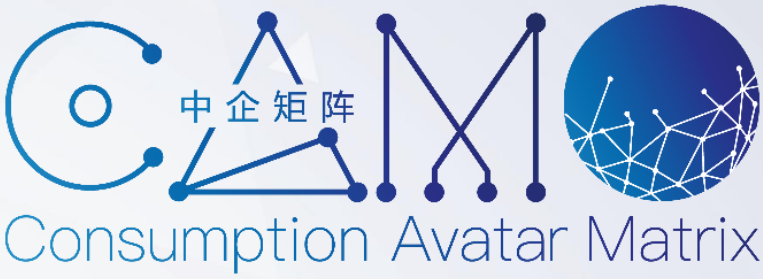

Consumption Avatar Matrix (CAM)中企矩阵

白皮书

V1.8

目 录

摘要

本文主要介绍中企矩阵（CAM）区块链的系统架构、核心功能、系统特色与优势、典型应用案例等。中企矩阵致力于打造中资企业深度融合商业生态环境的区块链解决方案。已取得了多项技术突破和创新，在性能、扩展性、安全和运维等方面形成独有的特色和优势。中企矩阵已在多个领域应用实践，包括数字资产、贸易金融、股权债券、供应链溯源、联合征信、公示公证、物联网共享、数据安全等。通过长时间在各行业中累积了大量的商业应用案例，致力于打造中资企业深度融合商业生态环境的区块链解决方案。

一、理念背景

1.1. 区块链历史

区块链的诞生，标志着人类开始构建真正可以信任的互联网。通过梳理区块链的兴起和发展可以发现，区块链引人关注之处在于，能够在网络中建立点对点之间可靠的信任，使得价值传递过程去除了中介的干扰，既公开信息又保护隐私，既共同决策又保护个体权益，这种机制提高了价值交互的效率并降低了成本。

1.2. 区块链现状

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，是一种基于分布式的稳定、可信、安全和高效的数字台账（会计）技术。其中共识机制是区块链网络中实现不同节点（提供存储服务）之间建立信任、获取权益（实现存储数据的收益和目的）的一种数学算法，确保了网络的稳定与有序发展。

区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。联合国、国际货币基金组织，以及美国、英国、日本等国家对区块链的发展给予高度关注，积极探索推动区块链的应用。中国政府也已经在 2016 年 12 月将区块链技术列入《国家信息化规划》（十三五规划）。

目前，区块链的应用已延伸到金融、能源、人工智能、农业、文娱 IP、大数据等多个领域。

1.3. 区块链的核心技术

区块链技术不是一个单项的技术，而是一个集成了多方面研究成果基础之上的综合性技术系统。我们认为，其中有四项必不可缺的核心技术，分别是：共识机制、密码学原理、分布式数据存储和智能合约。

- **共识机制**

所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、

行为或流 程达成一致的过程。共识机制是指定义共识过程的算法、协议和规则。区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数” 并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。

- **密码学原理**

在区块链中，信息的传播按照公钥、私钥这种非对称数字加密技术实现交易双方的互相信任。在具体实现过程中，通过公、私密钥对中的一个密钥对信息加密后，只有用另一个密钥才能解开的过程。并且将其中一个秘钥公开后（即为公开的公钥），根据公开的公钥无法测算出 另一个不公开的密钥（即为私钥）。

- **分布式存储**

区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。 跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。

- **智能合约**

智能合约是指一份能自动执行本需要手动才能完成任务的协、议。智能合约就是任何能自行执行部分功能的协议。例如，一份能自动计算合同当事人待付金额，并安排支付这笔金额的合约。

智能合约将减少协议执行过程中的人工干预。

智能合约这个术语至少可以追溯到 1995 年，是由多产的跨领域法律学者尼克·萨博（Nick Szabo）提出来的。他在发表在自己的网站的几篇文章中提到了智能合约的理念。他的定义如下：“一个智能合约是一套以数字形式定义的承诺（promises），包括合约参与方可以在上面执行这些承诺的协议。”

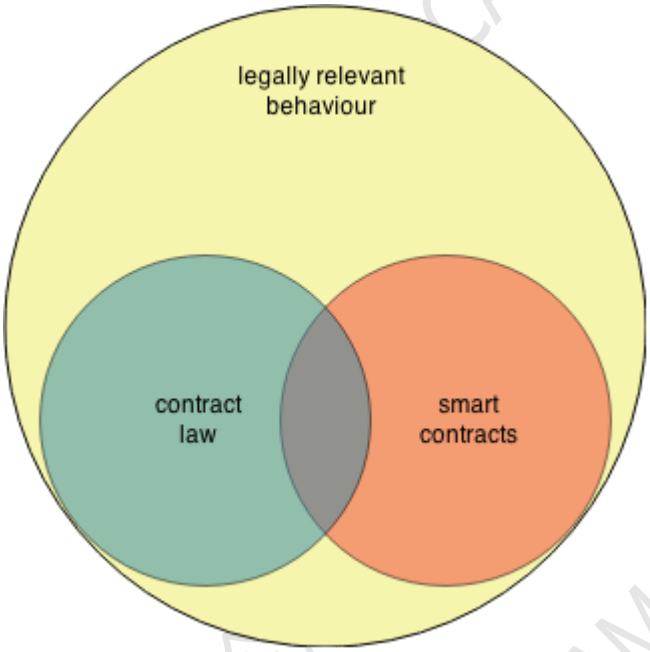

图 1.3 智能合约与法律的关系

1.4. 区块链技术发展趋势：应用领域急速扩张

比特币自 2009 年出现并开始流通至今，总市值已超过 300 亿美元，成为区块链技术在数字货币领域的成功应用。以太坊随后引入智能合约，把复杂的合同规则以代码的方式编程到区块链，在达到约定条件时自动触发执行， 为区块链的应用开拓了更广阔的领域；把区块链的承载对象，从比特币时代的电子货币交易记录，分别推广到了除金融类应用外，任何对信任、安全和持久性要求较高的应用场景——比如资产注册、投票、管理和物联网等领域。

作为区块链分布式实现的重要组成部分，共识机制经历了充分发展，先后产生了以下几个主要共识机制：

POW：Proof of Work，即工作量证明共识机制，亦称挖矿机制。比特币首先采用了 POW 机制来主导 Block 生成，节点通过不断的尝试计算每个 Block 帐本内容对应的 Block Hash 值，使之满足特定的条件，即由 N 个零作为前导。这将增加生成 Block 的难度，使迅速生成更长的恶意支链替换正确支链的危险性大大降低，但同时也造成了大量矿机运算资源的浪费。

POS：Proof of Stake，即股权证明共识机制。这是 POW 的一种升级的共识机制，根据节点拥有代币的多少和持有代币的时间，来控制挖矿时间的长短；它可以有效的降低挖矿时间，但是仍然没有避免矿机运算资源浪费的问题。

DPOS：Delegated Proof of Stake，即委任权益证明共识机制，它的原理是代币通过投票选出一定数量的节点，为它们完成验证和记帐的工作，这种共识机制可以大大减少参与记帐和验证的节点数量，达到快速的共识验证，但是这种机制也需要依赖代币的存在，使某些不需要代币存在的应用受到限制。

PBFT：Practical Byzantine Fault Tolerance，即实用拜占庭容错算法共识机制。它是一种消息传递的一致性算法，通过三个阶段达成一致性，确定最终的区块产生，假如有 3f+1 个节点，这种算法机制决定了可以容忍 f 个错误节点的存在，而使一致性结果不受影响，这种机制可以脱离币的存在，共识节点可由参与方与监管方组成，2-5 秒的共享延时也基本能满足商用要求。

各种共识机制在各自的业务场景和技术手段上都有自身的考虑和意义，相互之间有不同方面的改善和提升，又有不同方面的劣势，似乎没有最优的共识机制；实现各种共识机制的可插拔应用，能够根据具体的应用场景灵活选择合适的共识机制，最优化区块链的应用，才是打通更多应用领域的最佳途径。

1.5. 分布式商业生态环境

中企矩阵(CAM)从商业的最小元素（人、物、钱）出发，将每个元素进行数字化，进而建立一种通用的链接，通过不同的智能合约　　来建立映射现实商业的各个协同活动，提供与之匹配的相关的价值流动工具和体系，进而演变出基于这种协同模式上的全新的商业模式，逐步构建出一个运行在区块链之上的分布式的新型产业集群。

1）将目标数字化，并且是通用型数字化，这个数字化的结果在技术上可以被所有参与方接受、使用；

2）在不同的数据对象之间通过智能合约来建立关系型连接；

3）用抽象的智能合约配合相应的权限进行多层智能合约的组合建模和定制化，来映射现实商业世界的各个不同的商业活动；

4）全新的数字资产（CAM Token(CAM)）提供高速价值传导的支持；

5）进而演变出全新的万物可信互联的商业模式；

6）不同的商业模式互相融合贯通，构建分布式的商业生态；

通过这个方法，可以将行业的上下游企业、用户、政府的资源和信息最大程度的整合在一起，让各方之间的协同合作做到真正的数字化、系统化操作，相对应的价值流转同步执行，从而使行业甚至整个社会整体成本降低，效率提高，资

源可以被分布式的最优化部署，这必然会带来各种新的商业模式的诞生。区块链 3.0 时代将颠覆我们现在所有的认知，我们将跨入一个全新的时代，一个不再有信任危机的时代。

二、中企矩阵(CAM)的管理模式

2.1. 经济模型

CAM 中内置两种原生代币，CAM 和 GAS。

CAM 是管理代币，总量 2 亿份，用于实现对 CAM 网络的管理权。管理权包括投票进行记账人选举，CAM 网络参数更改等。CAM 的最小单位为 1，不可再分割。

GAS 是燃料代币，最大总量上限为 2 亿，用于实现对 CAM 网络使用时的资源控制。CAM 网络对代币转账和智能合约的运行和存储进行收费，从而实现对记账人的经济激励和防止资源滥用。GAS 的最小单位为 0.00000001。

在 CAM 网络的创世块里，2 亿份 CAM 已经生成，而 GAS 尚未生成，数量为零。2 亿份 CAM 所对应的 2 亿份 GAS，将通过一个衰减的算法在约 22 年的时间内逐步生成至 CAM 管理代币的地址中。CAM 管理代币转入新的地址后，之后的 GAS 也将在新的地址生成。

CAM 网络将通过投票设置一个阈值，对一定量的转账交易和智能合约运行存储免收 GAS，以提升使用体验。当发生大量垃圾交易时，可以通过 CamID 来优先处理具有合格身份的交易和智能合约。没有合格数字身份的交易和智能合约可以通过支付 GAS 来获得优先处理。

2.2. 分发机制

2.2.1. CAM(CAMToken）的分发

CAM(CAMToken）的 2 亿管理代币分为两部分

1)第一部分：1.02 亿（总量 51%）用于分发给社区，包含私募和公开售卖形式投放市场，按轮次和比例分发，主要为发展提供资源和资金支持，包括开发、市场、法务、代码安全审计、财务、第三方审计等方面。

2)第二部分：0.98 亿（总量 49%）由 CAM 理事会管理，用于支持 CAM 网络的长期开发、运维和生态发展。该部分的 CAM 处于锁定期，锁定期结束时刻不早于 CAM 网络运行满 2 周年，且会按照每年 20%比例逐步解除。按如下比例分配使用：

a)2000 万份（总量 10%）用于创始团队、最早期优质企业、开发团队等在 CAM 发展过程中作出了关键贡献的团体；

b)4000 万份（总量 20%）用于进行持续优质落地企业的开发、福建省区块链协会\CAM 中企矩阵生态建设、福建省商会重点资源企业的应用落地和数字资产置换、两岸新兴科技孵化中心区块链项目的孵化；

c)2000 万份（总量 10%）用于交叉投资 CAM 公有链上的其他优质项目，所获

得代币归属于 CAM 理事会，并仅用于 CAM 项目；

d)1800 万份（总量 9%）用于支持 CAM 中企矩阵相关学术研究、教育及市场扩张的培训费用；

e)每年使用的 CAM 原则上不得超过 3000 万份。

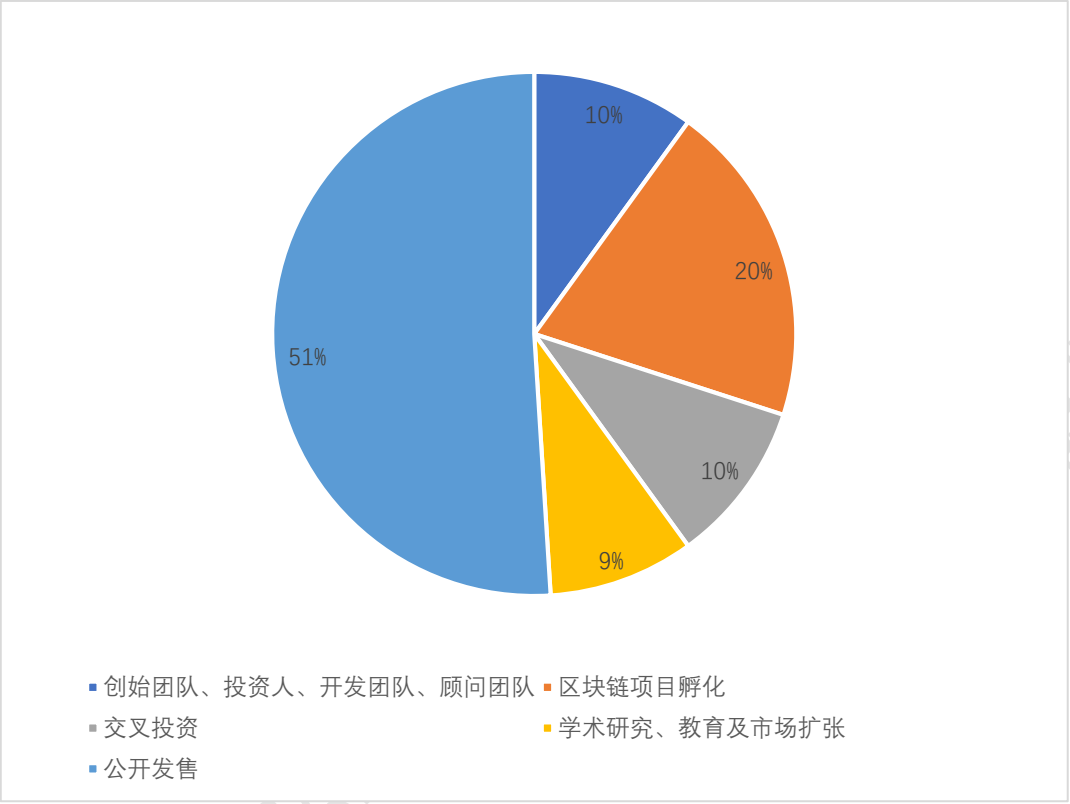

图 3.2 CAM 分配方案

2.2.2. GAS 的分发：

GAS 伴随着每个新区块的生成而产生。GAS 初期总量为零，伴随着新区块的生成逐渐增多，直至约 22 年后达到总量上限 2 亿。CAM(CAMToken) 每个区块的间隔时间约为 15-20 秒，200 万个区块约合 1 年时间。

第一年（实际为 0-200 万个区块），每个区块新生成 16 个 GAS；第二年（实际为第 200-400 万个区块），每个区块新生成 12 个 GAS；以此类推，每年递减 1 个 GAS，直至第 8 年递减至每个区块新生成 2 个 GAS；自此保持每个区块新生成 2 个 GAS 直至约 22 年后的第 4400 万个区块，GAS 总量到达 2 亿，则停止伴随新区块生成 GAS。

按照这样的发行曲线，第 1 年会有 16% 的 GAS 被创造，前 4 年会有 52% 的 GAS 被创造，前 12 年 80% 的 GAS 被创造。这些的 GAS 都会按照 CAM(CAMToken) 的持有比例，记录在 CAM(CAMToken)地址上。GAS 持有人可以在任意时间进行发起一笔认领交易，将这些 GAS 认领到 CAM(CAMToken) 的地址上。

三、中企矩阵区块整体架构

中企矩阵的架构思路是从应用需求出发，对每一个技术架构层进行标准化的抽象，让每一层都具备独立的普适性，并且每层的模块又可以进行快速有效的组合，从而用标准的单元模块组合成万千变化的应用。

中企矩阵区块链方案的整体架构分成三个层次：底层平台、服务层、应用层。底层平台提供区块链基础服务的功能。服务层在底层平台之上构建高可用性、可扩展性的区块链应用基础平台产品，其中包括共享账本、鉴证服务、共享经济、数字资产等多个方向，集成相关领域的基础产品功能，帮助企业快速搭建上层区

块链应用场景。应用层向最终用户的提供可信、安全、快捷的区块链应用，中企矩阵未来将携手行业合作伙伴，共同探索行业区块链发展方向，共同推动区块链应用场景落地。整体框架结构如下图：

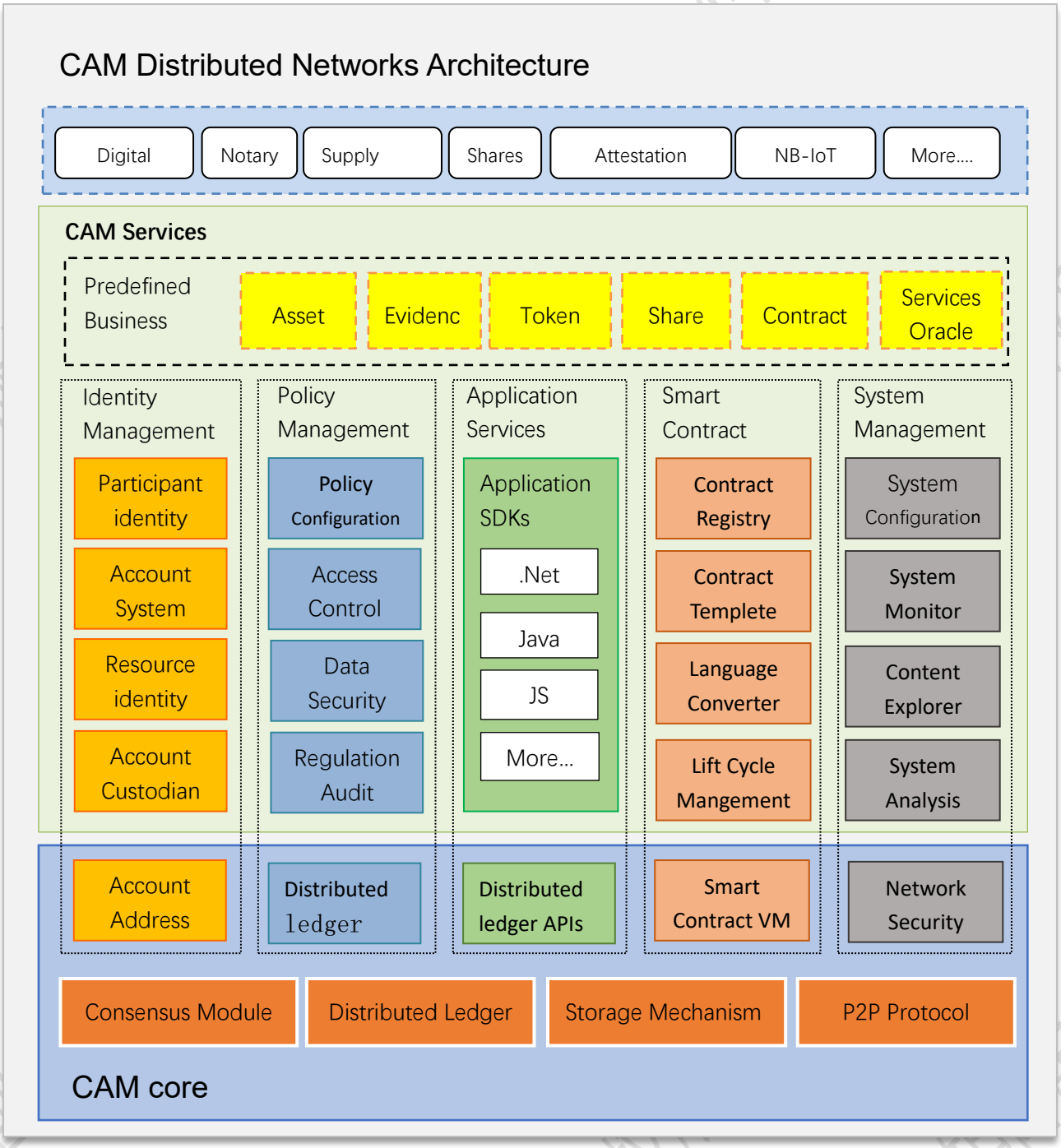

图 4 中企矩阵区块链基础框架

3.1. 底层平台

账户中心（Account）：公私钥生成，公钥写入，私钥签名与管理；应用层用户信息与区块链地址的映射；支持实名认证及审计的监管需求。

P2P 组网：对等协议（Peer-to-Peer）实现基础组网和通信，每个节点维护一张邻居列表，实现动态自组织网络；并可与现有的安全防护设施配合使用， 确保商用网络的安全性。

分布式账本与数据存储：解决数据格式、数据记录、数据存储问题，取保区块数据的安全可靠。

共识机制：共识服务是区块链的核心，也是区块链与传统分布式系统的最大区别之处。它保障底层数据的强一致性的同时，能抵抗“恶意”坏人的影响。

DBFT 全称为 Delegated Byzantine Fault Tolerant，是一种通过代理投票来实现大规模节点参与共识的拜占庭容错型共识机制。CAM 代币（CAM） 的持有者通过投票，可以选出其所支持的记账人。随后由被选出的记账人团体通过 BFT 算法，来达成共识并生成新的区块。投票在 CAM 网络持续实时进行，而非按照固定任期。

DBFT 对由 n 个共识节点组成的共识系统，提供 f=⌊(n-1)/3⌋ 的容错能力，这种容错能力同时包含安全性和可用性，可以抵抗一般性故障和拜占庭故障，并适用于任何网络环境。DBFT 具有良好的最终性，一个确认即最终确认，区块无法被分叉，交易也不会发生撤销或回滚。

在 CAM 的 DBFT 共识机制下，每 15~20 秒生成一个区块，交易吞吐量实测可达到约 1000tps，在公有链中性能优秀。通过适当优化，有能力到达

10000TPS，可以支持大规模的商业化应用。

DBFT 结合数字身份技术，使得记账人可以是实名的个人或机构。从而使得冻结、撤销、继承、找回、司法判决过户等非常规操作成为可能。这有利于合规性金融资产在 CAM 网络中的登记发行。

3.2. 服务层

数字身份：在区块链技术自有的公私钥体系下，身份管理负责：公私钥生成，公钥写入，私钥签名与管理；保存应用层用户信息与区块链地址映射关系；支持实名认证及审计监管需求。

智能合约：负责合约的注册发行以及合约的触发和执行。用户通过某种编程语言定义合约逻辑，发布到区块链上之后，根据合约条款的逻辑，由用户签名或者其他的事件触发执行，完成交易结算等合约的逻辑。

CAM 具备独立的智能合约体系：CAMContract。

CAMContract 智能合约体系的最大特点是无缝对接现有的开发者生态。开发者无需学习新的编程语言，就能用 C#、C、C++ 、Java 、Go、Python、JavaScript 等主流编程语言在熟悉的 IDE 环境（Visual Studio、Eclipse 等）中进行智能合约的开发、调试、编译。CAM 的通用轻量级虚拟机 CAMVM 具有高确定性、高并发性、高扩展性等优点。CAMContract 智能合约体系让全球百万级的开发者能够快速进行智能合约的开发。

数字资产：数字资产是以电子数据的形式存在的可编程控制的资产。用区块链技术实现资产数字化有去中心、去中介、免信任、可追溯、高度透明等特点。CAM 在底层支持多数字资产，用户可在 CAM 上自行注册登记资产，自由交易和流转，并且通过数字身份解决与实体资产的映射关系。用户通过合规的数字身份所注册登记的资产受到法律的保护。

中企矩阵中有两种形式的数字资产：全局资产和合约资产。

全局资产能够被记录在系统空间，可以被所有智能合约和客户端所识别；合约资产被记录在智能合约的私有存储区中，需要兼容该智能合约的客户端才能识别。合约资产可以参照某种约定的标准，从而实现与多数客户端的兼容。

策略管理：中企矩阵区块链平台提供策略管理，即可以管理维护区块链系统本身的配置和安全，也可以管理区块链存储数据的访问策略和隐私安全。

应用服务：为基于中企矩阵区块链技术的开发者社区提供 SDK 开发套件，同时提供 API 接口配合不同的应用快速对接基于中企矩阵区块链应用场景开发。

系统管理：配置管理服务主要提供的配置操作，针对安全、策略、权限、区块链节点、共识算法参数、系统参数进行配置；配置本身也作为区块链的事务类型，由节点共同投票确定生效。组网安全方面采用安全措施包括 IP 控制、专线、节点授权才能接入、节点信任列表等。

3.3. 应用层

为方便应用层理解和对接，在分布式账本适配层抽象出：资产（Asset）、记录（Record）、事务（Transaction）、合约（Contract）等各类组件。

资产（Asset）： 支持目前已经数字化的资产，以及未来可以通过资产证券化、资产数字化的资产。

记录（Record）： 需要利用区块链增加信息记录的真实性和信任的场景，例如：金融领域的凭证、供应链的溯源信息等。

事务（Transaction）： 与区块链底层交互的原子级操作，一个上层应用可以对应一个事务，也可以由一组事务共同完成。

合约（Contract）： 提供两种合约——标准化合约、可编程合约。标准化合约，它主要针对场景相对简单、标准化程度较高，同时对执行效率有很高要求的业务需求。例如资产交换时的交易一致性保障、资产交易的挂单与撮合等。标准化合约可以通过配置生成直接挂在链上，无需编程，也不用通过虚拟执行，降低上层应用使用的成本，提升合约执行的效率。为了应对用户复杂的业务逻辑，中企矩阵也支持用户自编程，并且提供丰富的组件供用户针对特定的需求快速构建应用，如加密组件、权限管理组件等。同时中企矩阵对于通用的场景如资产、存证提供相应的模板，用户不需要从头编写代码，只需要更改模板的关键参数，加上自己业务的特性就可以建立成熟的合约应用。

四、技术特色与优势

通过大量业务模型、应用模型的数据测试分析，中企矩阵在性能方面可达到：秒级交易验证、海量数据存储，高吞吐量、节点数据快速同步；在扩展性方面可达到：满足多业务区块结构、权限控制策略；同时，提供安全的私钥存取服务，以及隐私保护方案。

4.1. 性能方面

4.1.1.海量存储

中企矩阵借鉴传统金融系统中冷热数据分离存储、分表存储的机制，实现海量数据的有效存储。旧的交易数据，非活跃的资产数据等信息可以使用大数据存储平台进行存储（如 Hadoop，满足 PB 级别的数据存储）。

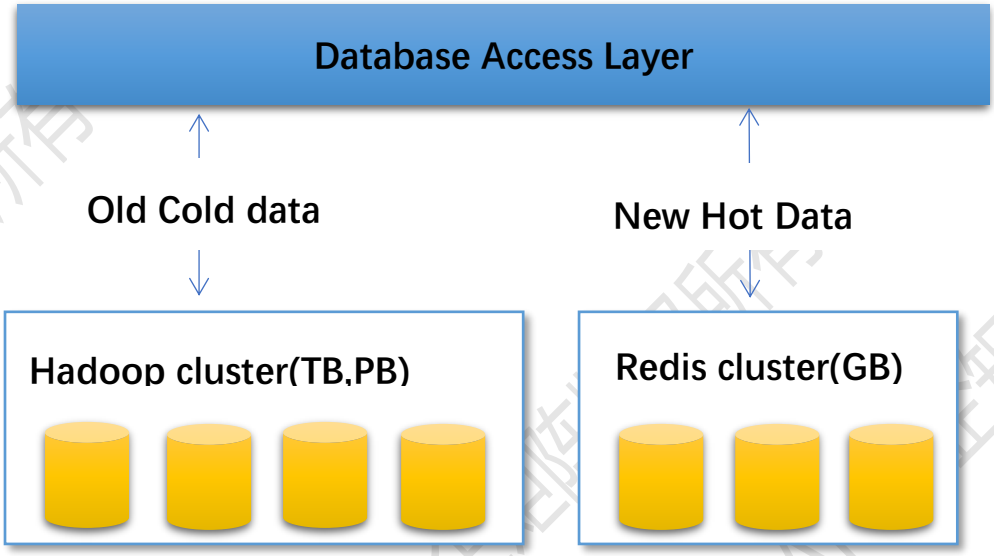

图 5-1 海量数据存储

4.1.2.交易快速确认

中企矩阵采用 DBFT 机制的共识算法，这种方式的优点是专业化的记账人、可以容忍任何类型的错误、并且每一个区块都有最终性，不会分叉。这就保证了共识完成即交易确认，并且对交易确认过程中的其他环节，如签名算法、账本存储方式等进行了优化，实现了秒级确认交易。

4.1.3.高速接入

在实际的应用场景大致分为三类：第一类，原有系统改造后接入区块链，第二类，原有系统上新的需求使用区块链开发，第三类，在全新的系统和场景使用

区块链。

中企矩阵为了加快区块链落地应用适应于上述三类场景，本着业务开发工作量尽量少、尽量满足用户原有开发习惯、方便的部署、保持原有的安全体系的原则，在用户业务开发方式、部署方式以及安全性继承上做了大量的兼容性设计，可以实现各种场景、各种开发习惯的用户能以较低的代价、较快的速度对接到中企矩阵智能经济网络上来。

4.2. 扩展性方面

中企矩阵的块链结构，能够满足不同业务领域的需求，提高系统的可扩展能力和维护效率，实现了跨链互操作协议：CAMX。

跨链资产交换协议：

CAMX 在已有的双链原子资产交换协议上进行了扩展，可以让多个参与者在不同的区块链上进行资产交换，并保证整个交易过程中的所有步骤全都成功或全都失败。为了实现这个功能，我们需要利用 CAM 智能合约 CAMContract 的功能，为每一个参与者创建一个合约账户。对于其它的区块链，如果它不兼容 CAMContract，但是只要能够提供简单的智能合约功能，也能够与 CAMX 相兼容。

跨链分布式事务协议：

跨链分布式事务是指，事务的多个步骤分散在不同的区块链上执行，且保证整个事务的一致性。这是对跨链资产交换的一种扩展，将资产交换的行为扩展成任意行为。通俗的说，CAMX 使得跨链智能合约成为了可能，一个智能合约可以在多个不同的区块链上执行不同的部分，要么全部执行完毕，要么全部退回执行前的状态。这赋予了跨链协作极大的想象力，我们正在探索跨链智能合约的更

多应用场景。

4.3. 安全方面

4.3.1.安全私钥存取

为了方便用户使用区块链产品服务，除了传统的客户端生成和保存的机制，中企矩阵还提供网络托管存取和私钥硬件存取（U-key）两种方案。网络托管存取， 即把用户名和密码通过特定算法映射成私钥并在服务端进行存储。服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；硬件私钥是为了满足金融行业及物联网行业的使用需求。

4.3.2.多重签名隐私保护

数据公开和隐私保护看似矛盾，中企矩阵使用基于多重签名的 Stealth Address 隐私地址方案很好的解决了此问题。使用隐私地址后，除了该笔交易的直接参与者，其他人都无法知晓该笔交易的参与者身份。隐私地址下的交易数据仍然是全部公开的，但每笔交易间不存在可分析的联系性。即使是同一人向你发送了多笔交易，这些交易也会分散在多个毫无联系的地址中，除了你本人没有人能发现或证明这若干个地址属于你。

比特币的 Stealth Address 方案为 BIP63 提案。中企矩阵在此基础上进行了扩展，加入了多重签名和查询私钥的特性，形成了自己的隐私地址方案，具体将另文详细详述。

4.4. 运维方面

4.4.1.全平台部署

中企矩阵区块链的所有代码均可跨平台编译运行，可以在 Windows、Mac OS 、Linux 和 Docker 中运行。

4.4.2.可视化运维

提供运维管理所需的可视化工具。中企矩阵区块链健康监控平台提供多层监控：物理层（CPU、内存、磁盘等）、网络层（时延、断线）和业务层（区块生成、交易验证）；并提供完善的告警、日志、消息通知机制体系，便于商用系统的运维。系统分析提供了分布式账本内存储的大量原始数据的查询接口，以满足应用层各种数据分析需求。

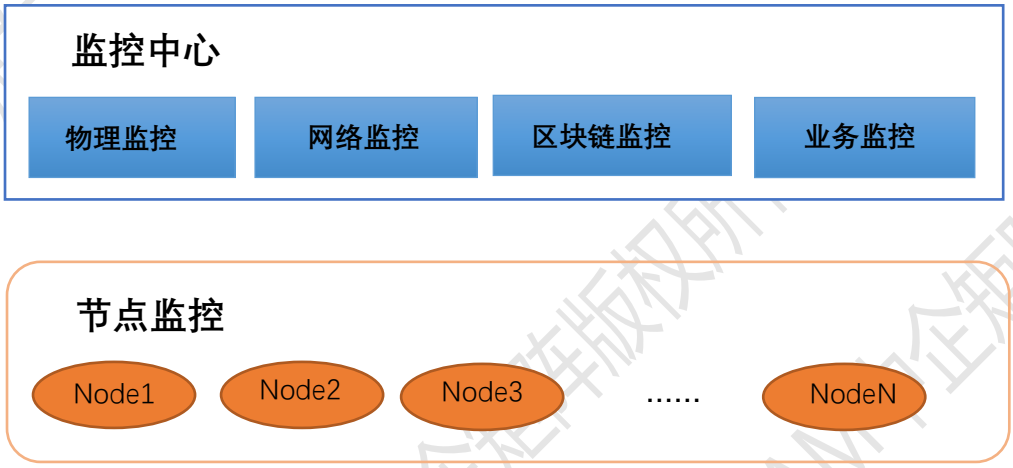

图 5-3 可视化运维

五、治理架构及管理哲学

本项目的基金会成立于 2017 年，称为 CAM 中企矩阵基金会。基金会致力于中企矩阵项目的开发以及应用推广的落地工作，并促进早期去中心化应用的开发，CAM 初始总量的 20%会被用于部分行业应用和初创项目，例如金融服务、供应链、物联网、区块链等，包括项目战略规划、项目扶持、项目推广和代币置换。基金会会挑选在中企矩阵上开发的去中心化应用，并基于应用上的实际用户数量提供奖励。

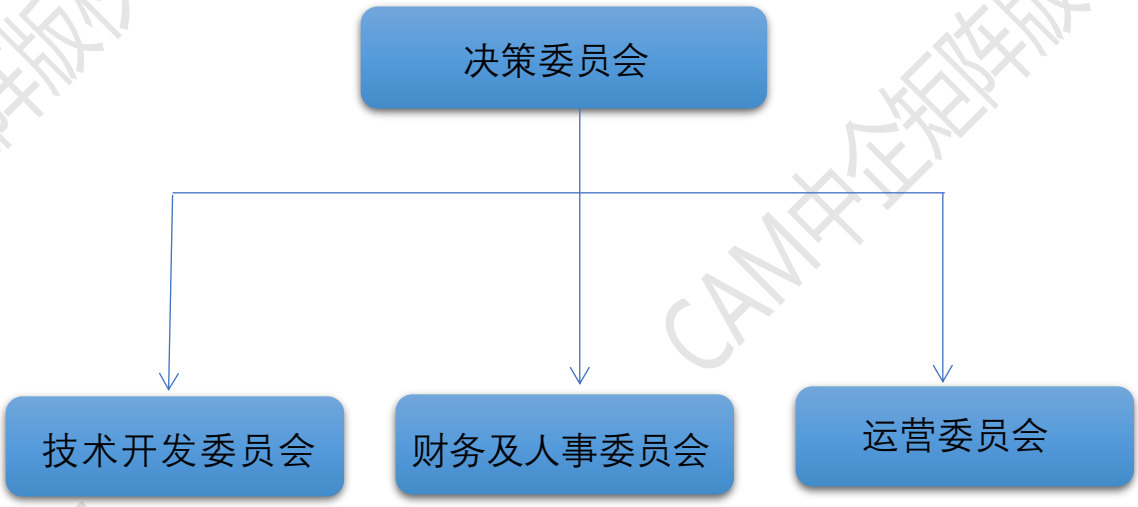

图 5-1 基金会的总体架构

基金会的总体架构如图 5.1 所示，决策委员会下辖技术开发委员会、财务及人事管理委员会、项目运营委员会三个子部门，分别负责技术开发战略的制定和实施监管；财务制度的制定和执行监管；项目总体运营及市场推广的决策及执行等事务。决策委员会成员四年一换届，成员一般由各个子委员会推荐两名代表，加上项目投资方代表、社区代表、中企矩阵团队成员代表各一名产生。各子委员会成员四年一换届，成员一般由具备相关行业杰出能力的人士担任。

基金会提倡透明高效的运营理念，促进中企矩阵生态体系健康发展。治理结构主要以项目管理的有效性、可持续性和资金安全性为主着眼点。基金会的使命就是推进区块链应用落地。

5.1. 理事团队

5.1.1.核心团队

✧ **郭易鑫** **创始人&首席执行官**

H264\265 专利视频编解码实验室建立者，《中国企业报》集团全媒科技副总裁；中国企业扶贫联盟副秘书长；中国企业家扶贫协会副秘书长；福建省新兴

科技产业促进中心副理事长；泉州商会名誉会长。

✧鲁志洪 联合创始人&首席技术官

拥有 10 年的 IT 技术规划及管理方面的从业经历，在多个知名企业负责技术系统规划工作。长期致力于人工智能和区块链技术的研发。曾为多家知名大型企业和创业公司开发区块链框架和商业应用项目，具有丰富的计算机系统设计、产品开发和工程项目管理经验。

✧练海翔 联合创始人&首席运营官

中国最早一批比特币矿工、区块链技术外汇全自动交易第一人；7 年加密数字货币投资经验，2012 年最早一批数字资产投资私募基金的发起人。

✧黄晓辉 首席财务官

厦门市“双百计划”人才评审专家，厦门市经信局专家库专家，厦门市金融办小额贷款公司及融资性担保公司准入审核专家，厦门市科技局专家库专家。

✧郑建平 首席战略官

厦门大学硕士研究生毕业，历任大洲集团、永同昌集团、中绿集团等综合型集团企业高管职位，在多家大型集团公司担任集团核心决策成员及重要部门决策，具有丰富的现代化管理经验，和各行业实际运作阅历，熟悉企业内部流程制度建设及先企业运营管理，集团公司的全面管理,熟悉项目投资，资本运营及企业上市筹划事宜。

5.1.2.天使投资人

✧景百孚 著名天使投资人

嘉年华国际控股有限公司 董事长北京百顺达房地产有限公司 董事长北京昂展实业有限公司董事长 实益掌握的 ST 明星福建实达电脑集团董事长福布斯中国富豪榜排名 165。2016 年胡润地产富豪榜 110 亿 5 千万排名第三十八位。

5.1.3.战略顾问

✧朱延平 战略顾问

中国台湾籍，工学博士（毕业于台湾成功大学），台湾云端服务协会理事长，中兴大学资讯管理系主任。曾获得台湾教育部青年发明奖，台湾十大资讯人才奖。多年来对区块链的应用有着深入的研究，带领区块链技术团队开发系统应用于健康大数据和农业溯源项目。

✧王朝治 战略顾问

资深学者，著名社会学、教育学、心理学、婚姻爱情心理学专家，著名演讲专家。北京大学“信用中国中国信用论坛”课题召集人。联合国全球资产数字加密委员会(World Assets Digital Cryptography Committee,UN)首席顾问、澳门宋庆龄基金会亚太区主席、“信用中国 中国信用”大型论坛组委会执行主席。

六、中企矩阵（CAM）多元化应用场景

以下是中企矩阵区块链已上线运行的几个行业应用案例，包括：数字资产的发行与流通，供应链金融，私有股权登记与转让，供应链溯源，公示公证， 联

合征信。

6.1. 数字资产

相比于传统中心化系统，区块链应用于数字资产领域的优势在于：资产一旦在区块链上发行，后续流通环节可以不再依赖发行方系统，在流通中，资产由单中心控制变成社会化传播，任何有资源的渠道都可能成为资产流通的催化剂。因此，区块链能极大地提升数字资产流通效率，真正达到“多方发行、自由流通”。

图 6-1 数字资产发行与流通

如图 6-1 所示，在数字资产发行与流通网络中，区块链用于资产登记、交易确认、记账对账和清算等。区块链数字资产网络，包括资产发行方、资产交易方、交易所、流通渠道在内的各个上下游机构，他们可以按照自身角色在链上自行开展业务。

- 任何可数字化的资产都可以在平台上实现登记、发行，各种主体（个人、机构）均可以在平台上登记、发行自己的数字资产。实现资产登记即公示，利

于数字资产追踪查询，可以有效减少资产纠纷问题。

- 资产流通的核心是渠道，区块链技术使资产流通由原来的单中心控制变为社会化流通，任何有资源的渠道都可以成为资产流通的催化剂，促进流通、提高流通效率。
- 区块链“交易即结算”的基本特性使得实时清算成为可能，大幅提高交易后处理的效率，实现资产流通情况的实时查询功能。
- 数字资产可以是已经数字化的资产，可以成为资产证券化和资产数字化的入口，将现实资产映射成数字资产在链上发行与流通。

中企矩阵区块链正在被应用于共享积分、跨境转账、游戏装备、数字票据、优惠券、股权登记&众筹、资产证券化等。

6.2. 贸易金融/供应链金融

贸易金融/供应链金融领域的业务链条中，天然就是多方参与协作。利用区块链，能将分散独立的各自单中心，提升为多方参与的统一多中心，打通贸易上下游各个环节，提高信任传递效率，降低交易成本，促进贸易金融的良性生态建设。

在贸易金融领域，信息散落在供应链各家自有系统中，流通和融资环节存在信息重复验证，效率低下；受各个供应链圈的信息流限制，中小企业和金融机构双向选择范围有限；缺乏统一可靠的中小企业征信系统，金融机构风控难度大，风控成本全部转嫁给融资企业。区块链可以促使供应链参与方共同创建和维护一份各环节都认可的统一凭证，并保障其真实有效、不可篡改；除了凭证的共享，项目/合同执行的过程也可以完整记录和跟踪，降低金融机构的风控难度，提升中小企业融资的可行性，降低融资成本；淡化供应链固有的圈子，扩大凭证授信

范围，成为资产证券化、数字化的入口，增强流通性；链信息的记录和积累，也是企业自征信的过程，基于这些征信数据，可以展开各种金融服务。

图 6-2 区块链贸易金融

- 统一凭证，保障唯一真实性，极大降低核验成本；
- 过程可视，增强履约透明度，提高融资管理能力；
- 数据记录，促进征信的体系，减小风险控制成本。

中企矩阵区块链正在被应用于食品、药品、高端消费品、艺术品等。

6.3. 供应链溯源

区块链账本本身具有不可篡改性，链上各方共同参与账本信息维护，保证写入区块链的数据实时、有序、真实不可伪造。应用层支持多种实物扫码或编码录入方式进行商品溯源，杜绝物品身份的造假、恶意仿制放大流通量的情况。

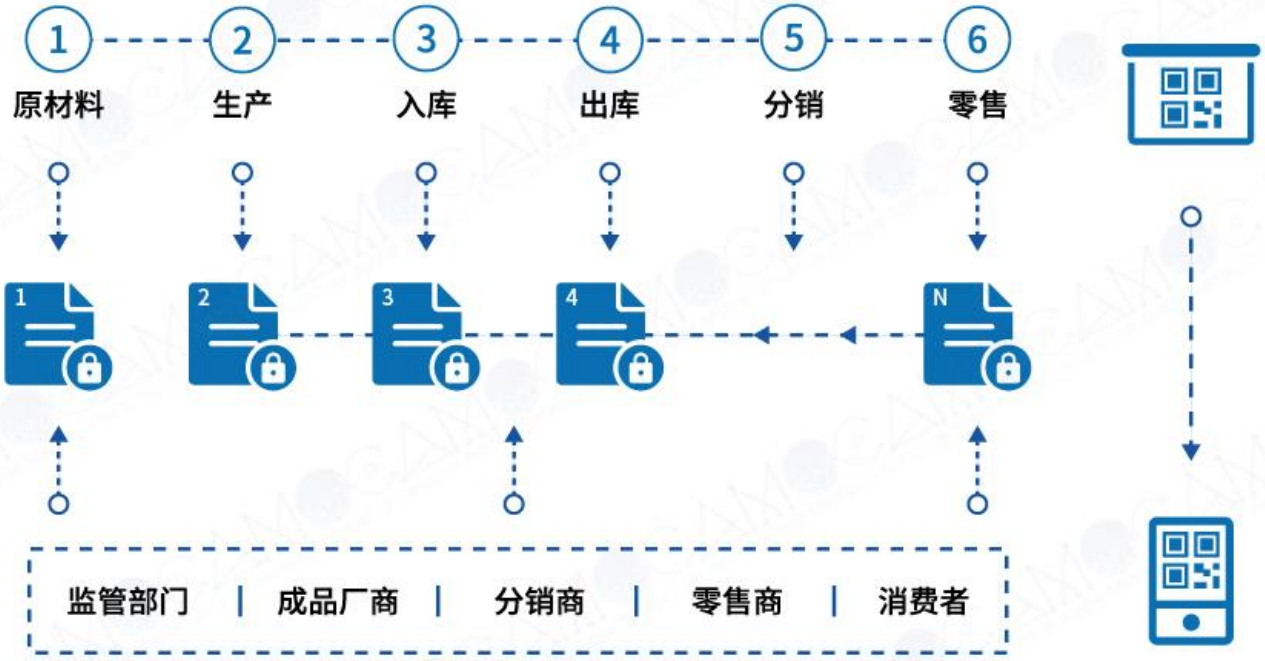

图 6-3 区块链供应链溯源

如图 6-3 所示，中企矩阵区块链对供应链特性的支撑，使每一个物品静态（固有特性）和动态（流转、信用等）信息能够在生产制造企业、仓储企业、物流企业、各级分销商、零售商、电商、消费者以及政府监管机构中共享、共识。区块链平台在链接商品供应链权属关系和上下游关系的同时，还可以有效链接了间接发生关系的上下游企业。

- **信息记录：**每个物品的关键信息会以明文或加密方式记录到区块链中，公开不可篡改的区块链属性，防止数据伪造。
- **信息跟踪：**商品码信息是平台中标识一个物品的唯一加密字串，也称为“一物一码”。通过使用智能手机、便携或大型射频、传感器装备等对物品的商品码进行自动识别，透明的共享的过程，连接商品权属及转移关系。

- **多方参与：**基于区块链开放、共识、多中心网络信任特性，企业不仅能够可靠的掌握上下游企业情况、建立交易关系、跟踪交易状况，了解间接环节直至最终消费者的状况；同时提供监管方介入接口，有利于政府/市场监督。
- **最终实现：**对品质型商品、作品的价值保护；对流通渠道和最终消费者的保护；具有公信力的价值转移和再生。

中企矩阵区块链正在被应用于应收账款融资、预付类和存货类融资、消费金融理财、大宗商品交易等。

6.4. 联合征信

当前，征信通常是单中心模式，即单机构通过自己的数据收集能力和信用做背书，进行风控和征信系统的开发和维护，为其它机构及个人客户提供有偿的征信服务。

单中心的征信模式有几个明显的弊端：首先，单中心维护数据信用的成本过高，包括系统建设的成本和数据审核的成本；其次，单中心提供的征信服务使用范围有限，只有密切合作并且充分信任的机构才会认可。

图 6-4 区块链公示公证

随着区块链技术在各个领域的点滴渗透，单中心维护的信用体系将被改善；由区块链构建多中心体系下的联合征信优势在于：

- **降低征信成本：**联合征信的可充分保护各方数据隐私的基础上，实现成本分摊式的征信系统搭建，降低单中心系统构建和维护的成本，从而降低整个征信平台的使用成本。
- **扩大征信服务使用范围：**征信数据的录入和累积，由上下游参与方共同验证和维护，这种方式产生的征信服务，将大幅提升使用范围。
- **数据自征信：**随着参与方越来越多，联合征信的生态越来越完善；企业、C 端用户的数据不断积累，其实也在完成各自自征信的过程。
- **数据共享，互利共赢：**区块链在底层提供数据确权、不可抵赖的访问记录、低成本的对账清算等功能；同一行业实现互利互惠的数据共享。

6.5. 公示公证

在信息公示中，公示主体的公信力是核心。因为数据完全受控于系统管理者，所以即使在数据时代，公信力的缺失问题并没有被有效解决。区块链的不可篡改、不可抵赖的特征，能够提高公示主体的公信力，打造新一代信息公示服务。

公示需求由来已久，在没有信息化技术之前，张榜公布、立碑刻字是曾经较为广泛采用的“公示”形式。公示的本质就是通过将信息公开化获得大众群体的确认及共识，这与区块链达成共识后不可篡改的本质具有异曲同工之处。区块链技术本身是提高公信力的有效途径：一是让更多的人知悉，从而提升抵赖难度；二是利用特殊介质，增强物理凭据的存在。

图 6-5 区块链公示公证

- 区块链是解决公信力的利器。区块链之所以能提高公信力，是因为它具有不可篡改、不可抵赖的特征。
- 公示中的“隐私保护”。由于数据本身并不能被篡改，所以在信息公示中，无论支持隐私保护和权限控制，或是支持完全公开和授权访问，都不会降低公示的公信力。

中企矩阵区块链正在被应用于个人企业资质证明、信贷记录共享等。

6.6. 股权登记转让

应用区块链技术的加密股权、债券等证券化资产，有助于完善登记与流转服务，尤其是区块链构建的多中心体系，能够大幅地提升资产跨域流通效率，降低交易成本，使管理更安全、高效、可信、低成本、合规。

当前，股权登记需要人工处理，股东名册维护繁琐、历史交易维护与跟踪十

分困难。传统股权交易，以双方信用为基础，需要建立双边授信后才可进行交易，信用风险由交易双方自行承担，而交易平台集中承担市场交易参与者的信用风险。

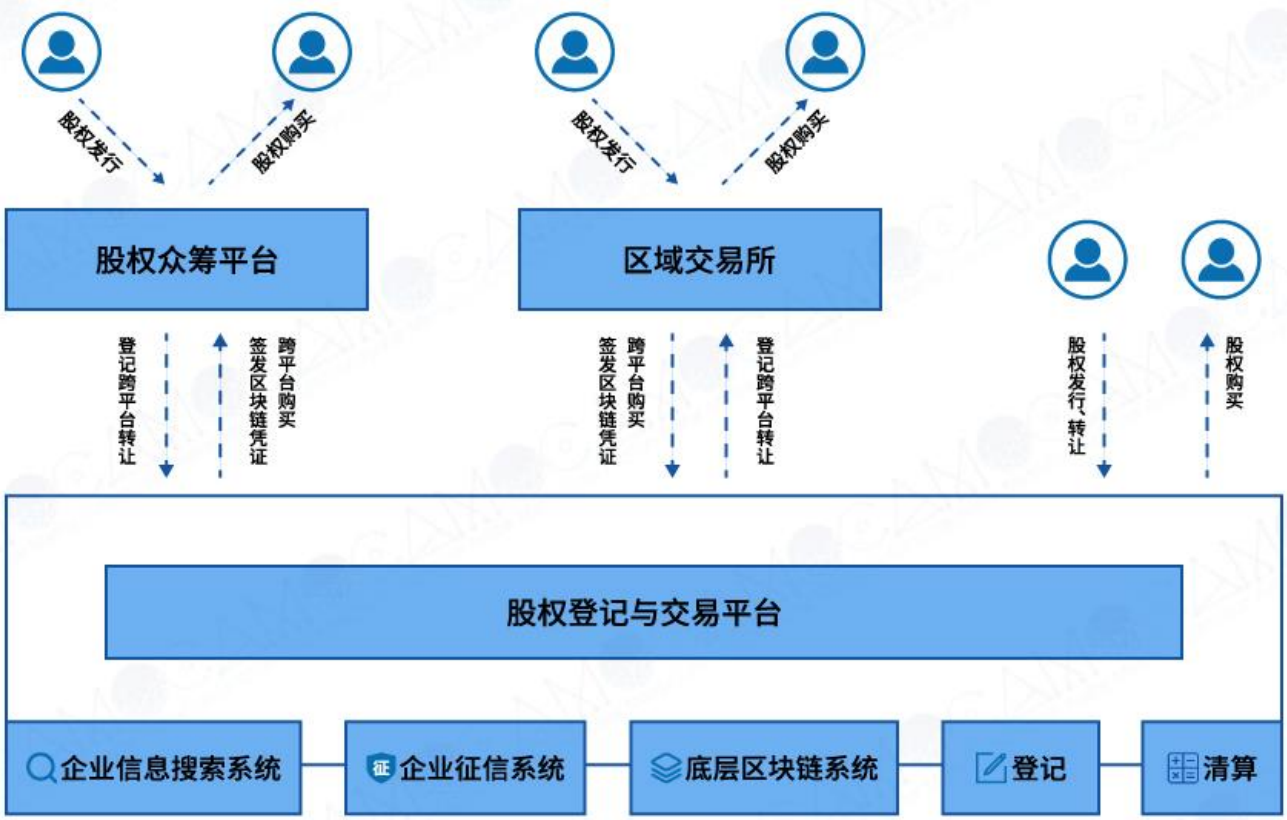

图 6-6 股权登记与转让

- 唯一真实的数字凭证，适于股权债券等证券化资产的登记；
- 跨域的多中心化信任，便于加密证券化资产的转让与交易；
- 增强的信息披露记录，易于符合监管满足合法合规性要求。

中企矩阵区块链正在被应用于众筹平台、区域股权交易中心、区域金融资产交易中心、私募管理平台等。

参考文献

1、《区块链：定义未来金融与经济新格局》，张健，机械工业出版社；

2、《区块链：将如何重新定义世界》，唐文剑，吕雯，机械工业出版社；

3、《区块链革命：比特币底层技术如何改变货币、商业和世界》，唐·塔普斯科特、亚力　克斯·塔普斯科特著，中信出版社；

4、《中国区块链技术和应用发展白皮书（2016）》，工业和信息化部信息化和软件服务业司；

5、《分布式账本技术：超越区块链》，英国政府首席科学顾问报告，万向区块链实验室编译；

6、《中国区块链技术和应用发展白皮书（2016）》，工业和信息化部信息化和软件服务业司；

7、《英国将区块链列入国家战略部署，并制定详细战略实施规划》，2016-05-13，蔡维德、赵精武，中国信息化百人会；

8．S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org, 2009.

9 .D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, Sequences II: Methods in Communication, Security and Computer Science, 1993.

10．A. Legay, M. Bozga, Formal modeling and analysis of timed systems, Springer International Publishing AG, 2014.

11 、 Blockchain Technology Market by Provider, Application, Organization Size, Vertical, and Region - Global Forecast to 2021, MarketsandMarkets, October 2016；

12、《The future of financial infrastructureAn ambitious look at how blockchain can reshape financial services》，world economy forum，August 2016；

开曼群岛 CAM 数字资产管理股份有限公司

Cayman Islands CAM Digital Asset Management Co.,Ltd

Address：12F，12 Albert Panton St, George Town,

Butterfield Bank, Cayman Island.

E-Mail：support@camatrix.org

Website：http://www.camchain.org