区块链+供应链金融白皮书

发布单位：中国区块链生态联盟

指导单位：青岛市崂山区人民政府

中国电子信息产业发展研究院（赛迪研究院）

编写单位：赛迪（青岛）区块链研究院

青岛地铁金融控股有限公司

齐鲁银行股份有限公司青岛分行

青岛闪收付信息技术有限公司

青岛闪收付区块链信息技术有限公司

2018 年 9 月

编写单位(排名不分先后)

赛迪（青岛）区块链研究院

青岛地铁金融控股有限公司

齐鲁银行股份有限公司青岛分行

青岛闪收付信息技术有限公司

青岛闪收付区块链信息技术有限公司

主要编写人员（排名不分先后）

刘 权、曾 晋、刘曦子、黄忠义、曹兆磊、袁 方

刘洪涛、陈健、姜晓平、刘大磊、陈洪顺、田亦农

目 录

1. 供应链金融发展现状

1.1 供应链金融概述

1.1.1 供应链金融内涵和特点

供应链金融（Supply Chain Finance，SCF）是基于供应链上企业真实的交易背景以及自偿性的收入，建立基于资金流转、业务信息等闭合化的交易结构，通过应收账款债权转让/质押、货权质押、保兑仓等封闭资金流或控制货权，对供应链上下游企业提供综合性金融服务。根据国际商会（ICC）的定义，供应链金融利用融资和风险缓释的措施和技术，对供应链流程和交易中营运资本的管理和流动性投资资金的使用进行优化。与传统金融产品相比，供应链金融具有鲜明的特点：

（1）自偿性贸易融资

自偿性贸易融资根据核心企业真实贸易背景和上下游客户资信实力，以单笔或额度授信方式，提供银行短期金融产品和封闭贷款，以借款人销售收入或贸易所产生的确定的未来现金流作为直接还款来源。

（2）操作的封闭性

金融机构对发放融资到收回融资的全程进行控制，既包括对资金流的控制，也包括对货权的控制，通过 ERP 系统的对接还可实现对关键信息流的控制。典型的产品如动产质押授信业务，银行将企业所拥有的货权进行质押，授信资金专项用于采购原材料，企业以分次追加保证金的方式分批赎出货物，随之进行销售。

（3）授信机制由“N”到“1”

传统金融模式下金融机构授信主体包括供应链上的每一家企业，即是对 N 个企业的授信。供应链金融模式下，金融机构可只对核心企业授信，由核心企业基于供应链上下游企业的购销情况、履约情况等进行授信额度分配，金融机构在已分配额度内为供应链上下游企业提供金融服务。

数据显示，我国 2015 年供应链金融市场规模约为 12 万亿元，2017 年全国供应链金融市场规模约 14.42 万亿元，且供应链金融在新兴经济体的年增长率超过 25%，受监管政策影响，互联网金融 C 端业务受到冲击，B 端金融业务有望爆发式增长，预计到 2020 年规模或将超过 27 万亿。

1.1.2 供应链金融功能

供应链金融以核心企业为出发点，重点关注围绕在核心企业上下游的中小企业融资诉求，通过供应链系统信息、资源等有效传递，实现供应链上各个企业的共同发展，持续经营。

供应链金融的核心意义在于针对中小供应商授信额度不高、融资规模较小的特点，利用信用替代机制，以供应链核心企业信用替代中小供应商信用，实现供应链上下游企业资金融通的需求。

1.1.3 供应链金融主要参与者

供应链金融主要参与方主要包括以下几类客户：

核心企业。在整个供应链业务中处于主导地位，通过对应付账款确权、提供回购、调剂销售等增信措施，助力供应链金融业务的开展。

融资企业。包括核心企业的上游供应商、下游经销商。

金融机构。包括银行、券商、保险公司、保理公司、小额贷款公司等，主要提供融资、信用保险、ABS 等专业服务。

供应链服务机构。包括物流企业、物流园、供应链金融服务平台等。

1.2 供应链金融主要模式

1.2.1 应收账款融资模式

应收类产品主要应用于核心企业的上游供应商，供应商履行完商务合同、已开立发票，但尚未收到货款，通过保理或应收账款质押等形式进行融资。

（1）应收账款质押融资，指企业与金融机构签订合同，以应收账款作为质押品，在合同规定的期限和授信额度内，向银行等金融机构申请短期借款的融资方式。

（2）保理业务，是一项以债权人转让其应收账款为前提，集融资、应收账款催收、管理及坏账担保于一体的综合性金融服务。在实际的运用中，保理业务有多种不同的操作方式，一般可以分为：有追索权保理和无追索权保理；明保理和暗保理；正向保理和反向保理等。保理是一种债权的转让行为，适用于《中华人民共和国合同法》，应收账款质押是一种物权转让行为，适用于《中华人民共和国物权法》。

1.2.2 预付账款融资模式

预付类产品主要应用于核心企业的下游经销商融资，包括先款（票）后货、保兑仓等多种业务模式：

（1）先款（票）后货模式。银行给经销商融资，预付采购款给核心企业，核心企业发货给银行指定的仓储监管企业，货入库后立即设定质押监管，作为银行授信的担保，仓储监管企业根据银行的出库指令逐步放货给经销商。

（2）保兑仓模式。保兑仓模式下核心企业不再发货给银行指定的仓储监管企业，而是本身承担了监管职能，根据银行的出库指令逐步放货给经销商，同时核心企业向银行提供回购、调剂销售等增信措施。

1.2.3 存货融资模式

存货类融资主要分为现货质押融资和仓单质押融资两大类。现货质押可分为静态质押和动态质押，仓单质押分为标准仓单质押和非标准仓单质押。

（1）静态质押融资是指企业以其自有或第三人合法拥有的动产为质押，银行委托第三方仓储监管企业对其提供的质押商品实行监管，经销商必须打款赎货，不允许以货易货。

（2）动态质押融资是对静态质押融资的延伸，指企业以自有或第三人合法拥有的动产为质押，银行委托第三方仓储监管企业对其提供的质押商品实行监管，银行对质押商品价值设定最低限额，允许对

限额以上的商品出库，允许以货易货。

（3）标准仓单质押融资是指企业以自有或第三人合法拥有的标准仓单为质押的融资业务。标准仓单是指符合交易所统一要求的、由指定交割仓库在完成入库品验收、确认合格后签发给货主用于提取商品的、并经交易所注册生效的标准化提货凭证。

（4）普通仓单质押融资是指企业提供由仓库或其他第三方物流公司提供的非交易所交割用仓单作为质押物，并对仓单作出质背书，由银行提供融资的一种产品。

1.3 供应链金融行业痛点

1.3.1 信用难以传递，中小企业融资难、融资贵

供应链金融的重要作用是依托核心企业的信用，服务上下游中小企业。在多级供应商模式中，一级供应商之后的其他供应商难以获得核心企业的信用支持，导致此类中小企业仅靠自身的信用难以融资。为解决多级供应商的融资需求，基于核心企业付款承诺的应收账款凭证多层流转模式开始出现，但金融机构对供应链金融平台上核心企业应付账款确权信息、应收账款凭证流转数据的真实性、有效性不能充分信任，导致供应链上持有应收账款凭证的中小企业难以获得金融机构的融资支持，融资难、融资贵的问题未能有效解决。

1.3.2 贸易背景真实性审核难度大

供应链金融整合了商流、物流与资金流等数据信息，金融机构通过对供应链上的历史交易数据进行分析，以此来分析商业逻辑，制定

风险控制模型，为供应链客户核定合理的授信额度。虽然供应链金融是基于核心企业的信用，但为了核实贸易背景的真实性，金融机构仍会投入大力的人力、物力，多维度验证上述信息的真伪，降低了供应链金融的业务效率。如果能够实现供应链历史数据全程可视、并且不可篡改，将大幅降低金融机构的尽调成本，提升供应链金融业务的整体效率。

1.3.3 供应链平台数据的有效性问题

目前越来越多的金融科技公司依托互联网技术，为核心企业、供应商、经销商以及金融机构提供线上供应链金融服务，一旦出现交易纠纷，需要进行责任划分。因此，需要确保原始交易记录的全生命周期可追溯，保证原始交易数据未被篡改。平台为提高数据的权威性，通常需要借助公证处这类第三方权威机构进行见证，但这种模式必然会增加交易成本、影响效率，可操作性不强。实践中，需要一种安全、高效、便捷和低成本的多方存储解决方案，确保各方都完整保存了数据信息，同时保证数据的安全性、真实性和可靠性。

1.3.4 供应链系统中心化架构，存在安全隐患

目前多数供应链金融平台采用中心化 C/S 或 B/S 架构，供应链金融平台的系统应用、交易数据、账户数据采用中心化存储，由企业独立维护。中心化存储模式有较大的数据安全隐患，容易出现数据丢失或被攻击造成整个平台瘫痪的风险，影响系统服务的连续性和可靠性。

而分布式存储的优势在于每一方都保存了完整的交易信息，不依赖某一个“中心”机构保存信息，相对更加安全、不容易篡改，而且信息的查询和交易理论上都能以更低的成本进行。

1.3.5 多方系统对接，费时费力，效率较低

供应链金融的开展主要基于核心企业的信用，需要技术手段把供应链中的信息流、物流、资金流进行整合，实践中多采用系统直联的方式，实现数据交互，涉及到核心企业 ERP、银行供应链前置系统、供应商 ERP、供应链服务平台等。由于各参与方之间非统一的数据标准，实现系统直联需要各参与方进行系统改造，耗费大量的人力、财力。实践中，也有部分核心企业出于系统安全的考虑，不愿开放 ERP 系统，无法共享数据。在系统直联的方式外，亟待新的技术解决方案，以实现更经济、更高效地共享数据。

2. 区块链+供应链金融应用综述

2.1 区块链技术概述

2.1.1 区块链简介

区块链不是一项新技术，而是一项技术创新组合，其关键技术包括 P2P 动态组网、基于密码学的共享账本、共识机制、智能合约等。狭义来讲，区块链是一种按照时间顺序连接数据存储区块从而形成一种链式数据结构，并以密码学方式保证不可篡改和不可伪造的分布式

账本（分布式数据库）。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

尽管不同报告中对区块链的介绍措辞都不相同，目前得到广泛共识的 4 个技术特点分别是去中心化、去中心化信任、可靠数据库及集体维护。

（1）去中心化（Decentralization）：区块链由众多节点组成一个端到端的网络，不存在中心化的设备和管理机构，任意节点停止工作都不会影响系统整体的运作。

（2）去中心化信任（Trustless）：区块链中节点之间通过数字签名技术（公私钥）进行验证，通过联盟链构建跨企业的信任机制。采用密码学哈希算法确保信息不可篡改，采用抗抵赖、抗攻击的共识算法保证区块链数据安全性、完整性和连续性，节点之间相互无法欺骗。

（3）可靠数据库（Reliable Database）：系统中每一个节点都拥有最新的完整或部分数据库备份，单个甚至多个节点对数据库的修改无法影响其他节点的备份数据，除非能控制整个区块链的网络共识机制，但这几乎不可能发生。区块链中的每一笔交易都存储在区块中并通过密码学方法与相邻两个区块串联，在确保不可篡改的同时实现追溯功能。

（4）集体维护：区块链是由其中所有具有维护权限的节点共同

管理的，系统中各个节点按不同角色分工参与系统的共识、交易及验证等工作。

按参与方分类，区块链可以分为公有链、联盟链和私有链；从链与链的关系来分，可以又分为主链和侧链。

（1）公有链：公有链的特点是无官方组织及管理机构，无中心化服务器，参与的节点按照系统规格自由接入网路、不受控制，节点间基于共识机制正常运转。在公有链中的共识机制一般采用工作量证明（PoW）或权益证明（PoS），用户凭借在网络中消耗或拥有资源的占比来争夺区块的记账权。公有链较适合于虚拟货币、电子商务、互联网金融等 B2C、C2C 或 C2B 的应用场景。

（2）联盟链：联盟链是一种需要注册许可的区块链，仅限于联盟中具有权限的成员参与账本的读写，网络中节点的角色及功能划分需预先设定，且网络中的共识、运维和接入均由预先设定的节点控制。联盟链多采用 PBFT（Practical Byzantine Fault Tolerant）、RAFT、PoA 等共识算法。一般来说，联盟链适合于跨机构的交易、结算、协同办公及存证等 B2B 场景。

（3）私有链：私有链建立在某个组织内部，节点间的运行规则根据内部要求进行严格设定。私有链的应用场景一般是企业内部的应用，如数据库管理、审计等；私有链的价值主要是提供安全、可追溯、不可篡改、自动执行的存储和运算平台，能够实现数据的完整性、安全性、连续性和真实性存储。

供应链金融具有多方参与、共同维护、共享数据的特点，并且供应链金融业务流程多为跨企业、跨系统的协同运转机制，所以大多采用联盟链技术结构搭建供应链金融区块链网络，实现自主可控、安全隐私、便捷高效的供应链金融新模式。

2.1.2 区块链技术原理

区块链是多种技术的创新性融合，主要包括了计算机数据结构、现代密码学、点对点通讯技术等。

（1）区块与链式结构：区块是记录交易的基本单元，区块链将已完成的交易打包成区块并与主链连接形成链式结构，所有参与计算的节点都拥有完整或部分区块链账本。区块由区块头和区块体组成，区块头封装了当前的版本号、前一区块地址、时间戳、随机数、当前区块的目标哈希值、Merkle 数的根值等信息。区块体只负责记录固定时间或固定交易数量的交易信息，主要包括交易数量和交易详情。

（2）哈希函数与 Merkle 树：哈希函数可将任意长度的数据经由 Hash 算法（单项哈希函数）转换为一组固定长度的代码，哈希函数具有易验证，难破解等优势，主流的哈希算法包括 MD5、SHA-256、SHA-384 及 SHA-512 等。Merkle 树是一种哈希值二叉树，可以快速校验大规模数据的完整性。在区块链网络中，Merkle 树被用来归纳一个区块中的所有交易信息，最终生成根哈希值，区块中任何一笔交易信息的改变都会造成 Merkle 树根哈希改变。

（3）非对称加密：非对称加密算法是一种密钥的保密方法，泛指公钥和私钥，其功能概括为公钥加密、私钥解密，私钥签名、公钥验签。因为加密和解密使用的是两个不同的密钥，所以这种算法叫做非对称加密算法。

（4）P2P 网络：P2P 网络又称对等网络，是没有中心服务器、依靠用户群交换信息的互联网体系。与具有中心化服务器的星型或环型网络系统不同，对等网络的每个用户既是一个节点，也有服务器的功能，P2P 网络具有去中心化与鲁棒性等特点。

（5）共识机制：共识即具有权限的节点之间对区块中存储的内容信息达成的一致性和有效性协议，共识机制具有一定的容错、防止篡改和抵赖的能力。目前主流共识机制有 PoW、PoS、PoA、DPoS 和 PBFT 等。

（6）智能合约：智能合约是一组情景应对型的程序化规则和逻辑，是通过部署在区块链虚拟机上的去中心化、可信共享的脚本实现的。智能合约封装了预定义的若干状态机及转换规则、触发合约执行的情景、特定情景下的应对行动等。

（7）隐私智能合约：隐私智能合约能够确保联盟链上交易的各方只能看到权限范围内的数据，并确保完整的交易数据并没有被窜改。与传统智能合约相比，隐私智能合约要严格设计权限划分，借助数字证书识别请求者身份并识别该身份下的权限，从而达到限制请求者行为的目的。

2.2 区块链解决供应链金融痛点

2.2.1 区块链构建“技术信任”

传统供应链金融企业融资依靠的是核心企业的控货能力和销售调控能力，银行只信任核心企业的一级供应商，导致供应链上中小微供应商的融资需求得不到满足，其根本问题是银行与中小微供应商无法建立信任体系。供应链金融平台的出现，能够对接银行、保理公司、核心企业、中小微供应商等企业，利用平台的公信力和业务能力为中小微企业信任背书，其实质仍是为供应链金融上下游企业建立信任体系，即对供应链金融公司、平台及其相关背书企业的信任。但这种信任是脆弱的、没有技术支持的信任。随着供应链金融平台的对接企业不断增多，平台业务量和交易金额不断上升，这种基于企业或平台的信任体系极易崩塌瓦解。

区块链技术采用多方维护共同写入的分布式账本技术将供应链上的合同、单据、发票等多种信息分享给具有权限企业，利用 P2P 网络将核心企业及上下游企业、金融机构等连在一起，解决了供应链金融信息无法传递、数据无法存证鉴权问题。密码学技术的引入使得每个参与者都具有各自的身份证书，区块链账本中的内容可追溯但不可篡改，任何有权限的参与者对账本的操作都会记录在案。共识机制能够确保链上共同协作的节点达成安全、有效、民主的一致性认识，从而代替或升级传统的供应链金融平台，并通过区块链建立基于技术的多方的信任供应链体系。

2.2.2 区块链解决票据难以分割流转问题

供应链金融本质上是为中小微企业提供快速灵活的贷款服务，中小微企业之所以出现融资难融资贵的问题，其原因在于上游供应商及核心企业之间的合同及债权难以拆分，供应商没有得到应收账款凭据且自身又缺少可用于抵押融资的资产，导致来自核心企业的信任无法沿供应链链条传递到末端，而包括银行在内的金融机构受政策限制及风险控制等因素影响，对供应链金融中小微企业贷款也存谨慎态度，经常以较高的利率和复杂的审核机制来降低信贷风险。传统的供应链金融平台可以依靠自身有限的公信力实现债权拆分，为供应商提供融资凭据，但随着供应链条的延伸，这种信任度将加速下滑。由其对于中心化的信息平台，还存在数据篡改、数据泄露等问题，难以自证清白，更增加了银行信贷风险。

区块链的引入能够完全解决现有债权凭据拆分问题，且基于区块链技术的信任可以延供应链条做无衰减的传播。首先，区块链采用P2P 网络结构，任何有权限的节点企业均可以获得与其相关的完整账本信息，实现多方参与，共同管理，避免传统中心化系统数据篡改、数据泄露等问题。其次，核心企业产生的债权凭据可以在区块链上按不同的应收账款额度灵活拆分，任何拆分行为都会通过有效的共识全网广播后记录在链上且不可篡改，银行可以完全信任链上业务数据。最后，区块链具有严格的身份认证体系和权限隐私体系，链上所有节点和用户均具有相对应的身份标识，不可抵赖不可篡改，核心企业及其供应商不必担心其商业数据在链上被公开，区块链将限制账本访问

权限并维护交易人的隐私，即在链上，某节点只能看到与其业务相关的业务信息及其他节点允许其看的信息。

2.2.3 区块链提高供应链金融业务效率

供应链金融相关业务大部分涉及多方协同处理，如合同签订、数据审批、融资申请、企业担保等业务，线下审核机制严格、流程复杂，由于必须由信任机构完成相应的认证和账务处理，资金通常至少要耗费数周时间才能到账，且手续费用昂贵。即使是采用供应链金融平台，也多需要线上申请、线下审批，数据跑在人后面，大大降低了业务处理效率。

可以将联盟链看做是“跨企业的业务协同办公系统”，区块链共识机制会将上链数据按照一定的规则进行同步，且确保链上内容不可篡改、可追溯，在办理供应链金融相关业务的时候可以灵活快速的获取账本中相关的证据，避免了传统业务流程线上申请、线下审批的繁琐流程，可以以较高的效率处理业务。此外，利用区块链特有的智能合约功能，银行、保理公司等金融机构可以在满足融资要求的前提下做到实时放款，例如，在一个融资流程中，从申请融资到资料审核，如果完全满足智能合约的约束条件，即刻触发智能合约的放款命令，这一过程中减少了办理者的信息审核、身份核验和放款流程的办理时间，大大提高了业务办理效率。

2.2.4 区块链降低供应链金融信息系统扩建成本及复杂度

传统的中心化供应链金融信息系统在发展到一定阶段后需要与银行、保理公司、核心企业、券商等企业进行业务对接，一方面能够扩大系统业务范围，另一方面也会增加系统的公信力。但在这一对接过程较为复杂，由其针对银行、券商等金融机构，数据对接更为困难，且这一过程中产生的成本较高，大部分为重复工作。区块链采用 P2P 网络结构，系统的对接只需将该企业以节点的形式纳入区块链网络中，如需要还可为其开发上层去中心化应用程序。区块链与供应链金融的结合能够有效降低与第三方系统交互复杂度，提供多种数据共享模式，规范数据共享接口，节约现有平台业务扩展成本，为数据真实性提供保障。

2.2.5 区块链增强供应链金融平台安全性

传统的供应链金融平台是由企业独立维护，采用中心化 C/S 或 B/S 架构，供应链金融数据中心化存储，带来了较大的数据安全隐患。采用的区块链技术后，具有权限的链上节点均按照一定规则参与维护各自账本数据，数据的分布式存储可以确保单一节点数据丢失或被攻击所造成的平台瘫痪和经济损失，若某个节点出现宕机状况，数据不会轻易丢失。此外，区块链数据存储的特点能确保账本数据的不可篡改和可追溯，结合完整的时间戳机制也能够确保数据的连续性，这对于后续平台进行大数据分析、人工智能等拓展应用提供了有力的数据支持。

2.3 区块链+供应链金融应用模式

2.3.1 发展现状

在供应链金融领域，基于区块链账本记录的可追溯和无法篡改性，整合供应链上下游企业的真实背景及贸易信息，有利于提高供应链金融行为的安全审计和行业监管效率，降低监管成本。此外，区块链技术在供应链金融领域的应用能够为企业进行增信，有助于企业降低融资成本。当前，通过行业企业与区块链技术服务企业的合作，一批基于区块链的供应链金融服务平台相继启动或上线，成为我国供应链金融业务创新的重要方向。2018年6月，华夏银行“链通雄安-区块链-供应链”首笔放款成功落地。“链通雄安”以雄安集团信用为基础，以银企直联方式接入雄安集团区块链项目管理平台系统，利用区块链平台数据溯源、行为规范、资金管理等功能，为建设雄安的分包商解决工人工资发放、原材料采购等资金问题。

2.3.2 体系架构

区块链去中心化网络结构，开放化、透明化、可视化应用模式可有效解决传统供应链金融中存在的诸多痛点，助力供应链金融打破瓶颈、创新发展。具体列举一下几点结合方向。

（1）区块链能够解决供应链金融多方信任关系问题。加密机制（公私钥对）的引入实现了对节点的身份验证问题，哈希函数的引入保证区块内数据不被篡改。区块交易内容的存储要求严格的时间戳及

签名信息，保障了信息记录的可追溯性，共识机制实现了供应链上多方企业的民主决策，确保全网共识后才能上链，且共识机制均具有一定的防止恶意节点攻击的功能。

（2）区块链+供应链金融不仅能够解决供应链上下游企业多方信任问题，还能够解决供应链信任传递问题。传统的供应链金融由核心企业发起采购需求开始，各供应商只能凭借核心企业提供的债务凭据和合同进行融资申请。但在供应链上，债权是无法拆分的，从而导致信任无法传递，供应链末端中小微企业完全无法凭借采购凭证进行筹融资。区块链的出现使得供应链金融信任得到传递，借助区块链账本不可篡改、可追溯的特点使得债权拆分更加灵活便捷。

（3）区块链+供应链金融能够整合贸易流、物流和资金流三方面市场，实现贸易流纵向延伸，物流的实时监控及溯源，资金流路径更加清晰透明，覆盖范围不断扩大，有效解决了传统供应链金融信任不能沿供应链条有效传递的问题。

（4）传统供应链金融业务流程复杂，所需材料办理效率较低，各种登记门类收费高昂，不仅影响效率，更造成了中小企业融资成本进一步提高。区块链+供应链金融可以将原本不同企业之间的线下业务流转移植到线上，提高业务处理能力及效率，降低融资成本。

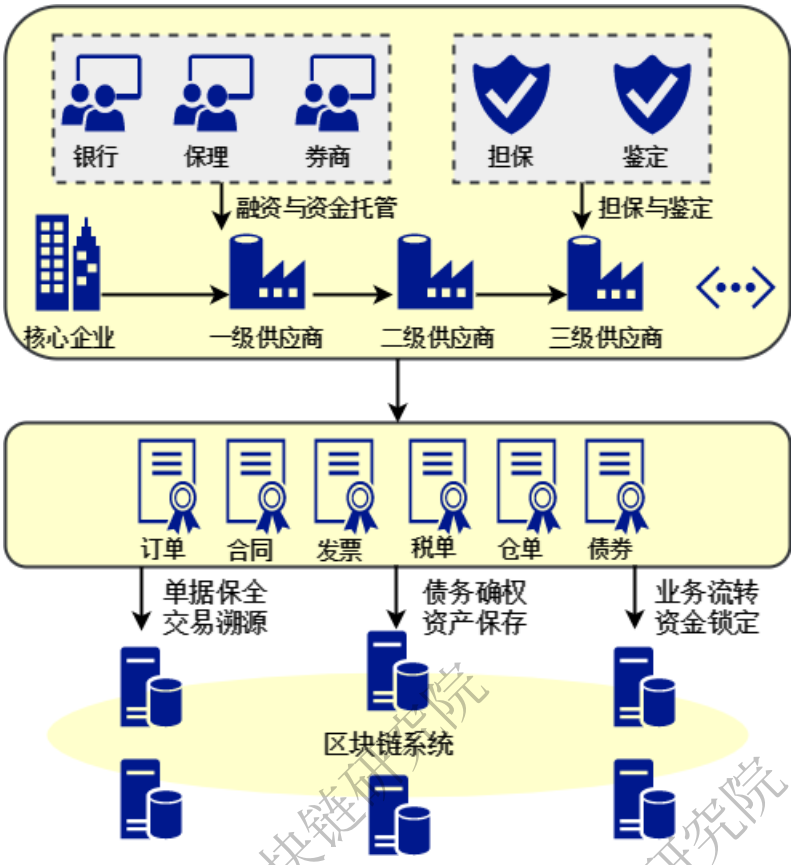

图 1 区块链+供应链金融框架图

在整个供应链金融系统中，不仅包括了核心企业及其供应商，还包括了经销商、银行、保理公司、券商、担保机构和鉴定机构等金融、背书、鉴定机构。区块链技术的加入能够促使供应链金融各方建立“技术信任”体系，并将这种信任模式传递到供应链末端中小微企业中，从而解决了中小微企业融资难、融资贵的问题。供应链金融所形成的订单、合同、发票、税票、仓单及债券都能够通过区块链账本进行共享存储，有权限的企业机构能够查阅并办理相关数据及业务。

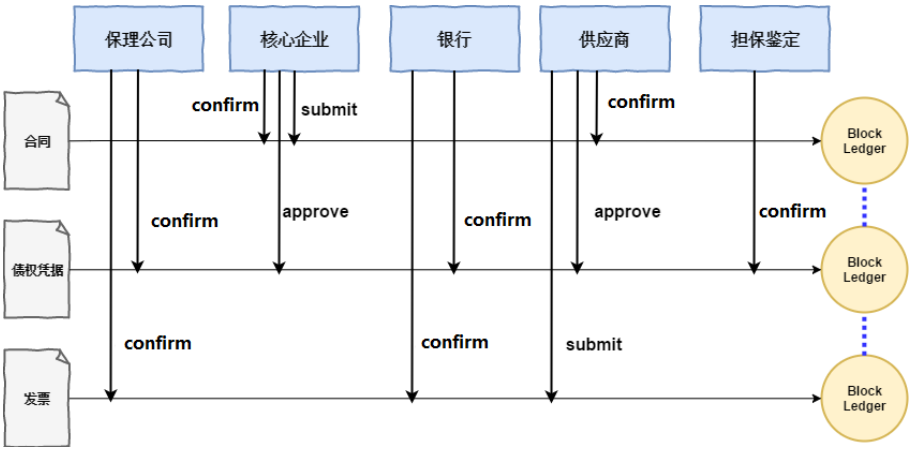

图 2 部分单据状态流转示意图

上图中，简单列出了业务合同、债权凭据和发票的状态变化情况，单据在写入区块链时候会附加状态变化参数，以方便办理业务过程中对单据状态变化的追溯和监控，以合同为例，由核心企业提交合同原件后，单据状态为 submit。合同需要得到核心企业和供应商的确认签字，后状态变为 confirm，至此合同签名生效。又如债权凭据，经由核心企业和供应商确认应付应收款后，单据状态变为 approve，保理公司、银行和鉴定机构在审核完债权凭据后，会将单据状态变为 confirm 状态。

其他单据按业务流程不同也分为不同的状态特征，区块链会记录所有单据状态变化情况用于后续的追溯和实时的监控。此外，在供应链金融系统中，涉及到各方企业或机构的协同办理业务时，在不引入区块链技术的情况下，这种企业及机构间的业务协同办理和数据传输是费时费力的，利用区块链技术分布式账本的特点，能够提供更有效更便捷的协同办理流程，节省了成本的同时并提高了业务效率。对于供应链中的上下游企业，基于区块链技术的解决方案能够有效的盘活核心企业的闲置资金，提高供应链中企业信任度及生态健康，激活供

应商应收账款，降低融资成本和采购成本的同时提高了采购效率。对于金融机构，能够拓宽并优化贷款渠道，降低贷款风险，并开阔了中小企业市场。

2.3.3 业务场景

基于区块链技术的供应链金融解决方案多以高可控性、高安全性的联盟链为主，联合供应链上下游核心企业及供应商，此外还涵盖了金融机构、银行、券商等金融资产企业。将各个主体的业务数据和贸易数据上链并存储，以区块链技术作为信任传递的基础深度赋能供应链金融中的各个中小微企业，具体业务包括了合同签约、债权确权、企业融资、债权转让、资金清收、ABS 融资等。

2.3.3.1 合同签约

区块链技术一大优势是与电子签名技术紧密结合，如 Hyperledger Fabric 会提供专门的 CA 认证接口，并支持与第三方 CA 机构进行对接，这样的功能为合同签订提供了基本的保证。供应链中的上下游企业通过节点认证后参与到联盟链中进行共识和业务交易，在合同签订过程中，上下游企业通过节点应用程序上传合同原件（如采购合同），经双方认定无误后进行电子签名认证，合同即可生效，同时将合同进行广播得到全网共识后写到区块链上，提高了传统合同签订效率并利用区块链技术进行合同存证。

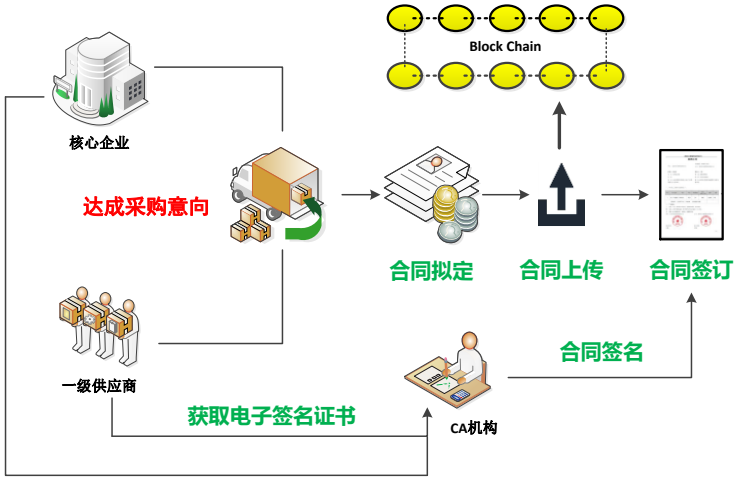

图 3 基于区块链的供应链金融合同签订流程

上图以一级供应商为例，当核心企业与一级供应商达成采购意向后，双方会协调并拟定一份采购合同，并将合同上传至区块链账本中，进行全网广播，确保合同上链且不可篡改后，区块链中核心企业及供应商要对账本中的合同进行签署操作，此时需要借助第三方 CA 机构为区块链网络中的各节点颁发的数字证书为合同签名，签名后的合同保存在区块链账本中供其他节点查看。

2.3.3.2 债权确权

合同签订双方在确定应收和应付权利后将生成债权应收应付合约，并将合约写入区块链。在供应链金融联盟链中引入第三方金融机构及保理机构节点，在债权合约共识生效后为其进行债务担保及资产托管等业务，并将相关数据写入区块链。基于区块链技术的债权确权解决了传统财务改造过程繁琐的弊端，同时利用区块链的存证及业务溯源的优势解决了债权纠纷及债权变动等问题。

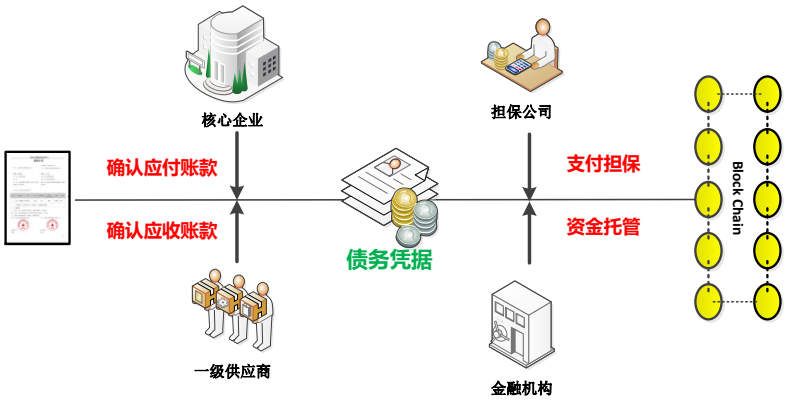

图 4 基于区块链的债权确权流程

核心企业与一级供应商签订采购合同后，后续供应商的融资贷款和债务凭据拆分处理，会生成债务凭据并进行债务确权。在核心企业和供应商分别确认了应付和应收账款后，形成债务凭据单。在基于区块链的供应链金融网络中会纳入担保公司及金融机构等企业，其目的是为供应链金融业务中产生的单据做背书、鉴定和担保。在确权业务中，金融机构将提供资金托管服务，而担保公司将提供债务担保，并将所有信息写入区块链账本。

2.3.3.3 企业融资

基于区块链技术的解决方案能够解决供应链上中小微企业融资信任问题。区块链可以将核心企业与一级供应商以及上游供应商之间的供应关系、合约及债务关系全部公开，从而建立基于技术的信任体系，联盟链中的金融机构可以通过区块链中的数据进行合理可控的信贷业务，解决了中小微企业融资难、融资贵、信任度低的问题。

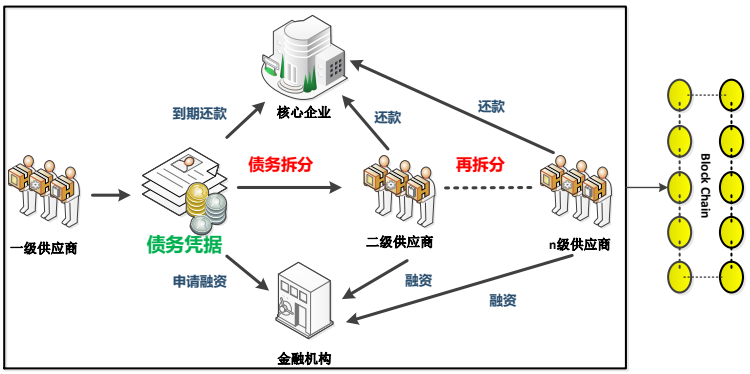

图 5 基于区块链的供应链金融融资流程

区块链能够解决供应链金融信任传递问题，通过如上图所示，通过拆分一级供应商与核心企业签订的债务凭据，使得二级供应商及以下供应商均能够获得在供应链中应收账款的债务凭据，从而向金融机构及保理公司提出融资申请。此外，债务凭据的拆分，及融资过程中涉及的业务流程均记录在区块链账本中，形成可信任、可追溯但不可篡改的记账模式。

2.3.3.4 债权转让

借助区块链技术可以使供应链上下游企业债权透明化流动，企业间债权的拆分可以通过区块链技术记录并保证不可篡改，债权可以在有效额度内进行有效拆分并记录。一旦出现债权纠纷，同样可以借助区块链溯源功能实现全生命周期的债权追溯及责任划分。

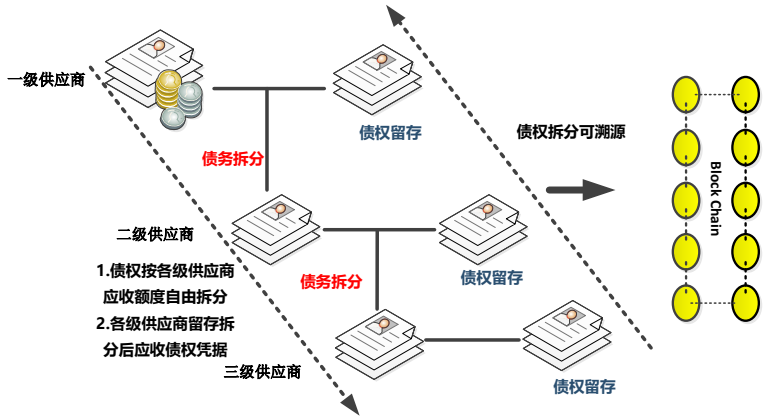

图 6 基于区块链的债权拆分流程

以三级供应商为例，若要获取拆分后的债权凭据需要通过一级供应商拆分、二级供应商拆分两个流程，拆分过程中各级供应商将留存属于自己的债权存证。各级供应商按照采购合同自身应收账款及下一供应商应收账款进行拆分，拆分过程及凭据全部记录在区块链账本中，实现了债权拆分的溯源。

2.3.3.5 资金清收

借助区块链智能合约技术，企业间可以指定双方都接受的清收条件，一旦满足条件触发智能合约，将自动进行资产清收。联盟链对接银行系统，合约触发后直接向有效凭据持有人兑付，提高了债务清收效率，避免了企业间坏账、烂账等问题。

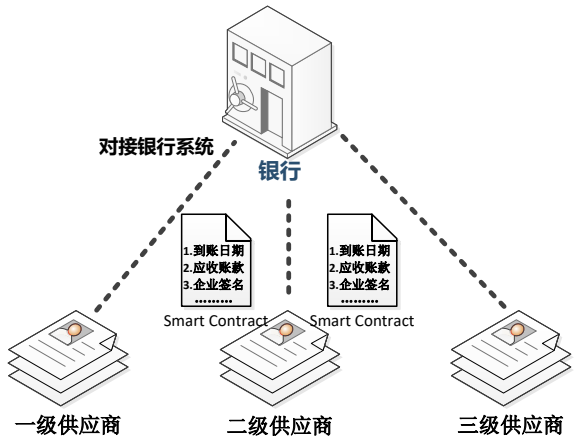

图 7 基于区块链的资金清收流程

各级供应商按照各自所持的债权凭据收取应收账款，这一环节通过区块链的智能合约技术能够实现安全、实时的资金清收。区块链系统中银行节点连接到银行内部支付系统，能够实现实时资金支付，智能合约中设计了到账日期、应收款额、核心企业签名等基础约束条件，一旦触发智能合约，银行系统将自动支付各级供应商应收账款。

2.3.3.6 ABS 融资

ABS 融资模式是以项目所属的资产为支撑的证券化融资方式。利用区块链技术可以将大型项目相关材料进行存证，同时将保理公司、券商囊括在整个联盟链生态圈里，通过链上的业务互通形成核心企业-保理公司-券商-供应商的 ABS 融资生态，提高协同业务效率。利用区块链技术，在确保项目数据和资产真实透明的情况下还可以延伸至证券评级测算、资产流转及监控等业务。

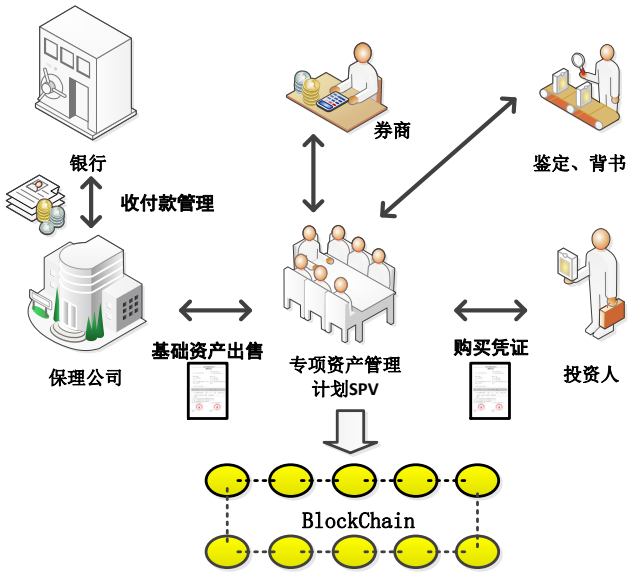

图 8 基于区块链的 ABS 融资流程

以供应链金融中保理商、银行、券商、鉴定机构及背书企业为基础形成了保理 ABS 融资业务，在 ABS 融资中保理商扮演发行者身份，SPV（专项资产管理计划）负责筹划管理发行计划，这期间将受到券商、鉴定机构和背书机构的监管，银行则负责管理保理公司收付款。在进行 ABS 融资过程中所产生的购买合同、管理单据、委托凭据、应收应付款管理凭据均写入区块链账本中，实现了透明化和公开化监督和管理。

2.3.4 技术实现

2.3.4.1 加密与隐私

加密与隐私是联盟链为适应供应链金融业务机密和隐私所必须考虑的问题。加密指的是对区块链账本内容的加密，只有具有权限的用户或节点才能解开相关内容的到数据。隐私指的是对业务发起者的保护，即做到不可追踪和不可关联。

（一）交易内容加密

目前各区块链平台对内容的加密多采用对称加密与非对称加密相结合的方法，将用户进行交易及上传的数据信息进行对称加密，并将随机对称密钥进行非对称加密，从而发送给接收端用户。具体加密解密的示意图如下：

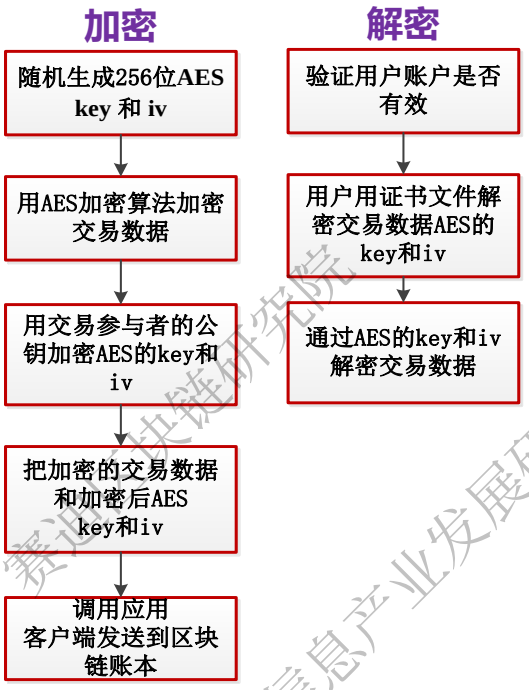

图 9 平台链上内容加密及解密方法示意图

链上业务数据内容的加密满足了平台对节点账本权限的要求，即业务相关用户可以通过自己的私钥解开加密内容，而不涉及业务相关内容的节点和用户则无法看到具体内容。另外，如果业务相关方希望将数据分享给其他节点，只需要将对称随机秘钥用接收方的公钥进行一次加密即可，避免了多次重复的对加密原文进行处理的复杂过程。由于加密算法会消耗大量计算机算力，所以应将平台对交易内容的加密放在平台应用层进行实现，这样做的好处是提高智能合约的处理效率，避免交易的卡顿。此外，采用非对称加密与对称加密相结合的办

法，可以将同一文件分别发送给不同的接收方，避免了传统的利用接收方公钥对内容加密而导致的大量算力消耗，提高了交易处理速度。

（二）交易人加密

基于区块链供应链金融平台要求对交易人的加密做到不可追踪和不可关联，对比了目前区块链平台采用的比较主流的对交易隐私的加密方法，如环签名、群签名、零知识证明等，从灵活性和易用性角度考虑，采用环签名的方法对交易人进行加密保护更具优势。环签名过程中签名者首先选定一个临时的签名者集合，集合中包括签名者。然后签名者利用自己的私钥和签名集合中其他人的公钥就可以独立的产生签名，而无需他人的帮助。

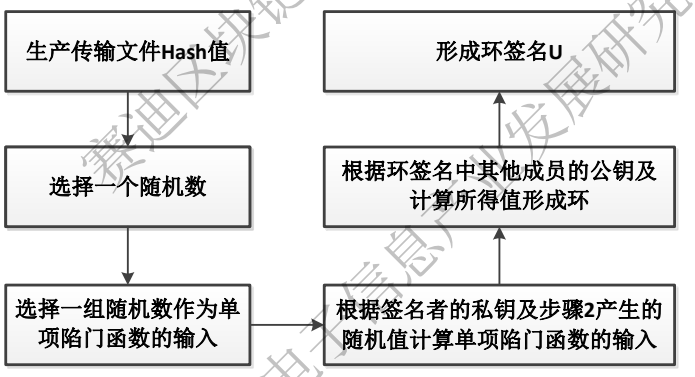

图 10 环签名流程图

环签名是一种模糊签名的方法，环签名的两个核心函数分别是 ring-sign 和 ring-verify，对于消息 m，用户 s 使用一组公开的公钥信息（P1，P2，…，Pr）以及其个人的私钥 Ss，生成签名 U；对于验证者，当其获得消息 m 和签名 U 时，通过 ring-verify 函数判断这个签名是否有效，其输出结果为 0 或 1。供应链金融上的企业无法追踪和关联业务相关方的身份，保护了链上交易的隐私性。

2.3.4.2 权限控制

权限控制是联盟链为适应供应链金融业务场景所添加的必要功能，由于供应链金融上下游企业本身具有不同的职责和功能，如核心企业和保理商等企业的参与度和重要性要大于中小微供应商，为适应供应链金融这样的特点，区块链的权限控制分为两部分，包括了平台节点功能权限控制及节点账本访问权限控制。

节点功能权限的控制是限制节点在网络中的行为权限，如共识、路由、全账本、交易等，在联盟链中一般通过共识机制来限制节点行为权限，如 DPoS、PoA 等共识机制。DPoS 参与共识节点采用社区投票选举制度，同时还会在共识节点中嵌入拜占庭容错共识确保安全性和有效性，这种方法比较复杂，需要较大的社区基础和节点基数。PoA 共识机制同样能够控制加入网络的节点的权限，共识初期形成可设定具有投票权和签名权的核心节点，区块链上的新发生交易需经过核心节点签名后才能够完成上链广播。对于后期新加入的节点，核心节点也可通过签名投票的方式来决定是否允许新节点的加入。整体共识机制流程大体可以分为三个部分：区块的产生、区块的验证和投票机制。

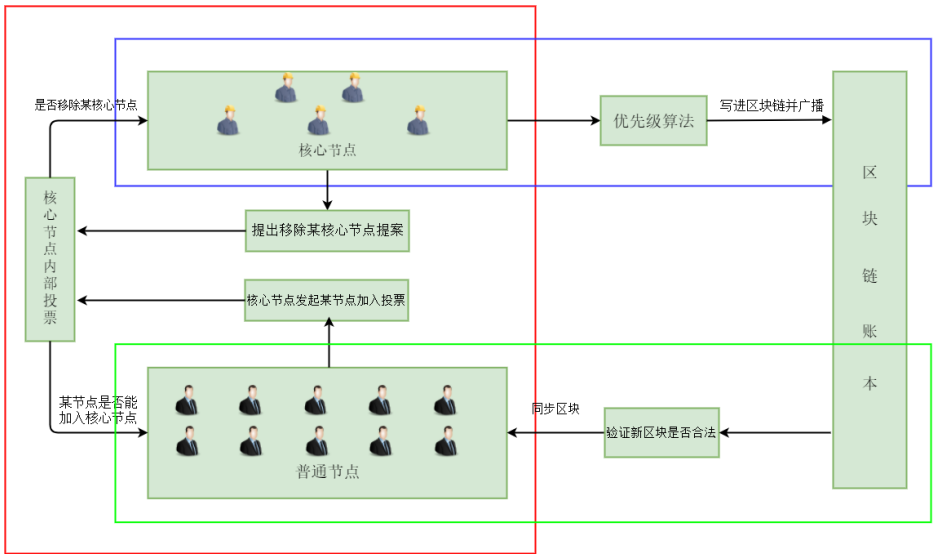

图 11 PoA 共识机制示意图

PoA 共识机制为平台提供了更加严格的权限控制。核心节点有权提出投票将任一节点纳入或移除已有的共识节点，核心节点超过 51%数量同意后才能共识出块。为确保核心节点出块具有平均性，共识机制采用随机算法实现核心节点中随机打包出块，并且限制同一核心节点连续出块次数。PoA 共识机制具有灵活轻量的特点，基于以太坊框架进行部署较为方便和实用。除通过共识机制限制节点权限外，还有如 Hyperledger Fabric 这种底层区块链框架，通过预先设定节点身份角色来控制节点权限，区块链网络中各节点按不同分工规范各节点任务及权限，并协同完成链上业务操作，具体的节点类型划分和流程如下图所示。

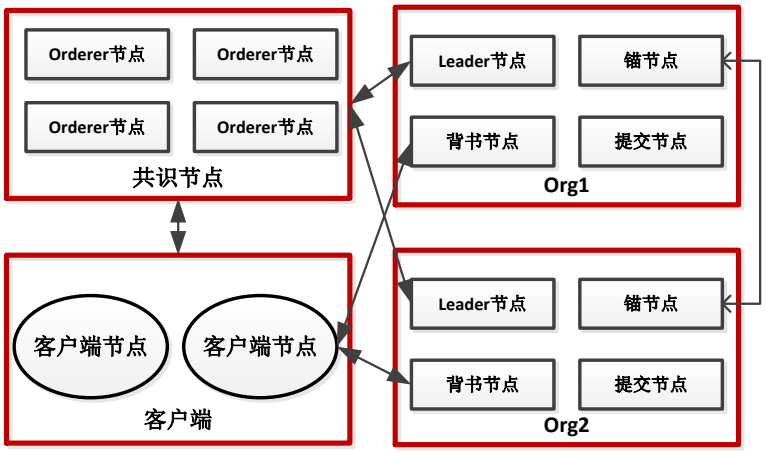

图 12 Fabric 节点功能划分示意图

节点访问账本权限的控制一般有三种方法，一是通过智能合约在上链数据接口中添加允许访问节点，从而限制账本读写权限。二是通过加密算法对账本内容加密，拥有密钥的节点或用户可以解锁加密数据，这一方法在加密与隐私中已经详细介绍。三是 Hyperledger Fabric 提供多链机制划分不同的业务通道，实现账本隔离。

通过智能合约严格管理核心节点的加入与移除，并利用智能合约严格控制上链数据的读写权限，平台节点虽然拥有全部的账本数据，但只能读取权限范围内的账本信息，超越权限外的访问将被拒绝，实现平台账本的权限控制。

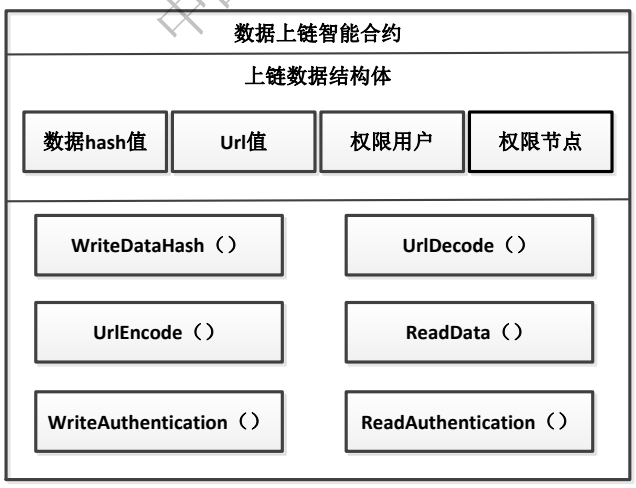

图 13 智能合约主体结构图

此外，利用 Fabric 的多链技术，通过设定不同的交易通道实现账本隔离，是实现账本访问权限的另一种方法。在共识服务上支持多通道消息传递，使得 Peer 节点可以基于应用访问控制策略来订阅任意数量的通道；也就是说，应用程序指定 Peer 节点的子集中架设通道。这些 peer 组成提交到该通道交易的相关者集合，而且只有这些 peer 可以接收包含相关交易的区块，与其他交易完全隔离。

2.3.4.3 数据上链

区块链平台大多通过智能合约将数据写入区块链中，如以太坊基于的 Solidity 语言的智能合约、Fabric 的 ChainCode，都提供了业务数据上链的功能。报告重点介绍利用以太坊智能合约的数据上链流程，经典以太坊只是涉及交易及账户信息，不涉及企业业务数据信息，区块链系统包含企业的实际业务数据，这些敏感的信息一旦泄露会造成严重后果，所以区块链系统需要先对数据进行加密然后存储到区块链系统。对于每笔业务数据，都只有交易参与双方可见，或是经交易双方同意后将数据查看权限分发给其他用户。以太坊提供了与智能合约相关的合约地址机制，通过智能合约写入区块链的数据将存储在合约地址下以供后续的查询服务。

将业务数据上链能够扩宽供应链金融业务范围，为用户提供数据存证、单据业务状态流转、数据溯源等功能。平台业务数据分为单据、合同、文档、交易信息及图片等多媒体文件，方案依据数据文件类型及数据大小进行分类存储。涉及业务单据状态流转、签发及重要单据

存证的数据不论大小都将进行数据加密后上链，不涉及重要业务单据存证且占用过大存储空间的数据将原价存入本地关系数据库，同时将文件进行哈希计算后加密上链，具体流程如下图：

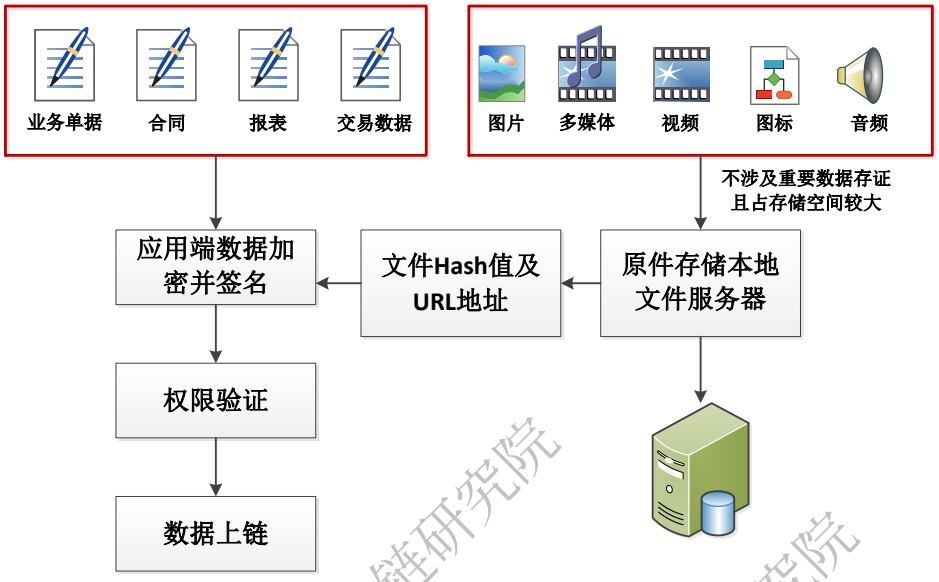

图 14 数据上链流程图

不涉及重要存证信息且占空间较大的数据需要先将数据原文存入文件服务器，然后读取文件的 hash 值和存储地址，并对文件的 hash 值和存储地址进行加密。加密后的哈希值及存储地址通过智能合约写入区块链。此外，消息发送者发送加密数据到区块链系统，区块链系统验证交易发送者是否有权限，如果有权限，则数据上链成功，否则提示权限不足，上链失败。

2.3.4.4 区块结构与存储

（一）区块结构

区块的结构设计与区块链的交易流程、共识机制、账本类型密切相关，如以太坊、比特币等区块链框架采用 PoW 共识机制，其区块

头需要添加与共识机制相关的大量参数，如 Hyperledger Fabric 区块链框架其交易流程复杂，需要多方签名最后写入账本，从而导致区块体结构较为复杂。

以以太坊基于 PoA 共识的联盟链框架为例，其区块结构是由以下部分组成的：区块整体信息片段组成的集合称为 block header，即区块头；由区块业务或交易信息（transaction）组成的 block body，即区块体，这部分占据区块大小的主要部分；剩余部分为称作 ommers，存储着平台叔块基本信息。平台具体区块结构如下图所示：

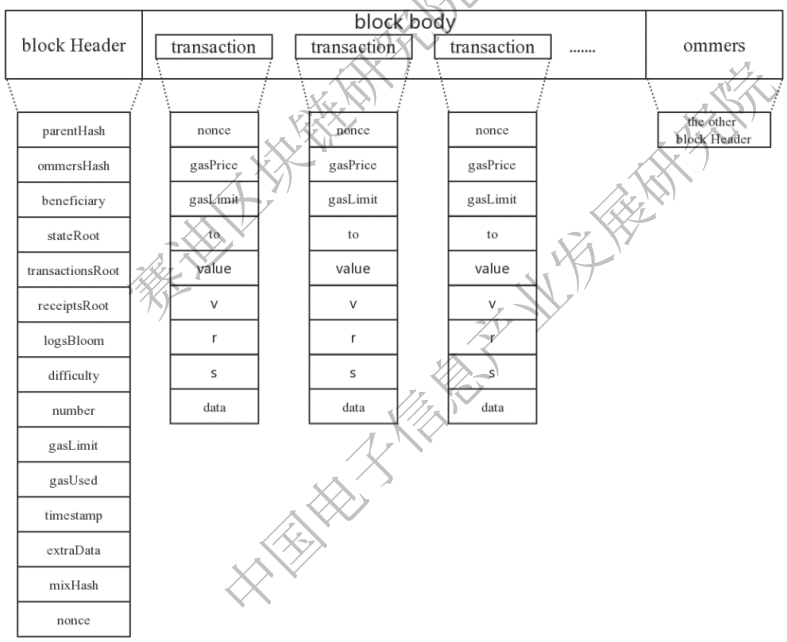

图 15 平台区块结构图

区块的验证主要通过验证区块头的方式实现。由于平台采用以太坊 PoA 的共识机制，区块的结构与以太坊基本一致，在部分参数包含的意义所有不同。平台区块头包含的重要参数信息如下表：

表 1 区块头重要参数

参数名称	参数意义
parentHash	父区块头的 Keccak256 位哈希
ommersHash	在 PoA 共识机制里为固定值

Beneficiary	被提名为核心节点的节点地址，默认为 0，仅在投票时修改。
stateRoot	所有交易被执行完且区块定稿后的状态树根节点的哈希
transactionsRoot	由当前区块中所包含的所有交易所组成的树结构（transaction trie）根节点的 Keccak256 位哈希
receiptsRoot	由当前区块中所有交易的收据所组成的树结构根节点的哈希
difficulty	区块优先级，优先级值为 1 或者 2。同一个高度的区块，只有一个核心节点的优先级是 2，且 2 的优先级最高
extraData	存储当前委员会集合矿工地址
nonce	提名分类，添加或删除(0xffffffffffffffff 表示加入，0 表示删除)

区块体主要由各个交易组成，ommers 用于保存孤儿块的区块头，PoA 共识下的核心节点均为可信任节点，系统并没有对矿工进行激励措施，ommers 部分没有实际意义。

（二）区块存储

区块的存储一般采用 LevelDB 数据库，其中，key 一般与 hash 相关，value 一般是要存储的数据结构的 RLP 编码，且区块存储时将区块头和区块体分开存储。对于区块头存储格式中 key 由区块头前缀、区块号（uint64 大端格式）、区块 hash 构成，value 是区块头的 RLP 编码。区块体的存储包括 key 由区块体前缀、区块号（uint64）、区块 hash 构成，value 是区块体的 RLP 编码，二者通过 key 值的前缀进行区分。具体流程如下图：

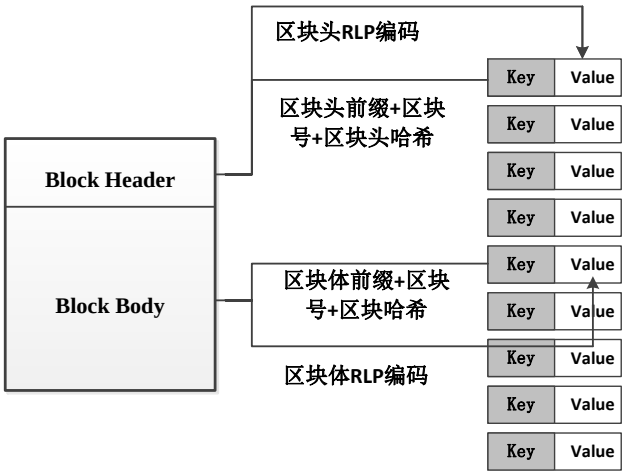

图 16 区块存储流程图

在数据写入时先将数据写入 Batch 后再写入 LevelDB 数据库，这样做的好处是减少数据的交互次数，提高数据存储效率。此外，目前主流联盟链平台都采用多种类账本存储机制，如 Fabric 采用了历史账本、文件账本、状态账本三类，为用户提供了多种数据库快速查询机制，为上层应用提供了更多可利用接口。

3. 区块链+供应链金融企业案例

青岛地铁金控、齐鲁银行青岛分行以及闪收付信息技术三方共同建设了“地铁齐鲁闪收付产业链金融——助力城市轨道交通建设发展”项目，围绕地铁集团的核心企业信用，借助齐鲁银行服务中小企业的先进经验和融资管控、支付清算以及账户服务方面的优势，发挥闪收付公司科技创新的实力实现互惠共赢金融模式。项目实施过程中，逐步暴露出传统中心化供应链金融系统信息不对称、交易风险高、交易效率低等问题亟需解决。

3.1 整体架构

区块链作为新一代信息技术能够助力供应链金融发展，通过多中心化的分布式结构实现了信息同步与共享，通过链式共享账本解决数据追溯与信息防伪，通过密码算法有助于关键数据保护和授权访问，通过智能合约的编程特性规范业务交易，丰富业务模式和应用场景。现有供应链金融平台目前的业务范围包括了保理、快信、债券转让及现金折扣四大业务板块，采用区块链技术将业务流程及数据进行数据存证、数据共享及业务协同办理，具体框架设计如下图。

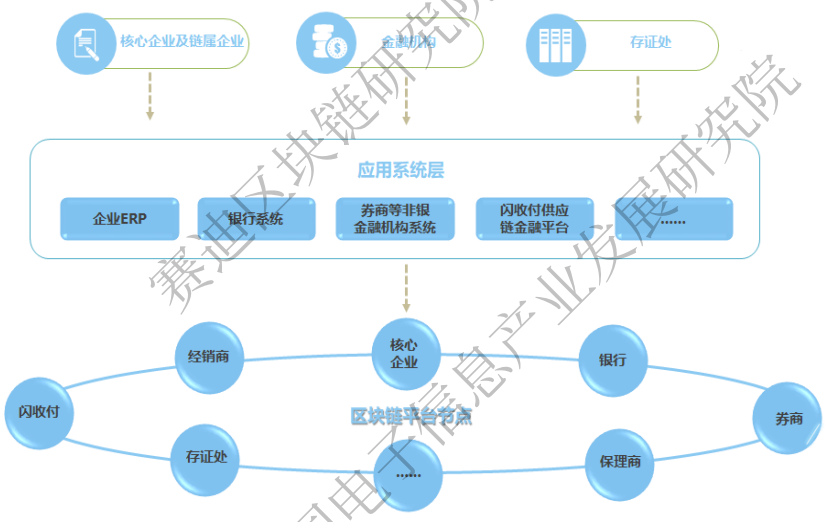

图 17 基于区块链的供应链金融平台整体系统框架图

整个平台架构自上而下分为用户层、应用系统层、区块链系统层三个层次，基于区块链的供应链金融平台框架是按照对现有平台最小改动原则设计的。在区块链系统层，区块链作为底层分布式数据库，存储平台业务流程产生的单据、合同、发票等重要信息，利用区块链分布式存储、不可篡改、可追溯等特点，提高平台用户对平台的信任度，保证核心数据的安全性和完整性。在应用系统层，区块链有独立

的应用服务器系统，其作用首先是与原有平台系统进行数据交互，其次是为金融机构及核心企业定制开发区块链的应用平台。在用户层，平台将覆盖多级供应商、核心企业、银行、保理公司、券商及公正单位等，为用户开发专有的去中心化应用程序（DApp），包括 B/S 架构与 C/S 架构两种模式，为用户提供友好的使用感受。

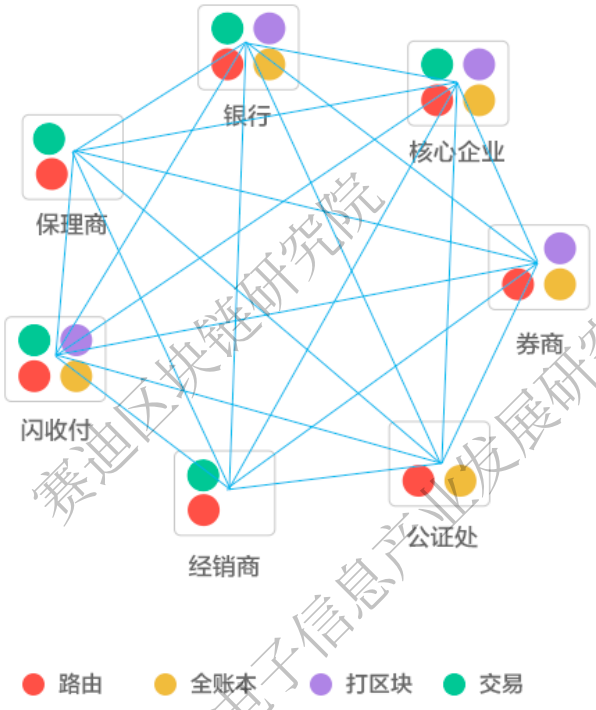

图 18 基于区块链的供应链金融平台网络结构图

区块链系统节点类型按照业务类型分类可以分为闪收付节点、银行节点、券商节点、公正节点、保理商节点、经销商和核心企业节点，按照节点功能及权限分类可以分为核心节点和普通节点，其中核心节点在配置 PoA 共识机制时进行绑定，并在后续发起投票并获取 51%核心节点通过后添加或移除其他核心节点。各个区域节点通过网络隔离设备后进行通信，闪收付核心节点可以为供应商提供账号（公私钥），

供应商以闪收付节点用户的身份加入区块链网络。保理商和经销商只具有交易和路由的功能，核心企业可以为下属的采购部门及财务部门划分账号，券商虽然是核心节点，但不具有交易的功能，公正节点虽具有全部账本但无法参与共识。

3.2 基本功能

基于区块链的供应链金融平台采用以太坊作为区块链系统的基本框架，整体架构至下而上分为数据层、网络层、共识层、合约层、接口层、业务层以及应用层六部分。数据层包括了区块结构、加密算法以及数字签名等技术，网络层主要以 P2P 网络为主，辅助功能包括了消息机制和验证机制，共识层采用了基于 Clique 共识算法的 PoA 共识机制，合约层指的是以太坊智能合约与以太坊虚拟机（EVM），接口层包括了以太坊提供的 API 接口和目前较为流行的 Web3.js 开发包，业务层包括了账户管理、节点管理和交易管理三大模块，平台业务核心是账号管理模块，所有交易及核心节点的投票流程都需要通过账号管理模块的关联认证后才能实现，具体的业务流程如下图：

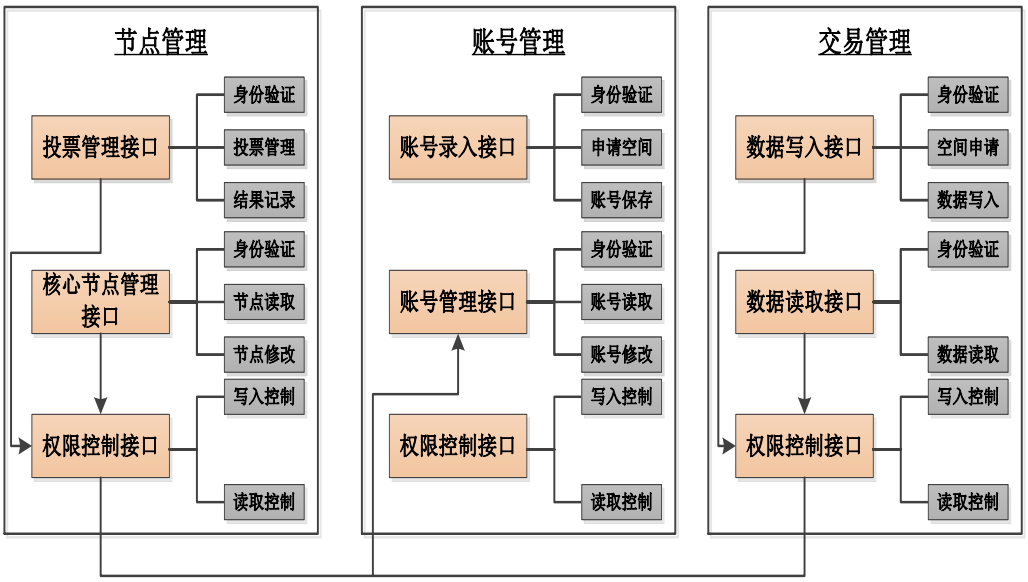

图 19 平台业务流程图

平台应用层包括了数据存证、债权确权、ABS 融资、数据共享、业务协同及单据审批等业务。区块链系统整体结构如图所示：

图 20 区块链系统架构图

与经典以太坊相比，平台采用以太坊基于 PoA 共识机制的联盟链基本框架。平台更加侧重权限控制及商业隐私，而取消了公有链基本的激励机制和代币等功能，与经典以太坊对比如下表所示。

表 2 经典以太坊与基于区块链的供应链金融平台功能对比

	经典以太坊	供应链金融平台
接入方式	只要有以太坊客户端，就可以接入	需要联盟核心成员同意才能加入
共识机制	PoW	PoA
账户体系	以太坊有两种类型的账户：外部账户（由私钥控制的）和合约账户（由合约代码控制）	核心账户和普通账户，账户有锁定功能，锁定的账户不能进行操作区块链。
权限	以太坊不带有权限功能	带有权限功能
数据安全	上链的数据，所有用户可见	上链数据只有交易参与者可见
交易	每发送一笔交易都需要 value（以太币金额），gas（本次消费消耗燃料）	不包含以太币和 gas，只包含业务数据
区块生成时间	15 秒	30 秒
TPS 峰值	实测大约 50 笔/秒	实测大约 1216 笔/秒

平台继承了经典以太坊的数据结构、数据模型、存储机制、智能合约及网络结构等基本功能，但在共识机制上采用了更加适合联盟链的 PoA 共识机制，增加平台的节点接入限制和节点功能权限控制，并且增加了对账户多种限制操作。在加密隐私方面平台采用对称加密、非对称加密及环签名多种加密算法结合的方法在保证平台交易隐私的情况下使平台更加商业化。同时平台配置可调节出块时间、削弱了 Gas 对平台交易的影响，并在实测中 TPS 性能远高于经典以太坊。

共识机制。区块链系统基于 PoA 委员会选举共识机制生成核心节点参与共识。PoA 是由一组授权节点来负责新区块的产生和区块验

证，是以太坊针对部分商业化许可区块链需求推出一种低成本、高效率的共识机制。PoA 共识初期形成可设定具有投票权或者签名权的认证节点，区块链上的新发生交易需经过认证节点签名后才能够完成上链广播，对于后期新加入的节点，认证节点也可通过签名投票的方式来决定是否允许新节点的加入。

加密与隐私。基于区块链的供应链金融平台对加密及隐私的要求包括两点，首先是要保证平台交易内容、单据内容加密，即平台交易过程中涉及到的成员能够通过解密看到交易内容，不涉及交易的成员无法看到具体的平台交易内容；其次，平台需确保交易参与者不可追踪和不可关联，即对于任何交易，无法追踪其发送者是谁，对向外发送的两笔交易，其他人无法证明其是否发给同一个接受者。

智能合约。平台提供智能合约功能，智能合约在平台的作用是支撑平台交易及业务数据上链，平台区块链系统采用以太坊基本框架进行改造，并沿用以太坊提供的智能合约功能。在以太坊中通过 EVM（Ethereum Virtual Machine，以太坊虚拟机）实现智能合约的执行。EVM 虚拟机是以太坊的一个重要创新，EVM 是由许多互相连接的计算机组成的，任何人都可以上传程序，并让这些程序自动执行，同时保证所有智能合约的状态总是可见的。

数据上链。基于区块链的供应链金融平台业务数据的上链是通过平台智能合约实现的，在智能合约中严格控制链上数据的读写权限，业务数据上链的功能能够扩宽平台业务范围，为平台用户提供数据存证、单据业务状态流转、数据溯源等功能。

参数配置。为适应业务体量的变化并保持平台高效率运行，平台能够灵活配置出块时间、区块大小及单笔业务内容大小等区块链基本参数。

系统安全。平台具有较高的安全性，具体涵盖范围包括了区块链应用程序端、网络传输端、共识机制、智能合约以及数据存储安全等领域。

3.3 功能亮点

3.3.1 高扩展性

基于区块链的供应链金融平台是以太坊为框架搭建的联盟链，具有较高的扩展性和兼容性。供应链金融产业结构较为复杂，除核心企业及中小微供应商外，还有金融机构、保理公司、担保公司及券商等多种类型企业。任何想加入平台的企业，只要分属上述类型中，都能够以普通用户的形式进行接入平台应用系统，减少平台中节点的数量，同时企业以用户身份接入平台也为中小微企业降低接入成本，能够吸引更多的企业加入平台。

3.3.2 高易用性

供应链金融是典型的多主体参与，行业结构比较复杂，在通过区块链技术进行信用延伸及传递的过程中同样需要保证商业机密及隐私性，允许设计交易的任何团体在同一许可网络隔离并共存。与 Hyperledger Fabric 采用组织和交易通道划分的原理进行隔离不同，平

台采用对业务内容加密及业务相关方加密的两种方法实现机密性和隐私性。针对业务数据，平台在数据上链前采用非对称加密结合对称加密的方法对数据进行加密，确保业务相关方才能解密数据；对业务相关人员采用环签名的方法进行隐私性保护。

3.3.3 高安全性

平台对共识层、合约层、网络层及数据层进行全方位的安全保护。平台在共识层采用 PoA 共识机制可以限制恶意节点参与共识出块，PoA 共识机制支持在全网核心节点中发起移除恶意节点的投票，投票通过后恶意节点将自动被冻结；在合约层将消耗算力较多的工作转移至应用层进行处理，并在开发智能合约时还加入了检测函数，对智能合约进行初步的代码逻辑和质量的检测；在网络层加入隔离网关及防火墙并严格控制用户接入；在数据层，通过账本共享及加密算法确保数据的连续性、安全性、完整性。

4. 区块链+供应链金融发展前景与趋势

4.1 区块链供应链金融应用的示范作用有助于区块链技术在更广泛的场景落地

以 TCP/IP 协议簇为基础的传统互联网技术解决了信息传输的效率问题，并没有解决信息的信任问题。在涉及多方主体协作的场景下，除了需要建设信息系统，保证数据信息的互联互通，还需建立中介机构以及额外的规章制度和措施以解决多方信任问题，这极大增加了各

方沟通和协作成本。区块链技术本质上是一种分布式账本数据库，它通过链式结构验证和存储数据，通过分布式共识生成和更新数据，通过密码学保证数据传输和访问的安全。区块链技术通过建立多节点参与共识、构建无需中介的信任机制，使得各参与主体从技术层面共同维护一本账本，从而在保证数据信息可信的前提下，极大降低业务协作过程中的沟通和人力成本。供应链金融就是以供应链为基础，银行将核心企业和上下游企业联系在一起提供灵活运用的金融产品和服务的一种融资模式，其整个融资过程涉及银行、供应链核心企业及其上下游企业为实现商流、信息流和资金流的统一而带来的频繁协作，区块链技术应用于供应链金融领域，充分发挥了区块链作为“信任机器”的优势，即区块链从技术层面保证链式账本所存储数据无法被恶意篡改，有助于解决多方业务协作场景中为维护信用而导致的成本居高不下的问题。

区块链技术在供应链金融领域应用落地，解决了供应链金融领域包括信任难传递、多方沟通协作效率低等诸多问题，反映了区块链技术易于构建多方业务协作平台，主要体现在：一是区块链降低系统对接复杂性，跨系统间的数据交互统一在区块链账本层实现；二是资产上链有助于提高数字资产流动性，方便价值传输；三是区块链有助于保证数据信息在安全的情况下进行全流程监控；四是多方协作可信，使得跨主体间业务协作变得极为方便。根据区块链技术特点，对于协作效率低下，数据信息需存证，需要多方记账等场景下，区块链技术都有用武之地。因此，区块链+供应链金融对于区块链技术应用于更

多类似场景具有重要的示范意义。

4.2 区块链+供应链金融市场规模将爆发式增长

区块链技术使得供应链数据变得真实可信、透明，构建可信的多方协作环境，有助于释放和传递核心企业信用，降低产业成本，优化融资成本和效率。鉴于区块链技术在解决供应链金融痛点方面具有独特的优势，传统企业、区块链初创企业、商业银行、B2B 平台、供应链公司、物流公司等纷纷布局区块链+供应链金融领域。初创区块链企业方面，例如复杂美、布比、趣链、秒钛坊等区块链企业均已研发出区块链供应链金融平台，提供仓单质押融资、应收账款融资、票据融资、授信融资等解决方案，并与相关企业展开合作和实现应用落地。传统互联网巨头方面，腾讯构建了区块链 BaaS 开放平台，并重点布局供应链金融领域。商业银行方面，农业银行推出基于区块链的涉农互联网电商融资系统-“e 链贷”，并完成线上订单支付贷款；浙商银行基于趣链科技底层区块链技术平台推出了基于区块链技术的企业“应收款链平台”。传统企业方面，广东有贝基于腾讯区块链 BaaS 平台建立区块链在大健康产业的供应链金融解决方案；丰收科技集团引入区块链、大数据等前沿技术，将供应链上所有行为（包括开闭、交易等）上链存储，支持资产的登记、转让、融资和兑现。未来，随着相关企业加速布局区块链+供应链金融领域，区块链+供应链金融的市场规模将爆发式增长，应用效果将快速显现。

4.3 供应链金融场景下区块链与大数据、物联网等技术融合发展成为趋势

供应链金融试图通过供应链中主体间信用的高效传递，打通信用流转，以更好的盘活资产，解决供应链中面临的中小企业融资难、融资贵的问题。然而，传统供应链金融并没有很好解决多主体参与情况下，协作机制缺乏、信息不对称、信用机制不完善、风控成本过高等问题。其关键点在于并没有通过某种工具和手段保证信息的生成、存储、流通、分析过程中的可信性、有效性和透明性。区块链、大数据和物联网融合发展正在成为趋势，有助于解决供应链金融场景下信息不可信和风控成本过高等问题。一是业务流程上融合。例如数据上链环节，物联网环境下通过传感器实时采集相关产品位置、温度、湿度、损坏程度等各项信息，得到供应链参与节点共识后数据上链，并进一步通过大数据可视化技术实施展现当前业务进展和流程，通过大数据风控建模实时评估风险，有助于金融机构实时监控业务流程，降低业务风险。二是技术实现与部署上的融合。基于区块链技术平台，通过提供 API 接口，集成现有信息系统包括物联网和大数据分析平台模块，有助于从技术层面形成多系统协作，提高了信息系统协作效率，降低信息时滞和风控成本。

大数据、区块链、物联网等信息技术有助于有效深入洞察供应链金融参与主体的行为，解决资金和资产对应匹配的唯一性和真实性等问题，实现物流、商流、资金流和信息流统一。大数据、区块链、物联网等信息技术正深入融合，推动供应链金融走向更加自动化和智能化的发展道路。

4.4 智能合约技术将深入应用于供应链金融场景中

当前，区块链+供应链金融场景中，智能合约在应用深度上还有所欠缺。随着智能合约技术成熟，以及其法律效用逐步得到社会认可，智能合约将深入应用于供应链金融场景中，有助于供应链金融业务中商品信息交互、合同协议履约的自动化完成。一方面，企业债权流转过程记录在链条上，通过智能合约的形式约定规则，使不同层级的供应商之间的债权可以拆分和流转，同时确保债权的真实性和不可篡改性。另一方面，通过将供应商之间约定结算规则写入智能合约，一旦执行条件满足，合约中的规则自动化执行，实现交易方约定的付款时间按时进行资金的自动化清算，保障还款来源，减少人为交互和操作失误，提升业务效率。

5. 总结

随着区块链技术体系不断完善，国内资本对区块链行业投融资力度逐步加大，区块链企业商业模式和场景逐步清晰，区块链技术应用落地速度加快，区块链市场将进入快速增长阶段，产业规模将引来爆发式增长。经过2016年和2017年区块链概念普及、技术逐步完善和场景探索，2018年进入区块链应用相对快速落地的阶段，包括金融、供应链、文化娱乐、社会公益、教育就业等多个应用场景的区块链技术应用都将逐步走进人们生产生活，区块链产业规模将迎来快速增长。

供应链金融领域，通过行业企业与区块链技术服务企业的合作，一批基于区块链的供应链金融服务平台相继启动或上线，成为我国供

应链金融业务创新的重要方向。本报告介绍了完整的区块链+供应链金融的解决方案，并在生产中进行实际业务运转，为区块链在供应链金融领域的应用提供了典型案例和技术支持。