 高并发异步执行

ZitChain 的双链并行技术，既可以保证主链的不可篡改性，又可以在分片链中保留灵活性。主链仍然采用传统的链式结构，而分片链中则使用 DAG 数据结构。

DAG 是一种全称为有向无环图的数据结构，由集合的顶点和有向边构成，每条边连接不同的顶点，这样顶点之间不存在循环返回的可能。DAG 结构，可以通过见证人机制快速找到相关的最短路径，提高交易确认效率和并发性能，分片链中只要符合主链规则定义的交易，都可以快速视为有效交易。

除区块链自身的特点去中心化、分布式账本、不可篡改之外，DAG 区块链技术不但可以支持高并发，结合双层共识机制，使用工作量证明共识算法，还能够防止“双花”问题。

### 3.2.3 分类动态账本技术

分布式账本是区块链的核心组成部分，对保证交易等各类信息的完整性和透明性具有关键作用。针对代码开发等的特殊性，围绕软件代码、存储空间的共享与交易等活动，ZitChain 设计了相应的分类账本，来实现对各类信息的存储和管理，主要包括交易账本、存储集群管理账本以及代码管理账本三类。

**交易账本**

主要用于记录代码交易、存储空间交易等涉及交易的相关过程信息，交易账本是不可篡改的。

**存储集群管理账本**

用于记录存储共享信息、集群节点分布信息、存储空间大小信息等涉及存储集群变更的数据。

**代码管理账本**

将与 Zit 协议相结合，用于记录代码的版本变更、代码提交、代码下载评论等信息。

### 3.2.4 双共识并行机制

目前的区块链应用为了保证分布式账本的一致性，主要采用以下 5 类共识机

制，即 POW、POS、DPOS、POOL、PBFT。其中，最具有代表性的方法是 POW（Proof of Work）和 POS（Proof of Stake），此方法也是目前业界价值最高的比特币和以太坊所采用的方式。然而，这些方法的局限性也较为明显。例如，POW 需要消耗大量的计算资源才能达成一次共识形成一个新的区块，而这些计算任务以解决密码学的复杂问题为基础，难以形成有效的计算力。

ZitChain 的混合链技术支持在公有链和分片链中采用双共识机制(PBFT 和 DPOS 双共识)。

在公有链中，我们采用 PBFT 共识算法(Practical Byzantine Fault Tolerance，实用拜占庭容错算法)维持基础交易的合法性。PBFT 共识在保证灵活性和安全性的前提下提供了(N-1)/3 的容错性，它使用加密技术防止欺骗攻击和重播攻击，以及检测被破坏的消息。每一个 Message 包含了抗量子公钥签名(RSA256 算法)、消息验证编码(MAC)、无碰撞哈希函数生成的消息摘要(Message Digest)等。

在分片链中可采用 DPOS 共识机制，对 Zit 代码托管业务层面进行验证管理。DPOS 通过投票选举中的超级节点完成交易确认，可大幅提高交易并发规模和确认速度，通过签名的可信任记账人证明，消除了交易等待验证的时间消耗，便于 ZitChain 用户快速提交业务请求，同时降低了交易手续费成本。

### 3.2.5 隔离见证与智能合约

为了保证 ZitChain 的高效运转和安全稳定，ZitChain 底层将采用轻量级的隔离式数据结构，将对不同类型的数据进行隔离存储、按需传输。此结构具体可分为：记录结余进出的“交易状态”、交易合法的“见证状态”，以及其他 ZitChain 中为了扩展区块链功能的特定状态信息。在传递过程中，不同角色的用户根据自身

的关注点可以个性化选择所需要的数据信息进行操作。因此，相对于完整的区块设计结构而言，隔离模式可大大减轻区块链中存储和通信的负载压力。

在隔离数据结构的基础上，ZitChain 的业务场景将采用智能合约的方式支持各类用户自定义的业务活动（如项目开发众包、代码版权交易等）和社区公共活动（如政策公投、创意征集等）。智能合约与隔离模式的有机结合，可以保证每一项信息或数据以按需、按权的方式进行交换传递，从而提高 ZitChain 运转的高效性和可信性。

## 3.3 基于 Zit 协议的分布式托管系统

### 3.3.1 IPFS 去中心化存储结构

传统的中心化存储方式存在访问性能瓶颈、存储可靠性与安全性低等一系列问题，ZitChain 将基于区块链技术构建一个完全去中心化的、可自由共享存储的高效分布式存储系统。基于该系统，平台用户可以共享空闲存储空间并获取激励，ZitChain 则基于用户共享的存储空间构建一个去中心化存储网络，并为软件代码托管提供高效、可靠、廉价的存储服务。

**存储空间的共享与交易**

用户通过安装 ZitChain 应用程序接入 ZitChain 社区，就可以自由的将个人电脑、手机等具有存储驱动设备上的空闲存储共享到 ZitChain 分布式存储网络，成为该网络的一个存储节点。ZitChain 则将用户共享的存储空间相关信息包括共享时间戳、存储节点标示、存储空间大小等记入存储管理账本。

当该存储空间被其他用户使用时，将根据相应的评估规则及共识算法，对共享存储进行计价并给予共享者相应的 Zit 币激励。

### IPFS 星际文件系统

去中心化分布式共享存储网络各个存储节点存在存储空间差异大、在线状态高度动态化等特点，为保证高效存储利用、高可靠数据存储与高效率数据访问等，我们采用 IPFS 星际文件系统对存储文件进行切割、映射和冗余存储。

IPFS 作为下一代文件网络传输系统，通过内容可寻址的对等超媒体分发协议，在 IPFS 网络中的节点构成一个分布式文件系统，可以让网络更快、更安全、更开放。全部的 IPFS 对象形成了一个被称作 Merkle DAG 的加密认证数据结构。

IPFS 对象是一个含有两个域的数据结构:

- Data – 非结构的二进制数据，小于 256kB
- Links – 一个 Link 数据结构的数组。IPFS 对象通过他们链接到其他对象

它具有如下特性：基于内容寻址，而非域名寻址；提供文件的历史版本控制器，可以让多节点使用保存不同版本的文件；IPFS 上运行的区块链，可存储 Zit 文件的哈希表；数字货币成为协调资源分享者和使用者的重要体系。

IPFS 对数据文件进行存储时，需要将大文件切分为多个小的分块，对其内容进行映射，并将对应 Hash 值通过多备份方式存储到多个不同的存储节点。各分块间关系及其存储位置等则被记录到存储管理账本中。数据文件进行下载时，则基于存储管理账本查找文件分块及存储位置信息，从多个服务器并行下载不同的分块，然后根据分块间关联信息聚合和重构整体文件。

### 存储位置选择策略

在进行文件分块存储时，需要首先确定各个分块的备份数量及存储位置，以

达到最佳的存储和访问效率。

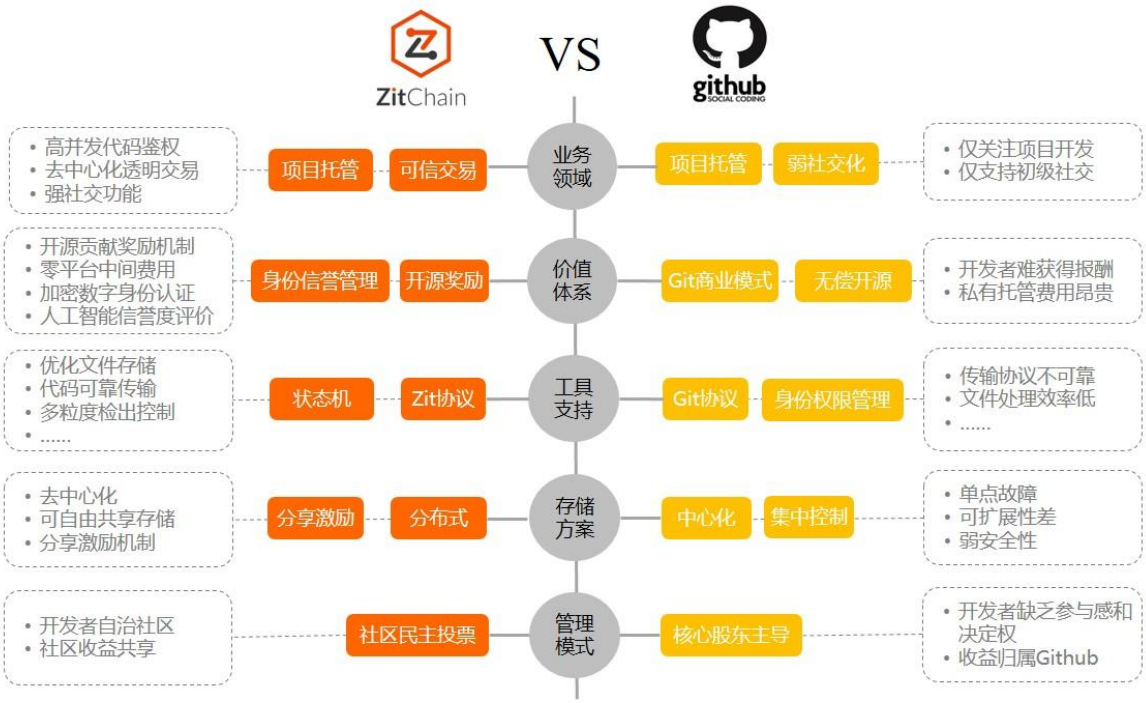
数据文件的存储基本策略是全局视图下的最优存储。通过围绕存储请求发起者节点及后续文件分块存储节点构建拓扑结构，设计采用多备份情况下多轮迭代的存储方式。在对初始分块进行存储时，我们采用最快到达原则，保证初始数据的快速存储；在后续备份块的传播存储过程中，选择了最远距离原则，保证后续文件下载时能够在全局视角达到最快下载速率。

### 3.3.2 Zit 分布式托管协议

Git 是目前在软件开发领域使用最为广泛的代码管理协议，围绕 Git 协议构建的社交化开发社区有 GitHub、GitLab 及开源中国等。尽管如此，Git 协议在实际使用过程中仍然存在较多问题，主要包括大文件的存储支持及大规模小文件的访问速度等。

ZitChain 的目标是结合区块链技术，针对 Git 协议面临的问题和局限，构建一个全新的面向软件代码管理的 Zit 协议，实现对大规模、分布式软件代码的高效管理，并在全网提供服务。

默克尔树文件处理是一种有效的碎片化文件管理方案。在 Zit 协议下载之前，先从可信的源获得文件的 Merkle 树根，一旦获得了树根，就可以从其他不可信的源获取 Merkle Tree。通过可信的树根来检查接受到的 Merkle Tree。如果 Merkle Tree 是损坏的或者虚假的，就从其他源获得另一个 Merkle Tree，直到获得一个与可信树根匹配的 Merkle Tree。




ZitChain 与 Github 对比图

### 代码文件存储优化

在软件开发过程中，项目相关文件中既有部分大的二进制文件，包括 Jar 包、设计资源库、SDK 等，也有数量规模非常大的代码小文件。对大文件进行高效存储与清理、对大量小文件进行快速读取等，是 Zit 协议需要解决问题。

Zit 协议将结合区块链技术构建代码管理账本，并基于分布式存储平台来解决高效大文件存储与小文件访问的问题。对于大文件的存储，将首先使用文件分割算法对大文件进行高效分割，切分为合适大小的文件分块，提交给分布式存储平台进行存储。

对于大量小文件的读取优化，则借助分布式存储平台多副本、多分块存储的

特点，通过多存储节点的并行多路下载，从而提升查询和检出效率。

### 多粒度检出控制

Git 协议的检出主要针对整个版本库特定版本进行，难以按需实现对不同粒度代码文件基于相应权限进行检出控制，对代码的检出效率较低。

Zit 协议以单个文件为最小检出单位，然后基于文件之间的关系对不同层级文件夹进行重构，实现对多粒度检出的控制。在提交存储时，将代码文件之间的关系以及文件权限信息记入代码管理账本。在进行检出时，获取文件存储位置及各文件之间的关系，然后将符合权限要求的各文件下载到本地，并根据文件间关系重构文件夹层级结构，实现多粒度按权限的文件检出。

### 代码文件可靠传输

ZitChain 基于分布式存储平台对代码数据进行存储管理，并对数据文件进行切割分块存储，可以有效实现代码文件的数据可靠传输，包括断点续传等。

在代码文件下载传输过程发生断网并在恢复网络后重新进行下载时，并不需要对整个数据文件进行重新下载，而仅需对部分未完整下载的文件分块进行下载。

具体过程为，首先对尚未下载到本地的文件分块开启下载；然后，对已下载到本地的文件分块，通过对文件内容映射的哈希值的比较，判断该文件分块是否已经完整下载，如果哈希值与预先存储的哈希值完全一样，则表明该分块已完整下载，不需重新下载。否则，则表明该分块未完整下载，则清除该分块并重新下载。在所有分块完成下载后，即可进行重构形成完整的数据文件。

### 3.3.3 跨链鉴权机制

ZitChain 的跨链鉴权机制包括用户身份管理和版权鉴定两个部分，以实现持续有效的代码版权保护。

**用户身份管理**

ZitChain 社区中每一位开发者都对应着唯一的身份信息，该身份信息用于标识开发者在社区内的各项活动，如社区讨论、交易、代码创作等。同时开发者身份信息也是用来保护开发者劳动成果原创性、侵权追责的重要依据。

在 ZitChain 社区中，开发者还可以围绕相同的兴趣或者目标组成小团体。在创建团体时，开发者通过协商的方式指定团体管理模式以及成员间的权益设定，如新成员是否需要通过邀请才能加入、团体成员间是否可以无偿共享资源等。

**版权鉴定**

ZitChain 为开发者提交的每一份原创代码生成 ECC(Encrypt Copyright Certificate,加密版权认证)证书作为它的唯一标记。ECC 证书是证明代码原创性的重要依据，能够有效地支持代码鉴权、授权、维权等服务。

ECC 证书主要包含以下几部分的信息：

**代码摘要** 利用散列函数，为每一段代码生成固定长度的哈希值作为代码摘要。散列函数是输入敏感的，它保证了不同的代码片段很难映射为相同的代码摘要值。

**代码作者** 用户在 ZitChain 社区的账户信息作为代码作者的身份标识，如果该段代码还曾使用过其它开发者的代码，那么这里还会包含被使用代码的 ECC 证书。

**创建时间** 使用 UTC 加盖时间戳确保了版权登记时间的权威性和可靠性，先创作代码并先申请的开发者优先对代码获取版权。

**授权协议** 代码所有者可以指定其它开发者以何种方式使用他的原创代码，包括授权策略和具体实施方式等内容。双方在智能合约的作用下自动履行授权协议，协议履行的效果被社区所接受和保证。

ECC 证书存放在区块链上，保证了公开性、不可篡改性和可追溯性。任何开发者可以随时查看 ZitChain 社区的代码版权信息，但其所包含的内容却很难被人恶意篡改。根据其所包含的代码授权记录，开发者还可以还原出完整的代码使用（授权）路径。

在生成 ECC 证书前，为判定代码的原创性，首先利用自然语言处理和抽象语法树等技术对给定代码进行分析建模，抽取出其所包含的功能性代码（如文件读取、数据库访问）和业务逻辑代码，然后从多粒度和多维度计算它与已登记的版权代码进行比对，从而判断提交的代码是否存在侵权问题。

### 3.3.4 MTSM-多任务并行状态机

MTSM(Mutlti-Task State Machine)状态机是 ZitChain 独创的多任务并行状态机技术，其核心任务是保证开源托管代码系统的代码安全性、鉴权业务、Zit 网络安全等。

MTSM 状态机与 ZitChain 系统并行运行，实时监测 ZitChain 系统安全，确保 Zit 网络数据输入输出的合法性，同时提供源代码鉴权服务。

MTSM 状态机重点完成以下三个任务：

**1、代码安全管理：**MTSM 状态机采用一种基于肯定选择分类算法的恶意代码检测机制，在后台实时对 Zit 碎片化代码库进行监测。代码输入后，MTSM 状态机将样本文件转换成十六进制格式，提取样本文件的所有 n-gram，计算具有最大信息增益的 N 个 n-gram 词频，然后做归一化处理。该算法优化了分类器训练过程，优于朴素贝叶斯、贝叶斯网络算法，支持向量机和决策树等算法。

**2、代码鉴权服务：**MTSM 状态机后台实时对链上代码库进行动态扫描，采用 BP 神经网络等多种技术，检测链上代码相似性。其中，人工神经网络试模拟人脑生物过程的人工智能技术，由大量的神经元互连形成复杂的非线性系统。误差反向传播（BP）神经网络可以实现输入和输出间的任意非线性映射，其核心思想是将代码转化为神经智能网络的输入向量，通过神经网络学习，检测代码之间的相似性，从而给出代码鉴权建议或结论。

**3、安全沙箱监测：**通过延时检测链上账本、链上节点等交易记录，MTSM 状态机可有效分析出节点的活跃特征和交易记录的合法性。当发现交易记录非法或恶意节点时，MTSM 状态机将采用事件驱动机制，通知共识节点，及时剔除非法账本（不可篡改的账本除外），并将恶意欺骗节点从网络中删除。

## 3.4 ZitChain 应用生态

ZitChain 提供了一系列的客户端应用软件。利用这些软件开发者可以方便快

捷地参与社区的各项活动。

**在线社区平台**

ZitChain在线社区平台支持开展社区运营、资产管理及用户交互等三类活动。各自的具体内涵如下：

**社区运营** 公开透明的社区运行模式是 ZitChain 成长为一个健康的共治社区的重要前提，社区委员会的各项事务均在线上公开进行，开发者对社区发展的建议和意见也都集中反馈到在线平台上。

**资产管理** 开发者可以在在线平台管理个人资产，还可以与其他开发者进行线上交易。开发者在使用资产服务前需要进行个人身份验证，以保证资产账号的真实性和安全性。安全可靠的资产服务是保障开发者合法权益的必要措施。

**用户交互** 基于在线平台，开发者之间可以开展一系列的交互活动，例如以众筹和悬赏的形式为某个新颖的创意和复杂的任务提供解决方案。丰富多样的用户交互渠道是充分发挥和利用开发者才智、发掘隐藏在社区中群体力量的有效手段。

**资源共享管理系统**

ZitChain 把开发者的源代码通过分布式的形式存储在全网，有贡献意愿的开发者通过资源共享管理系统来共享自己本地的计算资源。该系统提供图形化和命令行形式的管理工具，辅助开发者完成对共享空间和共享带宽的设置和调整。

**Zit 客户端**

开发者使用 Zit 客户端在本地完成代码提交、同步等操作。Zit 基于 Git 开发，

是对 Git 协议的一次重大改善和升级，它被设计为是 Git 用户友好的协议，兼容 Git 协议的绝大部分命令，Git 用户几乎可以零成本地采用 Zit。

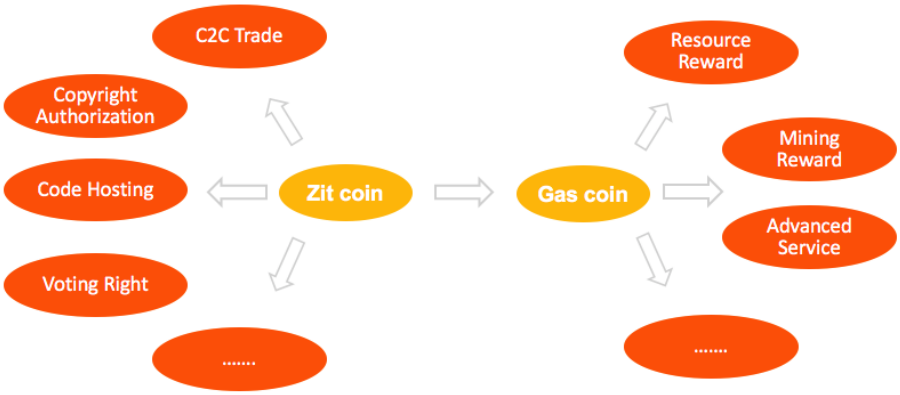
# 第四章 ZitChain 经济模型

ZitChain 是基于开源理念和区块链技术的全球开源应用新生态社区，其核心本质是围绕开源应用重新定义的商业价值体系。这个商业体系，由开发者共建、为开发者服务、使开发者谋利。

ZitChain 的经济模型包含 3 个主要的价值流转场景，具体包括：个人闲置计算资源的共享奖励、社区贡献的公共奖励、以及社区成员劳动成果的自由交易。前两个为数字货币的主要来源，最后一个是代币流通的主要场景。

## 4.1 数字货币体系

ZitChain 基本商业元素包括开发者、矿工、开源软件用户、开源应用服务机构、证书颁发机构、第三方组件开发者、商业合作伙伴等。在 ZitChain 系统中，所有社区参与者都是去中心化的共治者：参与者在既定的商业规则下共同完成开源托管相关业务活动，包括代码托管、版权管理、众筹打赏、付费使用、基础网络建设、资源共享等。




ZitChain 的货币体系和流转场景

执行商业模型、完成价值流转的核心协调机制就是数字货币。为实现这一目

的，ZitChain 采用双代币机制，代币分为基础代币和燃料代币两种。

基础代币用于以下场景：

**C2C Trade** 支付 ZitChain 常规业务的费用，包括代码托管、版权管理、众筹打赏、付费使用等。

**Copyright Authorization** ZitChain 用户之间的价值流转。

**Voting Right** 社区选举投票权的权重核定与价值持有凭证。

**Code Hosting** 当燃料代币不足以支付时，自动转换成燃料代币，以确保完成交易。

燃料代币用于以下场景：

**Mining Reward** 矿工提供基础网络设施和交易确认的账本费用。

**Resource Reward** P2P 资源共享者所收取的资源费用。

**Advanced Service** 用户使用高级功能所需要支付的服务费用。

## 4.2 价值核定与分配

ZitChain 完全采取去中心化的分布式计算模式，因此在计算资源基础设施建设方面，社区鼓励参与者积极贡献出自己空闲的存储空间、CPU 或 GPU 计算资源和网络带宽，从而从根本上保障 ZitChain 社区整体的信息处理能力。为了激励参与者积极主动进行贡献，社区将采取“贡献早收益早，贡献大收益大”的基本原则对资源贡献者进行奖励。从时间维度上来说，如果社区参与者早期贡献出一定量的计算资源，则其获得的奖励会比之后贡献出同等价值资源的参与者要高。同样的，从贡献价值来说，贡献的资源稀缺性越高、资源量越大，则其获得的奖励

越高。具体来说，社区对于某个贡献者在时刻 t（如 2018 年 1 月 1 日，12:00）贡献的某类资源 r（如 300M 存储空间）对应的奖励公式如下所示：

$$\mathrm{Award_{rt}} = Award_{stand} \times \lambda_t \cdot \frac{T_{init}}{T_{con}} \times \lambda_r \cdot \frac{R_{con}}{R_{total}} \cdot I_r$$

其中，$\lambda_t$和$\lambda_r$是收益调和因子，用于权衡时间维度和价值维度之间的比重；$\frac{T_{init}}{T_{con}}$表示社区开放时间（$T_{init}$）与资源贡献时间（$T_{con}$）的比值，用于保证越早共享资源的参与者获得更高的电子货币；$\frac{R_{con}}{R_{total}}$表示资源贡献量$R_{con}$与社区空闲资源总量$R_{total}$的比值，用于保证资源共享相对越大的参与者收益约高；$I_r$是此类资源 r 对于当前社区整体行为在计算方面的重要程度系数。例如，对于程序员需要提交上传 100 行代码这一特定行为来说，我们假设需要 1M 的存储和 10kb/s 的带宽，而当前社区中空闲了 100M 的存储空间和 1kb/s 的上行带宽。那么对于这一场景来说，存储空间的紧迫程度比带宽要小得多，从而贡献带宽的参与者将比贡献存储空间的参与者获得更高的收入。$I_r$系数是根据社区特定阶段所有交易的监控与分析结果从全局视角计算而来，并且会随着社区的持续演化而动态变化。

## 4.3 社区贡献激励机制

ZitChain 要打造一个彻底由开发者缔造、被开发者共有、为开发者谋利的共治社区。因此，社区要对积极参与社区公共建设的参与者给予奖励。目前，我们考虑两种最直接的社区公共贡献行为：贡献出优质的软件项目和提出了促进社区良性发展的意见。

### 4.3.1 内容共治激励

如同优秀的书籍对于图书市场、优秀车型对于汽车市场一样，优秀的软件项目是开发者社区良性生态构建与发展的基石。直至今日，无论是商业软件还是开

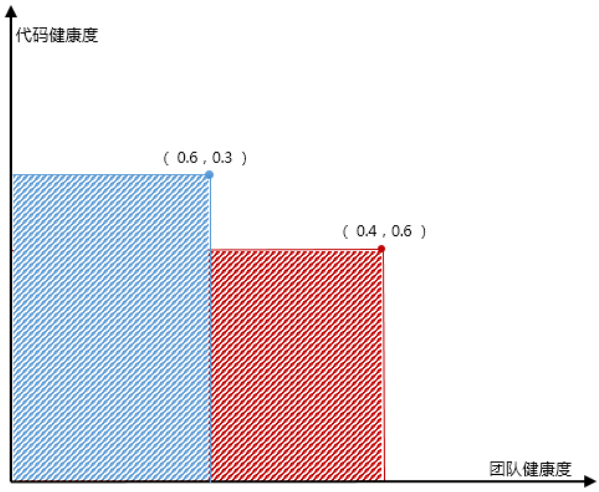
源软件都已经数十年的蓬勃发展，软件市场已经积累了种类繁多但质量又参差不齐的软件项目。因此，ZitChain 为了吸引优质的软件项目迁移到本社区，将根据项目的优质程度发放奖励货币，其中软件项目的优质程度可从传播效应、项目成熟度、代码健康度、开发团队健康度，和项目发展趋势五个维度进行度量，具体指标如下表所示。

| 度量维度 | 度量指标 | 度量指标介绍 |
|---|---|---|
| **传播效应** | 下载总量 | 软件在各大托管社区的下载次数，可衡量软件在市场应用的基本规模。 |
| | 复用次数 | 依赖于本软件进行开发的软件数量。 |
| | 用户讨论热度 | 软件在各大知识分享社区的用户讨论热度、相关技术介绍与培训材料等。 |
| **项目成熟度** | 持续维护年限 | 软件项目的从创建开始至迁移时的开发与维护年龄 |
| | 项目关注度 | 项目 fork、star、watch 的数量 |
| **代码健康度** | 缺陷解决速率 | 项目缺陷的平均修复时间 |
| | 缺陷修复率 | 缺陷修复的比例 |
| | 代码静态质量 | 静态代码质量检查工具的分析度量，涵盖了漏洞风险、复杂度、代码风格、注释率等 |
| **团队健康度** | 团队规模 | 代码贡献者数量 |
| | 人员增长率 | 当前时间段内新加入的贡献人员比例 |
| | 持续贡献率 | 上一个时间段的贡献者在当前时间段持续贡献的人员比例 |
| **项目发展趋势** | 提交活跃度 | 项目代码提交的增量 |
| | 任务增长量 | 项目开发任务的增量 |
| | 关注趋势 | 项目在社区受到关注人数的增量 |

基于上述 5 个维度的量化度量，我们在归一化后可以通过 5 位空间曲面面下体积衡量出被迁移项目的优质程度，则相应的奖励计算方法如下公式所示，其中$f(\mathrm{x_p})$为被迁移项目 P 的曲面函数，$x_p \in X$是每个维度的具体度量。

$$\mathrm{Award(P)} = Award_{stand} \times \iint \mathrm{f(x_p)}\, dS,\ x_p \in X$$

由于高维空间难以清晰的展示和表达上述思想，在此我们以 2 个维度，即代码健康度和团队健康度为例，简述本方法的基本思想。假设我们有两个被迁移项目 P1 和 P2，其中 P1 的代码健康度为 0.6、团队健康度为 0.3，项目 P2 的代码健康度为 0.4、团队健康度为 0.6。在二维空间中，P1 可表示为坐标（0.6，0.3），P2 坐标为（0.4，0.6），绘图表示后 P1 的曲面函数可表示成蓝色平面，P2 为红色平面。因此，P1 的优质程度为蓝色平面面积对应的值，P2 项目的优质程度为红色平面面积对应的值，即两个项目的优质程度被量化表示。同理，在高维空间中，项目的优质程度可对应曲面下体积，具体量化数值可通过双重积分求得。




ZitChain 中的软件项目评估模型

### 4.3.2 社区建设激励

ZitChain 的理念是充分的民主化，鼓励社区中的每一位成员对社区的现状和发展提出自己的意见和建议。意见征集模式类似于头脑风暴，针对社区中某一问题，社区全体成员行动起来一起贡献意见和建议。作为对参与用户的回报，社区会拿出一部分电子货币作为奖励。奖励的发放采取后验模型，即社区会对征集到

的意见进行多轮筛选，通过对可行性和有效性等多维度的考量，选出少数几个较优秀的方案进行实现并评估；最后，社区根据各种解决方案的实际效果进行奖励，具体的奖励计算公式如下：

$$\mathrm{Award(T)} = \mathrm{E}\,(1 - e^{-T}) \quad \mathrm{T} = 1,2,3,\ldots\ldots$$

其中 T 是对意见的实际应用效果的观察窗口期，比如社区可以规定以一个月或三个月为周期对其效果进行观察。E 是在第 T 个观察窗口期内，被观察意见所取得的效益值。比如，由于某位开发者的意见，社区改进了平台服务而吸引了越来越多的用户。假如社区指定每增加一个新用户就奖励意见提供者一个单位的代币，那么一个观察期内新增加的用户数就是该意见在该观察期内所取得的总效益值。该方案会使得那些能够产生长期效益的意见持续性地获得越来越丰厚的奖励。

## 4.4 开发者价值模型

开发者可以在 ZitChain 进行开发者之间的 C2C 交易，常见的交易场景如下。

**代码交易**

当开发者想要使用他人的原创代码时，他需要接受该代码的授权协议并付费。代码授权方式可以有两种可选策略：（a）先付费后使用（Pay Then Use, PTU），代码使用者一次性付清代码所有者要求的 Zit 币。付费完成之后，代码使用者后续对该段代码的任何应用和盈利等行为与代码所有者不再有任何关联。（b）先盈利后付费（Earn Then Pay, ETP），代码的直接使用行为不收取 Zit 币，只有在使用者利用该段代码获利后，代码使用者才需要向代码所有者支付 Zit 币。

### 任务悬赏

开发者遇到难题时，可以在社区发布悬赏任务并提供奖励金，提供解决方案的用户依据规则获取相应的奖励金。奖励金的发放有两种方式：(a)只有一名胜出者获得全部奖励金，该胜出者由任务发布者从提供正确解决方案的用户中选择，或者由平台通过多维指标评判出最优解决方案；(b)由全部提供正确解决方案的用户所共享，每位用户获得的奖励金份额为：$M/2^n$，其中 M 是总的奖励金额，n 表示该用户是第几个提供解决方案的，即越快提供正确解决方案，获得的奖励金额就越多。

### 咨询服务

开发者还可以通过向专家咨询的途径来解决自己的问题，具体的收费由被咨询的专家指定。由于每个开发者的能力和收费标准都公开在社区，开发者可以根据实际需求做出最经济的选择。

### 创意众筹

虽然个人的能力往往是有限的，但是开发者可以在社区通过众筹的方式来实现自己创意。感兴趣的用户可以投入资金或者技术，而投入的多少由用户自己决定，这些投入都记录在区块链上，在加速开发者创意快速实现的同时也保障了投资人的权益。

### 资讯订阅

开发者为保持对相关领域最新动态的持续关注，他可以订阅领域内权威开发

者或者活跃开发者的动态，以第一时间获取相关技术的发展趋势和线上线下讲座等信息。订阅费用由被订阅者指定，可以采用月费、季费、年费的形式。

### 社交互动

基于社区平台，开发者可以开展一系列的泛社交互动，在社交互动中开发者可以方便地进行各种形式的交易。如开发者在平台直播写代码时，观看者可以根据自己的喜好进行打赏，而打赏金额由打赏者随意支付。

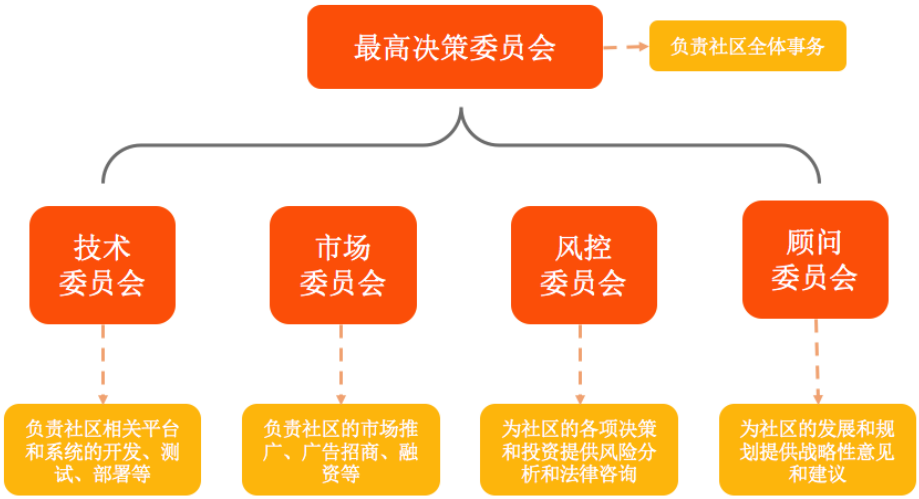
# 第五章 ZitChain 战略规划

## 5.1 社区治理架构

为保证社区持续、健康、高效地发展和运行，ZitChain 建立社区共治委员会。委员会由全体社区成员选举产生，并代理全体社区成员行使权力。

### 5.1.1 委员会机构设置

如下图所示，委员会设置最高决策委员会，下设各职能委员会。最高决策委员会负责社区的整体事务，各职能委员会分管社区相关事务。




ZitChain 社区治理结构图

### 5.1.2 委员会管理规定

ZitChain 为社区委员会制定管理规定，以确保其真正地服务于整个社区，并时刻保持活力，能够为社区的发展发挥积极正面的作用。社区委员会更多的是以组织者而非决策者的身份获取社区民主意愿，用公正、透明的机制保障社区运营，贯彻社区意图，履行社区使命。

### 人事任免

首届委员会成员由 ZitChain 创始人团队、开源领域专家、区块链技术专家以及前期投资人士和顾问组成。后续每两年选举产生新一届的委员会，新的委员会成员由社区选举产生，委员会成员可连任，上一届委员会成员有权利提名新一届的委员会成员候选人。在非委员会换届选举期，由于人员流动和自然离职造成的职位空缺，由委员会在任成员提名，经社区投票，可进行相应职务的人员替补。

委员会成员在任期间若出现违法犯罪活动会被就地免职，且永远不允许其重新进入委员会担任任何职务。委员会成员在任期间若未能较好履行职责或出现重大失误，经其他委员会成员提议并经社区投票后可被辞退，但保留其后续通过投票重新进入委员会的权利。

### 投票制度

ZitChain 社区所有的成员都有投票权，社区委员会发起的投票需要至少一半的有效票，任何提议的通过都需要获得至少一半的赞成票。社区成员拥有的代币的数量和币龄决定了其投票的权重，代币数量越多、币龄越长，其投票权重越大。

## 5.2 发展计划及说明


ZitChain 战略发展计划图

# 第六章 结论

IT 的世界就是开发者创造的，他们是一群充满创造力的能工巧匠。基于区块链技术，彻底解决天下开发者间的信任问题，ZitChain 创新地利用去中心化的协作模式，打造去中心化的开发平台，实现去中心化的利益分配机制，这是对开源精神的践行，对互联网协议的升级，对中心化利益分配机制的颠覆，对开发者的解放。全球目前约有 1 亿左右的开发者，每年创造着数万亿美元的市场价值。ZitChain 帮助开发者迅速崛起就是更有效地推动人类社会的进步。因此，我们相信 ZitChain 的数字货币将甚至不止于百亿美元规模：一旦开发者的创造力被无限激发，下一个伟大的技术很可能就诞生于 ZitChain。