

G R O U P C H A I N

# 社团链白皮书

社团链 - 链接每个人



全球社团通用积分

# G R O U P C H A I N



## 目录

CATALOG

- 1 GROUP CHAIN 项目背景**
  - 1.1 社团发展历史和社会意义
  - 1.2 新时代社团组织发展面临问题
  - 1.3 区块链技术发展带给社团的革新
- 2 GROUP CHAIN 项目介绍**
  - 2.1 全球社团通用积分介绍
  - 2.2 全球社团通用积分优势
  - 2.3 全球社团通用积分应用场景
- 3 GROUP CHAIN 功能模块和关键技术**
  - 3.1 全球社团通用积分技术框架
  - 3.2 全球社团通用积分参与方
    - 3.2.1 社团组织
    - 3.2.2 社团会员
    - 3.2.3 社团公共资产
    - 3.2.4 非社团成员

**3**

- 3.3 全球社团通用积分系统模块
  - 3.3.1 零知识身份认证系统
  - 3.3.2 社团链账户管理系统
  - 3.3.3 信息数据存储系统
  - 3.3.4 底层智能合约引擎
  - 3.3.5 资产管理系统和数字钱包
  - 3.3.6 匿名支付系统
  - 3.3.7 去中心化信息即时通讯工具
  - 3.3.8 任务合作体系
  - 3.3.9 用户积分体系

**4**

## 通证机制及发行方案

- 4.1 GTOKEN通证经济模型
- 4.2 GTOKEN通证发行及分配方案
- 4.3 GTOKEN通证交换及锁仓机制
- 4.4 创始团队通证解禁计划

**5**

## 投资机构和团队

- 5.1 核心创始团队
- 5.2 顾问
- 5.3 投资机构
- 5.4 技术支持
- 5.5 特别合作机构

**6**

## 全球社团通用积分执行路线图

全球社团通用积分（简称：社团链GROUP CHAIN）项目将围绕公链技术开发、用户导入、场景落地、大事件营销、社群生态建设五个维度加速推进。

**7**

## 联系方式

官方邮箱: universalgroup2018@outlook.com  
官方网站: gtoken.world  
法律声明  
免责声明





为了开展革命运动，孙中山决定加入洪门。于是，经洪门前辈、孙中山的叔父钟水养介绍，孙中山于1903年冬天，加入了洪门最大的组织——檀香山致公堂。与孙中山同时拜盟的有60余人，就在国安会馆举行入盟礼节，并由主盟人封孙中山为“洪棍”（洪门称“元帅”为“洪棍”）。

——摘自《司徒美堂》  
(广东省出版集团、广州人民出版社联合出版，张健人、黄继烨合著)

我旅美侨胞，过去尝有见仁见智之殊，而自抗战以来，亦能感于‘兄弟阋墙外御其侮’之箴言，输财出力，精诚团结，此种为民族为国家之正气，愿我同侨永保勿坠，抑更有当为我洪门兄弟告者，我洪门之共同目的，愿在为民族独立，为国家争生存，在昔赞助孙总理戮力革命，缔造民国，劳绩昭著，在人耳目，深望我洪门兄弟，念已往之光荣，思当前之天职，一德一心，共赴国难。

——中国洪门致公党创始人司徒美堂、《致旅美侨胞及洪门兄弟书》

洪门现有1000余万昆仲分布在世界各地，这1000余万昆仲身份涵盖三教九流。洪门需要有一个应用区块链技术的联系平台，让各国洪门兄弟之间的交流更紧密；让海外的洪门兄弟们和祖国联系的紧密；当祖国需要的时候，洪门兄弟可以拧成一股绳并形成一股能够助力祖国发展的力量。

——国际洪门世界总会主席刘沛勋

# 项目背景

PROJECT BACKGROUND

## 1.1 社团发展历史和社会意义

自人类形成社会制度以来，自发或被迫形成了各个组织社团。现代民权理论将结社自由视为一项基本人权，是历史发展到一定阶段的产物。社团形成的原因与人作为群居动物而产生的社群意识和本能有着千丝万缕的内在关联。它的形成基于人类的社会需要，基于人类合群的天性和个体综合资源的有限性。中国的结社活动发轫于先秦，自汉迄清再到现代一直延续，期间虽有盛衰但其活动却并无停歇。

社团的职能是基于社团所属成员的需求为成员谋取利益。可以说，社团的存在大大促进了社会的发展和人与人之间的和谐。首先，社团生活可以满足团体成员的精神需要。无论是宗亲类结社还是地缘性、宗教性结社，社团的存在大大加强了成员间的情感满足强度；其次，社团结合有助于社团成员抵抗生存困境，提高生存能力。再次，社团有利于个人的发展，在社团中，一些人潜在的兴趣和才能够得到充分的展示和发挥，大部分社团都会为其社团成员的发展提供直接的支持并在社团成员中发现和培养领袖人物，如科举制度下的“同年组织”，客居他乡的“同乡组织”。最后，社团还具有社会整合功能，通过社团将社会联结为彼此依赖、相互作用的有机体。社团的存在，为个人与个人、个人与组织、组织与组织的联系提供了载体，尤其是在城市，社团的整合功能是非常显著的，如清代中后期的汉口行会组织，为城市的经济发展起到了不可磨灭的作用。



## 1.2 新时代社团组织发展所面临的问题

进入新时代，互联网、通讯设备、管理工具等新科技、新应用降低了社团成员之间的沟通成本和社团组织成本，同时社团组织百花齐放，产生了各种特色的社团，极大地丰富了人类的社会生活。但是，也给传统的社团组织形式和管理模式带来新的挑战。

一是信息泛滥与信息安全。随着互联网新技术的发展，社会信息化程度日益提高，信息资源日益丰富，在推动经济发展给人类生活带来便利性的同时，与之相伴也会产生严重的信息泛滥及安全问题。无用和虚假信息的发布会严重扰乱社团正常的运作程序，降低整体的工作效率，甚至严重影响社团的良好声誉。同时，对于社团来说，成员的构成是使其不断发展壮大核心竞争优势，因此成员信息安全也就关系到整个社团组织的安定与发展。一个社团会产生大量的个人相关信息。然而在利益的驱使下，很多非法组织或个人会盗取这些社团成员的个人信息。因此，如何维护自身的信息安全与隐私，已成为保持社团持续发展的关键问题。

二是联系不紧密，流动性增大。社团以各个成员为点，相互连接构成一个庞大的组织，牵一发而动全身。这其中人与人的联系就成了维系社团安定的重要环节。传统社团通过组织各类活动增加成员间的相互联系和沟通，但当前社会形势下，各类社会团体纷纷涌现、诱惑众多，成员流失已成为不容忽视的问题。如何在众多社团中脱颖而出，增加社团会员的归属感是每个社团都要面对和解决的。能否提高社团成员的忠诚度，尤其是核心成员的长期忠诚及稳定决定了一个社团的兴衰成败。

三是信任机制很难建立。社团犹如一个小型社会，成员间各种利益关系错综复杂，因此产生的利益分配问题会引发社团内部的信任危机。社团成员之间关系的维系和合作分工大多依靠成员之间的信任默契，所以最早的社群组织源自于有血缘关系的宗亲家庭，随着社会的发展和分工的细化，进而又形成以共同目的维系社群稳定的帮派、政党、老乡、同窗、行业协会等各式各样的社团组织。同时，由于各级别社团所占据的资源不同，跨社团的合作需求是非常旺盛的，但因信任机制不成熟往往又难以满足。对于社团组织来说，其社群稳定并取得发展的核心因素就在于因各种原因形成的内部信任体系。

### 1.3 区块链技术发展带给社团组织的革新

区块链本质上是一个去中心化的分布式账本数据库，其价值在于通过构建自组织网络，使用密码学相关算法产生一连串数据块。每一个数据块中包含了多次交易有效的确认信息，且时间有序不可篡改。由此建立分布式共识机制，从而实现去中心化信任体系。

简而言之，就是一个数据库存储系统，相对传统数据库或者数据中心，区块链的存储系统分布在世界各地、能够协同运转，也就是所谓的去中心化。“区块链”技术允许任何有能力架设服务器的人都参与其中，都可以成为分布式数据库存储系统中的一个节点，这些节点都是平等的，可以对这个系统中的任意节点进行读写操作，并且所有节点都会同步，以保持数据的一致。

所以，“去中心化”具备开放性、自治性，数据库的信息也不会轻易地被篡改，而且交易双方具备一定的匿名性。

社团组织的运转靠内部成员之间的信任机制和社团不同层级间的信息传递形式来维系。区块链技术将会为社团组织的发展注入新的技术基因。一是为人类带来一种更可靠也更广泛的信任体系，区块链技术底层智能合约机制能够让合约按照事先约定好的事项自动执行，不可更改也不可单方撤销。同时区块链技术能够清晰留存合作相关的各方信息，甚至包括个人的历史背景，并无法更改。使每个人的违约成本大大增加，进而促进了社会全方位信任体系的建立。二是信息溯源杜绝欺诈，区块链技术能够对每一个产生的数据块进行历史数据留存，因而在某些需要溯源的关键信息中能够方便的找到信息源头，进而杜绝了虚假信息和欺诈信息在链上的传递。同时还能保证数据记录的客观公平，区块链的最长链机制，保证了记录的相关信息一定是受最大部分人认可的信息。社团的社交场景和组织形式与区块链技术的应用场景完美匹配，区块链技术的优势能够带给社团组织新的发展动力，为社群组织的管理、用户合作形式、社交行为偏好和资产交易手段带来新的改变。



# 项目介绍

## PROJECT INTRODUCTION

### 2.1 全球社团通用积分介绍

全球社团通用积分（UNIVERSAL GROUP TOKEN）旨在打造全球社团的第一公链（简称社团链GROUP CHAIN），利用区块链技术的去中心化、分布式账本、不可篡改的特性，围绕社群组织发生的场景，包括社团管理、用户社交、身份证明、任务发布、跨境支付、公共财产管理等，打造全维度社群生态逻辑，重构社团之间生产和社交关系。全球社团通用积分集成了区块链各底层技术，包括底层智能合约引擎、参与式决策（PARTICIPATORY DECISION MAKING）算法、点对点（PEER TO PEER）协议和零知识证明系统，为全球社团及其成员提供一个集资产管理、信息储存、私密社交、信用认证和交易结算等于一体的区块链化全维度社群生态服务。

### 2.2 全球社团通用积分优势

#### 2.2.1 国际洪门总会支持

社团链（GROUP CHAIN）得到了国际洪门总会的鼎力支持，国际洪门总会将作为基石投资人参与该项目，并率先将该区块链平台应用于全球洪门各山、堂等组织，作为洪门各地堂口的主要管理系统。社团链涵盖各堂口日常管理的各种场景，包括信息管理、数据储存，任务发布、用户信息认证以及线上投票等，将成为全球洪门昆仲的数字社交、经济、信息交流和管理平台。

洪门组织自开山立堂300多年来，帮众、隐秘分支众多，包括天地会、三合会、红花会、共济会、致公堂等，为中华民族保家卫国，抗御外侮，铲除军阀、发动革命做出了卓越的贡献，祖国两岸统一的坚定支持者。中国近代民主革命伟大先行者孙中山为了开展革命运动，决定加入洪门。于是，经洪门前辈、孙中山的叔父钟水养介绍，孙中山于1903年冬天，加入了洪门最大的组织——檀香山致公堂。与孙中山同时拜盟的有60余人，就在国安会馆举行入盟礼节，并由主盟人封孙中山为“洪棍”（洪门称“元帅”为“洪棍”）。当年黄兴开设的“同仇会”，陶成章、章太炎组织的“光复会”，黄花岗七十二烈士都属于洪门。伟大的爱国主义者、中国致公党创始人司徒美堂先生也是洪门大佬，并于1925年10月改组美洲致公堂为中国致公党，对发动海外华侨支援中国革命和抗日起到了较大的作用，成为新中国成立之后的八大民主党派之一，开国大典时司徒美堂先生在天安门城楼站位就在毛主席身边。

1992年7月28日在美国檀香山宣告成立国际洪门总会。总会章程中提出了“团结洪门昆仲，发扬洪门忠义精神，振兴伦理道德，提倡社会福利，服务人群，造福人类”的宗旨。2004年，刘沛勋先生就重新修订了国际洪门五大任务：发扬洪门忠义精神、宣扬中国传统文化、推动两岸经济文化交流、促进中国和平统一、实现中华民族伟大复兴。现今，全球洪门各地昆仲有1000余万人，洪门直接或间接控股、参股、投资的企业、基础设施、公共事业、旅游、酒店、博彩等实业分布在世界各地，洪门的综合资源将成为全球社团通用积分项目顺利落地的核心资源。

#### 2.2.2 社团生态天然和区块链技术匹配

社团的应用场景和组织形式天然与区块链技术相匹配。可以说人类结社的初衷就是源于共识，而区块链技术的核心就是就在于共识机制。区块链技术的DPOS机制和传统社团的组织形式亦高度匹配，每一个社团可以说都是一个节点，一个大的社团就是一个超级节点。而分社与总社更像是DPOS节点的多级委托机制。社团组织的核心是人流，区块链通证经济的核心也是用户数。区块链技术的去中心化、信任机制、身份证明体系、不可篡改的特性又与社团生态需求高度匹配。

#### 2.2.3 亦来云、IBM、微软等IT、公链巨头的鼎力支持

全球社团通用积分项目不惜重金，选取与亦来云、IBM、微软等IT、公链巨头进行技术合作。社团链平台云服务、代码审计、应用模块等将从上述公司进行技术采购、服务外包及咨询顾问。以确保应用场景落地的可靠性、稳定性，用户体验的流畅性、人性化。



## 2.2.4 清晰的通证经济模型

全球社团通用积分的将采用DPOS机制，根据节点的持币数、有效地址数进行实时动态超级节点决选。让更多社团（社团即节点）成员应用该系统，加入全球社团通用积分生态，共同分享持币红利。清晰的激励模型，会促进传统社团用GTOKEN替代法币进行工资发放、贸易往来、项目众筹、捐款。让更多的社团成员持有TOKEN，以支持所在社团在超级节点竞选中胜出。

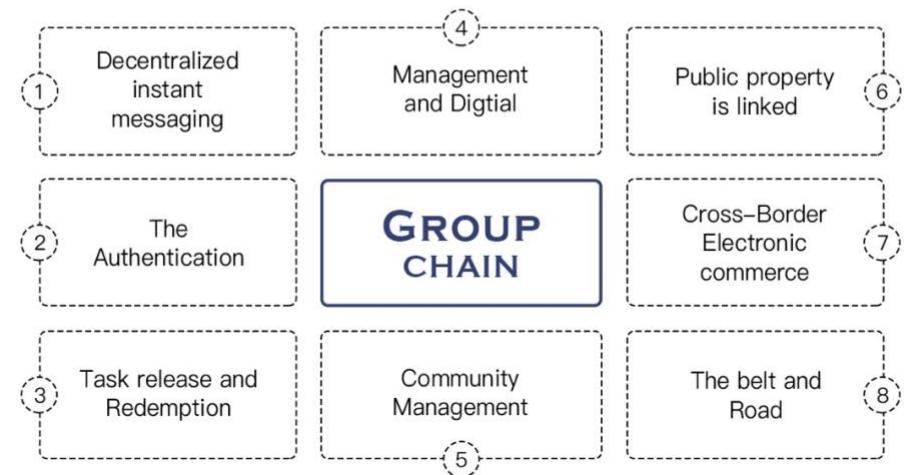
## 2.2.5 能够产生正现金流的八大场景

全球社团通用积分项目选取了去中心化即时通讯、零知识身份证明、任务发布和兑领、资产管理和数字支付、通证化的社团管理、公共财产上链、跨境电商、一带一路基础设施建设能够形成正现金流的八大场景。上述场景容易落地、跟社团生态高度匹配，且均为刚需型、资源依托型场景。能够导入人流的通证经济模型、能够产生正现金流的应用场景、洪门1000万昆仲的基础用户、强大的技术生态合作伙伴共同构建了全球社团通用积分做为明星项目的要素资源。

此外，通过DPOS投票机制，使社团数据上链、投票过程公开，能够最大程度的保证社团共识的公平公正。



## 2.3 全球社团通用积分应用场景



### 2.3.1 去中心化即时通讯

通讯信息安全无论是对于个人还是对于社团组织都十分重要，是未来社会中十分关切的问题。通讯信息安全是社团稳定发展的重要因素，其往往与社团的优势资源和核心机密相关。去中心化的即时通讯工具是全球社团通用积分项目的一个重要应用场景，区块链技术将会使该公开的数据无法被隐藏，该隐藏的信息无法被公开，全面提升人与人之间的社交信任和效率。全球社团通用积分将为公链上的所有社团组织、社团成员，不限制国家和地区，提供一款基于P2P协议的即时通讯社交工具，保障社团组织和个人的信息安全，防止信息泄露。

用户既可以直 接导入手机联系人、WHATSAPP、WECHAT等社交工具上的好友关系，以群聊的形式进行通讯，也可以通过公链上的即时通讯工具实现点对点的匿名社交，并支持阅后即焚等保障客户隐私和信息安全的社交形式，满足用户间不同的即时通讯需求。此外，该公链支持包括文字、图片、表情、语音、文件，以及免费语音，视频等多种形式的通讯，能够为公务和商务客户提供实时语言翻译的需求，使跨国社交无障碍，实现用户快捷方便的交流。

### 2.3.2 身份验证

在信息化时代，身份验证是保障个人信息安全和财产安全的重要凭证，一旦身份信息被冒用，将造成严重的社会和经济损失。对于社团组织来说，身份验证是用来判断是否为本社成员的重要手段，尤其是在涉及到一些机密的社团活动中，身份验证是一个必要的过程。洪门就有多种碰面暗号及喝茶手势用来互相确认身份。区块链技术的发展将会简化身份验证的过程并提高验证的准确性，保障个人以及社团组织的信息和财产安全。社团链能够对用户的信息如实的进行记录，并分布式储存在各个服务器节点中，任何具有记账权的节点都可以查看相应的信息。由于区块链技术的最长链机制，任何对已入链信息进行修改的行为都会留下记录，具有不可篡改、防止伪造的特性。应用区块链技术对用户信息进行管理、储存及验证能够保证相关信息的准确性和真实性，进而增进了用户之间的信任。区块链技术会沉淀下来每一位成员的交易记录，信用，擅长领域，评级等信息。社团链用户，可以通过这些信息，快速且直接的了解社团内外任何一个人的基本信息，为后来的合作、交易、交流等提供参考。

社团链将会基于区块链底层技术之一的零知识证明，开发一套身份验证系统，社团组织、社团成员、社团公共财产等社团链的各个参与方都会应用该身份验证系统，保障自身的信息和财产安全。社团链采用自证明公钥和零知识的身份验证方案，能够实现用户公钥注册的双向身份认证和密钥协商，可以有效的实现通信双方身份的自证明，并解决公钥分发的问题。整个身份认证过程交互次数少、数据存储量、通信量和计算开销少，能够有效的提高验证过程的效率和安全性。



### 2.3.3 任务发布和兑领

社团集体活动往往以任务发布的形式向社团成员传达。现代社会中，社团成员对社团活动的响应不如以往积极。其中原因除了与人的选择越来越多，社团活动不具有唯一选择性以外，社团对社团成员的激励机制不足也有很大的影响。此外任务下达不及时，通知不到位也是影响社团成员参与社团活动的直接因素。对于跨社团之间的合作来说，过去由于缺乏信任背书，社团之间合作往往取决于社团决策层之间关系的亲疏，没有形成以任务发布和兑领为主的常态机制。应用区块链技术能够很好的促进社团内部成员之间合作交流，还能够促进不同地域、不同类型的社团间的跨社团合作。

社团链将在公链范围内提供全球性的任务发布和兑领平台。由于有区块链信任机制做信用背书，社团链能够更好的促进社团内部、跨社团、跨国别、跨种族的广泛合作。既可以实现个人层面的服务比如跨境法律援助、留学、海外置业、海外安保、救援等，又可以提供社团层面、公司层面的公务合作及商务合作，比如某企业进军国际市场获取相应的战略咨询，或者获取某国的政治资源和经济资源等，都可以通过任务发布系统实现，向全球的社团组织和成员发出合作需求。

### 2.3.4 资产管理和数字支付

通过区块链技术给社团成员的个人资产和社团的公共资产进行数字化赋值，能够更好地掌握个人资产和社团公共资产动向，防止相应的资产流失。利用区块链去中心化特性，各个账户都具有记账功能，打破了过去中心化记账体系的信任质疑。同时，通过GTOKEN通证，社团成员可借此享受社团的用户福利，行使相应地社员权利如投票、参与决策等，还能作为享受社团集体资产服务的凭证，分享社团集体发展的经济红利，进一步增强了各社团成员对社团组织的凝聚力，减少了划账交易体系的中间环节，缩减了交易成本，提升了支付效率。

社团链将发行一个可与不同公链数字货币对接的数字钱包，实现资产在不同公链上的转移，成为全方位的数字资产管理平台。数字钱包将实现多资产支持，包括BTC、ETH、EOS等跨链多币种支付，并由此延伸到与数字货币相关的社交沟通、币币交易、支付、行情、咨询等功能，支持数字货币点对点转账功能，短时间内实现跨国资产转账。在转账过程中将利用我们的零知识证明身份验证系统，充分保障用户的资产安全。该数字钱包支持主流支付平台运营手段，比如：发放者可在点对点、点对群的聊天中发放数字货币红包，未来也将支持包括比特币、莱特币等多种主流币种的红包功能，用户可自由选择币种及其货币数量。

### 2.3.5 社团管理

区块链社团管理体系是基于通证经济对传统社团激励的重构。社团链平台将重构社团生态体系和用户社交关系。社团链将提供日常的社团管理服务包括会费、账目、投票、薪酬、考勤、OA等管理功能，还通过社群积分体系，团结更多的社团成员加强社团组织的凝聚力。社团将对社团成员参与社团的日常活动进行积分激励。社员所获得的积分将作为社员绩效考核和职务晋升的重要指标。比如参与慈善捐款、缴纳会费、赈灾扶贫、承担日常管理工作、完成社团分配的任务等，社团成员都会获得相应的积分激励。GTOKEN通证还可以在社团链生态体系的博彩机构、医院、学校、酒店等进行消费。消费的同时还能够获得二次TOKEN的奖励。



### 2.3.6 公共财产上链

全球社团通用积分将允许所有的合法社团将其社团的公共财产进行上链，比如洪门旗下的公共财产包括博彩、酒店、医院、学校等。通过资产上链赋予社团不动产一定的价值流动性，在为用户提供更便捷的服务同时也作为社员享受社团发展红利的凭证。通过社团链的社员积分体系，社团的公共财产将接受积分消费，既能够增加用户到社团公共场所的消费频次，同时以积分返利的形式加强用户对组织的凝聚力。流动性的提供，也方便后续社团事业以通证经济的形式进行众筹、发起、管理、投票、流转等。

### 2.3.7 跨境电商

跨境电商是指使用区块链技术协议取代商业中介，通过提供互联网服务，将供应商、消费者等个各种角色连接在一起，进而将服务商的交易成本直接分配给相应的贡献者。由于社团链的社团资源遍布全球，我们将利用区块链技术升级现有的跨境业务，打造新的跨境支付方式，为全球的社团链用户提供点对点的电商支付平台，推动跨境业务发展。当前的传统跨境支付方式清算时间较长、手续费较高且有时候会出现跨境支付诈骗行为，产生了一定的跨境资金风险。社团链通过区块链技术打造点对点的支付平台，撇除了第三方金融机构的中间环节，将全球的社团链用户资源链接起来，可以全天候支付、支持瞬间到账和提现、消除了交易过程中的隐形成本，降低了跨境电商资金风险，为社团链用户提供便捷性的购物体验。跨境电商的消费场景引入消费即挖矿、分享即挖矿、入住即挖矿的基于通证经济的玩法，让社团成员在经济增长中收益。

### 2.3.8 一带一路基础设施建设

一带一路是我国21世纪发展布局的顶层决策，也是中华民族伟大复兴的关键一役。洪门作为海外最大的华人社团组织，积极响应“一带一路”政策，促进两岸统一和中华民族伟大复兴。全球社团通用积分将借助洪门系统在海外庞大的昆仲资源，通过社团链平台支持一带一路的基础设施建设。

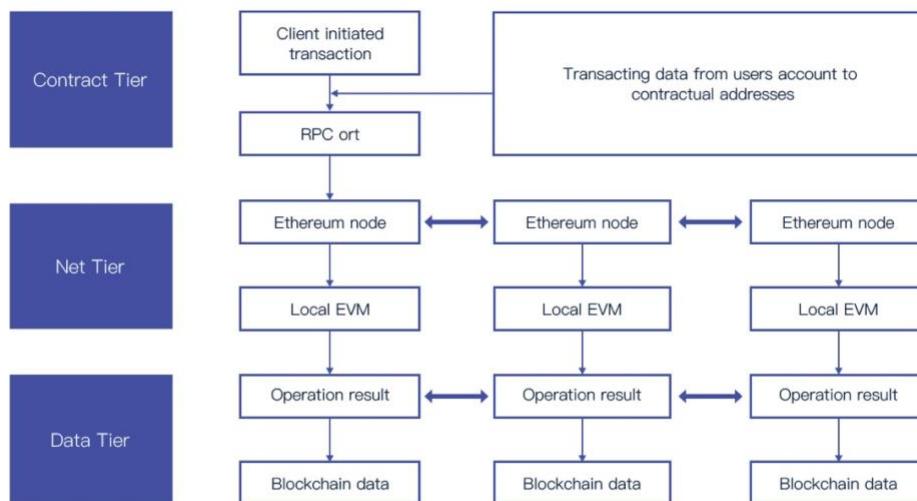
全球社团通用积分将成为洪门旗下一带一路沿线的基础设施项目、中国文化输出项目等唯一募款渠道，利用区块链技术优化工程项目管理，并作为一带一路沿线基础设施项目、中国文化输出项目、民生福利项目等项目的招投标平台。工程项目的相关方还可通过社团链平台交换海外政策信息和项目招标信息。由于区块链技术的可追溯特征，能够保障项目实施过程的质量安全、材料安全、监理责任等，做到资金融通、收益权流转、过程上链、材料溯源、上下游资金资信信息上链等。社团链将用区块链技术改造重大工程项目的生产关系、过程管理体系等，为一带一路这一世纪工程助力。

# 功能模块和关键技术

FUNCTIONAL MODULES AND KEY TECHNOLOGIES

## 3.1 全球社团通用积分技术框架

全球社团通用积分基于区块链3.0技术整体架构，由亦来云提供技术支持。其典型特征包括智能合约、DAPP（分布式应用）和虚拟机等，并支持POW、POS和DPOS等多种共识算法。本项目拟建立基础技术框架如下图：



社团链的底层技术框架里面，包含点对点网络设计、加密技术应用、分布式算法的实现、数据存储技术的使用等4个方面，涉及到分布式存储、机器学习、VR、物联网、大数据等方面。从架构设计上来说，社团链大致可以分为三个层次，协议层、扩展层和应用层。其中，协议层又可以分为存储层（也可称为数据层）和网络层，它们相互独立但又不可分割。

协议层，是指代最底层的技术，是一个完整的区块链产品。通过它网络节点并提供API供调用。我们会提供一个客户端，用来建立地址、验证签名、转账支付、查看余额等。协议层用到的技术主要包括网络编程、分布式算法、加密签名、数据存储技术等方面，其中网络编程主要考虑高并发的问题。协议层是整个社团链平台的产品基础，构建了网络环境、搭建了交易通道、制定了节点奖励规则。

扩展层，相当于B/S架构产品中的服务端（SERVER），主要包括两个方面，一是实现一个智能的交易市场，二是基于“智能合约”概念的应用开发，“智能合约”是一种“可编程合约”，或者叫做“合约智能化”，也就是说当达到某个条件，合约将自动执行，比如自动资产转移、自动付款等，扩展层涉及到的主要技术包括分布式存储、机器学习、VR、物联网、大数据等。

应用层，应用层为最外层，主要面向用户，负责协助用户搭建自己的分布式应用，用户可以借助公有链搭设专属于自己的私有链，即世界各地洪门昆仲及其他合法社团均可依托上级联盟链搭设专属私有链并成为点对点通讯和社交平台。此外，开发者也可以基于服务层的可视化开发环境或开放 API 接口自行开发去中心化应用，简单高效，它相当于B/S架构的产品中的浏览器端（BROWSER）。在应用层，社团链将为各社团成员提供各种服务，包括各个平台的服务软件，智能管理客户端等。



## 3.2 全球社团通用积分项目参与方

全球社团通用积分平台的参与方可以分为四类：即社团组织、社团会员、社团公共资产和非社团成员。每个区块链参与者都可以设定规则，区块链的治理规则分为两大层面：一是技术层面的治理规则，由软件、协议、程序、算法、配套设施等技术要素构成。二是技术外部的、监管法规层面的治理规则，由法规框架、条文、行业政策等组成，在本平台中，我们会兼顾两者保护所有参与者广泛利益，推进基于区块链技术上的商业应用场景的落地，最终构建一个由参与者各方共同参与的完整商业体系。

### 3.2.1 社团组织

全球社团通用积分平台的组织模式是联盟模式，就是由多家社团组织联合在一起，在互惠互利、共同贡献的前提下共同推动全球社团通用积分平台的发展。每个社团组织都有一定的准入标准，需要审核机构身份、资质、评估投入程度，持有TOKEN数量，有共同的章程，有合法组织形式，共享技术研究成果，一起构建商业模式。根据每个社团组织的能力不同，也会有不同的分工，技术实力较强的社团组织进入区块链技术服务提供商领域，而商业规模更大的社团组织则优先发展商业服务。

### 3.2.2 社团会员

每个社团组织由社团会员组成，社团成员借助去中心化的社团链，形成自己的社团朋友圈，以公有链作为记账人选举机制的依托，利用公有链的开放特性，让每个社团成员参与到私有链的登记节点和记账，并给予一定的回报和积分激励，从而实现权益、记账和交易的去中心化，同时又支持瞬时、低手续费的链上资产流转，提高交易效率。

### 3.2.3 社团公共资产

社团公共资产包括各社团控股、参股及投资的博彩机构、酒店、旅游景点、基础设施、私立医院和私立学校等，通过将社团公共资产的交易数据、日常管理数据等上链存储及权益交易赋予这些公共财产一定的价值流动性，并应用区块链的手段对社团的公共财产进行去中心化、透明化、可流转化的管理。各社团公共资产将允许全球社团通用积分购买其服务并作为其消费凭证，利用区块链技术建立客户数据管理系统，结合区块链、大数据等技术为用户提供针对性的推送服务，同时根据用户在数据库中所处的等级，给予TOKEN返利、定向优惠活动等激励手段，既促进了用户在该机构的消费水平，同时又可作为社团福利反馈给用户，增加用户对社团的凝聚力。为未来社团公共资产借贷、抵押、众筹、流转、评级等提供可能。

### 3.2.4 非社团成员

平台提供有去中心化的IM工具，社团会员在参与全球社团通用积分平台项目后，可通过IM工具邀请自己的非社团成员朋友、同伴参与到项目中，这些非社团成员也可通过平台的审核机制成为社团成员，同时平台会在此基础上给予社团会员和非社团会员一定的积分奖励。非社团会员可以通过主链发布的项目列表或者搜索功能直接搜索项目名称或智能合约地址，选择自己感兴趣的项目来参与。非社团成员依然可以参与DPOS投票、任务发布与兑领、跨境电商、项目众筹、慈善捐赠等事项。

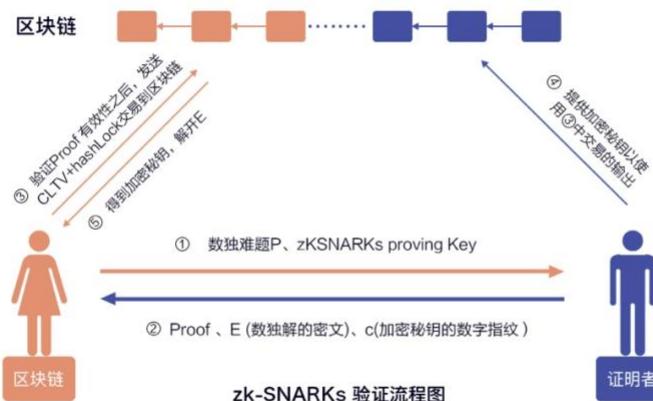


### 3.3 全球社团通用积分系统模块

本系统的架构基于区块链3.0技术框架，搭建定制化的全球社团通用积分系统。为此，我们建立7大系统模块和2大公共服务体系，分别是零知识身份认证系统、社团链账户管理系统、信息数据存储系统系统、资产管理系统和数字钱包、去中心化即时通讯工具、底层智能合约引擎、用户积分体系以及任务合作体系，以求为优质的用户服务保驾护航。

#### 3.3.1 零知识身份认证系统

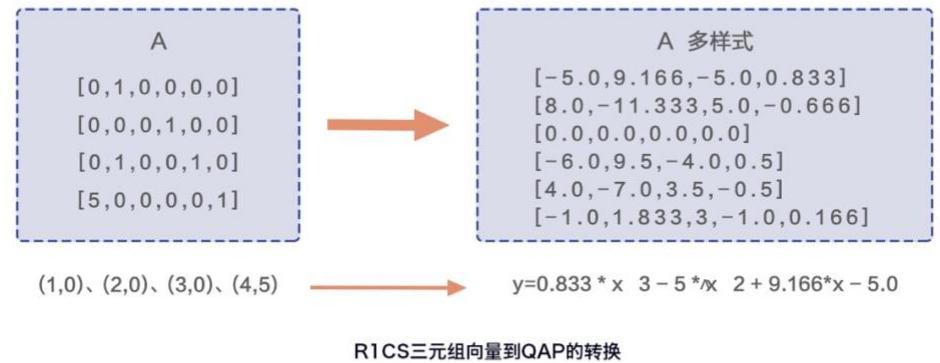
社团链的身份认证系统采用去中心化的身份验证体系，用户的身份信息和凭证不属于任何机构所有，真正完全掌握在用户自己手中。通过采用零知识证明ZK-SNARKS ( ZERO-KNOWLEDGE SUCCINCT NON-INTERACTIVE ARGUMENTS OF KNOWLEDGE ) 算法，能够确保数字身份同真实个人间的真实性的一致性。零知识证明是指一方（证明者）向另一方（验证者）证明一个陈述是正确的，而无需透露除该陈述是正确的以外的任何信息。采用ZK-SNARKS算法能够最小程度的生成零知识证据消息。在整个认证过程中，几乎没有任何交互，证明者（PROVER）只需向验证者（VERIFIER）发送一个消息即可。现阶段下，几乎没有任何的证明者有足够的计算能力去创建伪造的零知识证据以欺骗验证者。因此，对于一个证明者来说，在不知晓特定证明（WITNESS）的前提下，构建一个有效的零知识证据是不可能的，从而确保证明者的数字身份和真实个人保持一致性。



A	B	C
1	1	1
5	1	0
3	3	3
0	0	0
35	35	35
9	9	9
0	0	1
27	27	27
0	0	0
30	30	30

$$35 * 1 + 30 = 35 \\ \sim \text{out} = \text{sym\_2} + 5$$

ZK-SNARK 算法目前适用于所有的 NP 问题。我们要做的就是确定问题的验证规则，在社团链中，一笔交易是否有效的问题就是 NP 问题，验证规则主要是，输入的金额是否大于等于输出的金额，这笔交易是否有合适的签名，输入是否属于UTXO等。验证规则到R1CS形式的转换则是ZK-SNARK算法关键的一个步骤，所谓的 R1CS (RANK-1 CONSTRAINT SYSTEM) 就是一系列三元组向量 (A, B, C)，对R1CS的解S满足， $S.A^*S.B - S.C = 0$ ，它是验证规则的数学形式体现。



### 3.3.2 社团链账户管理系统

社团链采用去中心化的账户管理系统。去中心化的账户管理系统将用户的身份信息和身份验证过程在区块链网络中进行，分散在全球的完全等价的区块链节点，不存在某个权威的节点，保障了系统的安全性。智能合约作为公正的“中心化服务提供者”，代替传统的中心化服务提供者，实现对去中心化组织公开公平的“自治”，规避了中心化账户管理系统用户信息被泄露、被篡改的风险。

社团链的账户包括两种类型：外部账户（EXTERNALISED ACCOUNT）和合约账户（CONTRACT ACCOUNT）。外部拥有的帐户，由私钥控制。合约帐户则由合约代码控制。外部拥有的帐户没有代码，可以通过创建和签署交易，从外部拥有的帐户发送消息；在合约账户中，一旦收到其代码被激活的消息，将允许其实现读取、写入、发送其他消息、依次创建合同等功能。

社团链的账户生成过程会给每个参与者分配一个固定地址，这个功能不需要参与者拥有任何基础，人人都可以方便快捷的参与。每个账户具有一个20字节的地址，共包含四个字段：

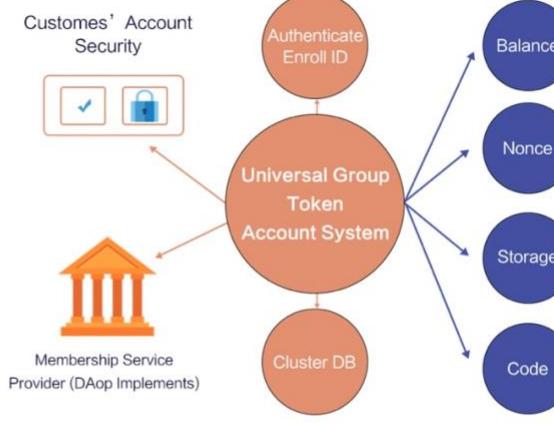
(1) NONCE：一个用于确保每个事务只能处理一次的计数器。在外部账户中，NONCE代表从该账户地址发送过的交易数量，该数量会出现在交易的字段中，起到防止双花的目的。在合约账户中，代表由该账户创建过的合约数量；

(2) 帐户的当前GTOKEN（社团链发行的TOKEN）余额；

(3) 帐户的合约代码：如果账户存在智能合约则存在相应的合约代码哈希值，当该账户地址接收到一个合约执行请求的时候，该合约代码会被自动执行。在智能合约控制下的，可以实现全流程无中介参与的用户身份验证和资产转移验证；

(4) 帐户的存储空间：包含了属于该账户的存储内容（一个关于256位整数值之间的映射）的编码，默认为空。

在账户生成的同时，还会给每个注册用户分配一个公钥/私钥对，这一对钥匙定义了一个特定账户。公钥（PUBLIC KEY）是作为用户身份的唯一ID，每个账户以地址为索引，地址由公钥衍生而来，公钥存储每个账户的余额信息。私钥是每个账户的特定密码，通过私钥我们可以访问一个账户。地址的生成流程是：私钥→公钥→地址。

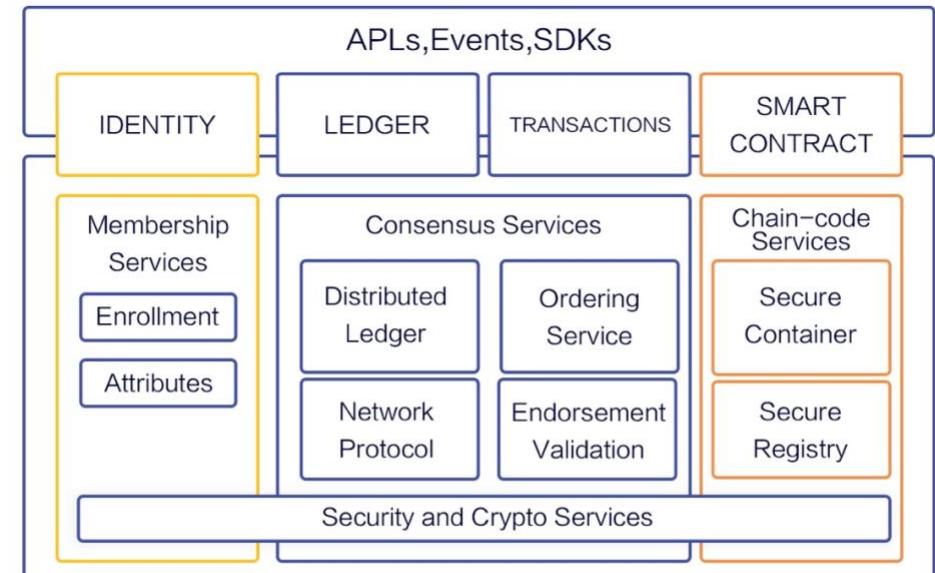


### 3.3.3 信息数据存储系统

社团链通过特定的编码方式实现对智能合约与账户数据的编码存储，同时又能在其数据基础上实现对区块交易及执行结果的完备共识证明。在信息数据存储系统中，用户可以即时地在区块链网络上查看到自己参与的项目列表，所有的参与记录和过程将存储在区块链网络中，无法篡改和否认。社团链官方平台提供链上数据查询功能，用户可以通过平台或直接链上交易，确保整个参与过程的公正性和安全性。

社团链以数据块的形式对数据进行封装，每个数据块组成结构包括区块头、交易队列、MERKLE PATRICIA 树的根哈希值、UNIX 时间戳等等。存储的数据类型主要有账户数据、账务数据、交易数据和底层智能合约。账户数据主要包括社团、个人等不同账户类型在注册过程中上传的个人信息、每个账户的属性和分配的账户地址；账务数据和交易数据，包括底层网络协议、分账数据、交易订单、认可背书等。社团链的编码RLP (RECURSIVE LENGTH PREFIX) 是数据序列化的主要编码方式，可以将任意的嵌套二进制数据进行序列化。社团链采用基于MPT (MERKLE PATRICIA TREE) 的数据组织形式，MPT上任何存储数据的细微变化都会导致MPT的根节点发生变更，因此可以校验数据的一致性，从而保证信息数据存储系统的公正和透明。

信息数据存储系统结构图



### 3.3.4 底层智能合约引擎

社团链平台的底层智能合约引擎，根据实际需求创建了以下几个方面的智能合约应用：任务发布和兑领、数字支付、社团管理、跨境电商、一带一路基础设施建设，并为用户提供智能合约模板开发新的智能合约应用场景。社团链的智能合约基于区块链3.0技术的智能合约机制开发，用户可以方便的利用智能合约模板进行新的应用场景开发。用户可访问的数据仅限于链内数据，外部数据需要通过交易来发送到合约。社团链智能合约的目标地址通过栈来传递，使得合约可以在运行时动态调用其它的合约代码，因此每个智能合约的参与节点在动态调用目标代码时一定会获得相同的目标地址。此外，社团链允许多个匿名的成员参与约束智能合约协议，每个参与者对交易完全知情，价值可以在账户间转移，或者放在智能合约中的第三方托管。

社团链的智能合约引擎将建基于公有链的底层SDK，提供订制化客户端应用程序方便用户调用和发布智能合约，使用户结合自己的需求开发新的智能合约应用场景，包括但不仅限于PC端、WAP站、APP(IOS & ANDROID)、PAD端、H5、小程序等。

基于社团链的域名注册系统：

```
def register( name, value );
if !self, storage [name];
  self, storage [name] = value
```

```
PUSH1 0 CALLDATALOAD SLOAD NOT PUSH1 9 JUMPI STOP JUMPDEST PUSH1 32
CALLDATALOAD PUSH1 0 CALLDATALOAD SSTOR
```

该字节码程序实现了域名注册系统，任何人都可以发送一个包含 64 个字节 DATA 的消息，其中 32 个字节当作 KEY，即域名注册者；另外 32 个字节当作 VALUE，即域名。合约检查 KEY 是否存在于合约账户的存储中，如若不存在，将其插入合约账户自身的存储中。

在执行过程中，一个无限可延伸的字节数组，称为“MEMORY”，程序计数器，指向当前要执行的指令，称为“PC”，和一个基于 32 字节的栈被 EVM 所维护使用。开始执行时，PC = 0，内存与栈是空的。现在假设，一个消息被发送，消息包含 123 位GAS 费用与 64 字节的数据，头 32 个字节是数字 54 的编码，后 32 个字节是数字 20202020 的编码。

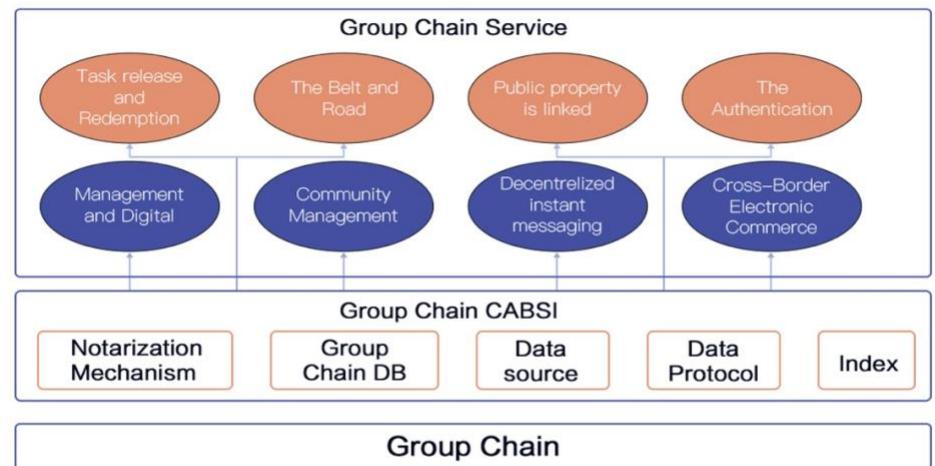
因此，初始状态是：{PC : 0, STACK : [], MEM : [], STORAGE : {}}，位于 0 处的指令是 PUSH1，代表将一个字节的数据压入栈中，并且在 CODE 中跳跃 2 步，即现在的状态是 {PC : 2, STACK : [0], MEM : [], STORAGE : {}}。位于 2 处的指令是 CALLDATALOAD，代表从当前的栈中弹出一个值 INDEX，装载位于消息 64 个字节数据中 INDEX 位置处的 32 个字节，并且将该数据压入栈中，即现在的状态是 {PC : 3, STACK : [54], MEM : [], STORAGE : {}}。

位于 3 处的 SLOAD 指令，从栈中弹出一个值 INDEX，将合约账户 STORAGE 中索引 INDEX 处的值压入栈中，由于该合约是第一次使用，因此值为 0，即现在的状态为 {PC : 4, STACK : [0], MEM : [], STORAGE : {}}。位于 4 处的 NOT 指令从栈中弹出一个值，如果该值为 0 则将 1 压入栈中，反之将 0 压入栈中，即现在的状态为 {PC : 5, STACK : [1], MEM : [], STORAGE : {}}。位于 5 处的指令 PUSH1 执行完成之后，状态变为 {PC : 7, STACK : [1, 9], MEM : [], STORAGE : {}}。

位于 6 处的指令 JUMPI 从栈中弹出两个值，A1 : 9, A2 : 1，如果第二个值 A2 为非 0 值，则跳转到 A1 指定的值。如果合约账户的 STORAGE 的索引 54 处的值不为 0，那么 A2 将会变为 0 (由于 NOT 指令)，那么我们就不会跳转到 A1 指定的值，那么接下来的指令就将会是 STOP，从而中止代码的执行。现在的状态是 {PC : 9, STACK : [], MEM : [], STORAGE : {}}。

位于 9 处的指令 JUMPDEST 不会对虚拟机状态造成任何影响，仅仅是标记一个有效的跳转地址，PC 变为 10，接下来位于 10 处的 PUSH1 执行完成之后，状态变为 {PC : 12, STACK : [32], MEM : [], STORAGE : {}}。位于 12 处的指令 CALLDATALOAD 执行完成之后，从栈中弹出一个值 INDEX : 32，然后将消息中 64 字节数据中位于索引 32 处之后的 32 个字节压入栈中，现在状态变为 {PC : 13, STACK : [2020202020], MEM : [], STORAGE : {}}。接下来执行 13 处的 PUSH1，状态为 {PC : 15, STACK : [2020202020, 0], MEM : [], STORAGE : {}}。

位于 15 处的 CALLDATALOAD，从栈中弹出索引值 0，再次将消息数据中前 32 个字节数据压入栈中，此时状态变为 {PC : 16, STACK : [2020202020, 54], MEM : [], STORAGE : {}}。位于 16 处的 SSTORE 操作从栈中弹出两个值 A1 : 54, A2 : 2020202020，存入合约账户的存储中，即 {PC : 17, STACK : [], MEM : [], STORAGE : [54 : 2020202020]}，位于 17 处没有任何指令，因此智能合约中止运行。



### 3.3.5 资产管理系统和数字钱包

社团链的资产管理系统将通过区块链技术给社群资产进行数字化赋值，从而帮助社团更好地掌握公共资产动向，防止集体资产流失。此外，该资产管理平台也对各社团成员提供个人资产管理服务，利用区块链去中心化特性，打破社团成员对传统中心化记账体系的信任质疑。区块链对资产的智能化管理将极大地提升资产管理的效率，同时也可以避免纠纷。

此外，社团链数字钱包还可接受BTC、EOS、ETH、USDT等主流资产转入和储存。法币和主流数字货币都可与平台发行的数字货币GTOKEN自由兑换，从而使社团链成为全方位的数字资产管理平台。同时，GTOKEN还可作为用户享受社团福利和社团公共资源服务的凭证。根据社团链用户积分体系，社团链鼓励用户使用GTOKEN到相应社团下属的公共资产进行消费，如医院、酒店、学校、博彩机构等，并根据消费价值和用户对社团的贡献度，给予二次TOKEN返利。因此，用户可一同分享社团发展的经济红利，进一步增强对社团凝聚力。同时数字货币支付减少了中间环节的分布划账，缩减交易成本，提高了支付效率。



### 3.3.6 匿名支付系统

社团链将采用 ZEROCASH 协议构建一种去中心化匿名支付模式 (DECENTRALIZED ANONYMOUS PAYMENT (DAP) SCHEME)，该数字货币交易模式是一种去中心化的模式，允许任意数量的直接匿名转账付款。ZEROCASH协议的构建包含以下步骤 (可基于任何基于 LEDGER 的货币，例如比特币、以太坊等)：首先使用 ZK-SNARKS 和承诺 (COMMITMENT) 模式给出一个简化的构建，令 COMM 为统计学上隐藏地非交互性承诺模式。随后，应用一种抵抗冲突的函数CRH压缩 CMLIST。再通过修改COIN COMMITMENT使得能够支持直接地匿名转账付款。在其中，为了提供付款的目标，我们使用 ADDRESS 的概念，为每一位用户生成一个地址密钥对 (APK, ASK)。并通过修改了地址密钥对的结构，使每一位用户拥有唯一的一个密钥对 (ADDR\_PK, ADDR\_SK)发送 COINS。整个交易过程都被包含在交易TXPOUR。因此，即使货币被要求赎回，在匿名支付的前提下也能够定义赎回金额的目的地址。

<b>Setup</b>	<b>Pour</b>
<ul style="list-style-type: none"> <li>• INPUTS: security parameter <math>\lambda</math></li> <li>• OUTPUTS: public parameters pp</li> </ul>	<ul style="list-style-type: none"> <li>• INPUTS:           <ul style="list-style-type: none"> <li>- public parameters pp</li> <li>- the Merkle root rt</li> <li>- old coins <math>c_1^{\text{old}}, c_2^{\text{old}}</math></li> <li>- old addresses secret keys <math>\text{addr}_{\text{sk},1}^{\text{old}}, \text{addr}_{\text{sk},2}^{\text{old}}</math></li> <li>- path <math>\text{path}_1</math> from commitment <math>\text{cm}(c_1^{\text{old}})</math> to root rt,</li> <li>- path <math>\text{path}_2</math> from commitment <math>\text{cm}(c_2^{\text{old}})</math> to root rt</li> <li>- new values <math>v_1^{\text{new}}, v_2^{\text{new}}</math></li> <li>- new addresses public keys <math>\text{addr}_{\text{pk},1}^{\text{new}}, \text{addr}_{\text{pk},2}^{\text{new}}</math></li> <li>- public value <math>v_{\text{pub}}</math></li> <li>- transaction string info</li> </ul> </li> <li>• OUTPUTS: new coins <math>c_1^{\text{new}}, c_2^{\text{new}}</math> and pour transaction <math>\text{tx}_{\text{Pour}}</math></li> </ul>
<ol style="list-style-type: none"> <li>1. Construct <math>C_{\text{Pour}}</math> for <math>\text{POUR}</math> at security <math>\lambda</math>.</li> <li>2. Compute <math>(\text{pk}_{\text{Pour}}, \text{vk}_{\text{Pour}}) := \text{KeyGen}(1^\lambda, C_{\text{Pour}})</math>.</li> <li>3. Compute <math>\text{pp}_{\text{enc}} := \mathcal{K}_{\text{enc}}(1^\lambda)</math>.</li> <li>4. Compute <math>\text{pp}_{\text{sig}} := \mathcal{G}_{\text{sig}}(1^\lambda)</math>.</li> <li>5. Set <math>\text{pp} := (\text{pk}_{\text{Pour}}, \text{vk}_{\text{Pour}}, \text{pp}_{\text{enc}}, \text{pp}_{\text{sig}})</math>.</li> <li>6. Output <math>\text{pp}</math>.</li> </ol>	<ol style="list-style-type: none"> <li>1. For each <math>i \in \{1, 2\}</math>:           <ol style="list-style-type: none"> <li>Parse <math>c_i^{\text{old}}</math> as <math>(\text{addr}_{\text{sk},i}^{\text{old}}, v_i^{\text{old}}, \rho_i^{\text{old}}, r_i^{\text{old}}, s_i^{\text{old}}, \text{cm}_i^{\text{old}})</math>.</li> <li>Parse <math>\text{addr}_{\text{sk},i}^{\text{old}}</math> as <math>(a_{\text{sk},i}^{\text{old}}, \text{sk}_{\text{enc},i}^{\text{old}})</math>.</li> <li>Compute <math>\text{snr}_{\text{sk},i}^{\text{old}} := \text{PRF}_{a_{\text{sk},i}^{\text{old}}}(\rho_i^{\text{old}})</math>.</li> <li>Parse <math>\text{addr}_{\text{pk},i}^{\text{new}}</math> as <math>(a_{\text{pk},i}^{\text{new}}, \text{pk}_{\text{enc},i}^{\text{new}})</math>.</li> <li>Randomly sample a <math>\text{PRF}_{a_{\text{pk},i}^{\text{new}}}^{\text{seed}}</math> seed <math>\rho_i^{\text{new}}</math>.</li> <li>Set <math>\text{addr}_{\text{pk},i} := (a_{\text{pk},i}^{\text{new}}, \text{pk}_{\text{enc},i}^{\text{new}})</math>.</li> <li>Set <math>\text{addr}_{\text{sk},i} := (a_{\text{sk},i}^{\text{new}}, \text{sk}_{\text{enc},i}^{\text{new}})</math>.</li> <li>Output <math>(\text{addr}_{\text{pk},i}, \text{addr}_{\text{sk},i})</math>.</li> </ol> </li> </ol>
<b>CreateAddress</b>	
<ul style="list-style-type: none"> <li>• INPUTS: public parameters pp</li> <li>• OUTPUTS: address key pair (<math>\text{addr}_{\text{pk}}, \text{addr}_{\text{sk}}</math>)</li> </ul>	
<ol style="list-style-type: none"> <li>1. Compute <math>(\text{pk}_{\text{enc}}, \text{sk}_{\text{enc}}) := \mathcal{K}_{\text{enc}}(\text{pp}_{\text{enc}})</math>.</li> <li>2. Randomly sample a <math>\text{PRF}_{\text{addr}}</math> seed <math>a_{\text{sk}}</math>.</li> <li>3. Compute <math>a_{\text{pk}} = \text{PRF}_{a_{\text{sk}}}^{\text{seed}}</math>.</li> <li>4. Set <math>\text{addr}_{\text{pk}} := (a_{\text{pk}}, \text{pk}_{\text{enc}})</math>.</li> <li>5. Set <math>\text{addr}_{\text{sk}} := (a_{\text{sk}}, \text{sk}_{\text{enc}})</math>.</li> <li>6. Output <math>(\text{addr}_{\text{pk}}, \text{addr}_{\text{sk}})</math>.</li> </ol>	
<b>Mint</b>	
<ul style="list-style-type: none"> <li>• INPUTS:           <ul style="list-style-type: none"> <li>- public parameters pp</li> <li>- coin value <math>v \in \{0, 1, \dots, v_{\text{max}}\}</math></li> <li>- destination address public key <math>\text{addr}_{\text{pk}}</math></li> </ul> </li> <li>• OUTPUTS: coin <math>\text{c}</math> and mint transaction <math>\text{tx}_{\text{Mint}}</math></li> </ul>	
<ol style="list-style-type: none"> <li>1. Parse <math>\text{addr}_{\text{pk}}</math> as <math>(a_{\text{pk}}, \text{pk}_{\text{enc}})</math>.</li> <li>2. Randomly sample a <math>\text{PRF}_{\text{an}}^{\text{seed}}</math> seed <math>\rho</math>.</li> <li>3. Randomly sample two <math>\text{COMM}</math> trapdoors <math>r, s</math>.</li> <li>4. Compute <math>k := \text{COMM}_r(a_{\text{pk}} \parallel \rho)</math>.</li> <li>5. Compute <math>\text{cm} := \text{COMM}_s(v \parallel k)</math>.</li> <li>6. Set <math>\text{c} := (\text{addr}_{\text{pk}}, v, \rho, r, s, \text{cm})</math>.</li> <li>7. Set <math>\text{tx}_{\text{Mint}} := (\text{cm}, v, *)</math>, where <math>*</math> := <math>(k, s)</math>.</li> <li>8. Output <math>\text{c}</math> and <math>\text{tx}_{\text{Mint}}</math>.</li> </ol>	
<b>VerifyTransaction</b>	
<ul style="list-style-type: none"> <li>• INPUTS:           <ul style="list-style-type: none"> <li>- public parameters pp</li> <li>- a (mint or pour) transaction <math>\text{tx}</math></li> <li>- the current ledger <math>L</math></li> </ul> </li> <li>• OUTPUTS: bit <math>b</math>, equals 1 iff the transaction is valid</li> </ul>	
<ol style="list-style-type: none"> <li>1. If given a mint transaction <math>\text{tx} := \text{tx}_{\text{Mint}}</math>:           <ol style="list-style-type: none"> <li>Parse <math>\text{tx}_{\text{Mint}}</math> as <math>(\text{cm}, v, *)</math>, and <math>*</math> as <math>(k, s)</math>.</li> <li>Set <math>\text{cm}' := \text{COMM}_s(v \parallel k)</math>.</li> <li>Output <math>b := 1</math> if <math>\text{cm} = \text{cm}'</math>, else output <math>b := 0</math>.</li> </ol> </li> <li>2. If given a pour transaction <math>\text{tx} := \text{tx}_{\text{Pour}}</math>:           <ol style="list-style-type: none"> <li>Parse <math>\text{tx}_{\text{Pour}}</math> as <math>(\text{rt}, \text{sn}_1^{\text{old}}, \text{sn}_2^{\text{old}}, \text{cm}_1^{\text{new}}, \text{cm}_2^{\text{new}}, v_{\text{pub}}, \text{info}, *)</math>, and <math>*</math> as <math>(\text{pk}_{\text{sig}}, h_1, h_2, \pi_{\text{Pour}}, \text{C}_1, \text{C}_2, \sigma)</math>.</li> <li>If <math>\text{sn}_1^{\text{old}}</math> or <math>\text{sn}_2^{\text{old}}</math> appears on <math>L</math> (or <math>\text{sn}_1^{\text{old}} = \text{sn}_2^{\text{old}}</math>), output <math>b := 0</math>.</li> <li>If the Merkle root <math>\text{rt}</math> does not appear on <math>L</math>, output <math>b := 0</math>.</li> <li>Compute <math>\text{hsig} := \text{CRH}(\text{pk}_{\text{sig}})</math>.</li> <li>Set <math>x := (\text{rt}, \text{sn}_1^{\text{old}}, \text{sn}_2^{\text{old}}, \text{cm}_1^{\text{new}}, \text{cm}_2^{\text{new}}, v_{\text{pub}}, \text{hsig}, h_1, h_2)</math>.</li> <li>Set <math>m := (\text{x}, \pi_{\text{Pour}}, \text{info}, \text{C}_1, \text{C}_2)</math>.</li> <li>Compute <math>b := \mathcal{V}_{\text{sig}}(\text{pk}_{\text{sig}}, m, \sigma)</math>.</li> <li>Compute <math>b' := \text{Verify}(\text{vk}_{\text{Pour}}, x, \pi_{\text{Pour}})</math>, and output <math>b \wedge b'</math>.</li> </ol> </li> </ol>	
<b>Receive</b>	
<ul style="list-style-type: none"> <li>• INPUTS:           <ul style="list-style-type: none"> <li>- public parameters pp</li> <li>- recipient address key pair (<math>\text{addr}_{\text{pk}}, \text{addr}_{\text{sk}}</math>)</li> <li>- the current ledger <math>L</math></li> </ul> </li> <li>• OUTPUTS: set of received coins</li> </ul>	
<ol style="list-style-type: none"> <li>1. Parse <math>\text{addr}_{\text{pk}}</math> as <math>(a_{\text{pk}}, \text{pk}_{\text{enc}})</math>.</li> <li>2. Parse <math>\text{addr}_{\text{sk}}</math> as <math>(a_{\text{sk}}, \text{sk}_{\text{enc}})</math>.</li> <li>3. For each Pour transaction <math>\text{tx}_{\text{Pour}}</math> on the ledger:           <ol style="list-style-type: none"> <li>Parse <math>\text{tx}_{\text{Pour}}</math> as <math>(\text{rt}, \text{sn}_1^{\text{old}}, \text{sn}_2^{\text{old}}, \text{cm}_1^{\text{new}}, \text{cm}_2^{\text{new}}, v_{\text{pub}}, \text{info}, *)</math>, and <math>*</math> as <math>(\text{pk}_{\text{sig}}, h_1, h_2, \pi_{\text{Pour}}, \text{C}_1, \text{C}_2, \sigma)</math>.</li> <li>For each <math>i \in \{1, 2\}</math>:               <ol style="list-style-type: none"> <li>Compute <math>(v_i, r_i, s_i) := \mathcal{D}_{\text{enc}}(\text{sk}_{\text{enc}}, \text{C}_i)</math>.</li> <li>If <math>\mathcal{D}_{\text{enc}}</math>'s output is not <math>\perp</math>, verify that:                   <ul style="list-style-type: none"> <li><math>\text{cm}_i^{\text{new}}</math> equals <math>\text{COMM}_{s_i}(v_i \parallel \text{COMM}_{r_i}(a_{\text{pk}} \parallel \rho_i))</math>.</li> <li><math>\text{sn}_i := \text{PRF}_{a_{\text{sk},i}}^{\text{seed}}(\rho_i)</math> does not appear on <math>L</math>.</li> </ul> </li> <li>If both checks succeed, output <math>\text{c}_i := (\text{addr}_{\text{pk}}, v_i, \rho_i, r_i, s_i, \text{cm}_i^{\text{new}})</math>.</li> </ol> </li> </ol> </li> </ol>	

### 3.3.7 去中心化信息即时通讯工具

社团链的去中心化信息即时通讯工具将基于点对点协议开发，通过区块链技术的公私秘钥机制确保信息通讯安全，防止信息被窃取。社团链的用户可通过该去中心化信息即时通讯工具发布项目信息，进而保证信息安全，防泄漏防监测。由于其去中心化的储存方式，信息不需要被中心服务器暂存，从而防止被中心化储存机构的数据备份。在本系统中信息流向是先节点记账再其他节点备份，通过在公链上搭设点对点通讯的私有链，整个信息记账权将会限制在该私有链的节点上，从而使信息能够在绝对封闭的环境中流通，进而实现私密和安全社交。去中心化信息交流平台可以使该公开的数据无法被隐藏，该隐藏的信息无法被公开，全面提升人与人之间的社交信任和沟通效率。

社团链将用户社交过程中产生的所有数据都存储在用户自有的“自由数据库”，即每个用户都是一个终端，用户拥有处理数据的一切权益，用户信息不被平台过滤和获取。其端对端加密算法，任何人都无法获取用户的私密对话，从而保证了用户资料的安全以及隐私。此外，区块链上的数据无法被篡改；在区块链中每个节点都有备份，这使得单点故障不会损害数据完整性；区块链技术能够做到多个私钥的复杂权限保管。



### 3.3.8 任务合作体系

区块链技术会沉淀下来的每一位成员的交易记录，信用，擅长领域，评级等信息，这些信息不可更改且如实记录的特性可以降低合作双方的阻碍，促进相互信任，提升合作效率。社团内部的人还可以通过这些信息，快速且直接的了解社团内任何一个人的情况信息，为后来的合作打下基础。信用社群由此建立，同时将延伸出新的合作模式。社团链平台将结合区块链技术优势，推出两种新的合作机制：

其一：社交成本机制。实力强，信誉好的成员可以设定自己的“谈话身价”，也就是说，想找他们谈合作，需要先付出一笔积分费用。这样，可以通过前置成本来明确社交诚意，让实力强信用好的社群成员既可以获取社交收益，也可以获取潜在的项目源。谈话身价的定价是否合理，将通过市场来检验。两个都有“谈话身价”的人，且都有谈话意愿时，交互时需要付出的成本是两人谈话身价的差值，由相对“谈话身价”低的人来支付；同时被约谈的人，也可以要求约谈方全额支付“谈话身价”，而自己不需要支付任何费用。

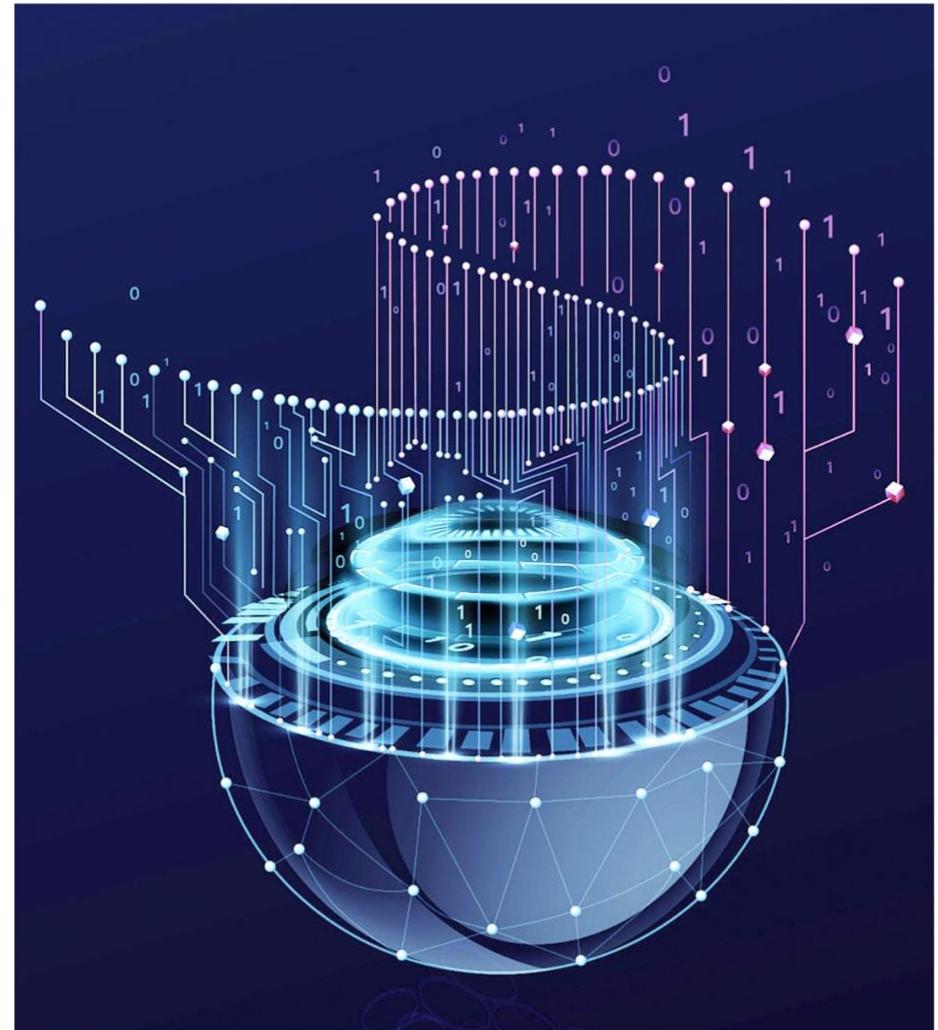
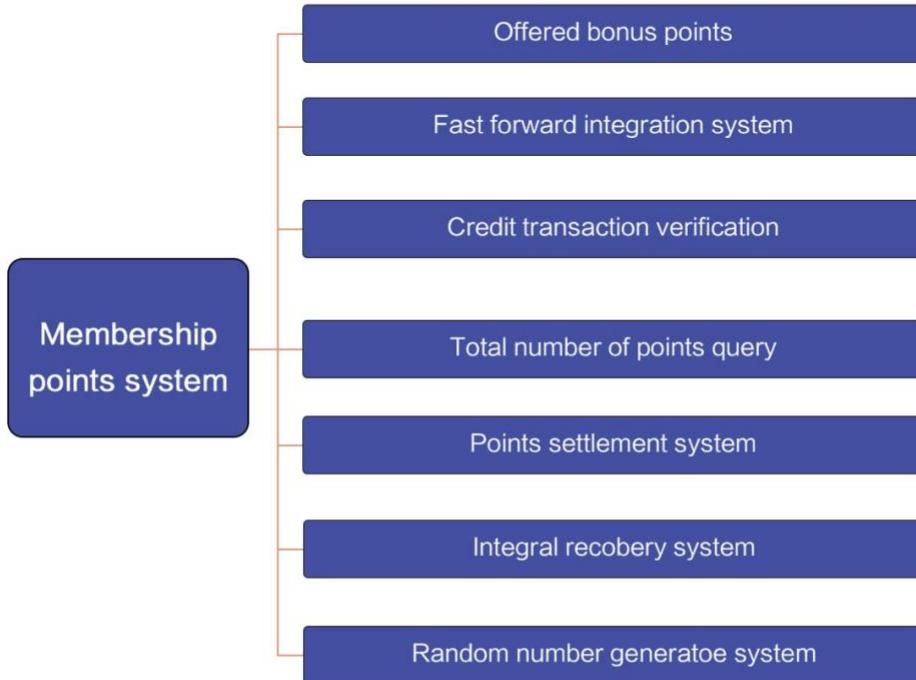
其二，合作匹配机制。社团内部会根据成员的身份、历史信用、技能特征等确定每一位成员的能力与需求，为其推荐相匹配的社团成员，由社团成员本人来做判断是否约谈。这保证了社团成员间的交互逻辑得以重新构建，社群内部的活力将大大提升。



### 3.3.9 用户积分体系

用户积分系统是每个企业提高用户粘性的一个常见客户维护系统，经常伴随着积分换现，积分换礼品等常规模式，但是绝大部分的企业对于积分的处理多半是闲置状态，传统的积分机制具有溯源难、安全性低、自动清零、难以流通、结算困难等缺点，无法真正体现增值体系的价值。

全球社团通用积分的用户积分体系将大大改善以上问题，用户积分体系发放的积分直接为平台发行的通证GTOKEN，其功能模块包括积分任务悬赏、快发积分系统、积分交易验证、积分总量查询，可利用区块链的清结算体系实施即时准确的积分结算与积分回收，整个流程遵循严格的加密算法和验证体系。社团链的积分结算系统将把链上所有分布式账本的积分记录联结到一起，再得到积分结果后将根据智能合约自动结算通证，不受任何中心化机构或第三方机构的控制，即时将奖金TOKEN分发给社团链用户的身份地址中，保障兑换过程中绝对的公开、公正和透明。



# 通证机制及发行方案

CERTIFICATION MECHANISM AND ISSUING SCHEME

## 4.1 GTOKEN通证经济模型

社团链将发行数字代币GTOKEN，又名“江湖令”。这个武侠风的昵称来自创始团队对GTOKEN的希冀，俗话说，有人的地方就有江湖，而社团就是一个个小的江湖，“江湖令”就是为了这些社团而生。俗语有云，有人的地方就有江湖，社团可以将之戏称为小江湖，于是团队的研发成员们便为GTOKEN起了一个武侠风的名字，江湖令，最终成了GTOKEN的昵称。社团链将采用通胀的经济模型，GTOKEN每年增发总量的5%。GTOKEN初期通证生成将基于以太坊合约技术，主网上线后，社团链将采用DPOS共识机制，通过投票产生49个超级节点作为区块生产者，对于他们的激励并不仅仅来源于手续费，还将通过增发来激励超级节点，超级节点将会按权重分享通胀收益。

关于超级节点投票，不仅考虑各备选节点总的TOKEN数，更强调有效地址参数对TOKEN总数的调节系数，以促进更广泛的共识生态。关于节点地址投票，将参照以下规则计算最终得票数：

$$\text{Value} = n * k \quad \text{其中, } n = \sum_1^i f(\alpha_i) = \begin{cases} 1, & \alpha_i > 100\text{GTOKEN} \\ 0, & \alpha_i \leq 100\text{GTOKEN} \end{cases}$$

$n$ 为有效地址数，有效地址判定条件  $\alpha_i > 100\text{GTOKEN}$  ( $\alpha_i$  为第*i*个地址的TOKEN值) 即只有大于100GTOKEN持币量的地址才可被判定为有效地址。

$n_i$ 为参选超级节点的有效地址数，对其进行排名，排名为前十名的K=1.5，排名为第11名到第20的K=1.2，排名为21-30名的K=1，排名31名及以后的K=0.8。

实时动态截取每日GMT+8 00: 00分动态VALUE值前49名的节点为超级节点，共同负责下一24小时的超级节点职责，并按VALUE权重分享增发收益。

## 4.2 GTOKEN通证发行及分配方案

分配对象	分配比例	分配数量（亿枚）	说明
社区激励	10%	3	用于维持社区的运营和推广
技术	15%	4.5	用于DAPP开发，公链开发
创始团队	10%	3	创始人团队持有，分四年解禁
基金会	15%	4.5	用于基金会的运营和维护
商务	10%	3	用于交易所、市场营销、市值管理等
通证交换	40%	12	仅面向机构及合格投资人
总量	100%	30	

## 4.3 GTOKEN通证交换及锁仓机制

GTOKEN通证的发售将严格按照世界各地的法律法规，以恰当方式面向合适人群进行发售，仅面向机构及合格投资人发售。GTOKEN通证初始发行总量为30亿枚，其中40%即12亿枚用于通证交换。

通证交换比例：1ETH: 6000 GTOKEN

锁仓条件：首发交易所当日解锁30%，次月同日解锁20%，再次月同日解锁20%，再次月同日解锁30%，总计分3个月释放完毕。

官方指定通证交换地址：0XFE61BA201D3778DD2482BFE4361706003BA20970

## 4.4 创始团队通证解禁计划

创始团队持有的TOKEN将锁定两年，并于四年内逐步释放，两年后解禁30%，三年后解禁35%，四年后再解禁35%。

# 团队和投资机构

TEAMS AND INVESTMENT INSTITUTIONS



## 创始团队

FOUNDING TEAM



**孔祥科**  
创始人/CEO

国民党行政管理委员会副主任委员、国际洪门总会副理事长、台湾中华儒学会理事长、CARRY AIR-LEASING LTD. 副总裁、台湾健行科技大学企管系主任等职务。曾负责管理国民党党产，具有多年的大型资产管理和金融从业经验。本科、硕士毕业于台湾大学经济学系、博士毕业于台湾科技大学管理系。



**熊育烽**  
创始人/VP

台湾农业区块链推广活动召集人、中国白酒区块链研究中心召集人、台湾扶农协会农业发展策略团大中华区首席代表、雅虎狮子会 300A1区块链创会副会长，在区块链投资和区块链技术领域有丰富的经验。



**李昭良**  
创始人/VP

云端文教事业股份有限公司营运长、掌声娱乐股份有限公司营运长、新五台创媒集团营运长，新五台集团主营云端运算、影音串流技术负责人等职务（新五台集团现为台湾最大的云计算公司之一）在区块链技术开发等领域有丰富的经验。

## 创始团队

### FOUNDING TEAM



朱邦文  
创始人/VP

中华台湾全球跨境电商协会会长、中华国际电子商务协会会长、中华海峡两岸事务交流协会会长、中天商宇国际电子商务有限公司总裁，在跨境电商、IT互联网领域多年的工作经验和人脉资源。



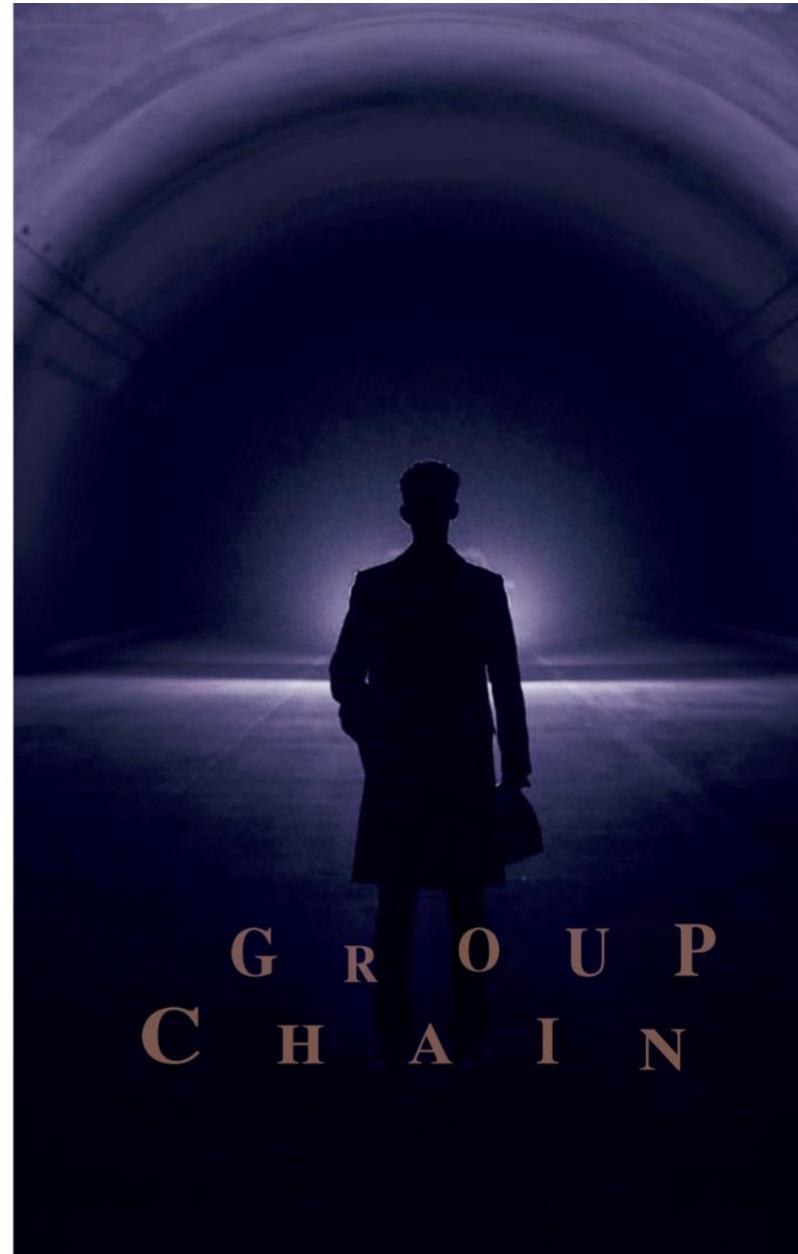
张凯钧  
创始人/VP

英国伦敦大学信息所博士、美国匹兹堡大学硕士。广东联速两岸科技园创办人、广东集成电路协会主任委员、欧洲台湾商会青年主席、欧洲台湾大学校友会主任委员，拥有15年高科技信息工程研发和跨国公司管理经验。



吴俊裕  
创始人/VP

北京中美集团医疗事业集团西安总部首席执行官、美国HYPERBARIC OXYGEN THERAPY CENTER台湾区总经理、国立中山大学国际人才培育中心顾问、台湾大哥大电信集团顾客服务部总经理，在社群维护、人力资源管理、团队建设等领域有丰富的工作经验。



G R O U P  
C H A I N

## 顾问

CONSULTANT

**刘沛勋**

现任国际洪门世界总会主席、曾任世界洪门总会总执行长  
国际洪门中华总会创会理事长

刘沛勋主席，现任国际洪门世界总会主席，为世界洪门社团的代表人物。祖籍江苏省徐州市铜山县，于台北出生，取得辅仁大学商学士、美国阿姆斯壮大学法学博士。1975年加入洪门南华山受封承行大管事，1981年至1991年遍访世界各洪门社团，曾于1992年担任世界洪门总会总执行长，2004年当选国际洪门中华总会创会理事长，2009年当选国际洪门世界总会主席。

**Carlos Chou**

原甲骨文/SIEBEL全球总裁、SAP全球高级副总裁  
惠普全球副总裁、CLZ创始人兼CEO

CARLOS CHOU曾在多家世界500强科技公司任职，曾任SIEBEL总裁，甲骨文亚太区总裁、SAP全球高级副总裁（负责全球CRM业务）、惠普全球副总裁（领导全球BUSINESS SOLUTIONS部门，管理30亿美元营收的部门），擅长通过创新和颠覆性的市场策略来推动增长。

**李克明**

台北哈佛商学院校友会创会会长、中华儒道研究协会名誉副理事长  
元大创业投资股份有限公司董事长、元大京华证券股份有限公司副董事长

李克明，中华儒道研究协会名誉副理事长、台北哈佛商学院校友会创会会长，曾任台北第三选区国大议员、元大创业投资股份有限公司董事长、元大国际资产管理股份有限公司董事长、元大京华证券股份有限公司副董事长等职。著有《当孔子遇上哈佛•首部曲：志业职场》等儒家解读著作，并于台湾政治大学 EMBA 和IMBA 学程教授《商业谈判》等课程。

## 顾问

CONSULTANT

**陈柏光**

中华民族致公党主席、中华民族致公文化总会总会长  
世界陈氏宗亲总会荣誉总会长、洪门华台山山主

陈柏光，台北人，中国文化大学国家发展研究所博士，长期投身于加强两岸交流，促进中华民族伟大复兴的工作中。现任中国台湾致公党主席，洪门华台山山主，中华两岸交流协会常务副会长，全国台湾同胞投资企业联谊会副会长，北京首都经济研究会台湾分会会长，世界陈氏宗亲会荣誉总会长，沃华国际投资控股集团总裁。

**曾万华**

国际洪门中华总会理事长、大六贸易有限公司董事长  
方川科技工程有限公司董事长

曾万华，现任国际洪门中华总会理事长，加入洪门20余年，是国际洪门总会的核心人物之一，长期致力于两岸交流工作，积极参与到中华民族伟大复兴的进程中。曾万华先生在工程营造界经营多年，现为大路贸易有限公司董事长、方川科技工程有限公司董事长，有丰富的项目资源，并积极参与一带一路沿线工程的建设，近年来开始布局区块链与工程项目管理的公司和企业。

**韩台玉**

现任国际洪门世界总会副主席、国际洪门慈善总会创会会长暨创会总会长  
百来得股份有限公司董事长、疯彩五千股份公司董事长

韩台玉，2015年至今担任国际洪门总会副主席，2017年至今担任国际洪门慈善总会创会会长暨创会总会长。曾于2010-2012年度担任第三届国际洪门中华总会第一副理事长，2012-2014担任第四届国际洪门中华总会理事长。在任期间贯彻落实“复兴中华，两岸一家”的和平发展理念，领团参加海峡论坛，并加强与中国致公党及其他各界团体的交流活动。

## 顾问

CONSULTANT

**林丽慧**

国际洪门妇女总会理事长、中华两岸房地产暨经贸交易协会副理事长  
敦扬建设股份有限公司董事长

林丽慧，现任国际洪门妇女总会理事长，加入洪门10余年，长期从事洪门妇女昆仲和社会妇女权益的提升和保障工作。多年往返两岸之间，致力于加强两岸交流，促进中华民族伟大复兴。林丽慧理事长从事房地产相关工作多年，现任中华两岸房地产暨经贸交易协会副理事长和敦扬建设股份有限公司董事长。

**陆思友**

澳门万国控股集团副总裁、澳门台商总会副会长  
澳门创意产业协会副会长

陆思友，现任澳门万国控股集团副总裁，澳门台商副会长等职务，多年来积极投身于两岸经济文化建设贸易交往工作。陆思友先生是杰出的台商代表，国光艺校副校长、中国电影制片厂厂长、佛山市台商协会秘书长、广东省台商服务中心秘书长等职务，在经济及文化领域都取得显著的成果，做出了突出贡献。

**吕意凡**

国美控股集团副总裁兼CIO

吕意凡，负责国美整个ERP系统建设。在系统建设过程中，成立了由全国不同层面的员工组成的一支强有力的实施团队，涵盖门店、各业务板块、IT等各个板块，给国美客户提供一个新的服务平台，既能满足企业内部需求又能满足企业发展的需要。吕总任内把国美财务组织变得更加规范化和有效化，使其在整个预算的编制、预算的执行和费用管控上，形成一个有效的机制。具有丰富的企业战略、企业管理、SAP、互联网大数据的从业经验和行业资源。

## 顾问

CONSULTANT

**陈世明**

中华青溪总会秘书长、台北城市科技大学兼任讲师  
财团法人汉辉文教基金会秘书长

陈世明，现任台北城市科技大学兼任讲师，汉辉文教基金会秘书长等职务。陈世明先生一直致力于推动教育事业的发展，曾任醒吾工商专教师，人文科学研究会社会活动组召集人和毕升文化事业有限公司总经理等职务，专注青少年教育及社会文化活动组织工作，在文化教育领域有着丰富的经验。

**张肇珩**

北京大学台湾校友总会荣誉理事长、中华道教总会秘书长  
中华道教学院执行长

张肇珩，任北京大学台湾校友总会荣誉理事长，中华道教总会秘书长，中华道教学院执行长等职。张肇珩秘书长毕业于国立台湾大学哲学系及北京大学宗教学研究所，长期致力于宗教文化研究工作，积极促进两岸民族融合，推动两岸间道教的发展及文化交往。

投资  
机构INVESTMENT  
INSTITUTIONS



## 特别合作机构

SPECIAL COOPERATION AGENCIES



### 国际洪门总会

国际洪门总会为全球最大海外华人社团，总会章程为“团结洪门昆仲，发扬洪门忠义精神，振兴伦理道德，提倡社会福利，服务人群，造福人类”。2004年，刘沛勋主席重新修订了国际洪门五大任务：发扬洪门忠义精神、宣扬中国传统文化、推动两岸经济文化交流、促进中国和平统一、实现中华民族伟大复兴。现今，全球洪门各地昆仲有1000余万人，洪门直接或间接控股、参股、投资的企业、基础设施、公共事业、旅游、酒店、博彩等实业分布在世界各地，洪门的综合资源将成为全球社团通用积分项目顺利落地的核心资源。



### 中华青溪总会（台湾退伍军人协会）

中华青溪总会于2000年，由中国台湾地区国防部军管司令部（现后备指挥部）司令金恩上将（现任中国国民党黄复兴党部主任委员）之积极策划指导下成立。以服务后备袍泽、凝聚后备向心、共创祥和社会、支援后备动员，协力全民国防为宗旨。中华青溪总会下设中国台湾地区22县市青溪总会，涵盖全台湾地区364个乡镇基层组织，现有会员人数100万余人。中华青溪总会将成为全球社团通用积分的战略合作方，积极在下设组织和会员中推广社团链平台。



### 中华道教总会

中国台湾地区中华道教总会最早于1912年9月在北京成立。中华道教总会以阐扬教义、整理教规、弘道护国、服务社会、树立民族正信、促进世界大同为宗旨，下设台湾省道教会、台北市道教会、新北市道教会、台中市道教会、台南市道教会和高雄市道教会等六个省级教会及十八个县（市）道教会，另并设置弘道委员会、志工委员会、青年委员会、妇女委员会、学术委员会，在宗教组织伦理建构下共同推行教务及会务，为复兴中华民族文化而努力。中华道教总会的会员是以宫庙为单位，目前共有一万多家宫庙会员，遍居台湾或海外华人地区。每家宫庙各有数百甚至上千的忠实信众。中华道教总会将成为全球社团通用积分的战略合作方，积极推广社团链平台在全台道教信众和下属会员的使用。

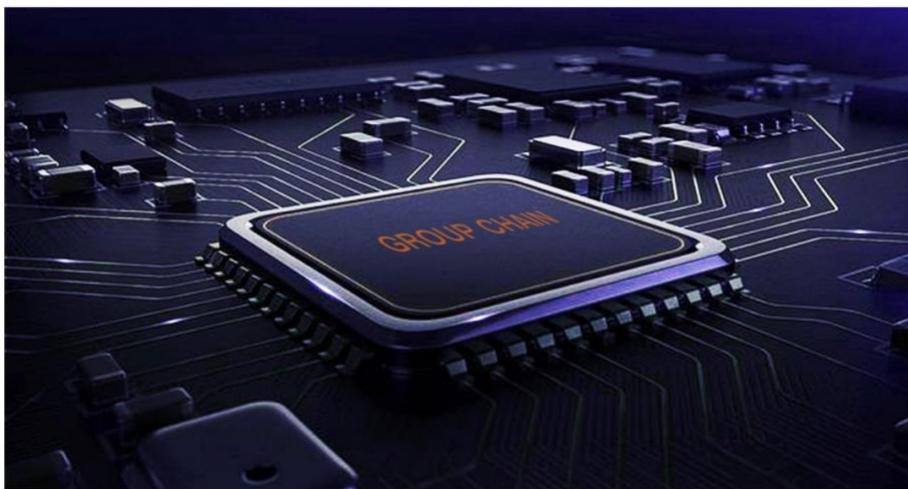
# 全球社团通用积分执行路线图

GLOBAL COMMUNITY GENERAL POINTS IMPLEMENTATION ROADMAP

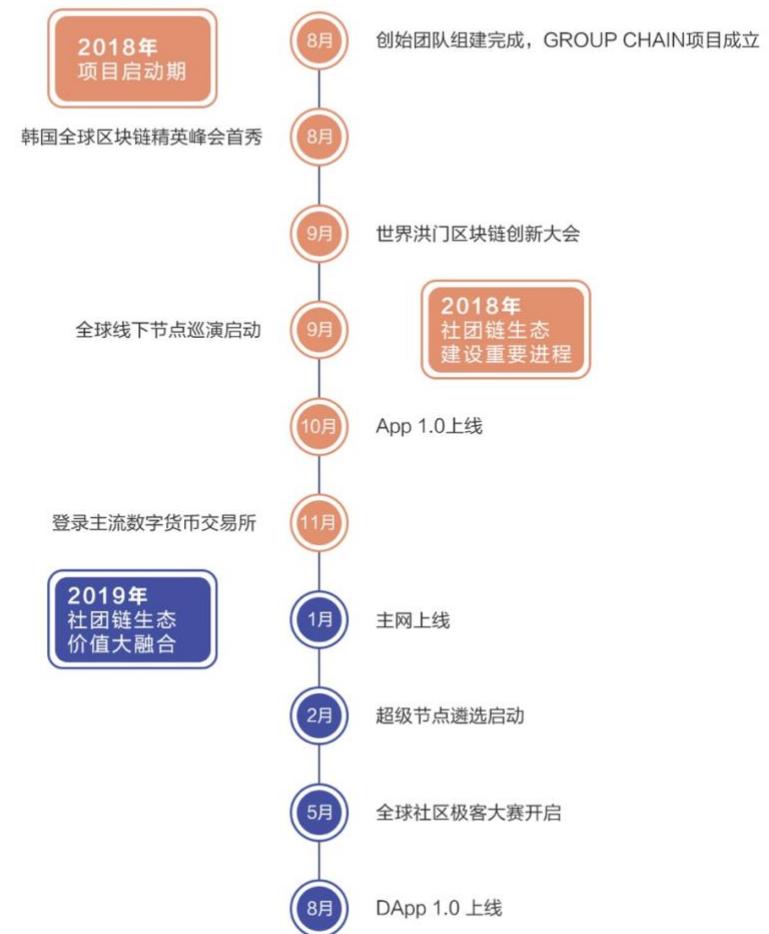
全球社团通用积分（简称：社团链GROUP CHAIN）

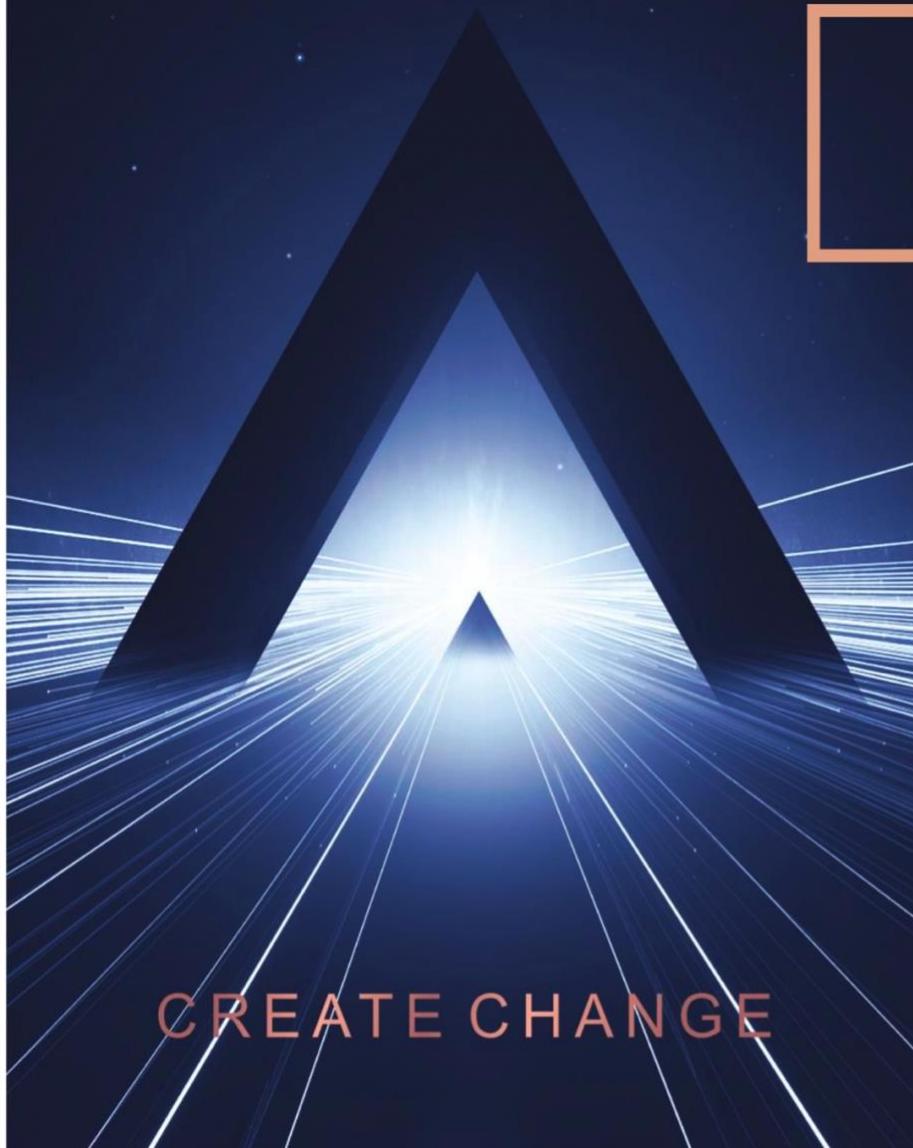
项目将围绕公链技术开发、用户导入、场景落地、大事件营销、社群生态建设五个维度加速推进。

GROUP CHAIN 的全部进展将会在项目官网：[gtoken.world](http://gtoken.world) 第一时间同步更新。



## TIMELINE 社团链时间规划





CREATE CHANGE



## 联系方式 CONTACT

官方邮箱: [universalgroup2018@outlook.com](mailto:universalgroup2018@outlook.com)  
官方网站: [gtoken.world](http://gtoken.world)

### 法律声明:

全球社团通用积分（简称社团链）白皮书所撰写的关于社团链的介绍、业务模型、平台架构、实施路线、治理架构等与社团链相关的原创文字和原创图片、表格等内容版权归属全球社团通用积分所有，如需使用请注明来源：“全球社团通用积分白皮书”字样。非法使用或转载的，全球社团通用积分将有权依法追究责任。

### 免责声明:

本文档仅为项目介绍，内容供参考，不构成任何买卖建议。

投资项目则代表参与者已经具备民事行为能力，与全球社团通用积分（社团链）之间的合约是真实有效的，并且双方本着自愿原则合作。

社团链将会做最大努力确保项目设计内容的落地和实现，但是不排除未来可能因为技术革新或其他不可抗因素对本文档内容进行修改升级，请各位即时通过官网获取最新讯息。

社团链平台已经明确向参与者阐述了可能存在的风险，参与者一旦参与项目投资，代表其已经理解并认可项目相关说明，接受潜在风险。



全球社团通用积分

社团链-链接每个人

谢 谢

THANKS