BCS

商信链白皮书

BCS基金会

目录

1.市场概述

新零售，即企业以互联网为依托，通过运用大数据、人工智能等先进技术手段，对商品的生产、流通与销售过程进行升级改造，进而重塑业态结构与生态圈， 并对线上服务、线下体验以及现代物流进行深度融合的零售新模式。科技发展日新月异，以大数据、云计算、物联网、虚拟现实为代表的创新科技，在新零售领域逐渐发挥出至关重要的作用，让零售业发生翻天覆地的变化，给人们带来全所未有的消费体验。2017 年我国新零售商店交易规模达 389.4 亿元，到 2022 年将至 1.8 万亿元，复合增长率将达 115.27%，由此可见，未来五年以无人便利架、无人零售店为代表的全新零售模式正在颠覆着人们对于零售业的原有认识！

新零售的核心一定是大数据，而对大数据高效的处理离不开人工智能。人工智能将对生产、供应、配送环节中的部分人工，实现有效替代。根据高盛的预测， 到 2025 年，人工智能将为全球零售业节省 540 亿美元/年的成本开支，同时带来 410 亿美元/年的新收入。中投顾问则认为上述预测仍较为保守，未来人工智能给零售业带来的利润和收益远不止如此。以京东的客服机器人JIMI 为例，仅2017 年便为京东节省人工成本上亿元。比如，百度大数据为朝阳大悦城专门制订人工智能+大数据推广计划，改计划更有针对性、更精准的推广计划。这种个性化的推广计划在很大程度上提升了朝阳大悦城的销售量，其会员销售额提高了12%，未购买品牌推荐转化率提升了五倍，非活跃会员到场消费率提高了 53%。

进入 2018 年，人工智能加速渗透零售行业，较为成熟的落地场景主要可分为五大类：智慧的无人门店、智能仓储与物流、智能营销与体验、智能客服、智能虚拟体验。比如智能仓储，同样存在巨大市场需求 预计到 2020 年规模超 954 亿元。

2.行业痛点

2.1 新零售的经营痛点

无论是哪个行业都会面临着痛点问题，经营瓶颈问题，愁客户、愁管理，客户流失、员工流失等各种问题，新零售也不例外。目前，新零售的经营痛点如下：

2.1.1线下新零售亟需提升科技手段

相比线上巨头动辄几亿十几亿的科技技术成本，线下新零售一方面销售数据积累体量有限，另一方面缺乏互联网基因，这让其线下发展远远落后于线上。总的来说，线下新零售在技术的深度和广度上，还远远比不过线上巨头。

2.1.2线上线下面临融合问题

线上与线下零售互为优劣势，线上电商优势有两个，一是大数据，二是垄断优势。因此，整合和调动资源的能力快速集中。线下新零售却是“战国七雄”，并没有如此强大市场份额的商超，整合能力自然较弱，要想在线上发展分一杯羹难度相当大。

2.1.3降低成本是绕不过的问题

除了线下实体店，线上零售也面临着成本控制的挑战。在零售布局线下门店方面，线上是通过在线交互体验，而线下则需要大量的离线操作，pos 机和计算体系等数据保持同步的话，对整个系统和架构对刚起步的新零售也是个不小的挑战。

2.1.4配送及库存问题

传统零售只支持上门购买，缺乏配送。而新零售需要接受线上订单，线下配送的要求。这就需要很好的进行商品进销库存管理，随着规模的扩大，需要进行大数据的最优匹配，否则将面临巨大的成本压力。

2.1.5中心化管理的困扰

新零售销售产品，与客户只有表面上的供求关系，无法真正将客户成为企业内在的资源，一旦市场变化或客户自身观点转移，则容易失去客户。互联网时代下的销售方式，销售场景呈现越来越多样化，消费者从被动的接受，变成了主动寻求，主动选择，主动

购买。伴随移动互联网的发展，去中心化应该是新零售的趋势，正如微信想要构建的体系——每个人都是一个中心节点，既是生产者也是消费者。

2.2 新零售的信用痛点

新零售体系的运转，离不开信用的支撑。征信作为信用体系中的关键环节， 奠定了新零售信用风险管理的基础。大数据时代来临，互联网金融兴起，面临新形势，传统征信业中信用信息不对称、数据采集渠道受限、数据隐私保护不力的问题愈加严峻。截止到 2016 年 6 月底，央行征信中心收录 2120 万户企业及其他组织与超过 9 亿自然人，其中仅 577 万户与 4.1 亿自然人有信贷记录。而全球征信巨头美国 Experian 的数据已覆盖全球 1.03 亿户企业和 8.9 亿人。对比美国的市场需求及征信市场规模，我国征信市场还存在诸多漏洞。

大数据时代下的新零售对隐私保护和数据安全的要求更高。央行对下发个人征信牌照非常谨慎，说明监管机构对于正式放开个人征信领域还存在疑虑，隐私信息保护、个人信用评价指标不统一等问题仍是央行最主要的担忧。此外，“暗网”中的个人信息交易灰色产业链，以其多样性、隐蔽性与复杂性成为监管部门查处的痛点与难点。为此，中国人民银行征信管理局明确指示要加强隐私保护， 要求征信机构采集使用用户信息应当经信息主体同意，并明确告知可能产生的影响等事项，信息主体有权要求征信机构将其纳入拒绝用于营销的范围内。然而， 传统征信系统技术架构对用户的关注度较低，并没有从技术底层保证用户的数据主权，难以达到数据隐私保护的新要求。

2.3区块链重新定义新零售

零售业市场鱼龙混杂，假货横行，花大价钱买假货的新闻更是屡见不鲜。而新零售以互联网为依托，这个过程更加容易导致产品质量参差不齐。区块链是使用分布式账本、通过去中心化计算机网络记录交易的技术，其去中心化、不可篡改的特点让该技术在新零售业能得到很好的应用。区块链技术运用到新零售行业后，真正实现了商家、消费者、监管部门之间的信任共享，全面提升效率、体验、监管和供应链整体收益。区块链在一定程度上重新定义新零售的整个销售模式。

如何在新零售中应用区块链？

首先，利用区块链技术将不同商品流通的参与主体的供应链和区块链存储系统相连接。其中包括原产地、生产商、渠道商、零售商、品牌商和消费者。使每一个参与者信息在区块链的系统中可查可看。

最后，零售行业天然具有交易数据碎片化、交易节点多样化、交易网络复杂化的显著特点，商品生产、流通、交付等信息的采集、存储和整合是端到端的零售供应链管理的核心命题。而全流程信息的可信、可靠、可查、安全性又是消费者、监管部门和电商商城最为关心的。

区块链技术具有整合多个交易主体的共识机制、分布式数据存储、点对点传输和加密算法等多项基础技术，天然适用于零售供应链的端到端信息管理。为消费者保驾护航。

3.解决方案

3.1 商信链介绍

商信链（简称 BCS）构建基于区块链的新零售商业信用经济生态；

通过区块链技术，打造成一个供应链可追溯、信用可量化，数据公开透明， 集消费购物，会员服务，精准营销，集中采购等场景于一体，形成线上电商交易、线下购物体验，构建多方参与、多方受益的新零售生态。商信链的整体架构如下：

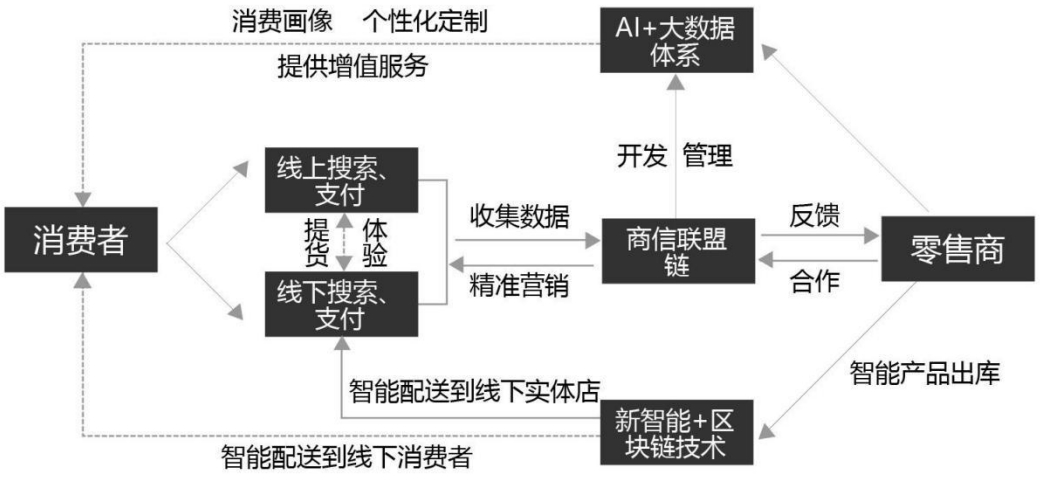


图 3.1-商信链平台架构逻辑

3.2 新零售痛点的解决方案

运用区块链重塑新零售体系，降低成本

商信链将全面启动零售溯源计划，利用区块链技术、物联网技术以及大数据跟踪零售商品全链路，汇集生产、运输、通关、报检、第三方检验等信息，给每个商品打上“身份证”，将商品信息完整地展现在用户面前，提升用户购物体验， 加强平台正品心智。

运用区块链技术，建立零售信任

区块链以分布式存储、点对点传输、共识机制与加密算法等技术，屏蔽了底层复杂的连接建立机制，通过上层的对等直联，加强用户数据的隐私保护，以低成本建立共识信任，以新模式激发行业新业态、新动力。具体表现为以下几点：

去中心化：中介化的信任系统自身保证其真实性，不需要外在信任背书主体介入，安全性高。

开放：系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人

公开，信息透明。

自治：任何人为的干预不起作用，减少外来的逆向干预。

信息不可篡改：通过记录钱包行为获得不可篡改的全面信息数据包，从而决定了交易的公开透明和不可篡改性。

匿名：交易对手无须通过公开身份的方式让对方自己产生信任，对信用的累积非常有帮助。

企业通过提取数据包建立属于自己的可视化信用分值系统，管理企业内部及用户。

建立智能信用量化平台，打破商业数据孤岛现象

通过人工智能+数据共享+云计算，打破各个网点间的数据孤岛，加快各行业信用数据的汇聚沉淀。

打造大数据体系

大数据系统的深入运用是商信链的最大特点，也是商信链与其他类似共有链的重要区别。有了大数据系统，从客户注册起，系统将关注客户的性别、年龄、职业、消费习

惯、产品及品牌喜好、消费周期及时间，通过对每个客户的深入分析，可获知客户需求，甚至店铺所在区域周边的消费力和消费习惯，在出现经营问题时，即可分析原因所在并作出调整。

3.3 应用场景介绍

商信链的应用运用场景如下：

图 3.2-业务运用场景

新零售：产品供应链溯源，库存管理，智能商业，用户价值管理，数据资源全景整合。

个人信用体系：个人可以从身份属性，信用记录，履约能力，行为特质，日常生活状态,社交影响等方面得到量化分析，建立个人信用资料,判断个人是否有信用风险。

商业信用体系：从品牌估值，品牌管理，企业互信，智能生态价值交互出发， 形成财务信用报告，深度信用报告，客户群体信用风险分析报告，客户信用监控报告，定制信用报告，风险管理解决方案，商账管理与催收等多种报告形式。主要为企业提供全面，准确的征信报告，完善客户群及数据库的管理。

3.4 应用场景实例

（1）支付交易

线上支付：线上商城系统中全线产品、各应用板块，均使用 BCS Token完成支付，包括：零售商城、招商入驻、娱乐版块、生活缴费等类美团的线上支付；

线下支付： BCS Token可用于线下新零售体系的支付。

（2）信用评定

根据多维度，对 BCS Token用户建立信用体系，通过信用评定，可以申请贷款，可以获得更多 BCS Token持有量，可以获得更多佣金收入，可以享有更多权益。

4.应用框架

4.1 新智能新零售

4.1.1产品供应链溯源

商信链的溯源和防伪体系充分发挥了物联网和区块链技术各自的优势，实现了技术上的优势互补。物联网可以收集零售商品的原产地、生产公司信息以及仓储、物流、交易等各环节的信息，确保原始数据的真实性。而区块链的分布式存储结构可保证了数据的可溯源及防篡改特性。采用这样的模型，既可为消费者了解商品的真实性提供便利，也可避免传统信息追溯过程中存在的信息层级对产品信息真实性和完整性的影响。

4.1.2溯源和防伪流程

零售商品在出厂时，商信链的账本将进行记录。首次记录将包括零售商品的原产公司、生产日期、质量情况。若在零售商品分销商 B 还未向供应商 A 下单时，该零售商品存储在仓库入库信息应记录在区块中。当分销商 B 下单后，供应商 A 将产品出库的时间同样需要记录在区块中。

此外，在零售商品供应商 A 至仓库 F 的所有信息均需填至区块链账本中， 且不可更改。在运至仓库 F 中时，零售商品分销商 A 应该将零售商品的入库时间以及货位信息记录至区块链账本中，如图 4.1 所示。

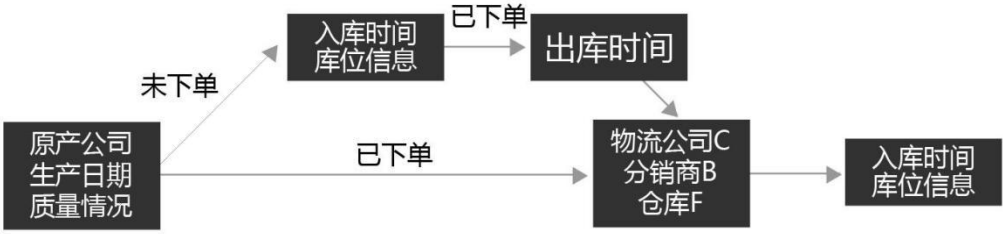


图 4.1-零售商品产品入库

区块链的每个节点负责将每两个交易节点之间进行的零售商品交易信息找到工作量证明并验证，保证这些交易信息在绝大部分的认证节点中保持最终一致性并达成共识，最终确认正确之后保存到区块链当中。因此，只有当下一个客户零售商品订单信息数据到来时，才能刺激智能合约继续解锁区块链，进行下一步区块账本数据记录。

消费者 E 通过商信链电商平台向分销商 B 购买零售商品。此时零售商品从仓库 F 中出库，则在区块上相应的记录出库时间。在物流公司 D 装车时，在区块中应该详细的记录下物流公司信息以及相应的消费者个人零售商品取件信息 如地址、电话等。由于分销商 B 和消费者 E 之间通常是在商信链电商平台中进行交易，为了保证消费者 E 的零售商品取件信息不被外人识别而使零售商品丢失， 商信链电商平台将植入区块链相应的非对称加密算法技术。

4.1.3溯源和防伪框架

商信链的零售商品信息可追溯和防伪包括以下几个部分

零售商品商家入驻及零售商品产品信息收集。商信链将诚邀全球各大零售商品商家入驻，并构筑零售商品产品跟踪物联网，由物联网通过状态传感器及射频识别（RFID）设备将零售商品的原产地、生产公司、运输信息收集起来，并存储到区块链系统中，进入区块链系统的零售商品产品数据具有安全、可靠、防篡改且可以进行数据追溯，能够确保零售商品产品信息真实可靠地输入产品追溯和防伪系统。

零售商品信息可追溯和防伪。商信链可以实现对多种类多零售商品供应链环节的信息整合，充分发挥自身拥有海量数据、供应链丰富、基础设施完善、活跃用户数量大等优势，实现对国家、多原产地、多企业的零售商品产品信息的追溯和防伪。

监管机制。提高消费者和生产者道德与法律素养、加强市场监管、明确交易过程各环节市场监管主体，也是零售商品产品信息追溯和防伪的重要影响因素。消费及交易。

消费者通过登录商信链电商平台账户，查询所购买零售商品产品的信息并验证产品真伪，选择合适自己的零售商品进行交易。

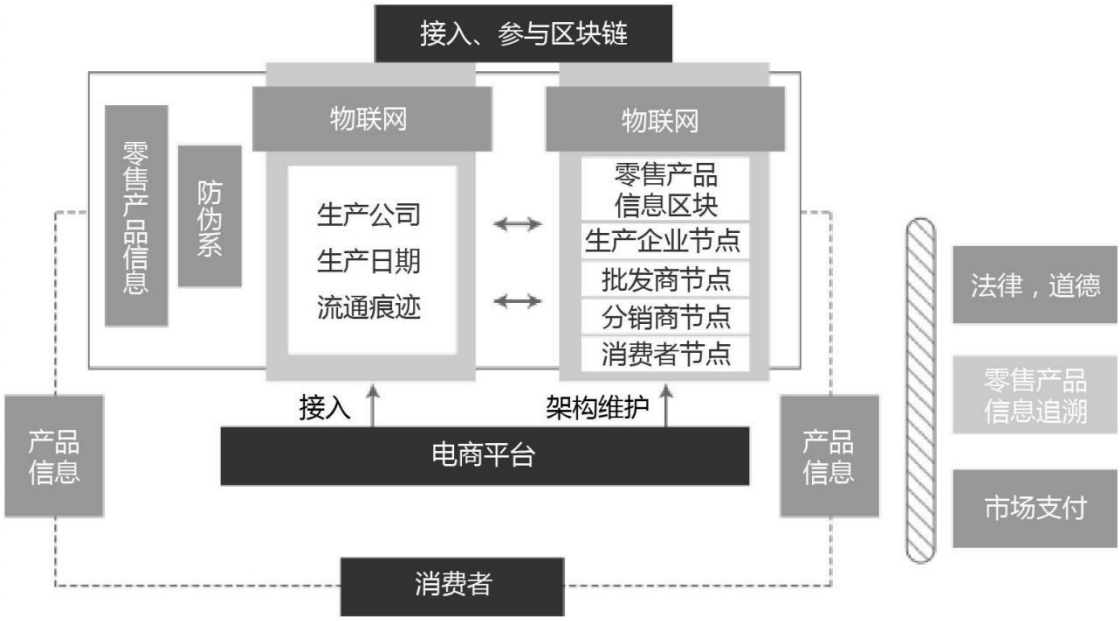


图 4.2-零售信息追溯和防伪

4.1.4库存管理

商信链采用智慧仓储的技术来进行库存管理，是利用 RFID 射频识别、网络通信、信息系统应用等信息化技术及先进的管理方法，实现入库、出库、盘库、移库管理的信息自动抓取、自动识别、自动预警及智能管理功能，以降低仓储成本、提高仓储效率、提升仓储智慧管理能力。同时，运用大数据、机器人、可实现自动预测、采购、补货、分仓，根据客户需求调整库存、精准发货，从而实现对海量零售商品库存的自动化、精准化管理。

商信链摒弃货物出入库逐条扫描条码，而是通过感应式读取信息通过科学的编码，还可方便地对库存货物的批次、保质期等进行管理。具有以下特点：

自动仓储系统利用无人搬运车系统、自动存取臂与条形码扫描设备。

感应式读取信息，最大距离可达 10M 进入库房自动读取数据，最多可 1700 件货物同时出入库，3 秒完成。

基于 RFID 物联技术，定制仓库管理系统 WSA，实时 3D 显示货物在仓数量、库位

以及商品状态，可以及时掌握所有库存货物当前所在位置，有利于提高仓库管理的工作效率。

轻松理货：智能仓储管理系统能快速查询库位上货物信息 ，快速提交理货动作，轻松解决理货难题。

4.1.5智能商业

商信链的智能商业将基于大数据分析，通过四类主要指标衡量商业的真正价值：一、财务类分析；二、顾客分析；三、企业内部运营分析。

财务分析：标准财务报告分析、收入分析、利润分析、预算分析、EVA 分析、杜邦分析、审计分析、财务风险预警分析等。

顾客分析：售后服务分析、客户满意度分析、市场占有率分析等。

企业内部运营分析

生产分析主题：生产质量管理分析、生产流程环节分析。

成本分析：基于作业成本法的产品成本分析、产品盈利能力分析、产品成本构成分析等。

销售分析主题：收入分析、渠道分析、区域分析、销售人员绩效分析、销售费用分析等。

4.1.6用户价值管理

在营销体系中，客户才是一个企业盈利和发展的重要资源，想客户所想正是利润翻倍的万灵丹。商信链凭借自身大数据系统，掌握地区消费需求和客户数据， 整个市场都牢牢掌握在手中。通过对客户喜好分析，结合整个市场的变化和趋势， 能精准获知客户未来的消费需求，补货变得准确无误，同时也能为客户推荐最适合的产品，培养客户消费习惯和增加消费粘性。

商信链细分存量用户后，需根据细分用户明显的性格特征和消费等层次，得出质量不同的黏性用户，结合销售的实际情况，制定出短、中、长期营销策略。对于低黏性的用户，制定优化用户消费结构的策略，提升用户实质性的可消费物质，包括实物性和非实物性物质。同时，配合用户特点，捕捉控制营销时间点及营销氛围,将用户保有为中黏性用户。

对于中黏性用户，积极培养用户消费习惯，主要从线上内容营销如互联网内容营销和线下战略合作伙伴营销如保险、银行、零售等，各方面入手绑定用户消费习惯，让战略合作伙伴开展利好营销，最终得到高黏性用户

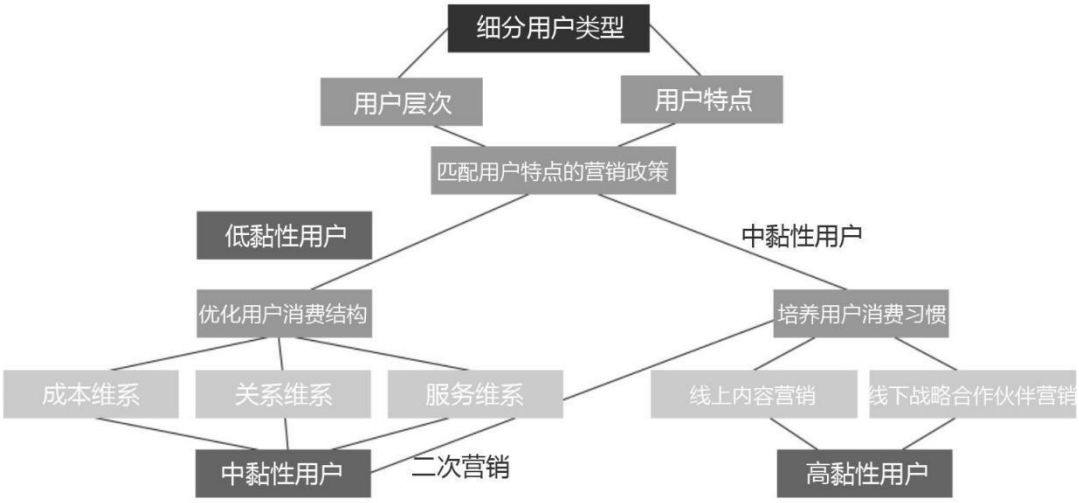


图 4.3-用户维系操作

4.2 AI+大数据体系

全球超过一半的受访企业中，业务主管主要将数据洞察用于同客户建立更强大的关系：其中有 31%的企业努力通过使用数据和分析技术提高赢得客户的能力，而其他 22%则注重客户体验的改进。大数据负责采集与分析消费者行为信息，为企业反向定制、零售商精准营销提供基础支持；物联网形成线下网点、线下与线上网点间的快速联动协作，促成生产端、销售端及物流端的无缝对联与接续驳运。而这些技术始终围绕一个核心：人工智能（AI）---以“智能化”贯穿所有技术，所有技术以实现并服务“智能化”为终极目标，并合力助推新零售目标实现。

商信链的“AI+大数据体系+”是商信链面向各行业开发大数据的平台，包括数据融合、洞察用户、智能模型和匹配能力，同时基于数据融合对群体用户进行立体画像描绘，对线上线下用户行为分析，对从“多屏”到“跨屏”的用户进行识别。

商信链有决策模型、推荐模型和绿色模型，此外，还开发了七大服务模块， 包括了

行业洞察、营销决策、社交舆情分析、客群分析、店铺分析、推荐引擎以及数据加油站。

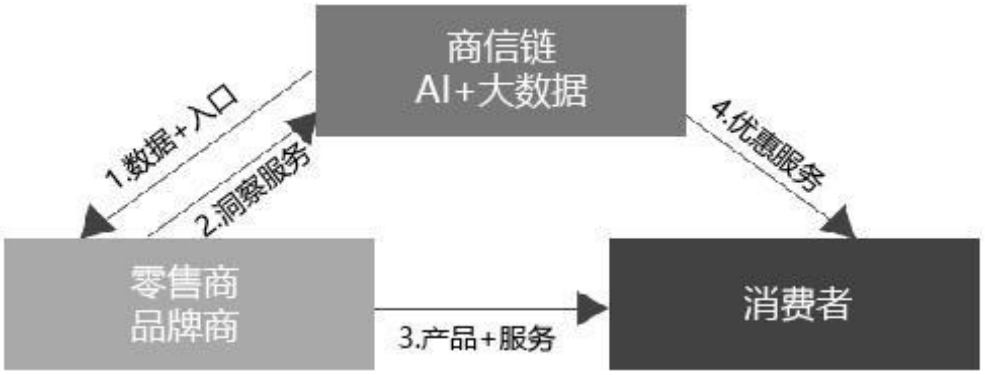


图 4.4-AI+大数据运营流程

4.3 全面信用评分系统

商信链使用 AI 学习算法和大数据相关技术，创新地对企业和个人进行全方位信用评级。

4.3.1企业信用系统

在企业信用系统，通过风险模型识别欺诈风险和信用风险，把诚信制度转化为可量化的指标，包括以下几大指标：

企业主征信信息。主要是指征信局所提供的企业主的信用资料，包括企业主的个人信用评分、企业主发生逾期的账户比例、负债信息、还款行为等。

企业征信信息。主要是指从企业征信局所获得的信息，例如企业的付款记录和付款

指数、营运状况及企业家族关系等。

企业财务信息。主要是指企业财务报表中的信息，包括资产负债表、损益表和现金流量表。

交易账户信息。主要是指企业在银行资产类账户中的交易行为数据信息，如存款、业主的储蓄账户等。具体包括企业与银行建立起账户的时间长度、上下游企业的现金流支付状况等。

客户关系。主要包括客户对产品质量的整体评分、客户的投诉率、差评率等等。

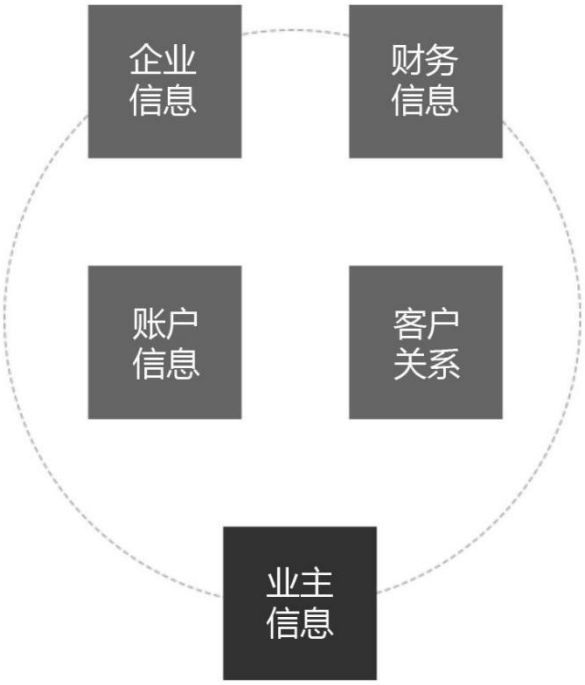


图 4.5-企业信用系统

商信链将企业信用划分成 4 个级别，A 级诚信企业，可以享受服务优先、贷款优先、产品推荐优先、营销合作优先等等。

4.3.2个人企业信用系统

商信链将传统建模与大数据建模结合起来，对个人信用信息进行评分，并且从不同维度的数据进行融合和分析，形成综合性的个人信用报告。信用评分主要包括市民的资历、工作单位、银行贷款记录、社保记录、手机欠费、水电费欠费等 40 多个要点，其中还款、信用卡透支还款等金融信用信息对评分的高低影响举足轻重。

信用评分标准从 320 分到 800 分, 共分为从 A 到 F 的 6 个等级, 每 80 分为一级，A 级信用等级最高为 720-800 分，属于信用优良，银行对 A 级的市民可

以放心贷款，分数递减，信用等级降低。F 级为 320-400 分, 等级最低，表示此类人几乎 100 %会违约。

商信链通过自主的信用评分系统，推出了个人征信画像报告，圈定一群 A 级信用人群，将这些人群的线上线下数据融合，为客户本人及零售商提供个性化的消费服务。

5.技术说明

5.1 技术基础架构

商信链的技术基础架构可以简单的分为三个层次：用户服务层（简称用户层）、网络层、储存层，它们相互独立但又不可分割。如图：

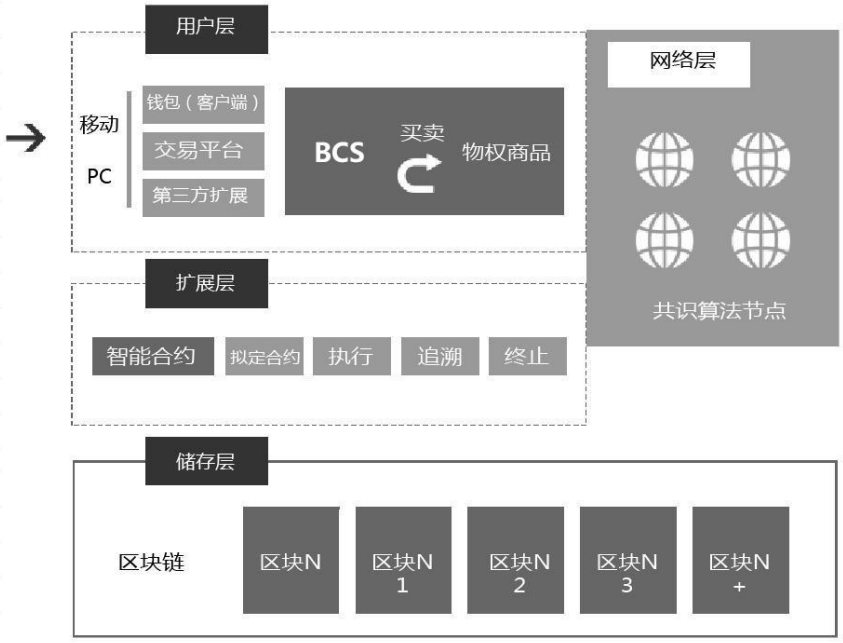


图 5.1-商信链的区块链架构

5.2 用户服务层

5.2.1账户

每个在商信链进行交易的客户都可以获得自己专门的账户，注册完账号之后需要进行一个身份的认证。商信链允许交易者存储、交易和提取超过国际上主流的 7 种法币，或者是将主流的 20 多种数字货币（比如比特币、莱特币）兑换成商信链Token。用户可以将商信链Token存入自己的账户，然后在商信链上的电商平台进行买卖支付。

5.2.2钱包

区块链钱包是存储加密币的软件程序，商信链每个注册用户都拥有者有一个私人密

钥（秘密号码）通往他们的钱包。 此密钥是访问他们数字货币地址的唯一途径，因此也是接收或发送信用的唯一方式。 在钱包中，用户保留他们的数字货币资产，数字货币就是一个平常钱包里“普通”的钱。 但是，用户不会把他们所有的钱放进一个钱包，因为不会觉得它非常安全。在这种情况下，用户需要使用备份副本和安全密码。 此外，用户可以将钱包视为一个存折（纸钱包）。这没有互联网接入，因此，它不更容易受到网络黑客的攻击。

管理数字资产的本质是管理私钥，而这一直是用户的一大痛点，一旦私钥丢失，几乎没有任何机会恢复，因此大部分用户会选择将资产托管在交易所，但这又面临资产被盗和平台跑路的风险，与去中心化的原意相悖。商信链希望为用户打造一个去中心化的数字货币存储管理系统，将私钥加密存储于本地，同时通过备份防丢、离线签名等方式提高资产安全性。具体手段包括：

第一是采取“冷钱包”机制，冷钱包是将私钥放在离线的手机里，通过离线签名配对的方式来做交易授权，别的应用程序无法读取。

第二是在私钥基础上让用户再次设定密码，通过几十万次哈希函数运算生成一个更强的密码，来加密明文私钥使其变成密文，再存入文件系统里，每次取用时候需要用户授权，输入密码解开私钥，再去做交易签名，当不使用时是密文状态，增加了私钥和资产的安全性。

5.2.3隐私保护

为了解决信息不对等、各种虚假等问题，无论是产品交易卖方还是买方（消费者），在使用商信链之前都必须进行 KYC 的认证。商信链将通过非对称加密技术将身份信息加密并保存到商信链系统中。以确保链上信息有效、真实和安全。商信链的具体应用原理如下所示：商信链上每一个环节的用户都需要在系统上进行注册，注册后的用户就拥有了独一无二的用以证明身份真实信息的私匙。每一个拥有私匙的用户都可以在区块链上记载信息，也可以在权限内查看信息.

商信链平台隐私保护的机制如下： 公钥与私钥的产生

用户首先要通过 SHA256（Security Hash）算法，将密文生成 256bit 的私钥。HASH 函数使用时， Data 长度改变，hash 值长度不变；每个 Data 字符对应于唯一一个 hash 值，它可以作为数据指纹来使用。

将此私钥用椭圆加密算法，生成公钥，这个公钥可以让大家都知道。每个人都可以

通过这个公钥，通过 HASH 函数得到用户的地址。

由于 HASH 函数的单向性，即：Hash(x) =y，通过 y 很难找到 x。如果想通过地址破解公钥，或者通过公钥破解用户的私钥，几乎不可能。

加密与解密

加密：如果某人（如用户）想加密数据，则使用公钥将其加密。解密：解密时需要用私钥，这个只有用户自己知道。

图 5.2-加密及解密

5.3 储存层

在商信链的储存层中，主要是实现交易数据存储记录的发布、保存和共享， 实现如下 3 个主要功能。

5.3.1数据存储发布

用户在商信链进行交易时，将产生交易数据存储(M) 。数据存储产生后， 商信链会为数据存储生成哈希，并将数据存储记录的摘要(Di-gest) 、哈希用发行方的私钥(sk isser) 签名后发布到商信链上。同时将数据存储记录用对称密钥(k) 加密，并将加密密钥用用户的公钥(pk patient) 加密后一起发送给用户， 具体过程如算法 1 描述。

算法 1：数据存储记录发布Procedure Issuing(M) Input: M

Output: 数据存储记录交易Begin

数据存储数据发行方产生一个数据存储记录 M；

生成需要保存在商信链的数据 {Digest；H(M)；Sig(Digest|H(M))}并创建数据存储交易广播到网络；

将原始记录和其哈希值签名后用对称密钥加密，将加密密钥用用户的公钥加密，形成消息{ Enck(Digest| M | H(M) |Sig(Digest| M | H(M))；Enc(k)} 后一起发送给用户；

end

5.3.2数据存储记录

商信链收到用户的交易数据后，将生成新的加密密钥，将数据存储及其签名加密存放到云存储中保存，具体过程如算法 2 描述。

算法 2：数据存储Procedure Storing(M)

Input: 加密的数据存储记录{Enck(Digest|M|H(M)|Sig(Di-gest|MH(M)))； Enc(k) }

Output: 数据存储位置Begin

用户用自己的私钥从 Enc(k) 中解密出对称密钥 k；

用对称密钥 k 解密出 Digest、M、H(M) 、Sig(Digest| M| H(M)) ； 根据公钥验证签名的正确性；

if 签名正确

根据 M 计算其哈希值并和 H(M) 比较；

if 哈希一致

数据存储记录数据真实； else

简单丢弃处理

end

else

简单丢弃处理；

end

if 验证数据真实

将是数据记录及其签名重新加密存储在云存储中，并记录下加密密钥和存储位置；

end

end .

5.3.3数据存储记录共享

商信链将所有交易记录进行数据共享，会将共享记录在云存储中的位置、使用权限、使用期限、公钥机密的解密密钥一起写入到区块链中。用户可以通过查询来读取商信链上共享的数据。具体过程如算法 3 描述。

算法 3：数据存储记录共享Procedure Sharing(M)

Input: 请求商信链的公钥和所需的数据存储记录

Output: 生成一个访问控制交易

begin

接收数据请求方请求，提取出请求方公钥和数据需求；根据请求方的数据需求，找相关数据存储记录在云存储中的位置 URI 和响应的加密密钥 k；

创建一个访问控制交易，并将响应的信息写入到交易中{URI；permission； pko；

expiration；Sig(URI；permission；pko)；Epko(k)}

向商信链网络广播该交易；

end .

5.4 共识机制

一个成熟的区块链系统，需要具备以下几个方面的特征。

信用体系

比起区块链和数字货币，在实体世界中已经有一套成熟的信用体系来支撑金融体系的运行。BCS希望引入现实世界的信用体系，来为匿名的区块链网络提供更好的运营和支撑。

TPS

TPS指的是系统吞度量，也是每秒系统处理的数量。假如TPS每秒并发太低，很容易造成网络拥堵严重，从而使得区块链在高价值的高并发业务领域无法落地。比如，由于TPS每秒并发太低，比特币和以太坊都存在交易费用高、确认时间长、扩展性差的问题。当前的公链虽然可以存储价值，但过低的TPS无法支撑真实落地应用的需求。除非区块链达到百万级用户的支持，否则无法出现有价值的依附应用。

迁移成本

因为区块链的数据存储方式是链式块结构的，单个的应用难以迁移以及成本过高也成为限制。有研究表明，一个以太坊智能合约的迁移成本大约是每个地址0.025USD。以30万用户BNB token 为例，单次的迁移成本大约为7500USD。而且，这只是账户金额信息的迁移，如果想迁移其他信息，成本可能更高。这对于DAPP的开发者来说，是一笔巨大的开销。

免费使用

用户不应该因为使用平台的功能而支付费用，免费/收费的策略应该是由应用开发者制定。同时，区块链平台的应该激励应用开发者免费自己的应用。比特币和以太坊未使用免费交易的主要原因是为了防止打包进无意义的或者没有真实价值的交易。EOS虽然交易免费，但设计了RAM，NET，CPU来阻止无意义的交易。

对于交易费的问题，有以下两个安全方面的问题：

节点激励来保证网络安全。对于节点奖励，BCS采用永久奖励的方式为记账节点提供激励。

防止DDOS攻击是主流数字货币未提供免费交易的主要原因。大量的交易发起一方面需要提供大量的基础手续费，在造成系统拥堵的情况下，还会大幅度推高基础手续费，这就形成一种负反馈，一定程度上保障网络的安全运行。BCS希望引入一种后结算的方式来阻止无意义交易的发生。具体策略是用户在交易的时候，需要按BC评分支付

一定数量的保证金来确保交易被正常处理。在固定数量区块被打包之后，这部分保证金会被释放出来。

延时（确认）和未打包

比特币和以太坊的PoW共识有极大的延时和未打包的风险，这给用户和应用开发造成了极大的风险。

智能合约

智能合约是区块链2.0得以快速发展的主要原因。通过智能合约，区块链应用开发者不需要发行公链平台就可以使用区块链来存储数据，执行合同逻辑。但是，也需要认识到，智能合约不是一种语言，而是一个体系，重新开发一个新的智能合约运行环境是没有必要的。会产生一系列的问题，比如难以搭建生态，资源浪费。EVM是当前最有完备生态和社区支持的智能合约体系。

在以上需求的基础上，BCS团队提出了POBC共识算法。POBC的核心共识基础就是商业信誉，这包括三个方面，身份，声明和身誉 。

身份是系统内最基础的角色。身份可以用来证明自己和他人曾发生过一些事，我们把这些事称作声明。随着时间推演，声誉会随着身份体系建立起来。

身份、声明，和声誉的协议，应该通过适当的接口相互交互。这个系统必须是模块化且可扩展的，同时具备以下特性：

去中心化（Decentralization）：协议规则应该由网络参与者制定和遵守，而不是由中心化权力机构执行。

自治（Self-sovereignty）：用户自行掌控属于自己的身份、声明，和声誉。这与 Web 2 网络形成巨大的反差；在 Web 2 网络中，比如在亚马逊；一个商家的产品积累的声誉，可能会因为亚马逊破产或单方面决定，而被移除。

可移植性 & 互操作性（Portability & interoperability）：系统不该扣留用户，而应该允许用户往其他系统上迁移属于自己的数据。

抗女巫攻击（Sybil resistance）：设计协议时，必须考虑参与者不能通过发布多个身份获得优势；除此之外，协议中旧身份更换成新身份没有好处。

隐私（Privacy）：参与者应该能选择性地与他人共享数据。此外，默认情况下参与者的身份能通过不公开的标识进行验证。

POBC将采用类似DPOS的轮流记账权算法，但需要记账权竞争机制，期望可以达到2秒钟/块的出块速度，并且计划在未来的版本中，将出块速度提高到500毫秒。

通过BC评分，BCS将选出30个超级节点，来分割每分钟的记账权利。BCS将通过一套竞争方法来允许记账权利在记账节点间的竞争，主要评价协议来决定竞争的结果。

这种良性的竞争将提高BCS记账节点的公信力和财力，也可以为BCS Token市场提供一个良性的流动性市场。我们设想，未来会有一个提供固定BCS Token权益租借利

率的流动性市场，来服务于记账权利的竞争。同时，公平的记账权利，也防止了矿池走向集中化。

5.5 特有技术描述

安全加密算法

加密技术主要应用在数字资产交易过程中, 对交易信息的签名进行加密处理。传统数字资产交易方法通常采用对称加密技术, 对称加密技术要求加密和解密过程使用相同的密钥, 该加密技术基于双方共同保证密钥的安全而实现的。

而商信链采用非对加密技术,加密和解密过程中使用不同的密钥，适用于互不信任的双方安全的完成交易过程。商信链提出的数字资产安全交易方法中, 采用双HA256 哈希函数与RSA 加密算法结合使用, 验证交易信息真伪性，防篡改。该方法中借鉴比特币区块链系统的双 SHA256 哈希函数, 将原始数据经过两次

SHA256 哈希运算后转换为长度为 256 位(32 字节) 的二进制数字。哈希算法因其不可逆性, 适用于验证机制。而 RSA 加密算法属于非对称加密技术, 非对称加密技术相比与对称加密技术, 加密与解密过程用的是不同的密钥, 分别为公开密钥和私有密钥。公开密钥和私有密钥相互配合，如果用户 A 使用它的公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用其对应的公开密钥才

能解密。公开密钥可以向其他人公开, 私有密钥则不公开，并且私有密钥无法通过公有密钥推算出来, 保证传输数据的安全性和完整性。

RSA 加密算法生成公私钥流程如下图所示。

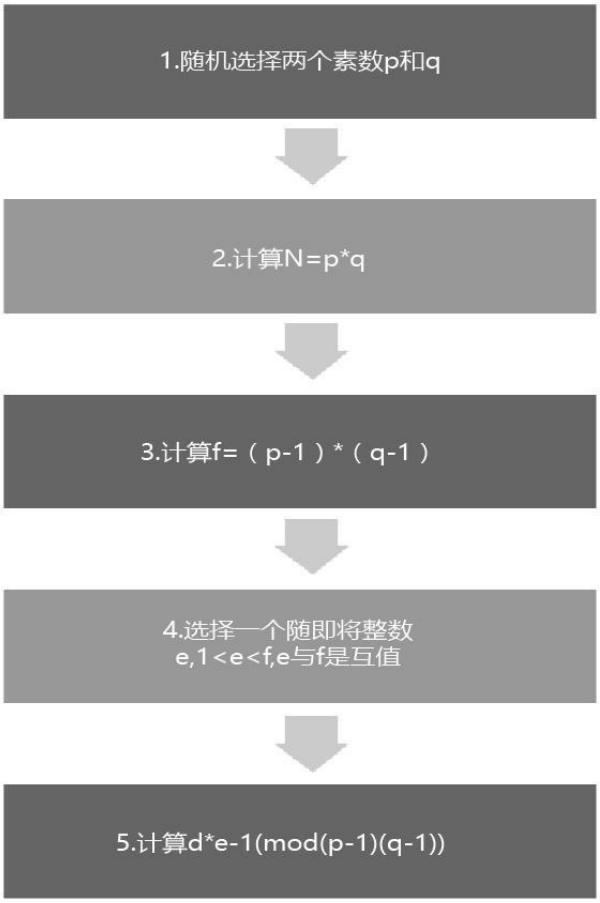


图 5.4-RSA 生成公私钥流程图

在实际应用中, 交易发送者 A 发起一笔新的交易，例如转一张价值 5 个比特币的数字资产给用户 B, 此时调用 SHA256 哈希算法对报文进行签名, 得到Hash 后的一段摘要。RSA 非对称加密算法生成一对公有密钥和私有密钥。使用公有密钥对签名加密, 发送方将 RSA 加密后的签名、报文一起发送给接收方。接收方使用发送方的公钥对签名解密，还原出一个哈希值。查看该哈希值与报文经过 SHA256 哈希算法处理得到的结果是否一致，验证消息是否来自发送者以及信息是否被篡改。

具体流程如下图所示：

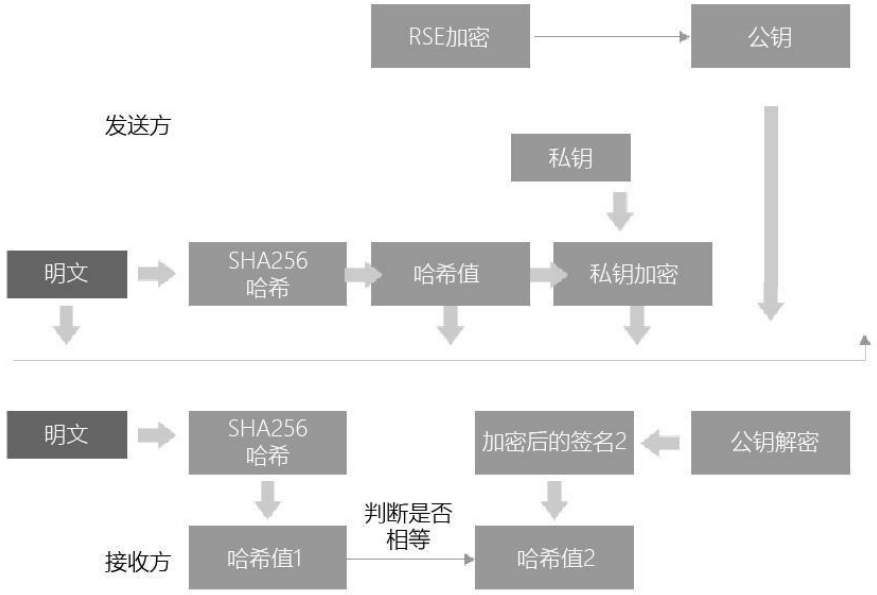


图 5.5-交易信息加密与验证过程

5.5.1智能合约协议

商信链通过“智能合约”规定着各方对承诺执行，可以实现零售买卖和交易的透明，同时合同可以让资金自动支付给卖者或其他利益相关者。

商信链合约式交易流程如下：

1，合约拟定。这部分是由零售卖方来进行合约拟定，将自己所要出售的零售商品写到智能合约中形成合约制代码，然后买者查看原生条例，进而在协商共识后存储到区块链的过程。商信链的区块链未来计划支持多种语言来编写智能合约。

2，合约触发。合约触发是在合约存储之后，通过商信链的外部条件来触发合约执行的过程，支持定时触发、事件触发、交易触发和其他合约触发的方式。定时触发是指满足合约中预设的交付时间之后，节点就触发时间共识之后，自动触发合约调用的过程。触发事件、交易和其他合约调用都是一次新的请求共识过程中触发合约执行。

3，合约执行。合约执行是合约代码在独立的环境中运行的完整过程，包括对合约构造镜像环境、代码执行、执行代码中状态修改的共识以及共识的异常处理。

4，合约注销。合约注销，是对已经执行过、过期作废或者业务需求变更不再需要的结算合约进行转存清理。而清理的过程需要多节点共识之后才能完成。

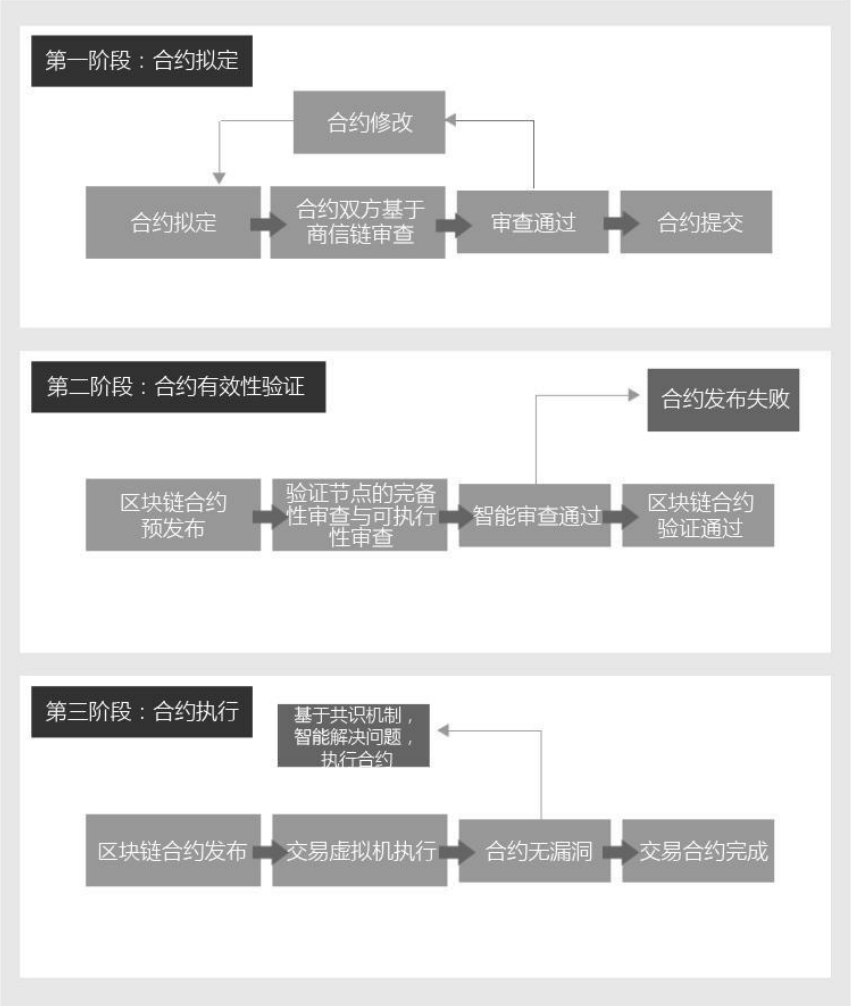


图 5.6-智能合约注册、触发、执行和注销环节

5.5.2溯源和防伪算法

算法 1.溯源数据存储

输入: 某零售商品产品的生成 P 以及各溯源部门的溯源信息 M1 ，

M2，...Mn 。私有链及公有链中没有该零售商品产品的信息。

输出: 对于每一件零售商品产品, 私有链存储该产品的生产 P 及各部门的溯源信息 Mi, 各部门的签名 Sig(i)，以及这些信息的哈希值 H(Mi，Sig(i)), 公有链存储上述信息的哈希值 H(H(M1，Sig(1))，H(M2，Sig(2))，...)。每一件零售商品产品其详细信息在私有链中的位置会存储到一个链接 Lpr 中, HPR=H(H(M1，Sig(1))，H(M2，Sig(2))，...)在公有链中的位置将会存储到另一个链接 Lpu 中。

过程 1.存储溯源数据

```
BEGIN
Pl.generrate(P);
 Sig(pl)=Pl.sign(P);
hP=H(p);
Pl.send(p,Sig(pl),hP ,Pr);
//发送者为生产商，接受者为私有链
for(i = 0 ; i<D. size();
++i ){ Di.generate(Mi);
 Sig(i)=Di.sign(Mi);
hMi=H(Mi) Di.send(Mi，
Sig(i),hMi，Pr);
}
h  =H(ΣhMi|Sig(pl));
Pr.send(h,X);
X.generate(ID);
hID=H(ID);
X.send(ID, Lpr，Lpu,Tag);
 X.send(ID, h, Sig(x), Pu);
Sa.genrrate(S);
Si=Sa.sign(S);
Sa.send(S, Si, Pu);
 END
```

算法 2. 溯源数据查询

输入: 某零售产品的 Tag 包括 Lpr , Lpu 以及 ID

输出: 该产品的详细溯源信息

过程 2. 溯源信息查询

BEGIN

get(Lpr , Lpu ,ID, Tag);//由 Tag 获得 Lpr , Lpu ,ID

Cl.send(Lpr ,Pr);

Pr.send(M1,M2,...,Mn ,P,Cl);//从私有链中获得信息

Cl.send (Lpu , M1,M2,...,Mn , P, ID, Pu); //将信息送往公有链验证

IF(! HPR=H(ΣH(Mi, Si(i))+H(P, Si(c)))

return error; //数据篡改或仿冒Pu.send(S,Cl); //从公有链获得销售信息

END

5.6 争议解决系统

5.6.1权益授权证明机制

在新零售交易过程中，零售产品买方和卖方之间有可能会产生争议，例如： 买方觉得零售的真实质量不达标。出现了这种情况，在中心化的平台中，往往由平台充当协调与仲裁者。一方面平台需要为此付出高昂的运营成本，另一方面交易双方都有可能认为平台是做出了不公允的仲裁。

BCS 基于权益授权证明机制（DPOS）所设计的争议解决系统，通过区块链很好地解决了以上问题。首先，在服务登记阶段，零售卖方可以明确指出自己愿意支付的保证

金额度。交易开始后，交易资金以及保证金都会被锁定在指定的区块链钱包中。如果在服务过程中产生了争议，任何一方都可以提出仲裁请求。

5.6.2争议解决流程

争议解决系统的工作流程如下：

1）提出争议的一方通过智能合约触发启动争议解决系统。提出争议者需要支付争议解决服务费（例如 0.5BCS token）。

2）争议双方上传证据到 IPFS 文件系统中，证据的哈希值会被记录在区块链中。

3）系统自动根据争议涉及的金额组建相应人数的仲裁委员会（最少 5 个）。

4）仲裁委员会的选择会以仲裁者的活跃度与信用评分做为根据。

5）被通知到的仲裁者根据证据作出投票，投票最终会被公布在区块链中。仲裁者将得到相应的 BCS token 作为奖励。

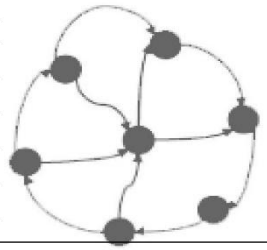
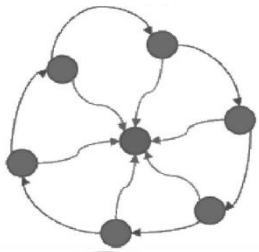
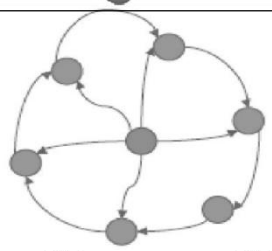
6）如果争议的任何一方对仲裁结果不满意，可以提出上诉。每次上诉的争议服务费都会翻倍，仲裁委员会的人数也会翻倍，直到争议服务费超出申诉的赔偿金额为止后不得再提出上诉。

7）争议系统会根据最后一次的最终投票结果将资金分配给相应的争议方， 得出结果

6.token 生态激励及应用

6.1 价值回路原则

人类社会组织存在 3 种价值回路

	①合理的价值回路：系统不存在价值奇点，任何角色都是平等的。每个角色可以接受别人的价值给以，同时也会回馈价值给别人。
	②短期可行但不可持续的价值回路：系统存在价值奇点，即存在某个角色，价值只流入不流出，周围角色只能围绕核心角色流动，并“供养”核心角色。
	③不合理的价值回路：系统存在价值奇点，即存在某个角色，价值只流出不流入，周围角色靠核心角色流出来“供养”。

奇点陷阱案例：中国北宋、南宋、元、明初都曾发行纸币（交子、钞），但在运行一段时间之后均告失败，一个重要原因是发行纸钞的中央政府成为一个只出不进的奇点，这是一种短期可行但不可持续的价值回路。

而现实合理的世界经济体往往都有多次的分配：

零次分配：货币在刚刚创造出来以后，按照平等原则进行分配，虽然货币增长本身不会增加财富，但是由于新增货币的分配有先后次序，因此零次分配可以改变真实财富分配。

一次分配：市场按照效率优先的原则，由自由交易而进行的自然财富分配

二次分配：政府按照公平的原则，通过税收、补贴等调节手段进行的财富再分配

三次分配：个人按照道德的原则，通过捐赠、慈善等手段进行的财富分配

价值回路原则清晰的说明，一个成功的交易群体，价值必须要有进有出，形成合理的价值回路，这同时也是商信链激励机制的设计原则。

6.2 激励机制设计

于价值回路原则，商信链的激励机制设计如下：

0次分配：用户、零售商家根据自己的贡献值获得商信链Token。

1次分配：用户、零售商家用 商信链Token 进行买卖交易。商信链获得各种手续费，服务费。

2次分配：基金会根据零售商品的评论，质量情况、用户和企业诚信情况， 给相关用户、企业奖励 商信链Token。此外，基金会补贴活跃度高的用户、零售商家。

基金会向商信链所有用户（包括零售商）承诺以某托底价格回收 商信链Token，并进行一定比例的销毁，强制通缩，制造升值效应。

3次分配：零售商可以从市场购买商信链Token，然后用商信链Token 去奖励给频繁购买自己零售商品的用户群。

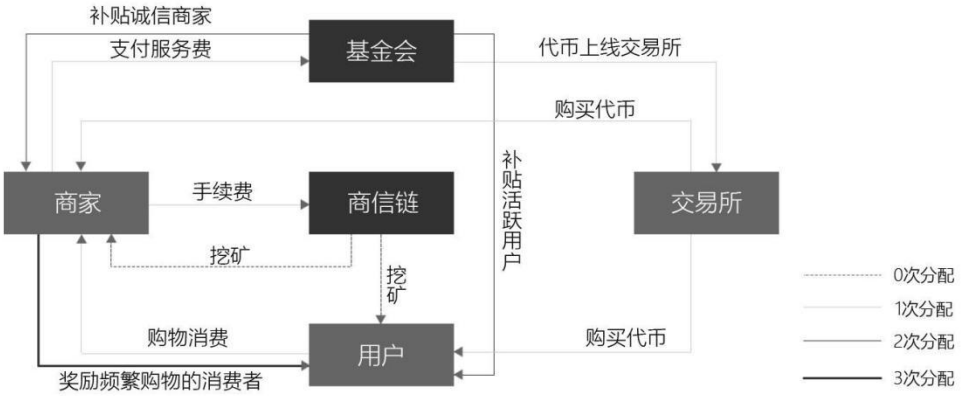


图 6.1-商信链激励机制设计

7.token 经济模型

7.1 BCS发行计划

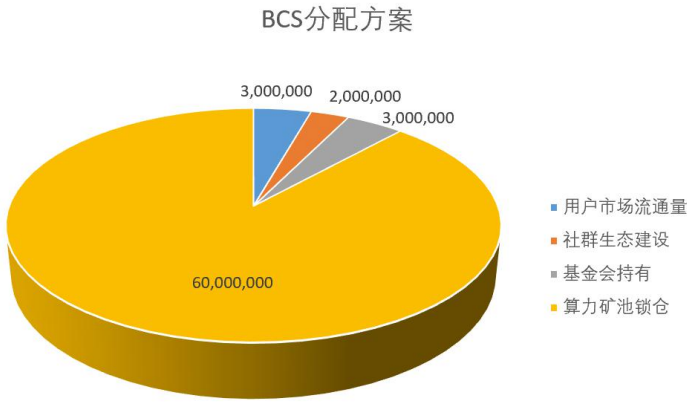
7.1.1发行的目的

BCS 是商信链构建的新零售商业信用经济生态的唯一价值衡量和流通协议，所有的数据采集、 交换、场景应用都需要BCS作交互介质。 BCS目前使用以太坊智能合约的新语言Solidity设计和发行的Token——BCS通证（BCS），并遵守ERC20协议，被用来作为BCS生态的价值交换协议。遵守ERC20协议，让它具有更容易互换、

更具兼容性等特点，让生态参与者能够完全控 制自己的资产。

通过首次Token发行筹集项目运营所需数字货币，众筹所得数字货币将按约定比例投入于产品研发，团队扩张，社区运营，市场营销等。随着项目推进，团队将逐渐释放预留的Token，用于邀请和激励高水平区块链开发人员加盟社群。

7.1.2 BCS Token分配方案



BCS总计发行量68,000,000，并被合约锁定永不增发

- BCS 市场流通：3,000,000 BCS，占总发行量的4%；
- 基金会持有： 3,000,000 BCS，占总发行量的4%；
- 社群生态激励：2,000,000 BCS，占总发行量的3%；
- 算力矿池锁仓： 60,000,000 BCS，占总发行量的 88%；

7.1.3 BCS Token归权时间表

市场流通所得数字货币的使用计划：本次通过初次流通Token所获得的数字货币将用于以下几个方面：

团队建设：30%的预算。这笔费用将用于加强技术团队，优化现有技术设计和研发新技术的支出；

计算能力采购：10%的预算。这笔预算将用于采购共有云或分布云提供的计算能力，以支援初期应用层的开发和发展。

运营管理：20%的预算，这部分预算将用于在相关法律、安全、会计、人事等运营管理方面的一系列开支。

市场推广：30%的预算。这笔费用用于应用的推广。主要包含： 流量购买、业务推广、与创业者社区、各大平台、各类广告资源的对接等。

其他开支：10%的预算。这笔费用将用于不可预见的偶然性开支。

7.1.4 BCS Token归权时间说明：

1，算力矿池锁仓60,000,000 BCS：由持币用户通过算力挖矿产出，前三年每日产出20,000 BCS；每三年减产一次，累计十年产出。

2，基金会持有并锁仓3,000,000 BCS：此部分作为基金会算力，分6次投入矿池，每次500,000 BCS；投放时间是当用户矿池算力达到50%时，基金会将续投500,000 BCS进入矿池，直至3,000,000 BCS投完。

3，社群生态激励2,000,000 BCS：用于BCS团队领导人奖励、BCS社群生态建设、运营中心、会议等方面。此部分限量支出，用完即止。

7.2 BCS 的应用场景

BCS 是商信链上的数据信用资产，是个人或机构用户使用的数字资产。它不仅具有流通价值，同时还是基于商信链应用的必备加密数字资产。

它的应用价值主要体现在以下几个方面：

1. 在商信链上开发、认证应用、使用链上服务（例如链上转账的矿工费）需要支付或燃烧BCS， BCS是作为链上应用运行唯一使用到的Token。

2. 随着商信链合作的客户和数据源越来越多，数据交易所的交易量越来越大，商信链Dapp就可以收到更多的佣金，团队会定期拿出佣金收入的10%按照当时二级市场的价格回购BCS并销毁。

3. 在选举产生见证人时可作为选票使用。

4.在Dapp中，BCS将作为重要支付手段。具体体现为：

（1）用户之间互相使用BCS进行结算；

（2）使用公共服务需要用BCS结算；

（3）商家提供的服务也需要用BCS来购买；

（4）当完成商户的任务，或是参与一些活动时，将会收到BCS作为激励。

7.3 BCS经济模型

在商信链的模型中，BCS作为沟通各参与主体的重要媒介，是整个商信链信用经济生态中不可或缺的重要部分。具体的使用场景如下：

（1）个人用户

获得途径：通过Dapp挖矿获得BCS；通过完成活动或任务获得BCS；

对社区做出贡献获 得BCS；信用数据交易收入BCS。

使用途径：使用Dapp的服务消耗BCS；使用BAAS服务消费BCS；

使用第三方应用消耗BCS；信用数据交易支付BCS。

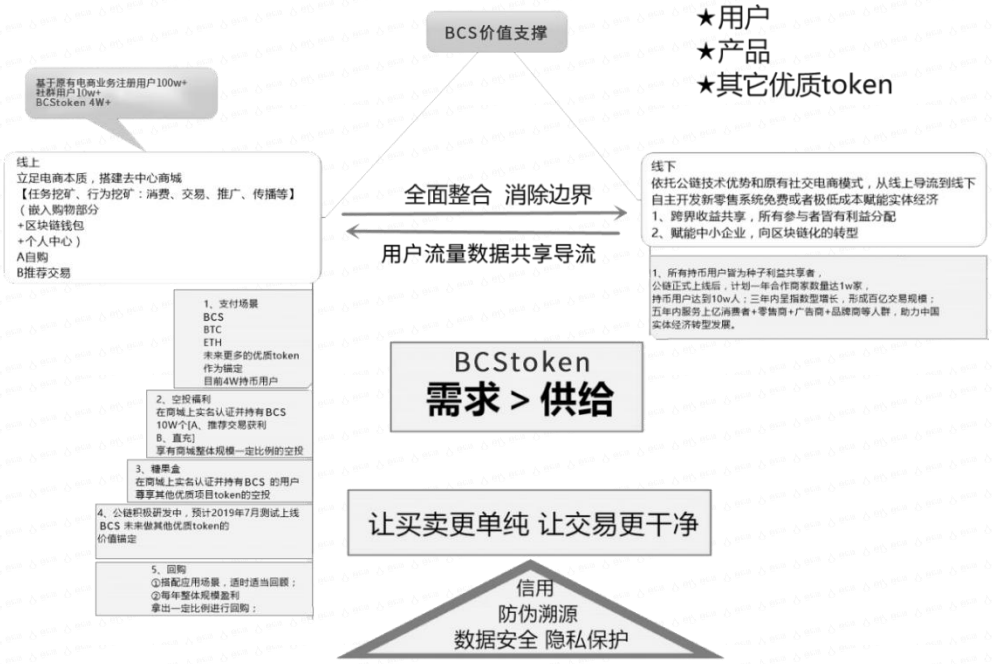
（2）开发者

获得途径：为社区做出开发贡献（包括BUG反馈）获得奖励BCS；通过

开发应用赚取服务费BCS；销售应用产生的信用数据获得BCS。

使用途径：使用BAAS服务消耗BCS；注册成为开发者消耗BCS。

▲BCS核心价值支撑



7.4 流通性及锁定机制

BCS Token 本身遵循 ERC20 标准，并且在智能合约的基础上带有原生的流动性。这意味着用户不必去传统的交易所购买和出售 BCS Token，而是可以通过本论述的方式，利用协议本身的去中心化撮合机实现。这得益于协议灵活的收费模式。

▲ 锁定机制

随着商信链系统的发展，其通过智能合约技术服务于新零售商业生态的过程中，存在需要锁定海量BCS作为信用保证的应用场合。这些大量、持续、短期内不可逆的锁定行为直接打破了供需平衡。

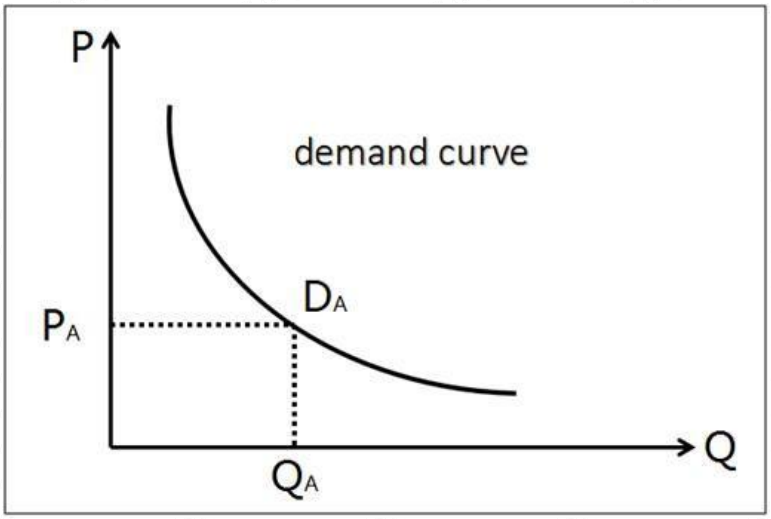


图7.4—1（供需价格关系模型）

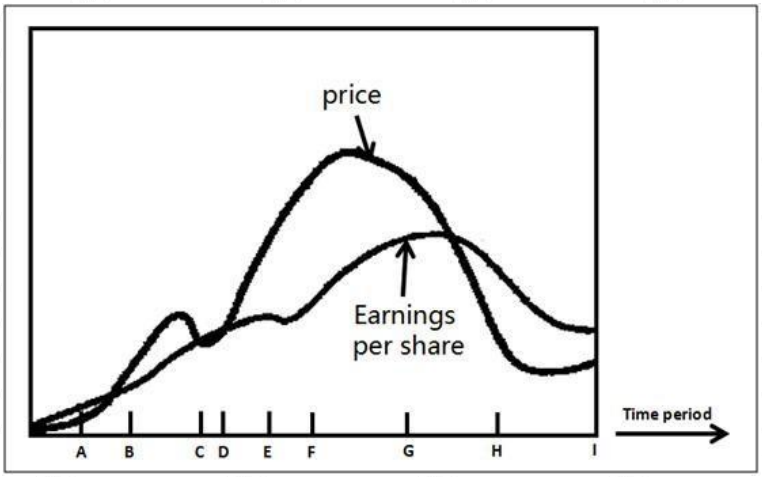


图7.4—2（资产价格模型）

8.项目路线

8.1 初期规划

具体规划如下：

Phobos 2019.7	BCS Beta主网上线
Deimos 2019.8	智能合约平台发布 POBC共识协议发布
Mars 2019.11	BCS 主网上线
Jupiter 2019.12	认证机制模块开发完成 POBC共识协议模块开发完成 BCS Solar TestNet上线

8.2 中期规划

为了使商信链面向零售商品领域方方面面的用户，发挥其价值。因此必须进一步加大平台的推广，比如在传统的零售商品领域、消费市场面向目标用户进行宣传， 寻找更多零售商品买卖双方、零售商品生产、销售商、零售商品其他各个有关公司入驻商信链。

Saturn 2020.6	BCS Solar主网上线 BCS 区块链浏览器发布 基于Solar主链的钱包发布 智能合约2.0平台发布
Saturn 2020.6	BCS2.0主网上线 BCS开发者生态圈建设

8.3 未来规划

未来的商信链将整合零售行业的上下游，包括生产到销售到用户购物习惯的方方面面。通过区块链技术，打造一个供应链可追溯，商家和用户信用可量化，数据公开透明，集消费购物，会员服务，精准营销，集中采购等场景于一体，形成线上电商交易，线下购物体验，构建多方参与，多方受益的新零售生态。目标是将商信链打造成一个集中百万商户，数亿用户，千亿市值的全球范围的基于区块链的新零售商业信用经济生态。

BCS团队

2019.4