



DIY CHAIN

基于区块链技术

全球C2M点对点交易生态白皮书

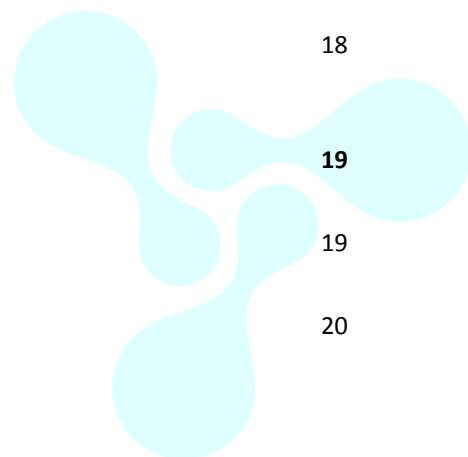
Global C2M point to point transaction ecological white paper

(内审版v1.3.0)

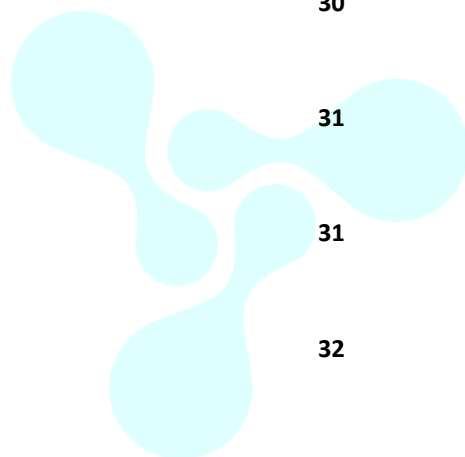
DIYchain Foundation (基金会)

目录

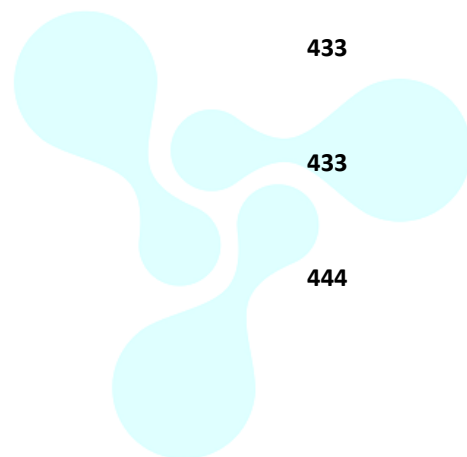
1.区块链背景	5
2.DIYCHAIN 项目介绍	7
2.1DIYchain 产生背景	7
2.2DIYchain 愿景	8
3.DIYCHAIN 功能说明	10
3.1 点对点交易	11
3.2 产品版权溯源体系	12
3.2.1 产品认证	12
3.2.2 版权维权	14
3.3 交易征信体系	14
3.4 智能支付体系	17
3.4.1 数字钱包	17
3.4.2 交易网络	18
3.5 售后仲裁体系	19
3.5.1 发起仲裁	19
3.5.2 反向仲裁	20



3.6 数据开放体系	20
4.DIYCHAIN 应用场景	22
4.1 定制 DAPP 应用链	22
4.2 IP 版权保护 DAPP 应用链	23
5.DIYCHAIN 如何落地	24
5.1 定制应用 DAPP	24
5.1.1 定制生产工厂 SaaS	24
5.1.2 小程序成为 DIYchain 用户分发节点	25
5.2DIYchain 经济生态	26
5.2.1 激励生态	26
5.2.2 价值生态	27
6.DIYCHAIN 技术说明	29
6.1 双链并行	29
6.2 共识算法层	30
6.3 数据存储层	31
6.4 全链通信层	31
6.5 智能合约层	32



6.6 DAPP 应用层	33
7. DIYCHAIN TOKEN 分配方案	34
8. DIYCHAIN 发展路线	36
9 DIYCHAIN 基金会	38
9.1 基金会的设立	38
9.2 基金会架构	38
9.3 各委员会职能划分	39
10. DIYCHAIN 团队介绍	40
10.1 团队	40
10.2 顾问	411
10.3 合作伙伴	422
11.风险提示	433
11.1 合规、运营性风险	433
11.2 市场风险	433
11.3 技术风险	444



11.4 资金风险

444

12.免责声明

455



1. 区块链背景

在传统的互联网贸易上，几乎所有的交易都需要依赖第三方信任机构来处理电子信息，而这类系统仍然受制于“基于信用的模式”，比如在淘宝、亚马逊等购物平台，这些平台其实就是第三方信任机构，能够让客户产生信任在平台上进行交易。而这种交易往往需要受制于这个中心化的第三方机构，根据以往经验，这样做至少有两个缺陷，其一，第三方机构一旦出现问题，无论是内部管理问题，还是外部攻击，都将会给基于第三方平台的服务带来致命的打击。比如曾经的如家身份证被盗事件，比如索尼服务器被黑客攻击。其二，一旦第三方做大，比如中国的 BATJ，外国的 facebook,google 等，个人信息安全往往不受个体掌握，大公司可以任意调用个人信息为其牟利，个体甚至是小型组织的一切服务将受控于大型第三方机构，个体的诉求很多时候无法得到有效回应。在这种情况下不单是信任成本增加，一旦第三方做大，个体将会沦为整个体系中被操控的对象。因此去中心化的区块链概念被提出。

区块链的本质是不可篡改的分布式账簿，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术解决方案，使用三项底层技术来实现，他们是：共识机制、密码学原理和分布式数据存储。

区块链的概念首次在 2008 年末由中本聪（Satoshi Nakamoto）发表在密码学邮件列表中的论文《Bitcoin: A Peer-to-Peer Electronic Cash System》提出。论文中区块链技术是构建比特币数据结构与交易信息加密传输的基础技术，该技术实现了比特币的挖矿与交易，催生出了去中心化比特币，随后比特

币进入了快速发展的阶段。可以说区块链技术是比特币产生后抽象出来的底层技术，一开始，人们并没有认识到区块链技术可能对人类商业社会带来的影响，直到 2014 年 Ethereum 项目提出了基于区块链技术的智能合约系统，以及基于智能合约体系的分布式自组织结构（DAO），无数基于 Ethereum 平台的项目吸引了传统投资人的眼光，直到 2017 年，数字加密货币兑换法币有了重大突破，更多的人开始关注区块链技术和智能合约技术。



2. DIYchain 项目介绍

DIYchain (Do It Yourself Chain) 将区块链技术与电商交易相结合，利用区块链去中心化、不可篡改、可溯源的特性，建立一个去中心化的 C2M (顾客对工厂 Customer To Manufactory) 全球电商点对点交易生态，立志打造全新的定制化电商交易生活方式。

DIYchain 将利用技术积累建立全球电商的底层公链，前期将从定制电商行业入手，在 DIYchain 公链上建立第一款定制电商的应用链，后期将底层公链对全球推广，对所有的开发者进行开放，所有开发者都将可以在公链基础上开发属于自己的电商应用链。

2.1 DIYchain 产生背景

随着 20 世纪末互联网的出现，互联网线上交易的电商模式风靡全球，经过 20 多年的发展，整个全球电商都进入了鼎盛时期，根据相关数据统计显示，全球电子商务市场规模达到 25 万亿美元，主要市场集中在美国、欧洲、中国等地区。

根据中国国家统计局电子商务交易平台调查显示，2017 年全国电子商务交易额达 29.16 万亿元，同比增长 11.7%。其中商品、服务类电商交易额 21.83 万亿元，同比增长 24.0%；合约类电商交易额 7.33 万亿元，同比下降 28.7%。

虽然电商市场份额仍在不断的发展，但是仍然存在诸多的问题并未解决：

- 1) 过于集中的中心化越来越严重
- 2) 假货无法认证，越来越猖狂
- 3) 电商货款账期问题越来越突出
- 4) 数据被巨头掌握，消费者、商户无法获取
- 5) 售后问题处理难

而区块链作为新兴的数据库技术解决方案，拥有天然的分布式节点存储，不可篡改等属性，它兴起被认为是继蒸汽机、电力、互联网之后的又一次技术浪潮，是一场新技术革命，同时 2018 年被认为区块链应用落地的元年，但是目前现有的区块链公链也存在很多问题：

- 1) 以 POW 为基础的比特币消耗资源过大，且交易速度慢
- 2) 以 POS 为基础的点点币存在信用基础不够牢固的缺点
- 3) 以 DPoS 为基础的 EOS 存在节点投票的积极性不高等缺点

伴随着电商中心化等问题和区块链底层公链存在的一些问题，DIYchain 因此应用而生，结合电商行业现状和痛点，将 POS 和 DPOS 共识机制结合，提出打造区块链的电商生态体系，形成真正意义上的点对点交易，打造去中心化的 C2M 交易模式。

2.2 DIYchain 愿景

DIYchain 旨在通过区块链去中心化、不可篡改、溯源追踪的特性，结合电商行业的实际情况，打造 C2M 的全新交易生活方式，降低消费者的交易成

本，提高生产厂家的生产效率，让全球化点对点交易融入生活的方方面面，让人人皆可交易，物物皆可交易。

点对点的交易生活方式：DIYchain 期望通过区块链技术将 C2M 交易模式普及到人们日常生活之中，打通消费者与厂家之间的信任壁垒，降低信任成本，实现点对点的定制化电商交易方式。

全球电商底层公链：DIYchain 期望利用 POS 和 DPOS 共识机制建立全球范围内电商交易公链，建立基于区块链技术的交易征信体系、产品版权溯源体系、智能支付体系、交易售后仲裁体系、数据开放体系，开放给全球开发者，让区块链技术服务电商的各行各业。



3. DIYchain 功能说明

DIYchain 将基于区块链技术建立人人都可以参与的 C2M 点对点交易生态，主要参与方有：消费者、生产厂家、开发者，实现点对点的去中心化交易。

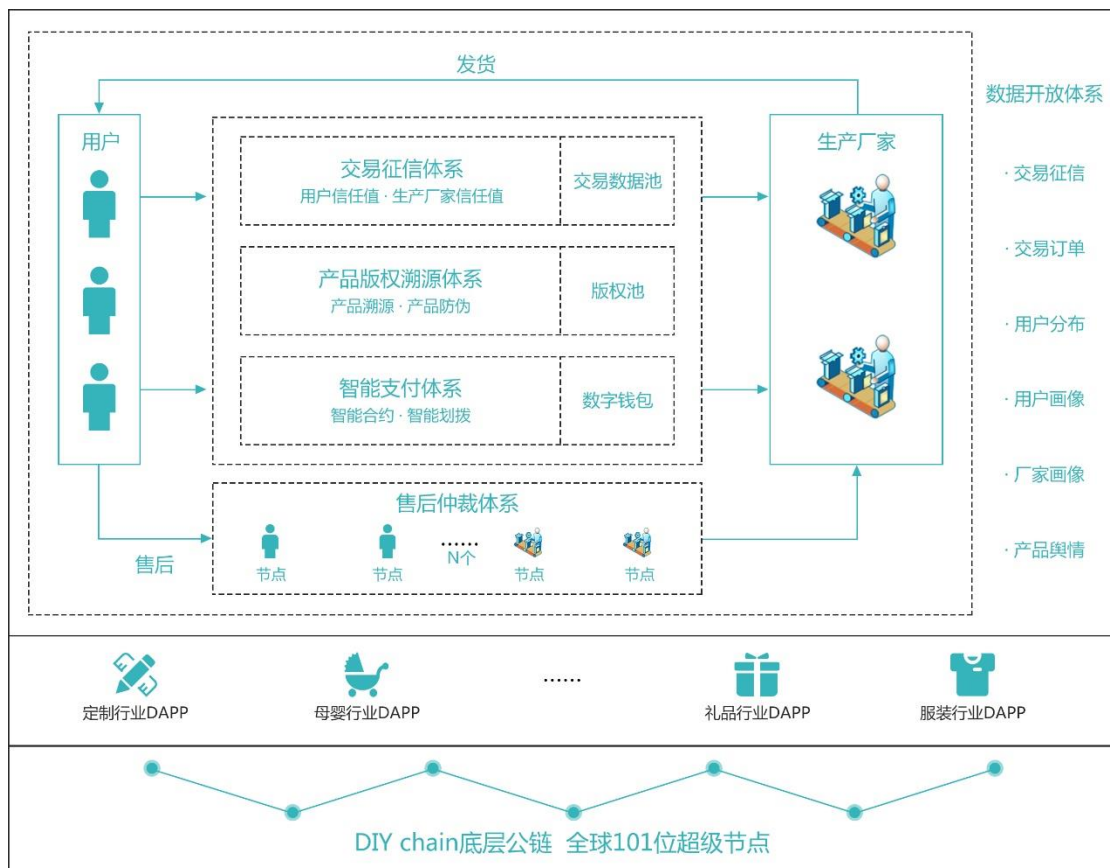


图 3.1 DIYchain 功能框架图

在整个 DIYchain 生态中，以交易征信体系、产品版权溯源体系、智能支付体系、售后仲裁体系、数据开放体系 5 大体系为生态基础，建立个人到工厂的 C2M 点对点交易生态。

3.1 点对点交易

对于当前电商行业，大多数交易都是通过第三方代理完成，买家向代理商提出购买需求，代理商再传递给后端的生产厂家，中间代理商获得中间价格差，而这个价格差往往是厂家出售价的 50% 以上，造成客户购买费用增加，同时中间传递过程会导致效率低下。

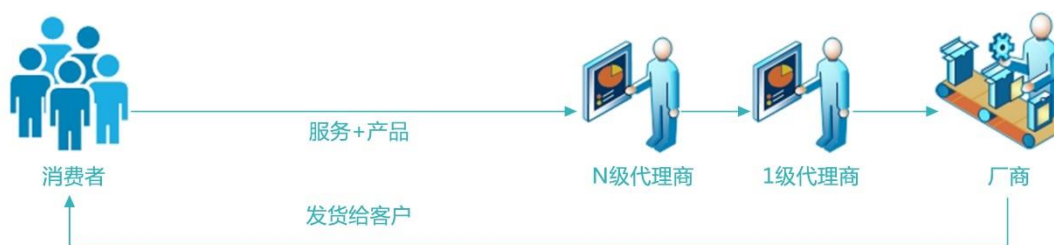


图 3.2 当前电商交易模式

利用区块链分布式节点的去中心化特性，建立起去中心化的交易生态，这个交易生态由所有的消费者、生产厂家共同进行维护，所有的消费者都可以自主的上这个生态找到终端的生产厂家，直接点对点进行交易，减少中间环节。



图 3.3 C2M 的点对点交易模式

3.2 产品版权溯源体系

在当前电商环境中，无论是号称无假货的京东还是国内最大的电商平台淘宝，都存在或多或少的假货，甚至有的假货可以以假乱真，版权方对假货维权也存在诸多困难。

针对这种情况，DIYchain 将建立点对点交易生态中的产品版权溯源体系，对全链上线的产品都将实行版权认证，和全链其他节点已上线产品进行匹配，认证通过后将对产品形成全链唯一且不可篡改的版权标识并广播全链。

3.2.1 产品认证

在版权认证这一块儿，将利用采用数字认证水印技术，将产品上传者的个人信息、图片信息、产品信息、图片信息等进行加密处理，采用 RSA 和 DES 双重加密算法形成数据比特流，再对比特流进行逐字切割，转化成十进制数据，得到元素值位于 0 到 255 之间的加密数组，然后以修改宿主图像矩阵元素值的方式实现水印的嵌入，并最终得到内嵌水印的载体图像。



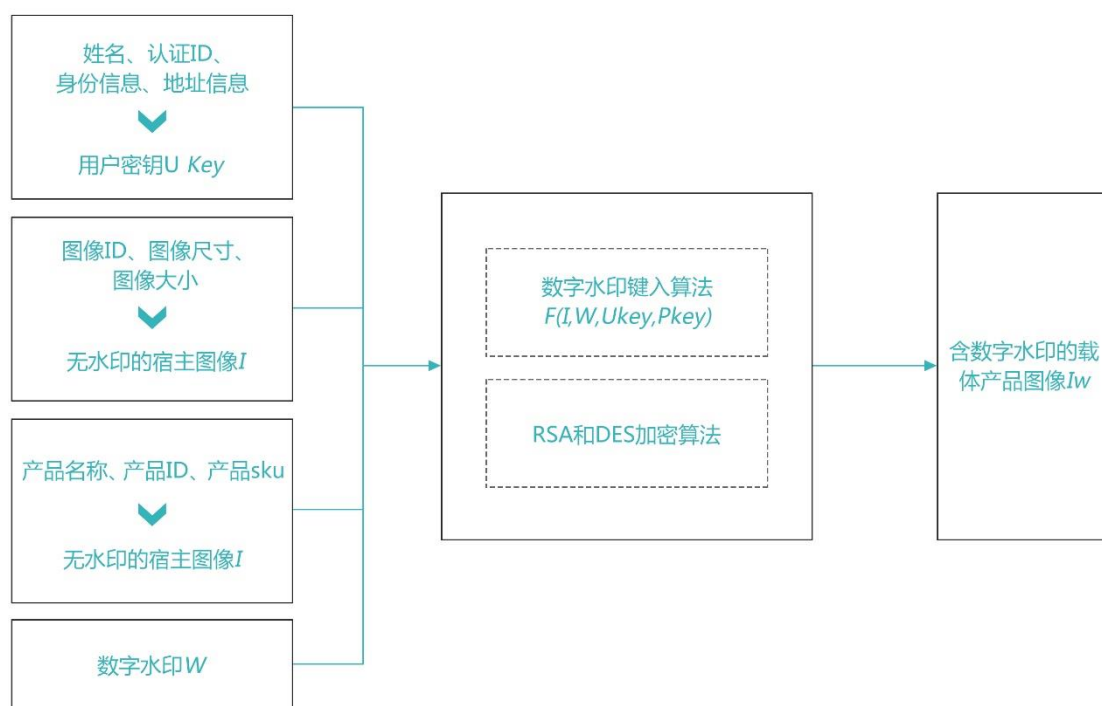


图 3.4 数字认证水印技术流程

在版权认证后，DIYchain将通过版权智能合约的方式将认证信息存入全链区块之中，形成不可篡改可溯源的区块记录。同时对于产品的基础信息，将扩展产品的数据基础字段，扩展字段有：

字段	字段类型	字段长度	字段描述
product_id	Int	11	产品id
product_key	String	255	产品密钥key
user_id	Int	11	用户id
user_key	String	255	用户密钥key
product_img	String	255	宿主图像I
watermark	String	255	数字水印w

product_img_watermark	String	255	含数字水印的载体 产品图像 I_w
-----------------------	--------	-----	------------------------

3.2.2 版权维权

针对产品版权，如果出现产品侵权现象，DIYchain提供基础的版权维权模块，用户可以直接在链上发起版权维权仲裁，发起后系统将广播至全链101个超级节点，同时广播给全链101位消费者类型的节点和101位生产厂家类型的节点，由这三方共同发起仲裁决定。

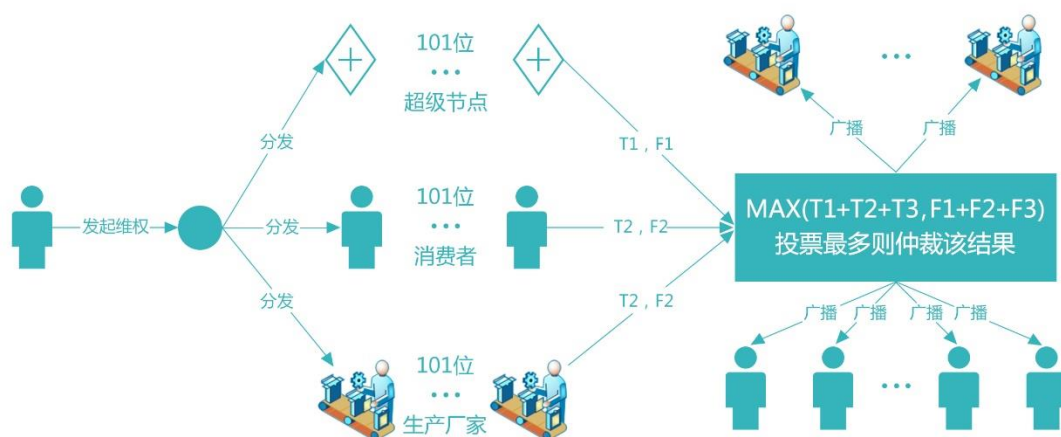


图 3.5 版权维权流程

3.3 交易征信体系

不管是对消费者还是后端生产厂家，信任都是从 0 到 1 开始进行建立，而这种信任往往需要一个中心化平台或者中心化代理商来进行背书，信任建立成本大。

利用区块链不可篡改的特性，对上链的消费者和生产厂家形成不可篡改的交易信用记录，真实、透明记录每一笔消费，建立全球全链不可篡改的交易征信数据池，同时利用智能合约建立信用机制，使用代码而非某个中心化机构动态评估消费者、生产厂家的交易信用情况，形成动态的信用值。

DIYchain 将通过全链用户的基础信息、消费信息、仲裁信息等相关信息去建立信用身份。

基础信息主要包含：

- A. 用户姓名
- B. 用户履历
- C. 用户身份证号码
- D. 用户联系信息

消费信息主要包含：

- A. 交易时间
- B. 交易次数
- C. 交易金额
- D. 交易数量
- E. 交易的服务产品
- F. 定制交易完成时间
- G. 智能合约结束时间
- H. 交易账单清算时间
- I. 是否仲裁



仲裁信息主要包含：

- A. 仲裁数量
- B. 仲裁金额
- C. 仲裁时间
- D. 正向仲裁次数
- E. 反向仲裁次数

关于算法方面，基于贝叶斯算法的投票式组合模型的思想，选择 Logistic 回归、聚类分析和神经网络进行组合，同时使用基于粗糙集算法对两个混合模型 FA-RS 和 MEPA-RS 模型进行优化，选取了 Fisher 判别分析、Logistic 回归、Probit 回归、多元线性回归 4 种常用的统计学模型，结合投票器的方法对影响个人信用的特征向量进行显著性排序。另外由于人工智能方法的判别精度较高，因此采用步长遍历算法，以 BP 神经网络和支持向量机两种精度较高的个人信用评级模型的平均精度为判别标准，输出显著性权重，对个人信用评级指标体系进行显著性加权，提高指标体系的合理性和科学性。

采用等权投票的方法决定最终指标显著性顺序 I；

设指标显著性权重向量为 $W_k = (w_1, w_2, \dots, w_n)$ ，其中

$$\sum_{i=1}^n W_i = 100$$

在权重可赋值范围内进行遍历，得到 W_k 所有可能的取值情况的取值情况；

对信用样本中的特征值数据进行显著性加权处理，得到修正指标体系为

$$I_k = I * W_k$$

随着系统数据的积累，我们将通过机器学习的方式不断修正和完善信用值的建立体系。

3.4 智能支付体系

在电商交易行业，很多情况交易都存在账期，如定制电商，客户往往定金给经销商，经销商又在后端加工厂拿到一定账期，客户在约定时间找各种理由不付尾款，经销商拿不到，自然又不给后端的加工厂，导致收账难，甚至在有时候会出现坏账的可能性。同时，在全球跨国交易环节中，各国通过各自的法币进行结算，存在诸多的兑换中间环节，一定程度上增加了支付成本。

DIYchain 将发行属于电商交易行业的流通数字资产 (DIY)，通过数字资产的全球流通性，省去中间退换结算环节，加快交易效率。同时利用区块链智能合约技术，一旦交易形成将形成不可篡改的智能合约，在一定条件下自动执行合约，及时划拨款项给生产厂家。

3.4.1 数字钱包

另外，DIYchain 将建立电商行业的专属数字钱包，此钱包将作为数字资产的存放和兑换，整个 DIYchain 生态中将不仅仅只支持 DIY 的虚拟和实物的流通，也将实现其他数字资产如 BTC 与全链生态中的实物直接兑换，打通数字资产相互兑换带来的兑换成本，加速流通。

3.4.2 交易网络

另外，为了电商行业高频的交易行为，DIYchain 在整个交易体系中将采用闪电网络来作为整个交易网络的支付基础，主要核心包含序列到期可撤销合约 RSMC (Revocable Sequence Maturity Contract) 和哈希时间锁定合约 HTLC (Hashed Timelock Contract)。

RSMC 其主要原理，在消费者和 DIYchain 生态中和生产厂家在交易时会建立一个“微支付通道”，双方都会往这个通道里面预存一部分资金，交易时，双方就资金的分配方案共同确认，同时签字作废旧的版本。交易完成后，通过智能合约按照前期约定的分配方案进行划拨，同时将最终的交易结果写到区块链网络中。

而整个微支付通道是通过 HTLC (Hashed Timelock Contract) 来实现的，其实就是限时转账，其主要原理通过智能合约，双方约定转账方先冻结一笔钱，并提供一个 Hash 值，如果在一定时间内有人能提出一个字符串，使得它哈希后的值跟已知值匹配（实际上意味着转账方授权了接收方来提现），则这笔钱转给接收方。

RSMC 保障了消费者和生产厂家之间的直接交易可以在链下完成，HTLC 保障了任意两个人之间的转账都可以通过一条“支付”通道来完成。整合这两种机制，就可以实现任意两个人（点对点）之间的交易都可以在链下完成了。

在整个交易中，智能合约起到了中介的重要角色，而区块链则确保最终的交易结果被确认。

3.5 售后仲裁体系

由于整个电商行业的极度分散化和某些品类极度不标准化，总会出现一定的售后纠纷，买家、生产厂家都各有说辞，难以达成一致，造成定制问题积压难处理。当前主要处理定制问题则一般由平台方或者经销商进行协调解决，让买方和生产厂家各自妥协。

一旦出现售后，通过区块链分布式节点的结构，用户发起仲裁，通过节点信任值、和相关度动态匹配一定数量的节点参与仲裁评估，不是单个个体，也不是单个中心化结构，而是全链动态匹配多个节点参与，提升仲裁公平性和可靠性。

3.5.1 发起仲裁

在仲裁阶段，系统将根据相关度和信任值等情况，向全链 N 个消费者节点、 N 个生产厂家节点发起仲裁任务，由节点进行确认投票，如果 10 分钟内未进行确认，系统将自动将仲裁权分配给其他相应节点。在收到各自 K 个确认投票结果数之后（ k 为奇数），结束仲裁，根据仲裁结果数大于 $K/2$ 的结果定为仲裁结果，结果将会发往仲裁的过程参与的先关方。

在仲裁过程中，仲裁结果也将影响仲裁所需费用的承担方，比如仲裁结果利好买方，费用将由服务或者生产者承担，反之由买方承担。而对于仲裁费用，系统将按照二八原则分发给所有仲裁确认者，与仲裁结果一直的确认者将获得 80% 的费用以作奖励，与之相反的获得 20% 作为奖励。

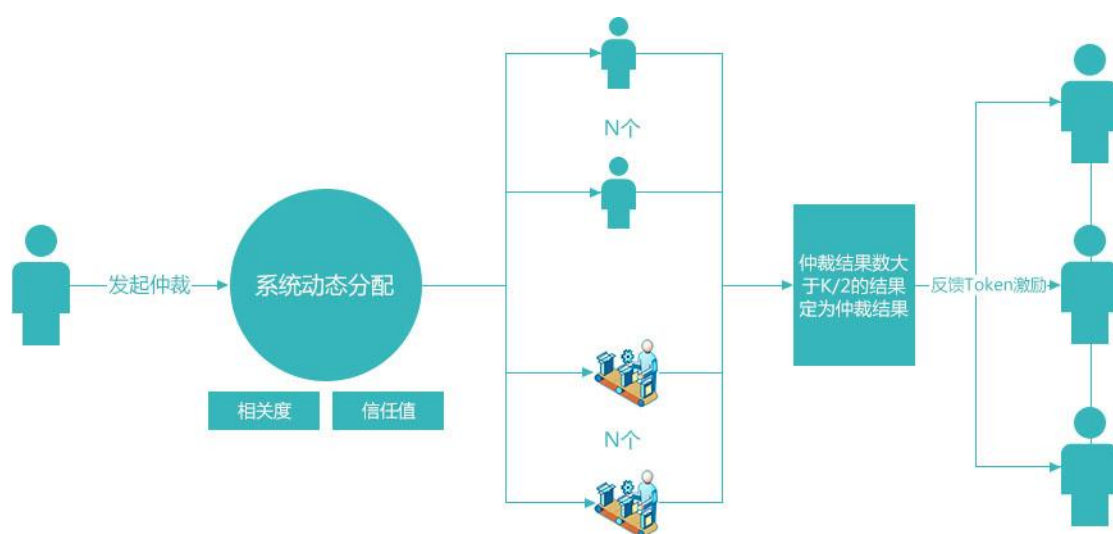


图 3.6 仲裁流程

3.5.2 反向仲裁

针对仲裁结果，将存在全链 3 天的公示期。在公示期内，消费者和厂家都可以提出反向仲裁机制，此机制将对仲裁结果发起新的仲裁，并分发给除去上次仲裁的之外的其他节点进行新的仲裁，而仲裁结果将同样广播给全链所有节点。

对于反向仲裁，DIYchain 只提供 2 次反向仲裁机会，加上第一次仲裁，最多 3 次仲裁，对于 3 次仲裁结果，将取 2 次相同结果的为最终仲裁结果并进行实时 Token 奖惩。

3.6 数据开放体系

在当前行业中，每个生产厂家、经销商都有自己的生产数据、交易数据，但这些数据仅仅只有自己的，在行业里面只是其中的九牛一毛，无法获取到可靠、完整的行业数据，无法共同协作提升行业效率，另外在现有的中心化平台

中，如淘宝、亚马逊，掌握了全球电商领域的巨大数据，而这些数据并未对全行业全用户进行公开，也因此用这些数据形成自己的数据壁垒，形成中心化电商寡头。

利用区块链公开透明的特性，打通数据壁垒，实现全行业信息共享，相互合作，进一步提升整个行业效率。

在数据开放方面，将主要针对交易征信、交易订单、用户分布、用户画像、厂家画像和产品舆情等方面进行开放，实行分层开放形式。

对于消费者层，开放：交易征信、交易订单、厂家画像

对于厂家层，开放：交易征信、交易订单、用户分布、用户画像、产品舆情。

另外，对于其他数据类型进行的开放，DIYchain 将采用全链投票的形式对需开通的数据层进行投票，超过 51%的赞成将实施开放。



4. DIYchain 应用场景

DIYchain 提供全球电商的底层公链，建立基于区块链技术的交易征信体系、智能支付体系、交易售后仲裁体系、数据开放体系，开放给全球开发者，全球开发者都可以基于 DIYchain 建立各行各业的专属应用链，实现让人人皆可交易，物物皆可交易。

4.1 定制 DAPP 应用链

随着全球经济变暖，企业对自身形象越来越重视，对团体服装定制、办公用品定制等需求越来越大，定制员工服几乎成为了企业的标配，杯子、笔、本子等定制也几乎成为常态。

在现有情况下，企业很难直接找到后端的定制生产厂家，一般都会通过电商平台（如淘宝）去进行定制采购，但通过这种途径绝大多数情况只能找到中间代理，因此面临高昂的中间费用。

DIYchain 将提供全链的底层开发接口，提供 DAPP 标准化 UI/UX 方案，开放给全球的区块链开发者，开发者可在 DIYchain 的基础上建立定制行业的应用 DAPP，为全球用户提供点对点定制交易，通过企业的定制需求智能化提供最优的生产方案，企业也可以通过生产厂家地点、信任值、服务内容自行选择生产厂家，省去中间环节，节省定制、交流成本，让企业低成本的进行定制，同时每一个产品都可以进行溯源追踪，查询产品从生产到定制发货的全过程。

4.2 IP 版权保护 DAPP 应用链

DIYchain 生态中，在虚拟资产如 IP 版权方面也可以直接进行应用，开放者可以在 DIYchain 公链基础上，针对 IP 版权这个行业的特殊性进行开发，对于 IP 服务提供者，提供 IP 版权和预售两大板块，提供者可以将自己的 IP 上传到全链上，系统将自动为该 IP 进行识别，同时提供不可篡改的版权标识，IP 提供者可以进行定价，所有用户可以购买使用。

通过这种方式，DIYchain 基础上产生的 IP 版权 DAPP 不仅仅对 IP 进行了有效的保护，同时也让 IP 提供者获得收益。

另外，开发者也可在 DAPP 中让 IP 提供者直接将 IP 与定制实物结合，形成 IP 定制产品，全球消费者都可以进行购买，通过这种方式，DIYchain 可以成为全球 IP 实物化的正版发售平台。

比如：漫威发布印有钢铁侠的 T 恤，全球限量 100 件，正版授权。消费者进行购买，同时可以扫产品的二维码溯源 IP 提供方的信息，确认正版授权。



5. DIYchain 如何落地

DIYchain 团队结合自身的资源优势，将在 DIYchain 公链基础上开发第一款定制行业的应用 DAPP。

5.1 定制应用 DAPP

在开发 DIYchain 公链之前，我们将在定制行业建立定制生产工厂 SaaS 和小程序，以此积累一定的用户数据、交易数据、售后数据，用于 DIYchain 公链开发时的数据检验和智能合约算法优化。

5.1.1 定制生产工厂 SaaS

DIYchain 已初步建成中国最大的定制生产工厂 SaaS 系统，在平台上，注册并使用的全国服装定制生产厂家 2000 家，实际注册终端用户数达到 10 万，日均注册人数达到 533 人，日交易订单个数达到 700 笔团体服装定制订单，日交易服装件数达 23000 件。这些都将成为 DIYchain 链上首批真实的使用者。

另外，截至目前为止，共计上线定制款式 SKU 达 5180 款，涵盖品类 280 个，主要有服装、礼品、办公用品三大品类定制。





图 5.1 定制生产工厂 SaaS

5.1.2 小程序成为 DIYchain 用户分发节点

DIYchain 目前已与多家合伙人进行合作，分发小程序达 74 个，每个小程序至少辐射 1000 名合伙人周边朋友，用户总数达 74000 名。通过小程序的模式，快速发展首批链上种子用户。



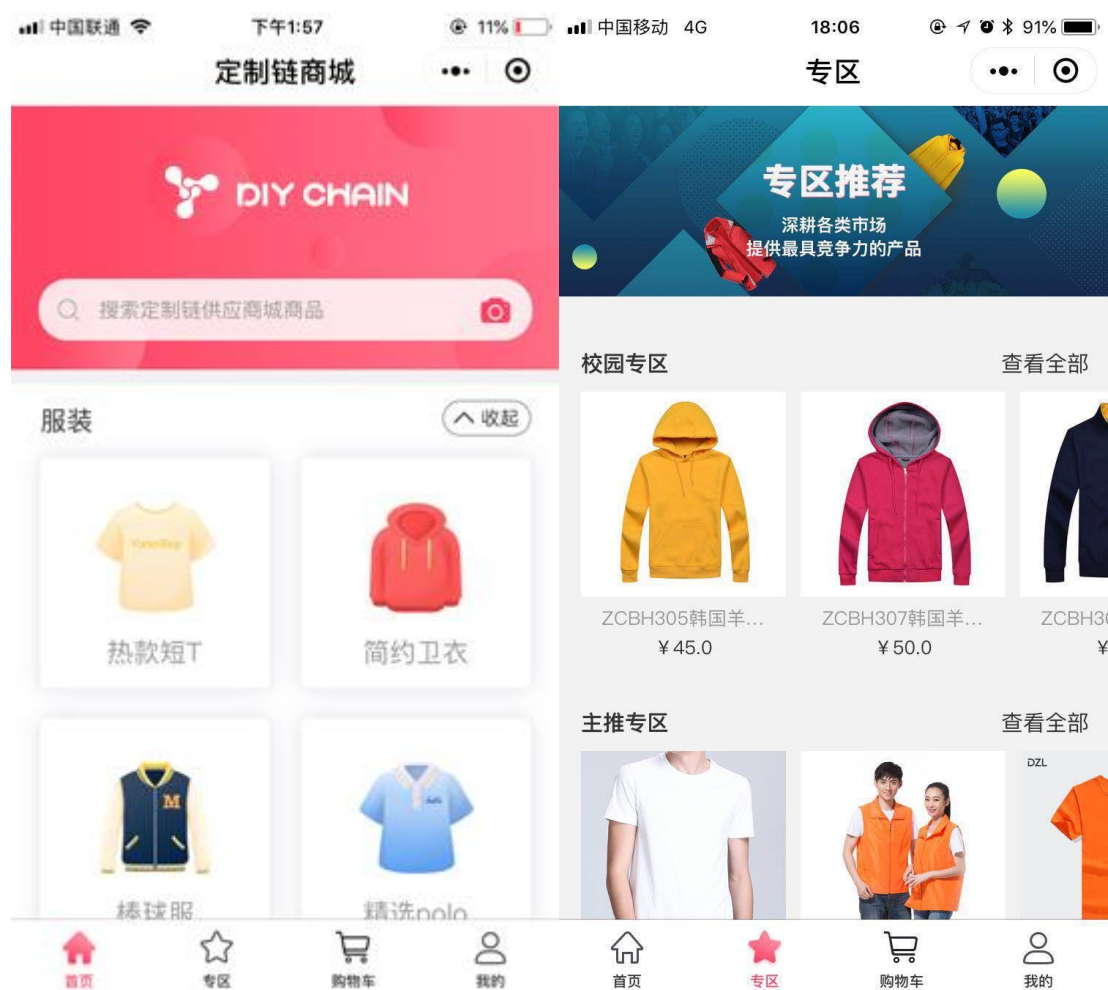


图 5.2 小程序

5.2 DIYchain 经济生态

作为全球去中心化的电商点对点交易的公链底层，DIYchain 将发行数字资产 DIY，同时为了更好的让消费者、生产厂家以及开发者维护全链，在整个生态中，DIYchain 将拿出大部分的 DIY 分发给全链的节点。

5.2.1 激励生态

1) 仲裁激励

对于参与仲裁的的节点，将获得一定的 DIY 激励，同时，如果最终仲裁结果和自己的仲裁一直，将额外获得 DIY。

2) 交易激励

不管对于消费者还是生产厂家，只要无任何售后仲裁的完成交易，都将分别获得 DIY。

3) 上链激励

为了鼓励消费者和生产厂家上链，将自己的信任情况等数据开放，都将获得一笔初始 DIY。

4) DAPP 激励

对于开发者而言，只要在 DIYchain 公链基础上成功开发 DAPP 并在全链进行推广，将获得 DIY，以此鼓励更多的开发者开发适合各行各业的电商 DAPP。

5) DIY 利息激励

为了让更多的用户持有 DIY 并维护全链网络的正常运行，在 DIY 到达一定市价时发放糖果激励。

5.2.2 价值生态

DIY 作为全球电商行业的流通数字资产，随时随地，线上线下点对点交易各种产品，如服装、礼品、服务、办公用品

1) 费用支付



DIY 将作为整个 DIYchain 生态中的数字资产，在点对点交易时，可以直接支付交易所产生的费用，以数字资产购买实物资产。

2) 仲裁支付

任何仲裁行为都将支付一定的 DIY 给全链的 DIY 仲裁节点，以此记录节点参与到仲裁之中，保证整个仲裁的可靠性和公正性。



6. DIYchain 技术说明

DIYchain 为了方便测试，前期将依托以太坊作为开发和测试的平台，但以太坊采用的 POW/POS 混合共识算法，存在消耗资源过大，且交易速度慢，无法适应电商行业的高频、快速的交易形式，因此 DIYchain 将结合 DPOS 和 POS 混合的共识算法，提升整个生态的交易处理速度。



图 6.1 DIYchain 技术架构

6.1 双链并行

DIYchain 底层架构将采用双链并行的架构体系，分为主链和副链。主链负责执行整个链上生态的交易体系、仲裁体系，同时维护交易历史和信任关系信息等，同时主链上可以存在全局依赖的动态数据结构。副链则主要负责维护各消费者、生产厂家的账户信息和信任值指数。

6.2 共识算法层

在 DIYchain 整个共识算法层面，将采用 DPOS 和 POS 混合的共识算法，DPOS 是目前兼备确认速度快、处理性能高等特点的共识模型。它的原理是让每一个持有 Token 的人进行投票，股权持有者可以选择任意数量的见证人来生成区块。

但是这种投票产生超级节点的做法，存在诸多的弊病，绝大多数持股人（90%+）从未参与投票。这是因为投票需要时间、精力以及技能，而这恰恰是大多数投资者所缺乏的。同时对于坏节点的处理存在诸多困难。社区选举不能及时有效的阻止一些破坏节点的出现，给网络造成安全隐患

针对以上存在的问题，DIYchain 共识算法中，将传统的 DPOS 投票选出 101 位代表调整为：由智能合约自动选出全球信任值占据全链前 101 位超级节点。通过交易征信体系中信任值来动态确定超级节点，利用全链共识的交易所产生的的征信信任值来确定超级节点，避免了全链节点投票需要的时间、精力和技能。同时在这 101 位超级节点中，其中 50 位来自消费者，51 位来自生产厂家，虽然这 101 位超级节点中，分为两种类型，但是双方的权利都是一样的，用于区块的产生、记录。

另外 DIYchain 为了避免超级节点不作为，如提供的算力不稳定，计算机宕机、或者试图利用手中的权力作恶，全链节点可以发起节点投票，剔除不作为的超级节点，剔除之后，系统将在 24 小时内对全链节点的信用值重新评估并最终确定 101 新的超级节点，而剔除的节点将在未来的 101 天内不可再次被选上，以此达到超级节点的公平性和公正性。

另外，DIYchain 的算法中，将 POS 中根据用户持有货币的多少和时间（币龄），发放利息的一个制度引入 DIYchain 之中，对于首批用户都将发往一定的 Token 激励，通过此方式吸引更多的用户、厂家上链，以此保证整个 DIYchain 生态网络的安全性。

6.3 数据存储层

DIYchain 的区块数据采用链式结构进行存储，所有区块都带有上一区块的指针引用，保证数据不被篡改。采用 sha256 函数对数据进行哈希散列，采用 ecc 非对称加密算法进行身份认证，采用 aes 加密算法加密私钥，采用 Merkle 数验证和存储交易。

对于大的文件内容，将存储在 off-chain 的文件系统中，现阶段已经开发出基于 ethereum geth 和 IPFS 的原型系统，同时将摘要（数字指纹）保存到链上用以自证。IPFS 是一个点对点的分布式超媒体分发协议，它整合了过去几年最好的分布式系统思路，为所有人提供全球统一的可寻址空间。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。

6.4 全链通信层

通信层包括分布式组网机制、数据传播机制和数据验证机制等，采用完全 P2P 的组网技术，具有自动组网功能的。在通信安全方面，可以灵活支持

HTTPS、TLS、SS(SecureWebsockets)等安全通信协议，在需建立平台应用对外服务接口上，可以扩展支持 OAuth 的认证集成。

6.5 智能合约层

对于每一项智能合约，作为一项链上资产进行全生命周期管理，对智能合约的提交、部署、使用、注销进行完整可控的流程管理，并集成权限管理机制对智能合约操作的各项机制进行综合性安全管理

DIYchain 将建立一个智能合约集合，以此用来管理所有开发者在 DIYchain 公链基础上对 DAPP 开发的智能合约，同时用于用于合约的升级、销毁。另外对于 DIYchain 对征信信任体系、智能支付体系、全链超级节点产生的合约都将放入此集合，所有开发者都将对公链的合约进行继承，以此衍生适合自己行业交易的合约，减少开发者的开发工作，快速实现 DAPP 并进行应用。

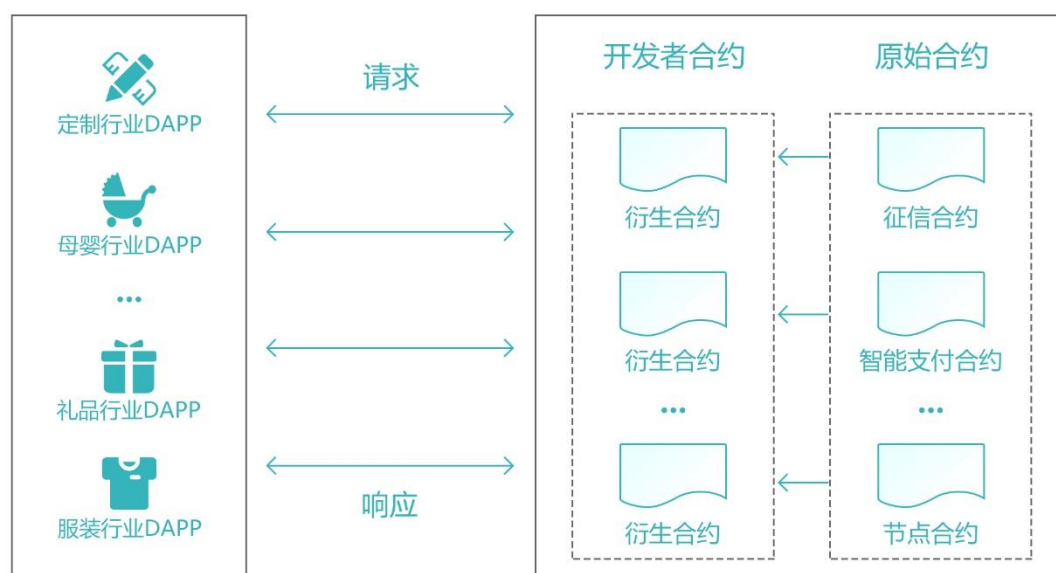


图 6.2 DIYchain 智能合约集合

6.6 DAPP 应用层

DIYchain 将基于 DPOS 和 POS 混合的共识算法建立点对点的电商交易公链，同时对全球开发者进行开放。为了节省开发者的开发成本，DIYchain 将不仅仅开放底层接口，同时还为对 UI/UX 提供标准化的组件，加速开发者开发 DAPP，减少不必要的成本。

另外，关于开发语言方面，DIYchain 将提供多元化开发语言的数据访问接口和交互接口，支持多语言集成和功能扩展，将支持 Java、JavaScript、Python 等多当前主流语言。



7. DIYchain Token 分配方案

DIYchain 总量 (以下简称总量) 为 10 亿个 Token , 分配形式为以下几种方式 :

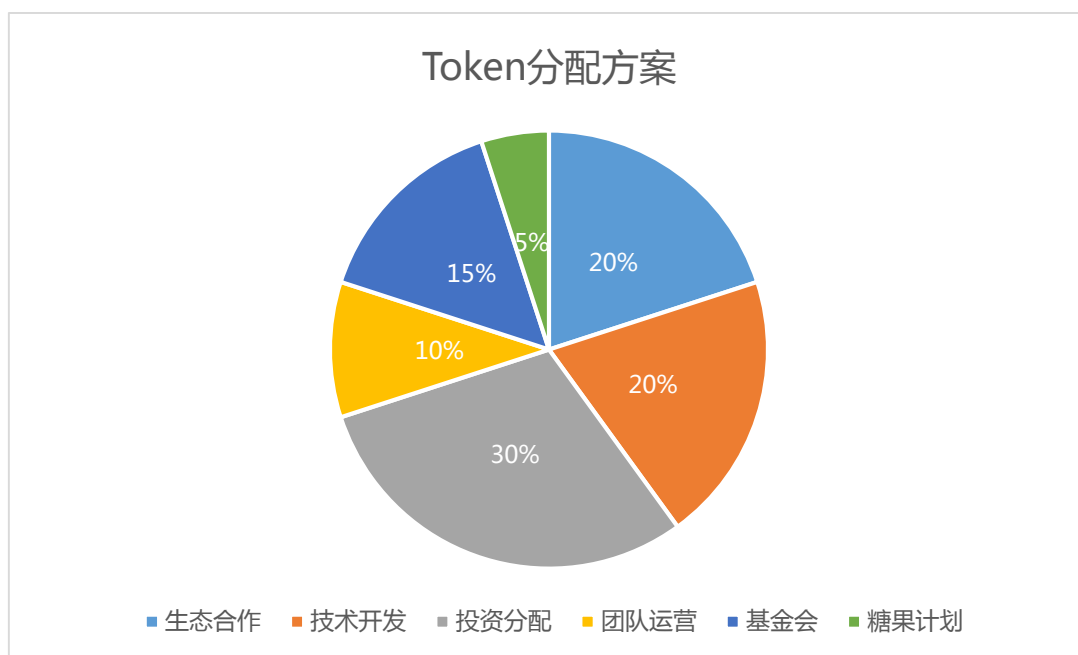


图 6.1 DIYchain Token 分配方案



总供应量:10 亿 代号 : DIY
20%生态合作，共计 2 亿个 Token。用于平台生态合作方在平台建设、活动、发展以及其中的人力、物力、才力贡献者和机构。
20%技术开发，共计 2 亿个 Token。将分配技术平台、技术开发以及维护升级过程中的技术团队，包括小程序、SaaS 等软件、硬件研发。
30%投资分配，共计 3 亿个 Token。其中 10%战略投资方，20%天使投资机构及个人，30%基石投资人，40%早期投资者。此阶段仅面向特定群体开放，根据阶段进行 6-12 个月的锁定和释放
10%团队运营，共计 1 亿个 Token。将分配给创始团队核心人员中做出努力和贡献的个人和团队，包括投资人与顾问团队在项目启动、设计、资源的组建商业环境的孵化的过程中持续投入的人力、物力、财力。
15%基金会，共计 1.5 亿个 Token。基金会主要用于生态孵化、市场推广、商业开辟、法律合规等，保持社区及整个生态环境的快速成型和后续健康、持续的发展。
5%用于糖果计划，共计 0.5 亿个 Token。主要用于整个生态用户的激励，持续维护整个生态的可持续发展。



8. DIYchain 发展路线



图 8.1 DIYchain 发展路线



时间	规划
2017 年 Q4	项目调研，了解行业痛点
2018 年 Q1	项目立项，成员搭建
2018 年 Q1-Q2	定制 DAPP-SaaS、小程序打磨并上线
2018 年 Q3	完成公链架构设计和开发
2018 年 Q4	开发交易征信体系
2019 年 Q1	开发智能支付体系
2019 年 Q2	开发交易售后仲裁体系
2019 年 Q3	开发数据开放体系
2019 年 Q4	完成公链迁移，整体平台上线
2020 年 Q1	定制 DAPP 应用上线
2020 年 Q2	持续开发，全球推广底层公链



9 DIYchain 基金会

9.1 基金会的设立

考虑到 DIYchain 国际化的定位，DIYchain 基金会(以下简称“基金会”)是一家设立在海外的 BVI 公司。基金会致力于 DIYchain 的开发建设和透明治理倡导及推动工作，促进开源生态社会的安全、和谐发展。

9.2 基金会架构

DIYchain 基金会治理架构包含了针对日常工作和特殊情况的操作流程和规则。

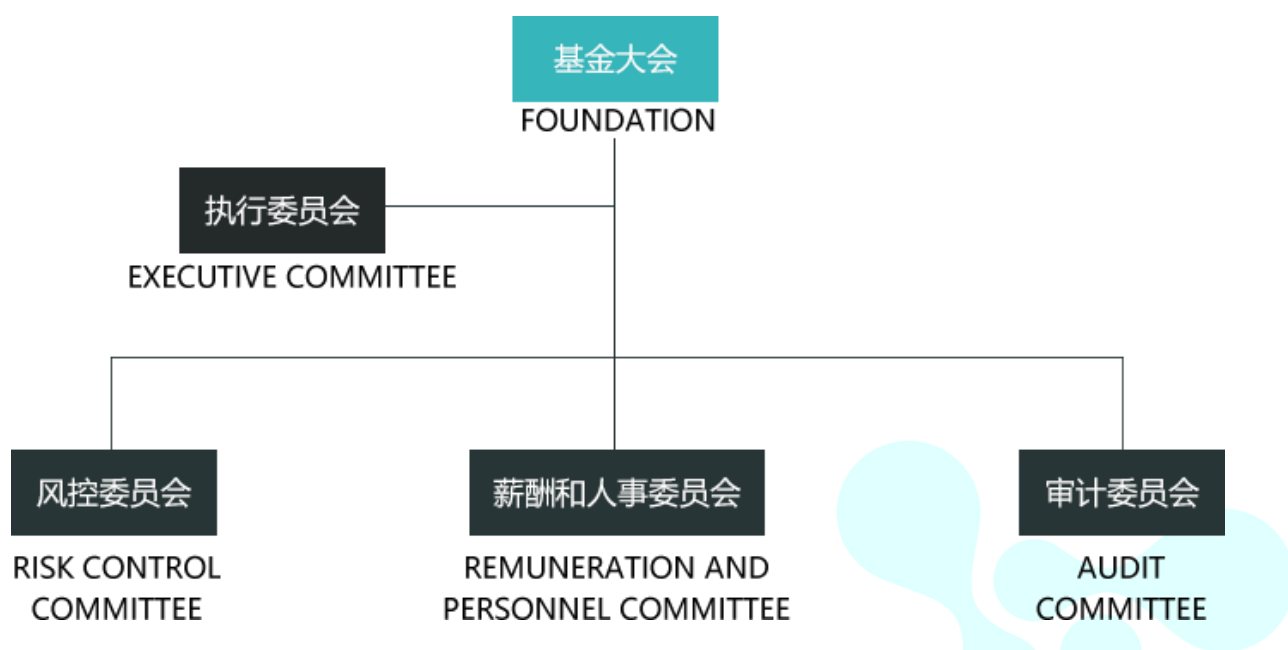


图 9.1 DIYchain 基金会治理架构

9.3 各委员会职能划分

1) 执行委员会：

研究和拟定长期规划，指定章程和管理制度，新项目可行性分析研究及批准，管理日常运营。

2) 风控委员会：

研究和制定风险控制策略，制定风控标准，审核整体运营风险，召集项目风险审核会议并组织审核结果发布。

3) 薪酬和人事委员会：

拟定和修改薪酬、激励方案，审核机构设置及岗位设置，进行人员的聘请。

4) 审计委员会：

负责运营审计、财务审计、代码审计及 TOKEN 销毁等工作。



10. DIYchain 团队介绍

10.1 团队



Chingiz

创始人兼CEO，曾就职于某研究院高级研究员，资深区块链研究员



Lance Winstein

欧美区运营负责人，曾就职于知名电商公司担任市场营销总监，2年区块链产品运营经验



Varun Kapoor

技术负责人，主要研究方向为区块链和物联网，区块链技术资深研究员，拥有6年区块链开发经验



Janyoung

项目落地负责人，拥有国家授权专利两项，荣获湖北省科技厅科技创业专项立项，在定制行业的供应链和落地方面拥有丰富的经验



Chason

亚洲区负责人，由米定制创始人，CCTV2创业榜样，武汉市创业先锋人物，从事定制电商8年，区块链研究3年

10.2 顾问



王焜

六禾创投总裁&合伙人，哈佛大学MBA、上海交大本科，曾就职于BCG、IBM、Siemens等，08年起专注PE投资，10年起专注VC投资



杜挺

技术孵化器demo++创始人，西安交通大学博士、北邮本科，Ink墨链、原本区块链早期投资人



徐刚

工信部中国软件行业协会区块链专委会特聘专家、中国区块链创业学院深圳分院副院长、区块链创业学院专家智库讲师团高级讲师、云链科技创始人、云钱包创始人



陈璧葵

六禾创投合伙人，麻省理工计算机硕士和MBA，清华本科，曾就职于甲骨文公司从事软件开发



吴桐

中央财经大学金融学博士，亚洲区块链学会荣誉顾问，国家发改委国际合作中心特约研究员，国务院发展研究中心金融所助理研究员，中央财经大学国际金融研究中心研究员



张晓俊

筹帷资本合伙人，图灵基金创始人，原天使湾创投、蓝山投资投资总监，币圈头条&币圈daily公号联合创始人，深度参与了初链、深脑链、拓扑链等知名项目

10.3 合作伙伴



11.风险提示

本项目存在以下方面的风险,请认购人注意：

11.1 合规、运营性风险

合规、运营性风险是指 DIYchain 在认筹资金以及开展业务的过程中违反了当地法律法规,造成经营无法继续的风险。

针对合规、运营性风险运营团队采取的避险方式为：

- 1) 运营团队和决策委员会采取分散式运作方式，排除单点风险；
- 2) 在开展业务的当地聘请专业律师,在法律框架下设计开放平台、数字资产发行、数字资产交易、区块链金融、区块链应用等方面业务；
- 3) 为了满足和遵守当地的法律法规，DIYchain 平台可能会在有些国际和地区无法提供正常的服务。

11.2 市场风险

市场风险是指 DIYchain 没有被市场接纳，或者没有足够用户使用，业务发展停滞，没有足够利润支撑。

针对市场风险运营团队采取的避险方式为：

- 1) 经过近一年来的市场实际运行经验,确认市场痛点客观存在；
- 2) 利用创始团队在体育、互联网及金融市场服务中积累的经验，迅速孵化平台生态并产生利润。

11.3 技术风险

技术风险是指底层技术出现重大问题，导致 DIYchain 无法实现预期功能，以及关键资料被篡改或丢失。

针对技术风险运营团队采取的避险方式为：

- 1) 基于成熟、开源、安全的区块链技术，采取已经被商业客户认可和验证过的架构开发 DIYchain 系统；
- 2) 认筹足够资源后，吸纳更多的相关行业高端人才加入开发团队，奠定基础，充实力量，借鉴成熟开发经验。

11.4 资金风险

资金风险是指项目资金出现重大损失，例如：资金被盗，资金亏损，储备金，大幅贬值等。

针对资金风险运营团队采取的避险方式为：

- 1) 储备金采取多重签名钱包+冷存储方式由决策委员会共同掌管，在 5-7 多重签名方式下，当出现 3 名董事同时不能履行职责的情况时，储备资金才会面临风险；
- 2) 运营团队常年服务于金融行业，有丰富的风控经验，流动资金在市场出现价格剧烈波动(50%以上的跌幅)时才会出现亏损可能。

12.免责声明

针对 DIYchain 项目，会成立一家设在海外的基金。该基金会将作为独立的法律主体，全权负责组织团队开发、推广和运营 DIYchain 项目，并承担所有相关责任。

DIYchain Coin 作为一种具有实际用途的虚拟产品，不是证券，也不是投机性的投资工具。

除了 DIYchain Coin 作为 DIYchain 平台官方指定的虚拟数字 Token 外，不代表任何现实世界的资产或者权利（如基金会的股份、表决权等）。

除本白皮书所明确载明的之外，DIYchain 基金会不对 DIYchain 或 DIYchain Coin 做任何的陈述或保证。该文档只用于传达资讯之用途，并不构成买卖 DIYchain Coin 的相关意见。以上资讯或分析不构成投资决策。本文档不构成任何投资建议，投资意向或教唆投资。本文档不构成也不可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。

相关意向用户明确了解 DIYchain /DIYchain Coin 的风险，认购者一旦参与认购即表示了解并接受该项目风险。

DIYchain 基金会在此明确不予承认和拒绝承担下述责任：

(1) 任何人在购买 DIYchain Coin 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；

- (2) 任何人在购买 DIYchain Coin 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求, 以及由此导致的无法使用或无法提取数字筹码 DIYchain Coin ;
- (3) 由于任何原因, DIYchain Coin 的售卖计划被放弃 ;
- (4) DIYchain 的开发失败或被放弃, 以及因此导致的无法交付或无法使用 DIYchain Coin ;
- (5) DIYchain 开发的推迟或延期, 以及因此导致的无法达成事先披露的日程 ;
- (6) DIYchain 及 DIYchain Coin 源代码的错误、瑕疵、缺陷 或其他问题 ;
- (7) DIYchain 平台、DIYchain Coin 的故障、崩溃、瘫痪、回滚或硬分叉 ;
- (8) DIYchain 公有链或 DIYchain Coin 未能实现任何特定功能或不适合任何特定用途 ;
- (9) 对 DIYchain Coin 售卖计划所得的使用 ;
- (10) 未能及时且完整的披露关于 DIYchain 开发的信息 ;
- (11) 任何参与者泄露、丢失或损毁了 DIYchain Coin 的钱包私钥 ;
- (12) 任何人对 DIYchain Coin 的交易或投机行为 ;
- (13) DIYchain Coin 在任何交易平台的上市、停牌或退市 ;
- (14) DIYchain Coin 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物, 以至于受到禁止、监管或法律限制 ;
- (15) 本白皮书披露的任何风险因素, 以及与该等风险因素有关, 因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。