众享比特 PeerSafe | ChainSQL

# ChainSQL区块链白皮书

# ChainSQL Blockchain White Paper V3.0

北京众享比特科技有限公司

2020年9月

# 前言

区块链技术带来价值互联，构建可信的网络环境。

回顾人类社会发展的不同时期，我们可以发现信息技术、信息生产和信息处理手段在不断的发展，自 19 世纪中期以后，人类学会了利用电力和电磁波进行生产和工作，尤其是电话、电报的发明，使信息交流和传递更加快速和有效，第二次世界大战以后，集成电子电路、半导体材料和计算机的发明，使人类利用信息的手段发生了质的变化。世界第一台计算机于 1946 年问世，但当时的计算机体积庞大，制作成本高昂，最初只是用于军事部门和大型科研机构，后来随着平面半导体和集成电路的问世，电子计算机逐渐进入了企业和家庭。

1983 年 1 月 1 日，美国远景研究规划局用 TCP/IP 协议取代了旧的网络控制协议 NCP，从而一举将局域网升级为信息互联网，此后，TCP/IP 协议被确立为全球信息互联网所统一采用的标准通信协议，奠定了今天信息互联网的基石，开放共享也成为了信息互联网至今的内在精神。

互联网一方面带来了生产力水平的大幅度提升，另一方面，其无界、无价、无序的特征也开始暴露于公众面前。互联网引发了数字壁垒和信任缺失等问题，目前很多行业和领域的数据被封闭在各个系统内部，对整个社会而言就是一个个的“数据烟囱”。有价值，但是没有使用价值，是信息互联网的基本特征。

2009 年比特币的诞生是个标志性事件。在密码学技术支持下，区块链带领我们走进了价值互联网的世界，这就好像沸水顶开了壶盖，将人们带进了蒸汽时代一样。

那么区块链如何构建可信的网络环境呢？区块链类似于信息互联网时代的 TCP/IP 协议，本质是一个安全传输与存储的协议。为确保数据传输的安全性，

区块链技术将传统加密技术和互联网分布技术相结合，对各设定区块的成员进行身份验证，确定不同区块之间成员的资产和交易情况，并进行连续不断的认证和记录，避免了人为的干预和弄虚作假，由此形成了区块之间相互连接的区块链，这是一种全新的网络应用技术。

如果说 TCP/IP 协议让我们进入了信息自由传递的时代，那区块链的创新则把我们带入信息的自由公正时代，TCP/IP 解决信息传输问题，区块链解决信息互联网的信任问题。

区块链引发了世界性的关注，中国也开始从国家层面设计区块链的发展道路，我们正面临区块链重大的产业机遇。

# 目录

前言.....1
目录.....3
1. 区块链的概念与特征.....5
1.1 区块链的概念.....5
1.2 区块链的特征.....6
2. 区块链的核心技术.....7
2.1 密码学.....7
2.2 分布式账本.....8
2.3 共识机制.....8
3. ChainSQL 介绍.....10
3.1 设计背景.....10
3.2 设计原则.....11
3.3 整体架构.....12
3.4 功能模块.....13
3.4.1 数据库操作相关功能.....13
3.4.2 隐私安全相关功能.....14
3.4.3 特色功能.....15
3.4.4 工具包.....16
4. 技术创新.....17
4.1 共识算法.....17
4.2 分片共识.....18
4.3 共识可拔插.....19
4.4 多链技术.....19
4.4.1 架构设计.....19
4.4.2 特性.....20
4.5 存储.....21
4.5.1 数据对象管理.....21
4.5.2 数据缓存.....22
4.5.3 数据索引.....23
4.5.4 数据存储.....24
4.5.5 分片存储.....24
4.6 密码算法.....24
4.7 用户身份.....25
4.7.1 准入机制.....25
4.7.2 隐私保护.....26
4.8 智能合约.....26
4.9 区块链服务平台.....26
4.10 众享区块链超级工作站.....27
4.11 自主可控国产化适配.....28
4.12 技术优势对比.....29
5. 应用服务.....30
5.1 区块链应用程序接口（APIs）.....30
5.2 应用开发包（SDKs）.....31

6. 落地案例.....32
6.1 存证平台.....32
6.2 溯源平台.....33
6.3 数据共享.....34
6.4 分布式资产交易平台.....36
6.5 供应链金融.....37
6.6 区块链扶贫.....39
6.7 资产证券化.....40
6.8 积分商城.....42
6.9 安全生产监管平台.....43
6.10 档案管理平台.....45

# 1.区块链的概念与特征

## 1.1 区块链的概念

区块链（Blockchain）起源于比特币，包括了分布式账本、密码学、共识机制、智能合约、P2P 网络等综合技术。更确切的说，区块链是一个由不同节点共同参与的分布式数据库系统，它是由一串按照密码学方法产生的数据块或数据包组成，即区块（block），对每一个区块数据信息都自动加盖时间戳从而计算出一个数据加密值，即哈希值（hash），每一个区块都包含上一个区块的哈希值，从创世区块开始链接到当前区域，从而形成区块链。以下区块链技术的六层结构模型，可以帮助我们全面的认识区块链技术有哪些，建立整体的认知。

图 1.1-1 结构模型

按照区块链的开放程度（应用场景范围和节点准入规则），区块链可以分为公有链、联盟链和私有链；我们在谈论区块链概念，通常是没有区分区块链类型，其实不同的区块链类型适用的场景是有差别的，而且所采用的技术、达到的效果也有较大的差异。

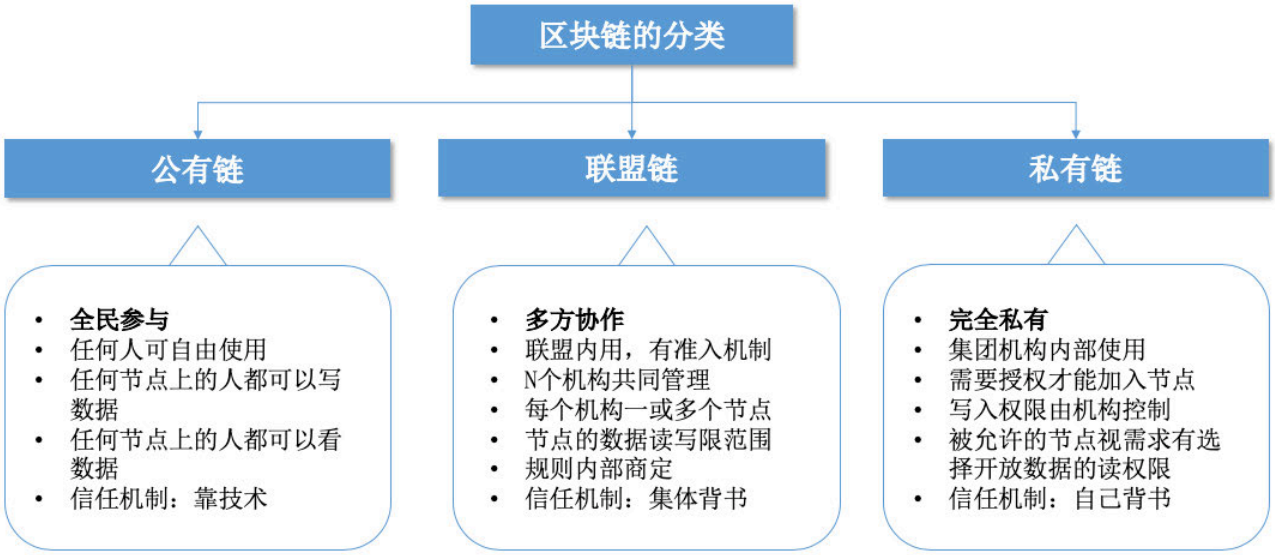


图 1.1-2 区块链的分类

综上所述，区块链是使用密码技术将共识确认过的区块按时间顺序链接而形成的分布式账本。这种新的记账方式正在导致一场革命，让生产者、消费者、投资者、参与者合为一体，去掉中间的传导环节，改变了社会生产关系和价值的分配模式。因为区块链技术的出现，过去的信息互联网正在向价值互联网发展。

## 1.2 区块链的特征

- **去中心化**

区块链存储数据时使用的是对等网络技术，使用分布式计算和存储，不存在中心化的硬件或管理机构。所有节点的权利和义务都相等，所有节点共同为数据背书，任一节点停止工作都会不影响系统整体的运作。但区块链本身不创造信任，而是作为信任的载体存在。

- **集体维护**

系统是开放的，除了交易各方的私有信息被加密外，系统是由其中所有具有维护功能的节点共同维护的，任何人都可以查询区块链数据和开发相关应用，

因此整个系统信息高度透明。此处的多方仅指记账参与方，不包含使用区块链的客户端。

- **高安全性**

一旦信息经过验证并添加至区块链，就会永久的存储起来。生成一套按照时间先后顺序记录的、不可篡改的、可信任的数据库，从而可以限制相关不法行为。因此区块链的数据稳定性和可靠性极高。

- **公开透明**

每个节点都会独立记录区块内容，各节点都拥有最新的完整数据库拷贝且所有的记录信息都是公开的，任何人通过公开的接口都可查询区块数据。但是公开账本指的是可访问性的公开，并不代表信息本身的公开。

# 2.区块链的核心技术

区块链不是一个单项技术，而是新的技术组合。其关键技术包括：密码学、P2P 网络、分布式账本、共识机制、智能合约等，在具体应用中有时会再辅以激励机制，从而解决多方合作中的信任问题。我们认为，其中有三项必不可缺的核心技术，分别是：密码学、分布式账本和共识机制。

## 2.1 密码学

信息安全及密码学技术是整个信息技术的基石。在区块链中，也大量使用了现代信息安全和密码学的技术成果，主要包括：哈希算法、对称加密、非对称加密、同态加密和零知识证明等等。其中最常用到以下三类密码算法：第一，非对称密码算法，例如 ECDSA 或者 RSA，这种密码算法多用于数字证书和数字签名，为身份认证做基础；第二，哈希散列算法，例如 SHA-1、SHA256 等，这种

算法多用于数据完整性验证；第三，对称加密算法，例如 AES，这种加密算法多用于数据的私密性保护。

在实际系统应用的过程中，对国密算法的支持也是区块链系统的一个安全指标，SM2、SM3、SM4 分别对应着非对称加密算法，哈希散列算法和对称加密算法，支持国密算法的区块链系统在实际应用更加广泛。

## 2.2 分布式账本

区块链的最终目的是在分布式网路基础上达成统一账本（即：统一数据库）。分布式账本，从实质上说，就是一个可以在多个站点、不同地理位置或者多个机构的网络里进行分享、同步和复制的去中心化数据存储技术。由于各个节点均各自维护了一套完整的数据副本，任意单一节点或少数集群对数据的修改，均无法对全局大多数副本造成影响。换句话说，无论是在无授权情况下的蓄意修改，还是网络黑客的恶意攻击，均需要同时影响到分布式账本集群中的大部分节点，才能实现对已有数据的篡改，否则系统中的剩余节点将很快发现并追溯到系统中的恶意行为，这显然大大提升了系统中数据的可信度和安全保证。

## 2.3 共识机制

共识机制是区块链网络中各共识节点对网络事件达成一致（包括事件顺序与执行结果）的实现方式，是保证区块链系统在分布式架构下的一致性方案。分布式系统的共识机制达成需要依赖可靠的共识算法，共识算法通常解决的是分布式系统中由哪个节点发起提案，以及其他节点如何就这个提案达成一致的问题。目前常见的共识算法有工作量证明(Proof of Work，PoW)、权益证明(Proof of Stake，PoS)，股份授权证明(Delegated Proof of Stake，DPoS)、实用拜

占庭容错算法(Practical Byzantine Fault-Tolerant，PBFT)，以及超级账本使用的背书策略+排序服务。不同共识算法的对比如下：

| | PoW | PoS | DPoS | PBFT | 背书+排序服务 |
|---|---|---|---|---|---|
| **适用场景** | 公有链 | 公有链、联盟链 | 公有链、联盟链 | 联盟链、私有链 | 联盟链、私有链 |
| **去中心程度** | 完全 | 部分 | 部分，存在超级节点 | 节点数量有限 | 节点数量有限 |
| **共识机制** | 参与者执行计算密集型任务，其他网络参与者验证 | 权益证明要求所有参与者抵押一部分他们所拥有的通证来验证交易 | 通过 token 的持有者投票产生一组交易验证者（超级节点）验证交易 | 通过三轮投票共识以及场景切换(View Change)保证交易一致性 | 通过多节点背书签名，排序服务对交易排序以及最后提交节点验证交易保证一致性 |
| **应用** | 比特币、以太坊 | 未来币（NXT）、点点币（PPC） | EOS、比特股 | Hyperledger Fabric v0.6 | Hyperledger Fabric v1.0 |
| **容错** | 50% | 50% | 50% | 33%（N=3f+1） | 跟背书策略设定相关 |
| **资源消耗** | 计算资源 | 网络资源 | 网络资源 | 网络资源 | 网络资源 |

上表看出，达成共识越分散，其效率就越低，但满意度越高，因此也越稳定；相反，达成共识越集中，效率越高，也越容易出现独裁和腐败现象；因此，区块链存在不可能三角，高性能、去中心化和高安全性只能取二。

# 3.ChainSQL 介绍

ChainSQL 是北京众享比特科技有限公司自主研发的全球首个基于区块链的数据库应用平台，国内最先获得国家密码管理局颁发的商用密码产品型号证书的区块链软件产品。该平台集合了区块链技术与传统数据库的优点，不仅具有区块链的分布式、去中心化、可审计的特性，同时兼备传统数据库的快速查询、数据结构优美的特性。两者的结合使得数据库的恢复变得快速，数据可靠性得到质的飞跃，同时使得基于区块链的应用开发变得简易。

ChainSQL 于 2017 年底在 github 开源，地址为：github.com/chainsql。

## 3.1 设计背景

从宏观上讲区块链是一个数据库，与传统数据库相比，前者是一个过程数据库，但是对数据的查找速度、数据格式化处理方面有天生的不足；而后者则是一个状态数据库，如何结合这两者的优势，既能使数据生成过程不可逆转，又能对数据进行快速、多维度的访问，这是 ChainSQL 的设计初衷。

以日志为中心的设计思想。分布式系统中，以日志为中心的设计思想就是日志即数据；在区块链中，区块可抽象成日志系统，日志系统是链的操作日志，记录着链的状态变化过程。区块的产生就是日志连续产生的过程。

ChainSQL 把对数据库进行操作的 SQL 语句转换为对区块链网络的交易，使得原来针对数据库的操作变为对区块链节点的操作。提供合理的 API 接口调用或通过解析源数据库在线日志或归档日志获得数据的增删改变化，再将这些变化应用到目标数据库，实现源数据库与目标数据库同步、多活，并且易读、好

用；同时提供基于 SQL 语句的代理节点方案，将 SQL 语句直接翻译成区块链交易，便利企业数据库对接区块链。

## 3.2 设计原则

ChainSQL 设计目的是让用户像使用传统数据库一样使用区块链，在技术上遵循自主创新、自主可控、易用高效和开源共享的设计原则。

**自主创新：**研发并申请了多项 ChainSQL 技术区块链专利，授权专利数目国内领先，在共识算法、数据存储、密码算法、隐私保护、智能合约等方面具有深厚的技术积累。

**自主可控：**拥有基于最快国密算法的区块链底层密码体系，兼容国产自主可控服务器、操作系统和数据库。ChainSQL 通过鲲鹏服务器、麒麟软件和人大金仓等产品的兼容性测试。

**易用高效：**ChainSQL 和企业已有传统数据库无缝对接，具备高可用性（异常处理能力）、交易和区块链实时监控的能力、简单可行的上层开发架构以及丰富完备的对外 API、灵活热插拔机制和扩展性能。

**开源共享：**建设 ChainSQL 区块链开源社区，围绕核心功能、关键技术、行业应用解决方案研究、标准制定等开展交流与合作。

## 3.3 整体架构

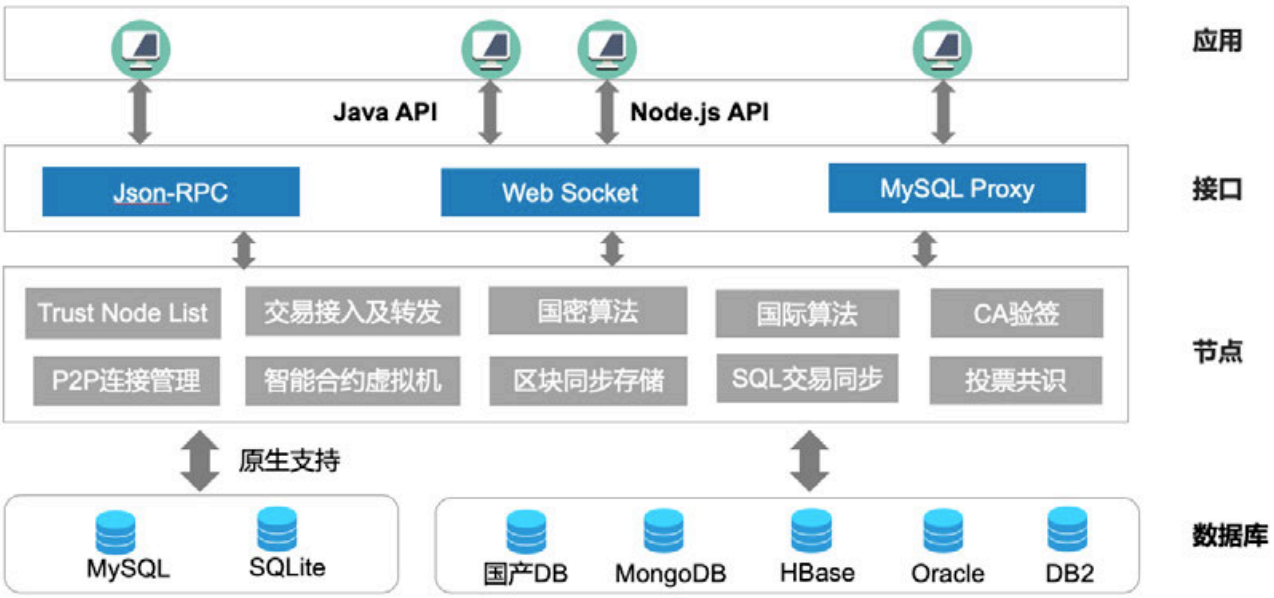


图 3.3 技术架构

ChainSQL 对数据表的所有操作以交易记录的形式记录在区块链上，用户可以自主配置想要同步的表到本地数据库，从而建立一个分布式、可溯源、公开透明、不可篡改的系统。

- **数据库层**

在 ChainSQL 中，包含两种数据库，一种是存储区块、交易数据的链数据库，一种是同步表交易数据的用户数据库。ChainSQL 中的用户数据库原生支持 MySQL 与 SQLite 数据库；并可以通过 MyCat 支持 MongoDB、HBase、Oracle、DB2 等数据库；同时支持南大通用、武汉达梦、人大金仓、神通数据等国产数据库。

- **节点层**

① 底层使用信任列表机制，需在配置文件中配置信任列表；

② 使用自研共识算法 PoP，结合了 PBFT 与 RPCA 共识算法的优点；

③ 支持多种交易类型，所有链上状态的修改都需要通过交易来完成；

④ 支持国密算法；

⑤ 支持账户级 CA 证书，启用 CA 验证功能后，没有证书的账户无法发起交易；

⑥ 内置智能合约虚拟机 EVM，并对 Solidity 指令做了扩展；

⑦ 表交易同步，表相关交易共识通过后，可以自动同步到数据库，也可以在需要时再进行同步；

⑧ 表数据查询功能，交易数据同步到数据库方便用户检索，有查询权限的用户可对数据进行复杂查询。

- **接口层**

ChainSQL 底层支持 Json-Rpc 格式的 http 接口、WebSocket 接口，并基于 WebSocket 接口实现了 Java、Node.js 两种语言的 API 及多种语言的签名库。

- **应用层**

基于 ChainSQL 底层区块链网络实现前端各类场景的应用（包括 WEB、APP、小程序等形式）。

## 3.4 功能模块

### 3.4.1 数据库操作相关功能

数据库操作相关的功能是 ChainSQL 的核心技术模式，可以把链上的每一笔交易都以数据库操作的形式进行上链。

- **表操作：**建表、表授权、删除表、表重命名，用户可通过 ChainSQL 创建不同的表来区分不同的业务，对于创建的表自带权限控制，每张表只属于创建者。

- **数据操作：**插入、更新、删除、查询（支持复杂查询），对于链上创建的表可以进行一系列的数据操作，通过授权让其他用户进行访问操作表里的数据，保证链上数据的可控性。
- **数据库事务：**一系列操作的集合称为事务,事务操作可以同时创建多张表,同时对一张表或多张表进行一系列的增删改查操作。
- **数据库日志导入：**可以导入现存数据库操作日志到区块链中，实现数据库日志上链存储，平滑对接企业已有数据库系统。

### 3.4.2 隐私安全相关功能

隐私与安全是 ChainSQL 交易的核心保障功能。

- **表加密功能：**ChainSQL 在创建表的时候可以选择对表进行加密，对于加密表，链上节点同步的时候要有表的权限，才能把数据同步到自身的数据库，并做进一步的审计工作。
- **表的行级控制：**在建表时设置增删改查条件，对表进行操作是必须满足设置的条件，否则交易失败，该功能是对表的可控权限操作。
- **字段加密：**对表的某些字段的值进行加密之后插入到表中，数据库查看插入的数据是密文显示，需进行解密之后得到明文数据。
- **交易的 CA 验证：**ChainSQL 可以在配置文件中配置根 CA 证书列表，用户交易中需要带上自己的证书，ChainSQL 节点验证交易中的证书是由配置文件中配置的某一根 CA 签发的。
- **国密算法：**支持可插拔式的国密算法。

- **表的授权：**在 ChainSQL 中新建的表默认只有表的创建者有操作权限，只有在表的创建者给其它账户授予权限（如插入、更新、删除、查询）后，其它账户才有权限对表做相应操作。

### 3.4.3 特色功能

ChainSQL 的特色功能是根据区块链业务场景以及用户需求对链进行的一系列优化功能，这些功能在安全使用区块链的同时也避免了用户的痛点。

- **表、交易的订阅：**用户可以对表或某个交易进行订阅，订阅后关于该表或交易的每次动态信息，节点都会进行实时通知。
- **链的瘦身：**目前链上产生的数据过多对于服务器的性能会有很大影响，关于此问题，ChainSQL 支持删除数据库里的部分数据和日志文件再重新存储该表的记录，同时保证数据的不丢失。
- **表交易的 Dump：**用户的某张表,把链上的所有操作以 json 的格式保存下来，可用于交易的溯源。
- **表交易的审计：**可以对数据库表的指定条目、特定字段进行追根溯源，将所有影响了指定条目、特定字段的数据库表操作都记录下来。
- **智能合约：**内置智能合约虚拟机 EVM，并对 Solidity 指令做了扩展。智能合约里面也可集成对表以及数据库的所有操作，通过调用合约来进行交易的发起；同时也支持在智能合约里直接发行不同的积分，通过调用接口来进行积分的一系列操作。
- **跨链：**不同区块链系统之间进行业务交互的关键技术。

- **表同步：**为了保证链上数据的一致性以及可回溯性，ChainSQL 的表同步机制可以根据时间点、区块号、交易 hash 来对表里的数据进行指定同步，同时也保证了数据库的空间存储。
- **链空间特性设计：**区块链的存储空间是一大难题，因为区块链的机制，区块链在运行的过程中没有产生交易的情况下也会产生区块，由于区块链存在区块的结构信息，这样就会占用空间。ChainSQL 对于空区块的产生可以进行控制，支持在没有交易的时候不产生空区块。另外对于落块的条件也进行了相应的设计，根据交易池数量、区块里交易数、共识时间来进行自行配置控制交易落块。

### 3.4.4 工具包

工具包贯穿整个区块链系统。工具包包括：可视化功能调用平台、区块链浏览器和配置管理。

- **可视化功能调用平台：**ChainSQL 所有功能的可视化汇集平台，使用者可以在该平台上对 ChainSQL 的所有功能进行调用并调试。
- **区块链浏览器：**能够帮助使用者获取节点状态、链上交易信息、数据内容、性能数据等系统运行信息，实现运维管理和实时监控。
- **配置管理：**节点的配置信息进行同步管理，在增加或减少验证节点的情况下，保证链上信息的安全性的同时，对链上节点信息进行同步更新。

# 4.技术创新

## 4.1 共识算法

区块链上采用不同的共识算法会对系统的共识效率、去中心化程度产生不同影响。ChainSQL 采用自研的 PoP(Proof of Peers)共识机制，PoP 结合了 PBFT 与 RPCA 共识算法的优点，整体来看可分为交易集共识、区块共识两个阶段。

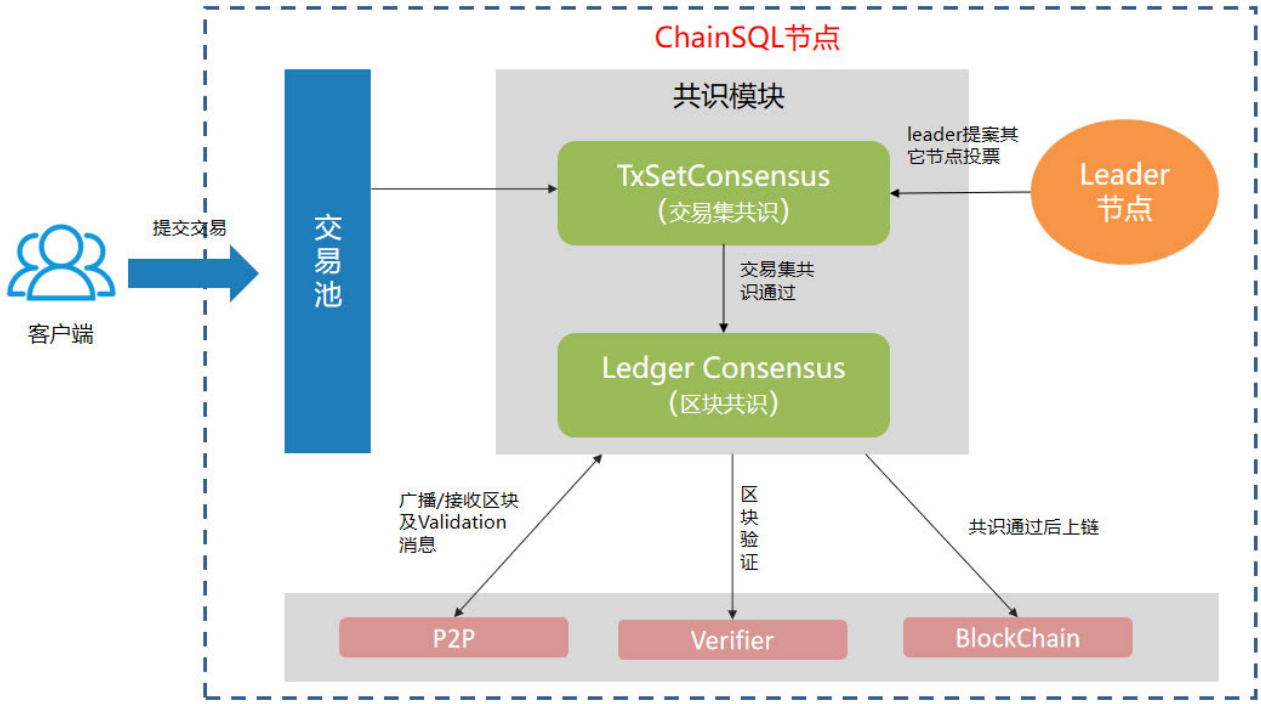


图 4.1 共识算法机制

在交易集共识阶段,每轮共识由全网唯一的 leader 节点(根据区块号轮换)对交易集提案，其它节点对这一提案进行投票最终达成共识。这样的优点是在交易量大时，使用 leader 提案的机制相比所有共识节点各自提案交易集然后解决分歧的机制更容易达成共识。

在区块共识阶段，每个节点在交易集达成共识后按顺序验证交易集中的每一笔交易，最终得到一个状态树根 hash，并结合交易集构成的交易树根 hash、区块号、时间戳等构造区块头信息，然后每个节点各自对自己生成的新区块投票并收集其它节点的投票，得票数超过阈值的区块被认为验证通过。由于每个节点在这一阶段已经达成一致的交易集，所以很容易达成共识。

## 4.2 分片共识

ChainSQL 中通过分片架构对共识性能进行提升，在对所有节点进行网络分片的基础上对交易进行分片，提高共识 TPS。分片网络的整体性能随着分片数的增多而增大。

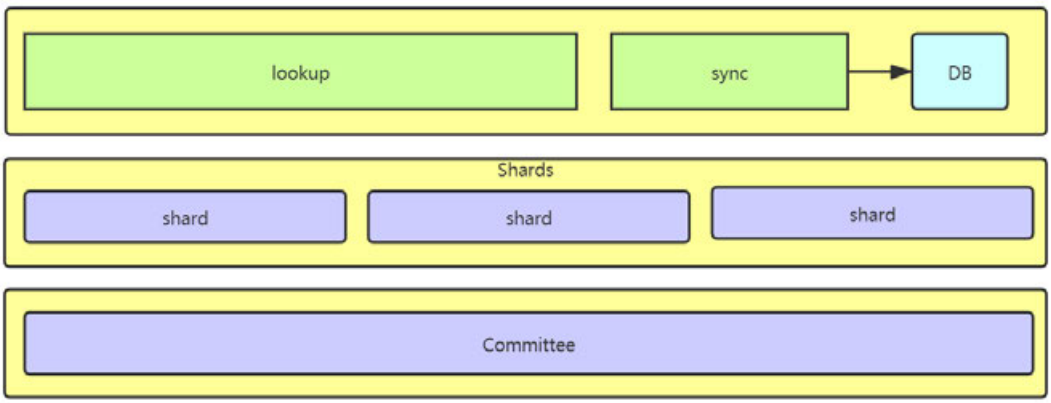


图 4.2. 分片架构

分片架构最上层为直接与客户端对接的节点和数据库组件，Lookup 节点主要负责接收交易、分发交易到各分片，持久化、发布区块等。Sync 节点作为 ChainSQL 表同步功能执行单元，可插件式灵活接入。

各分片主要执行交易以及共识。在这一层，共识的结果主要是由各分片上的交易产生的状态变化而不是最终状态。分片节点主要负责执行交易，产生状态

变化，并提交给最下面一层委员会。各个分片独立并行运行，互不依赖和干预，大大增加了整个网络的共识能力。

委员会合并所有分片共识的结果，并对最终区块进行共识。将区块分发到全网同步，分片网络中每个节点都具有全网状态。

## 4.3 共识可拔插

在配置文件中配置共识算法及参数，可兼容更多共识算法。

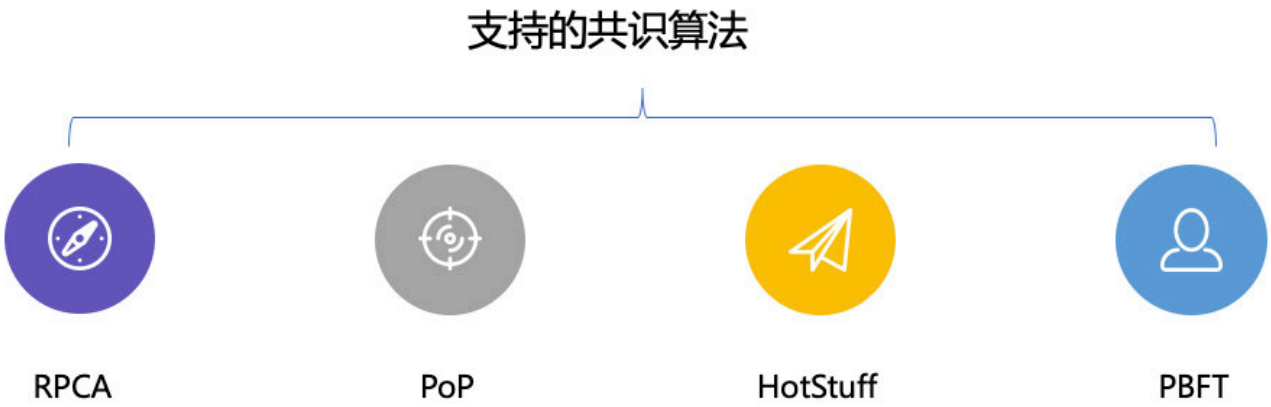


图 4.3 支持的共识算法

## 4.4 多链技术

### 4.4.1 架构设计

在多链的设计中，通过主链的世界状态管理各子链；每条子链都有独立的 P2P 网络、交易池、共识、存储以及数据库模块。

主链：管理子链共享的数据。

子链：实现具体业务。

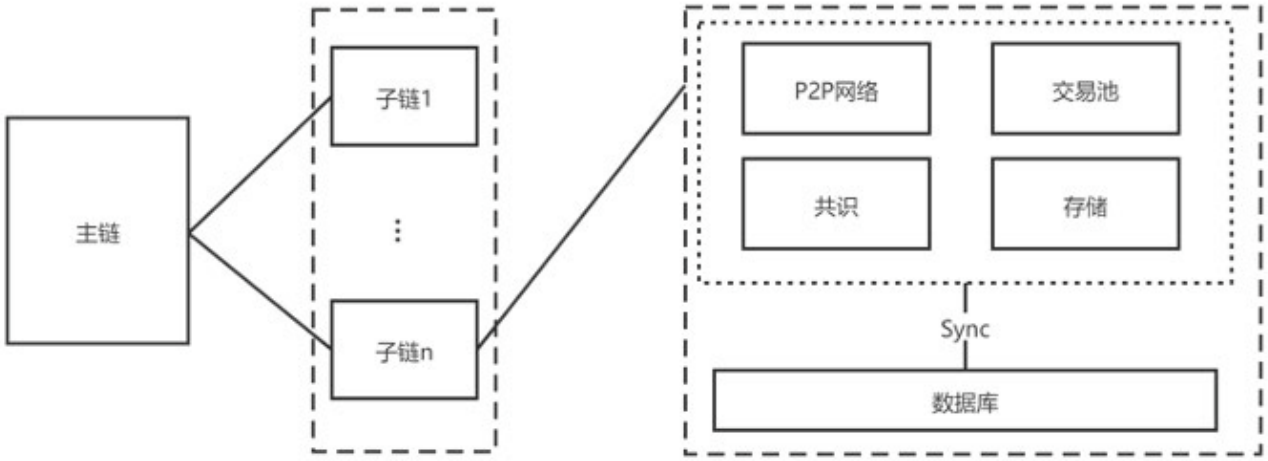


图 4.4.1-1 架构设计

- 子链不继承主链任何状态，是一个全新的链；
- 子链只继承主链账户状态，需要锚定主链上的区块；
- 主链与子链共享账户余额，使用跨链的方式从主链向子链兑换积分。

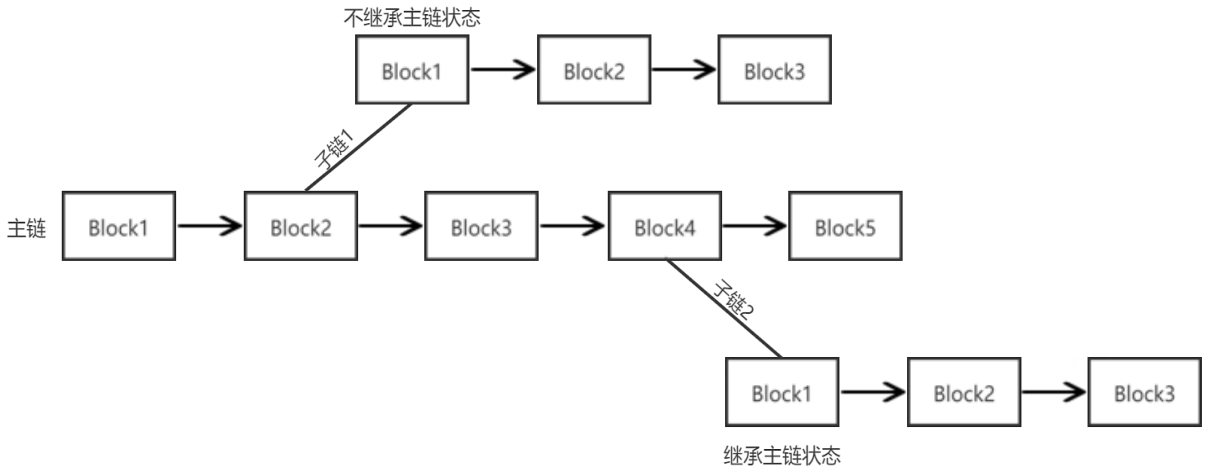


图 4.4.1-2 方案设计

### 4.4.2 特性

- 先有主链：子链是在主链的基础上创建的，而且每个子链成员都需要同步主链数据；

- 去中心化管理：通过主链上的世界状态对子链进行管理，子链的创建、子链节点的增删都需要通过交易完成；
- 存储隔离：每条子链之间的存储是隔离的，对于一个参与多条子链的节点来说，多条子链在磁盘上的存储是通过文件夹隔离的；
- 主链可继承：在创建子链时，可选择继承主链的账户状态，这样可以实现主链初始化一次，多条子链共享同一主链状态的效果；
- 治理多样化：子链中节点的增加与删除，可以通过指定的管理员进行中心化操作，也可以不指定管理员，通过多数节点投票的方式实现；
- 网络隔离：只有属于同一子链的节点才能收到主链相关的消息，不同子链的节点消息不互通，在网络层实现数据隔离。

## 4.5 存储

### 4.5.1 数据对象管理

利用基数树与默克尔树的混合算法来存储数据。使得数据查询、定位的算法复杂度降低到了对数级别，根据数据的摘要值能快速定位到数据在树上的位置。

树共设计有 64 层，每个节点最多有 16 个子节点，同一位置上不会存在不同的两个数据，链元数据全部存储在树的叶子节点中。

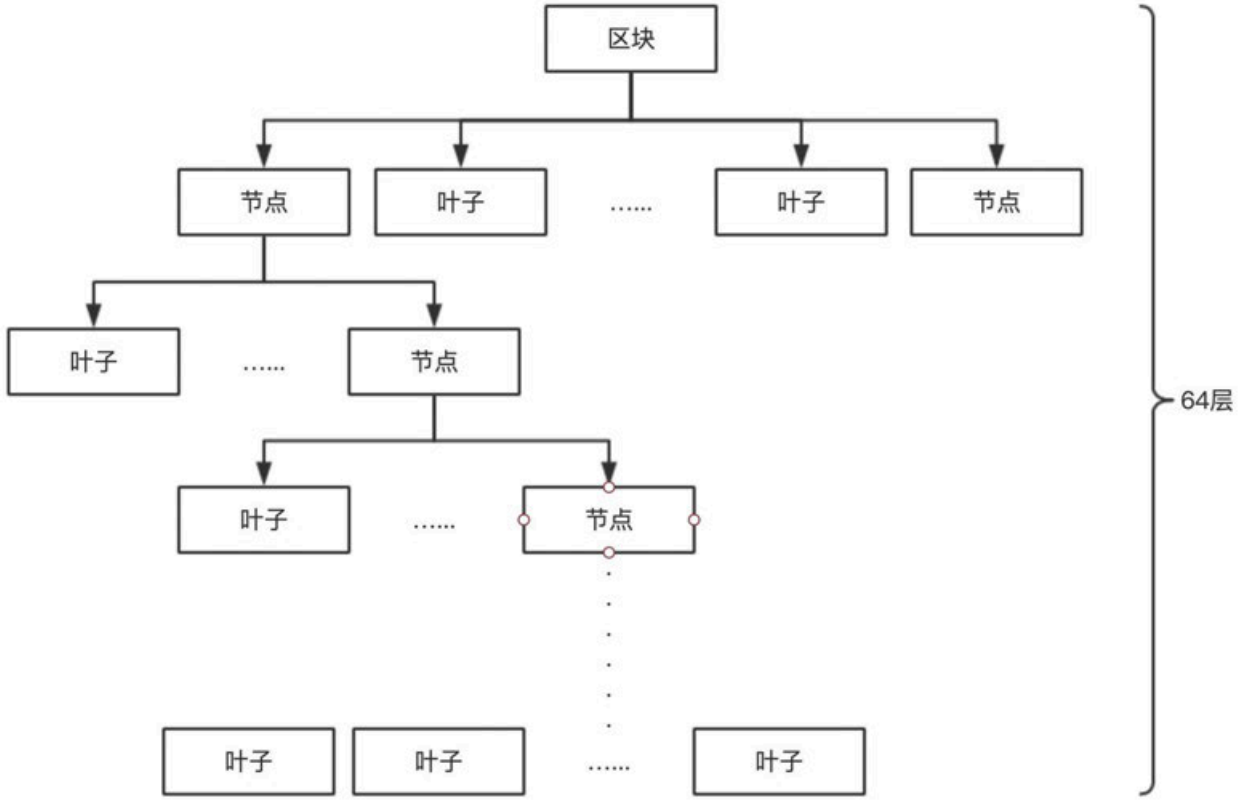


图 4.5.1 树状结构

### 4.5.2 数据缓存

数据的读取与写入都进行了二级缓存处理：数据库到内存数据的第一级缓存保证串行化数据存取的效率，内存数据到结构化对象数据的第二级缓存保证数据对象构造与销毁的合理性。

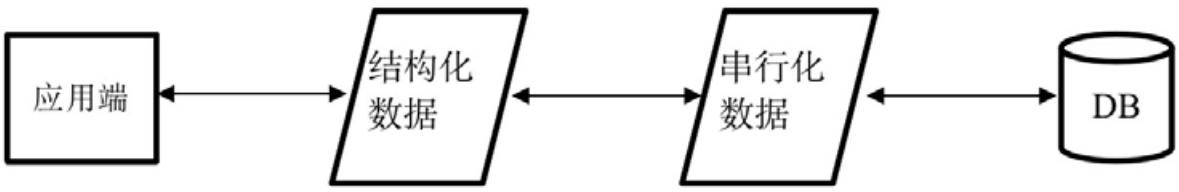


图 4.5.2 数据的读写路程

单个区块上的数据形成一个树状结构，多个区块上的数据互相引用，最终在内存中的数据呈现一个网状结构，合理利用了内存中的每一个对象，使得查找整个区块链历史上的任何一个细节变得像查询普通数据库一样迅捷。

### 4.5.3 数据索引

交易产生日志，结构化数据库则是这些日志的消费者，日志系统中记录的过程日志可转化为结构化数据库所能表现的最终数据状态。这个日志的消费转化过程在 ChainSQL 中称为表同步，日志系统中的数据流被打向这个表同步模块中，原始数据也会原封不动的在区块中保留，根据日志记录过程中建立的相关索引，表同步模块可按序将每条操作日志在数据库中执行，也可灵活按需要对数据流进行同步，最终在数据库中呈现可靠的数据状态。

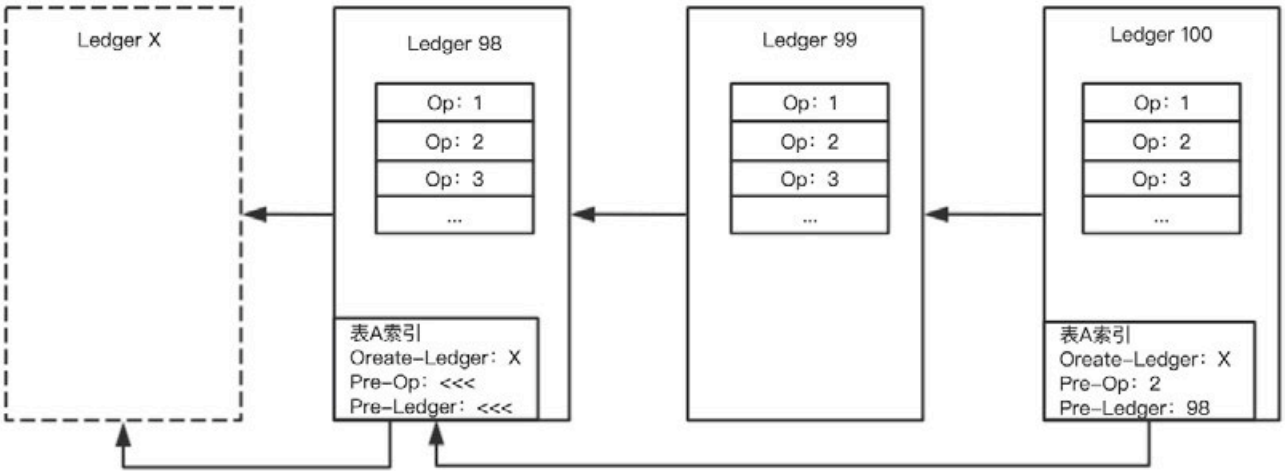


图 4.5.3 数据索引

### 4.5.4 数据存储

ChainSQL 中对数据的存储既用到了关系型文件数据库 SQLite，又使用了 Key-value 存储 RocksDB/NuDB。RocksDB/NuDB 中存储所有区块数据，而 SQLite 数据库中按类别存储了各种索引数据。

这种结合使得 ChainSQL 很容易就能支持一些复杂查询操作，比如查询某个账户在某个区块范围做过的所有某种交易，查询区块链中总的交易数量等等。

### 4.5.5 分片存储

区块链一般使用冗余存储的方案来存储历史数据，并且一般是全冗余存储，也就是在每台数据服务器需要存储所有数据。这样的问题是当存储的数据超过配置的空间限制时，需要不断扩充存储空间。

使用历史数据分片存储技术，ChainSQL 可以实现类似分布式数据库中数据分布式存储的效果。单个 ChainSQL 服务器可以只存储部分历史数据，而无需存储所有历史数据。

## 4.6 密码算法

ChainSQL 设计了可插拔的密码框架，使用开关的形式同时支持国密加密算法与国际通用密码算法。国密算法可由硬件设备或者软件代码提供，如国密 SM2/SM3/SM4；国际密码学算法包括非对称性加密算法：ECC，同时支持两种签名算法：Secp256k1 与 Ed25519，哈希算法：安全散列算法 SHA 家族，对称密码算法：AES 等等。

## 4.7 用户身份

### 4.7.1 准入机制

区块链中，用户身份一般不做限制，任何人只要有一个合法的钱包，就可以在链上发交易。但是在某些安全级别较高的应用场景中，只有某些授权用户才被允许在链上操作。

ChainSQL 中通过给用户发证书(CA)的方式来实现用户身份准入机制，用户需要向链的管理方申请证书，并在发交易时附加证书。节点会配置它信任的根证书，只有交易中的证书是这些根证书签发的证书，交易才会被验证通过。

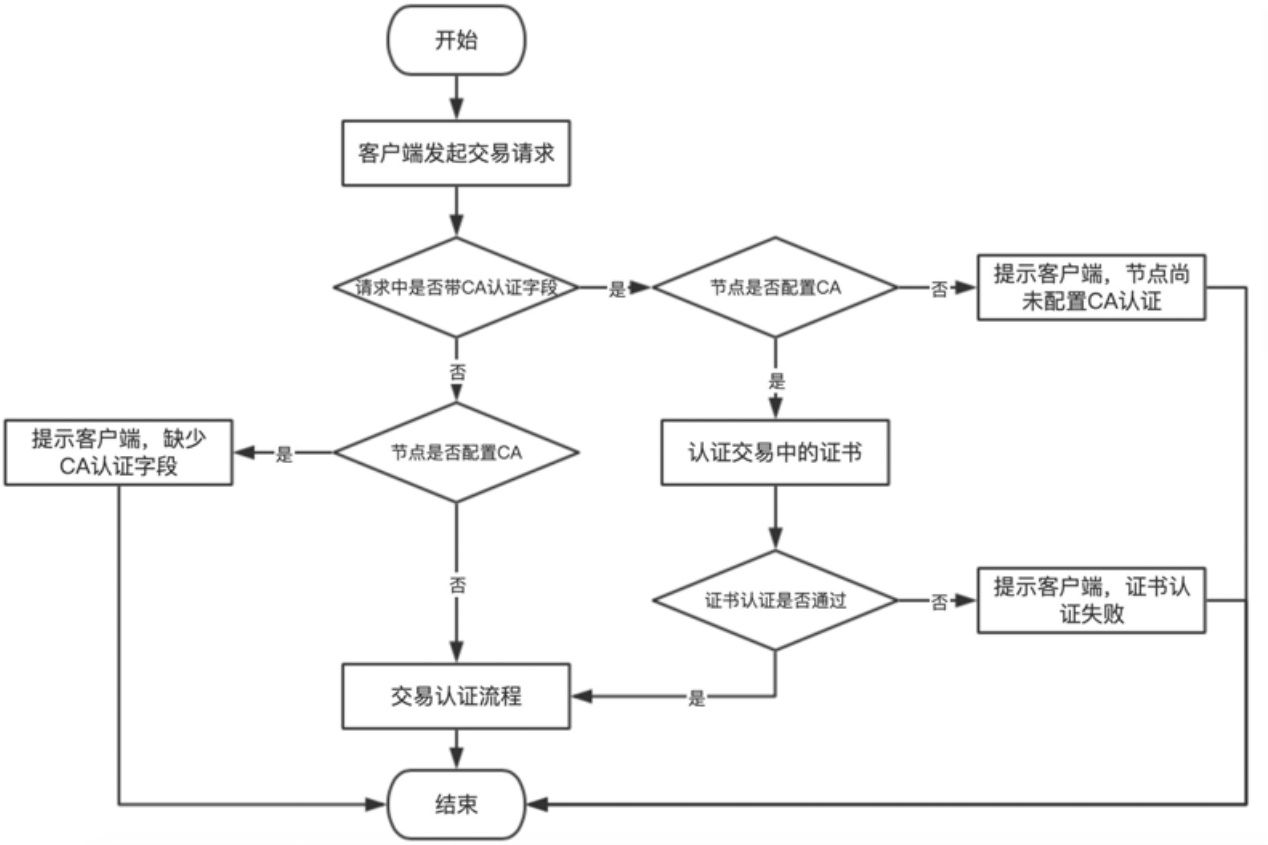


图 4.7.1 准入机制

### 4.7.2 隐私保护

利用零知识证明保证用户身份，在链上不暴露交易对象的身份（包括签名、公钥、地址等），由原来的依赖签名确权方案变为依靠证明的确权方案。签名对象、签名数据都在本地进行保存，链上只存储证明数据。证明的计算在线下完成，证明的验证在链上进行。

## 4.8 智能合约

扩展智能合约指令，打通了与 ChainSQL 中其它交易的调用，使合约数据与链元数据的交互成为可能。不仅可以通过区块链交易改变合约内部数据，还可根据合约的内部逻辑判断来影响合约外的区块链世界状态。

## 4.9 区块链服务平台

众享的区块链服务平台（BaaS）旨在构建高效、安全、智能、可扩展的企业级区块链架构体系。用户通过部署资源、搭建区块链网络、编写智能合约、构建去中心化应用，即可搭建出属于自己的区块链系统和应用，降低企业开发和使用区块链的成本。

通过创新的一键部署、多链技术及多区块链框架支持，实现不同联盟方区块链网络的快速搭建、可视化维护、多链连接及扩展。平台通过和企业 CA 系统平滑集成，为区块链网络提供可靠的接入安全认证；另外，还提供一套完整的解决方案，包括资源接入、访问控制、服务监控等管理功能以及区块链网络维护服务。

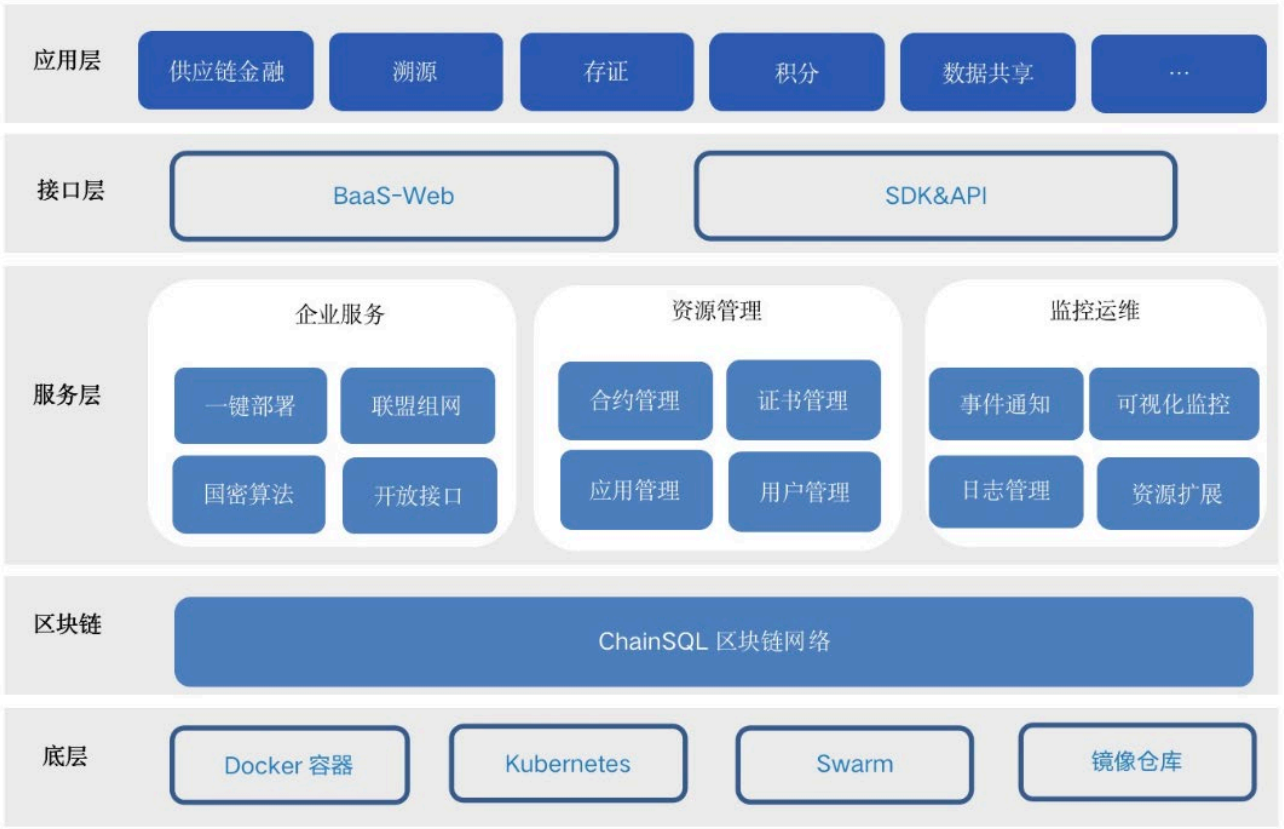


图 4.9 系统架构

## 4.10 众享区块链超级工作站

众享区块链超级工作站实现物理主机+区块链网络+应用系统+运维监控全场景服务，让企业级区块链应用进入极简时代。采用超融合设计，开箱插电即用，一键启动，区块链系统自动部署、分布式文件系统自动搭建、应用系统自动启动、运维系统主动管理，无需专业区块链部署和维护技术人员。各节点预装区块链底层架构软件 ChainSQL，全面支持国密算法，并可与第三方 BaaS 平台融合对接。

众享区块链超级工作站服务器采用特殊的“四子星”高密度结构设计，把 2U 机架式空间发挥到极致，集成了 4 个独立的可热拔插的 Intel 新一代至强系列双路子系统，全新架构打破了 Intel 传统产品的规格限制，综合性能得到大

幅提升。本产品把计算能力、存储空间和存储网络三者融合一体，跟传统架构相比有性能卓越、管理性强的优点。

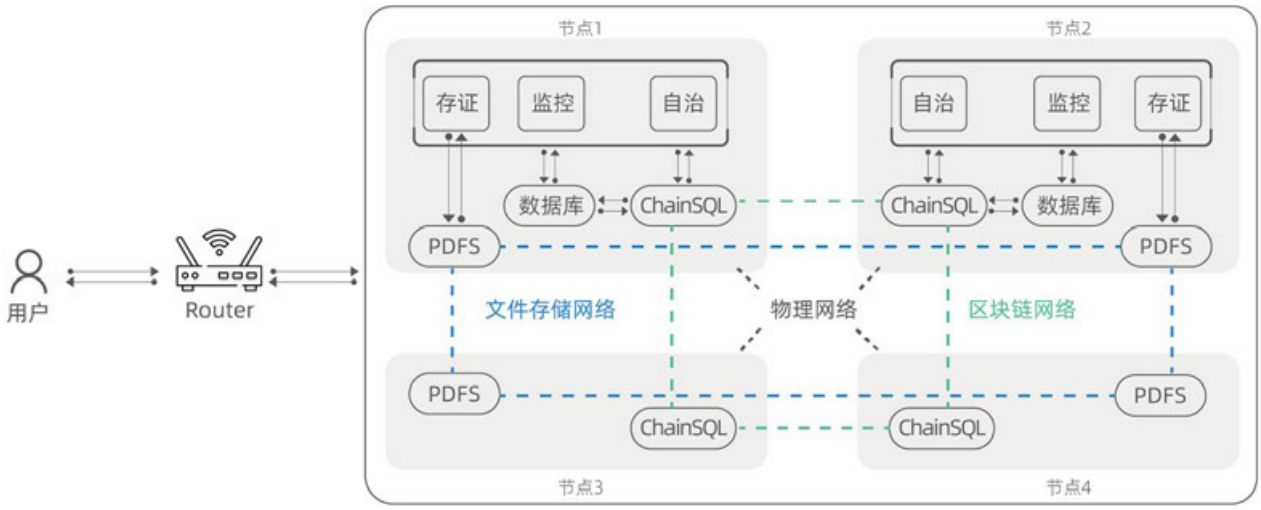


图 4.10 产品架构

## 4.11 自主可控国产化适配

ChainSQL 区块链系统国产自主可控。相继完成与中标麒麟高级服务器操作系统软件 V7.0（X86-64）、人大金仓数据库管理系统 KingbaseES V7 和 V8、华为技术有限公司 TaiShan 200 系列、银河麒麟高级服务器操作系统（飞腾版）V10 和中标麒麟高级服务器操作系统软件（ARM64 版）V7.0 的兼容性测试，获得三项麒麟软件 NeoCertify 认证、人大金仓产品兼容性认证及华为技术认证书。

目前，ChainSQL 已经完成自主可控认证的国产服务器、操作系统、数据库等，为从硬件到软件全部由国产自主可控厂商提供官方认证的区块链底层软件产品。

## 4.12 技术优势对比

| | ChainSQL | Fabric | FISCO-BCOS | 京东智臻链 | 百度 XuperChain |
|---|---|---|---|---|---|
| **共识机制** | PoP(Proof of Peers)共识机制,PoP 结合了 PBFT 与 RPCA 共识算法的优点 | 背书+排序+验证 | PBFT、实用拜占庭容错算法(Raft) | 优化的 BFT 共识协议 、可插拔共识协议、拜占庭容错、动态调整节点 | 可插拔共识机制，包括但不限于 POW、POS、PBFT、Raft 等，创新 TDPOS 共识 |
| **吞吐量** | 万级 | 2000 | 万级 | 万级 | 万级 |
| **确认时间** | 1 秒 | 时间可调，最低 1 秒 | 秒级 | 秒级 | 秒级 |
| **数据库** | MySQL 、 SQLite 、 MongoDB 、 HBase 、 Oracle、DB2、南大通用、武汉达梦、人大金仓、神通数据 | LevelDB CouchDB | LevelDB external(mysql) | NoSQL | 通过抽象的 Key-Value 接口设计，使得能够集成各种底层存储引擎，例 如 ： Leveldb 、 Baddger、Rocksdb， 只要实现了 Put、Get、Iterator 等接口，就可以将第三方的存储引擎集成进来。 |

# 5.应用服务

## 5.1 区块链应用程序接口（APIs）

ChainSQL 提供命令行接口、JSON-RPC 接口、WebSocket 接口、Java 接口以及 Node.js 接口。

命令行接口主要功能包括：

- **链的状态信息查询：**查看节点的运行状态、查看已连接的其他节点的连接状态和同步状态等；
- **数据库表 dump：**将数据库表的操作以文档的形式进行记录；
- **数据库表审计：**对数据库表的指定条目特定字段进行追根溯源，将所有影响了指定条目特定字段的数据库表操作都记录下来。

JSON-RPC 接口、WebSocket 接口、Java 接口以及 Node.js 接口提供了 ChainSQL 各项功能的支持，用户通过调用相应的接口，可以实现 ChainSQL 的各项功能：

- **基础转账交易：**实现 ChainSQL 的系统通证转账功能；
- **数据库表操作：**即在 ChainSQL 上实现对于数据库表的创建、数据库表的插入、数据库表的更新、重命名数据库表、数据库表的删除、数据库表权限的授权、数据库表数据的查询以及加密表的支持；
- **智能合约：**即将 Solidity 智能合约在 ChainSQL 网络上进行部署和运行；
- **积分发行：**支持积分发行机制；
- **CA 证书：**提供接口设置 ChainSQL 账户的 CA 证书信息。

详细的接口介绍及使用方法见 ChainSQL 官方技术文档。

## 5.2 应用开发包（SDKs）

ChainSQL 区块链提供 Java 以及 Node.js 的 SDK 开发包，代码是完全开源的，源码地址为 JAVA SDK 地址、Node.js SDK 地址。

通过 Java 和 Node.js 的 SDK 开发包，用户可以便捷地与 ChainSQL 区块链节点进行交互，进而实现 ChainSQL 区块链的基础转账交易、链数据查询、数据库表操作、智能合约操作等交互操作。

具体的 SDK 使用文档见 Java SDK 使用，Node.js SDK 使用。

# 6.落地案例

## 6.1 存证平台

利用区块链技术实现数据的可信存储，使用数据多级加密和多维权限控制技术，解决传统数据易伪造、易篡改、难溯源、难校验的问题。同时平台支持一键仲裁/一键诉讼，仲裁机构或法院被授权后可直接从链上查看数据，大大提高了办事效率。

区块链存证平台联合司法公证处、司法鉴定所、仲裁机构、法院等机构，建立联盟链，以电子数据为操作对象，将证据固化在区块链存证平台，实现电子数据的采集、存证、取证、公证、鉴定、调解、仲裁等全流程服务。在电子证据的获取和保存过程中应用区块链存证，可以有效、完整地向法庭呈现电子证据形成的全过程，让这些机构可以在未来任意时间验证某一电子数据的原始性、真实性。证据信息一经存储，任何一方无法篡改。

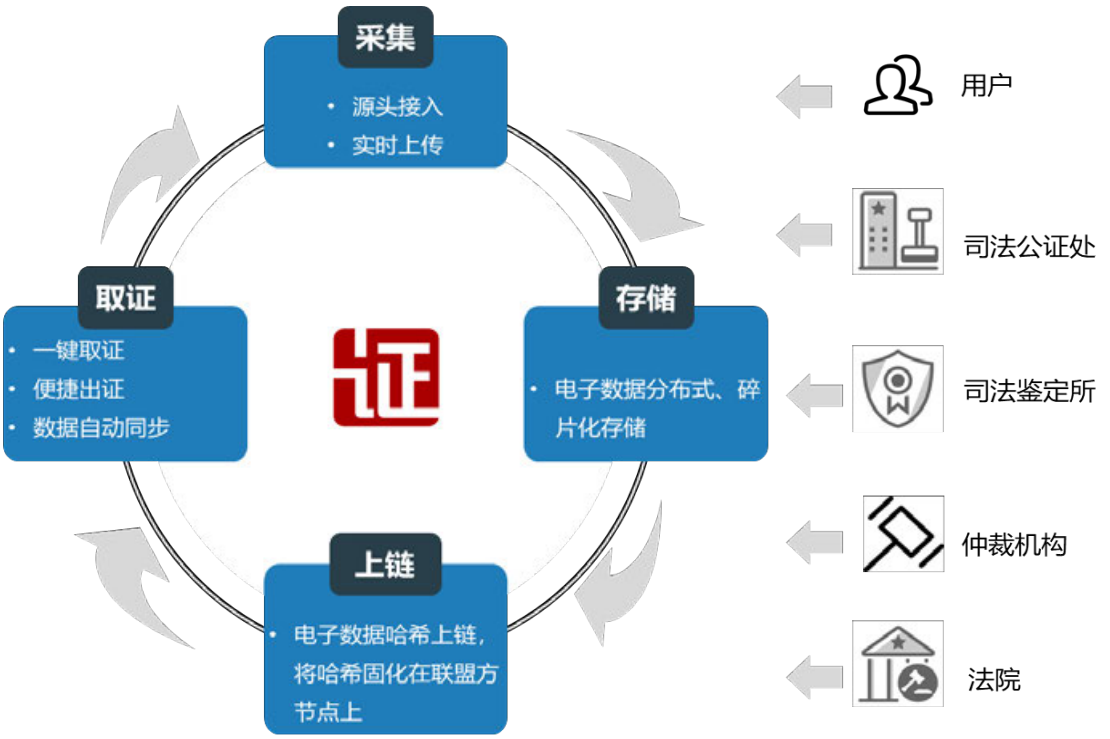


图 6.1 存证流程

**受益角色：**

- **监管机构：**一旦产生纠纷，监管机构可从联盟链中的司法鉴定、审计、公证、仲裁机构随时取证监督，更便捷。
- **裁决/公证机构：**仲裁/公证机构可直接从其运维的节点中获取和验证数据，把存证数据视为直接证据，不再需要第三方机构出具证明，方便易用。
- **存/取证人：**区块链存储，确保信息完整、不被篡改，提高数据的公信力；全流程操作链上完成，减少传统方式中涉及人员多地奔波取证问题。

## 6.2 溯源平台

溯源平台结合物联网、大数据、人工智能等先进技术，将商品从原材料采购、加工、生产、质检、物流、经销商、零售商的全流程信息记录上链，平台包含了信息录入、溯源查询、监管报送等主要功能。

区块链溯源平台面向政府、企业、认证等各类型溯源行业组织提供安全、可信、易用的信息录入、设备管理、监管报送、溯源查询服务。平台关键环节采用物联网技术保证信息的自动生成和上链，降低人力成本；消费者在平台中将由被动受益者变为溯源生态参与者，汇聚营销大数据，帮助企业优化生产、提升政府监管效率。

平台彻底改变目前溯源方式普遍存在的消费者不信任、企业不积极、流程不透明、监管手段缺失等问题。

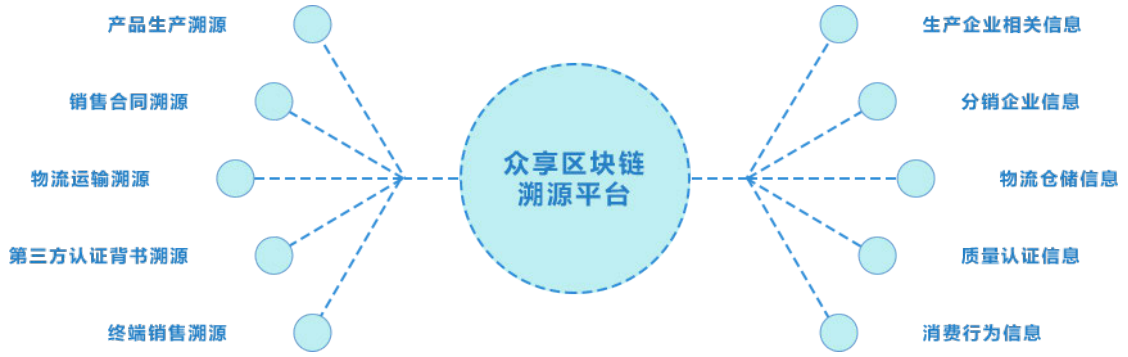


图 6.2 溯源平台

**受益角色：**

- **企业方：**企业方可汇聚大量的营销数据，实现精准营销，降低营销成本，帮助企业优化生产，提高生产效率。
- **监管方：**每一个环节的信息写入区块链，信息公开透明、不可篡改，提升监管方的监管效率。
- **消费者：**扫描二维码对商品进行自动识别，对商品的真伪鉴别可通过区块链上的信息快速溯源验证。

## 6.3 数据共享

数据共享通过数据加密和签名技术，使双方实现数据的精准交换和共享，平台包含数据上传、数据合约、数据共享和数据查询等主要功能。

数据共享平台连接数据使用方、数据提供方、建模服务方、监管方等，共同组成可信的区块链网络。将数据收集、存储、管理、共享、开放、分析、结算过程上链存证，实现数据全生命周期可信管控，形成数据使用事前审核、事中监控、事后溯源的数据监管机制。

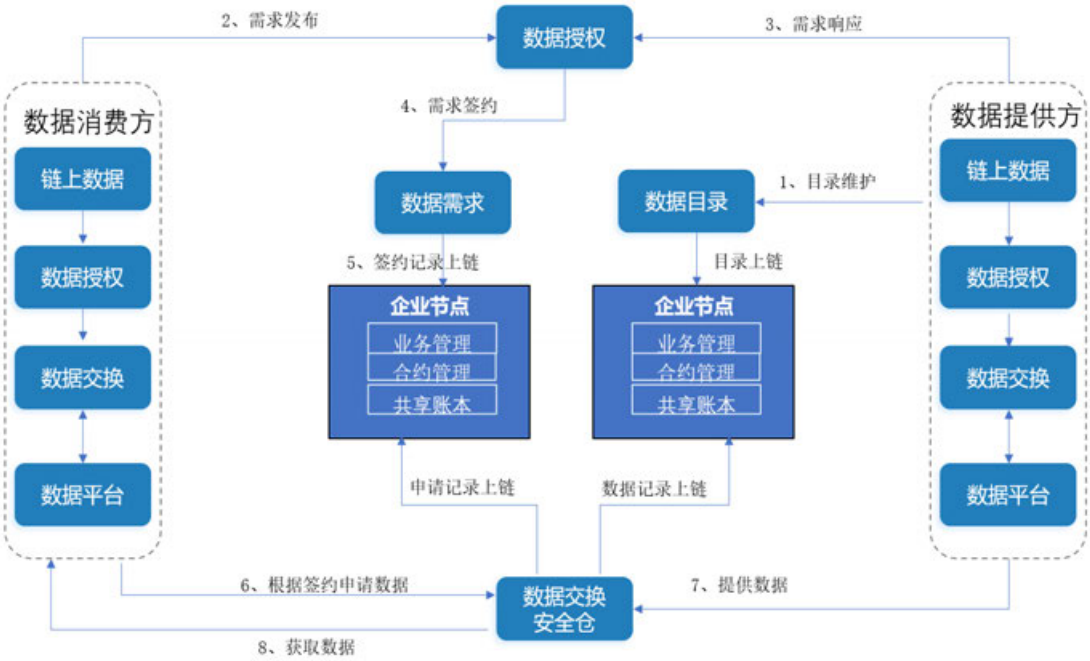


图 6.3 数据共享流程

平台支持多种数据交换模式，可以支持加密密文数据交换和共享，支持基于数据目录、数据授权的共享，也支持基于数据模型、数据计算的数据共享。旨在解决各方之间信任壁垒问题，细化数据确权机制，精准实现身份数据、数据目录、数据定义、数据需求、共享数据的链上操作，保障数据的所有权、使用权、收益权不受侵犯。

**受益角色：**

- **政府部门：**政务数据的共享能够更大的发挥政府部门职能，并能够打造真正意义上的数字政府、数字城市，进而推动整个社会的数字化转型进程。
- **数据交易平台：**实现数据在共享及流通过程中对数据确权，明确数据的产生者、使用者、管理者及受益者，实现数据的精准授权，促进数据的共享及流通。
- **数据提供方：**应用零知识证明技术，可以在密文情况下实现数据的关联关系验证，在保障数据隐私的同时实现数据共享。

## 6.4 分布式资产交易平台

分布式资产交易平台包含资产发行及管理、自动撮合交易、信息认证、充值提现、账单查询、人员管理等功能。

在传统的交易模式中，资产进入流通后，仍必须依赖资产发行方系统才能完成使用、转移，这就将资产流通范围限制在发行方系统用户内。应用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；且区块链“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。

平台适用于数字资产交易、能源交易、版权交易、奢侈品交易、艺术品交易、精准扶贫等众多场景。

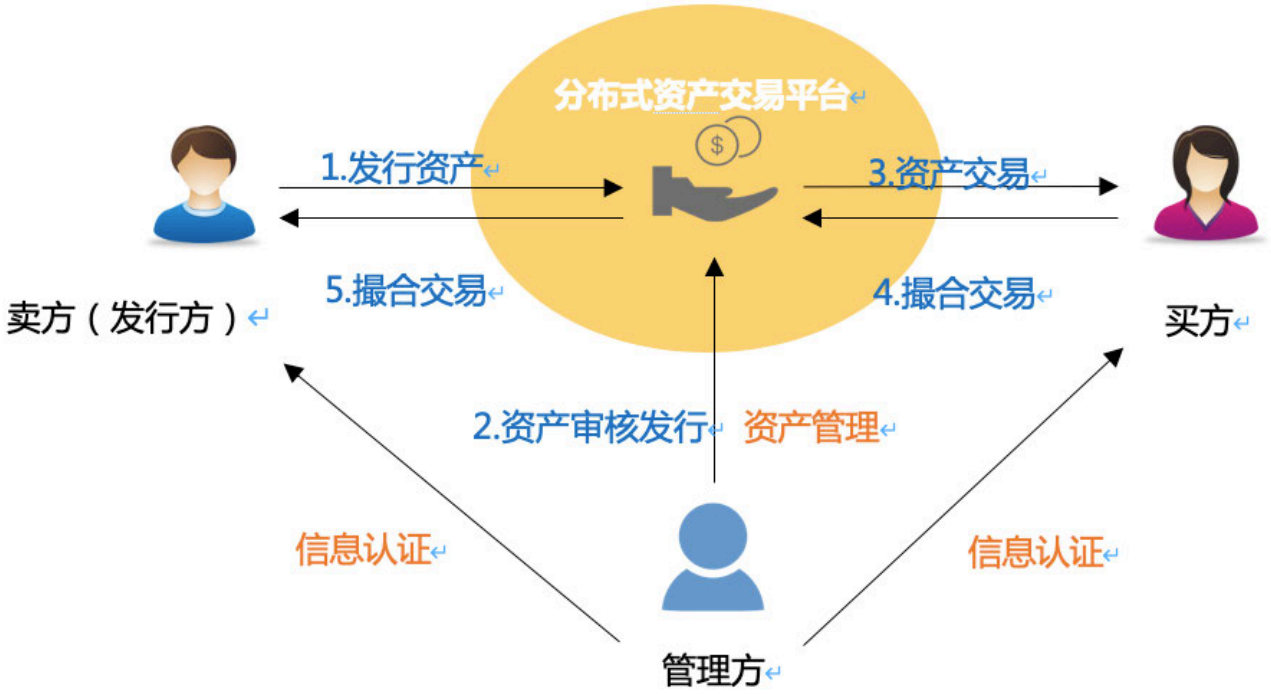


图 6.4 交易流程

**受益角色：**

- **平台管理方：**基于区块链的分布式交易平台天然地具有技术信任属性，交易真实有效、可查询追溯，能有效解决传统交易平台数据不透明或数据造假、中心化平台易受攻击等问题，极大地降低投资风险。
- **发行方：**发行资产受众更广，且资产链上登记，保证产权的唯一性；撮合交易进行变现，每笔交易链上可查，避免纠纷；近乎“实时结算”，有效解决对账繁琐，对账效率低等问题。
- **买方用户：**获取真实可靠资产信息，交易透明、可追溯。

## 6.5 供应链金融

平台覆盖供应链金融全链条，包含了应收账款登记和确权、应收账款提前撮合支付、保理融资等主要功能。

区块链供应链金融平台围绕核心企业，覆盖其上下游中小微企业、商业银行、保理公司等资金端及物流、仓储企业。平台核心功能为整合贸易基础信息的聚合，确保账款信息来源的真实性、平台交易的信息不可篡改、交易的过程信息透明公开、交易成功的信息可溯源查询。

平台聚焦应收账款登记、确权及应收账款转让后的管理，通过撮合应收账款提前支付、应收账款的保理融资等方式帮助供应链上的供应商更快更稳健地获得资金支持。

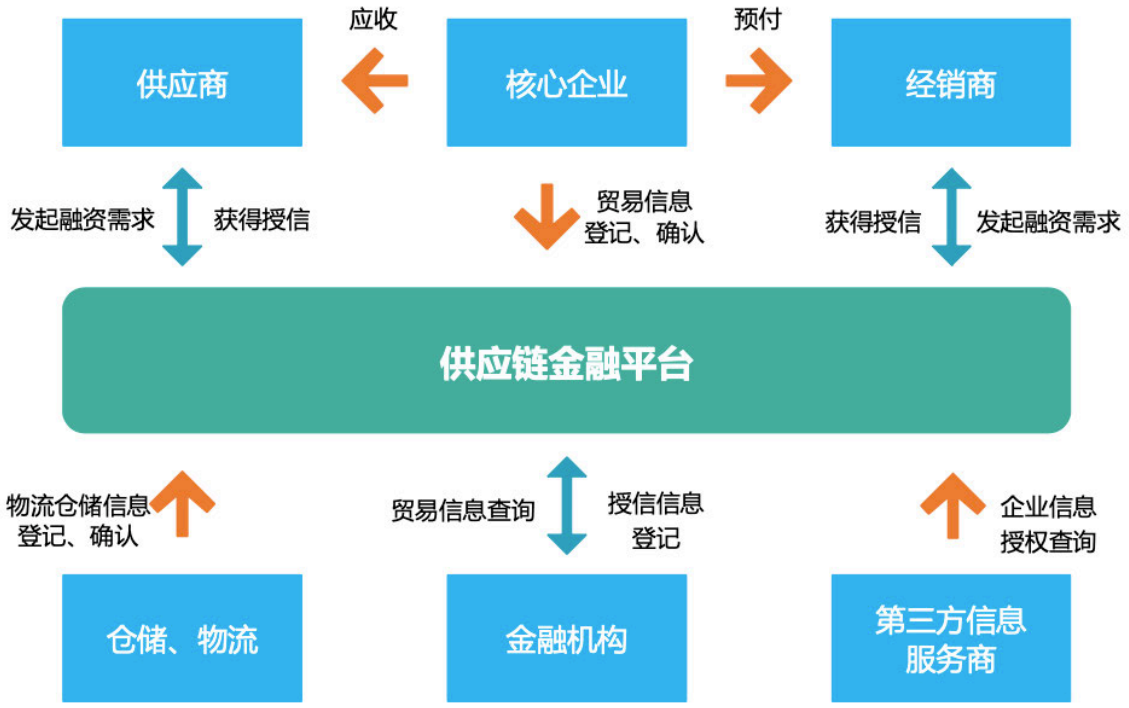


图 6.5 供应链金融流程

**受益角色：**

- **应收企业：**在平台上进行快速、低成本的融资，优化企业现金流，提升资金周转效率。
- **应付企业：**在平台上向应收企业进行提前支付撮合赚取收益，使得资金最大化的合理有效运用。
- **金融机构：**在信息透明、风险可控的条件下为企业融资并赚取融资利息。
- **核心企业：**平台解决了上下游供应商、经销商的融资问题，优化供应链整体效应，增强企业的核心竞争力。

## 6.6 区块链扶贫

利用区块链实现扶贫款项的流转，保证了扶贫信息的公开透明、可追溯，从而实现专项专用，精准扶贫。

区块链扶贫将传统的人工管理、资金管理方式与区块链技术应用有机结合，让扶贫款项沿着规定的用途、条件、时间等，透明精准地下发。此举既保证了扶贫款项使用过程中的规范性、合理性；又简化了扶贫基金的使用流程，实现扶贫资金的下拨不走样、不截留、不挪用，遏制了扶贫造假等现象，有效避免人为因素导致帮扶资金过多消耗在“路上”，从而提高扶贫款项使用效率。在扶贫过程中，每一笔扶贫资金的使用都会在链上留痕，使扶贫款项的运作更加透明化，为扶贫资金的监督管理创造了有利条件。

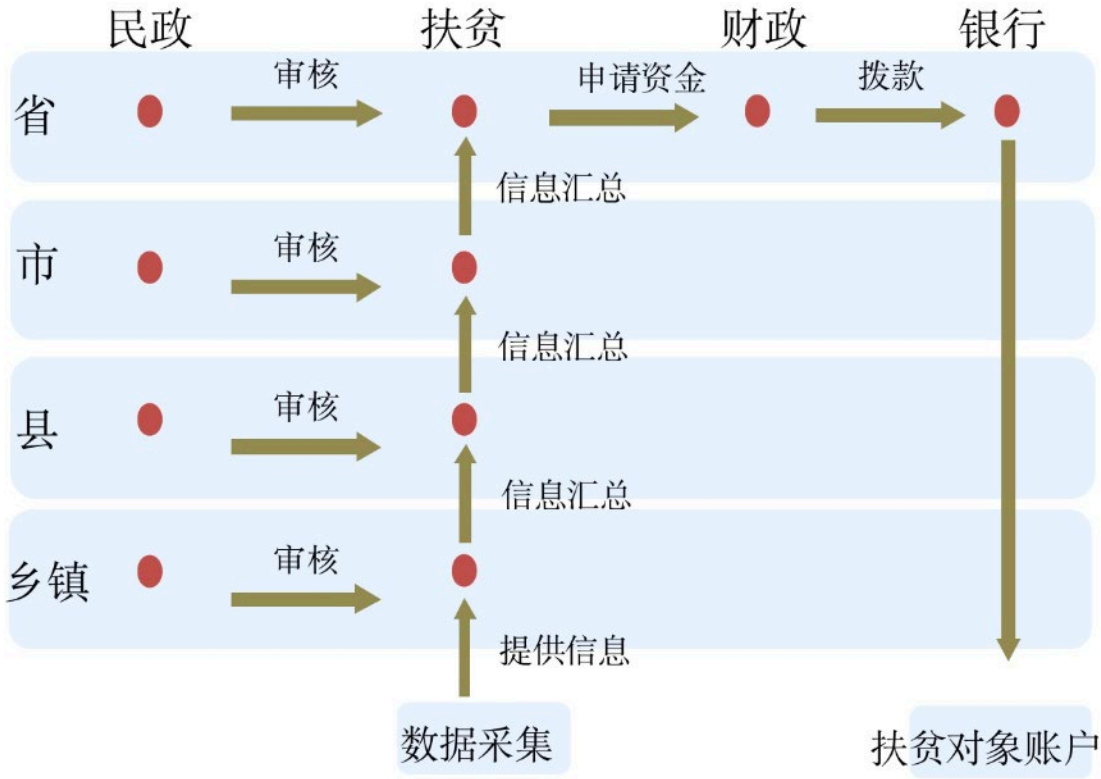


图 6.6 扶贫流程

**受益角色：**

- **扶贫方：**可直接将拨款给指定的人或机构，实现款项定向下发。
- **监管方：**扶贫款项的每一次流转都会直接记录在链上，不可造假，不可篡改；监管方可实时追溯钱款流向，减轻监管负担。
- **扶贫对象：**区块链一定程度上保证了钱款各个环节流通的公开性、透明性与真实性，有效助力帮扶对象快速、公平的拿到帮扶资金。

## 6.7 资产证券化

资产证券化包含了资产包管理、资产发行管理、资产风险管理、现金流管理和资产挂牌管理等主要功能。平台旨在利用区块链技术穿透底层资产，将底层资产信息上链，保证数据公开、真实、不可篡改，让链上的产品设计全流程透明化，建立新的信任机制，大幅优化交易流程。覆盖资产证券化的六个阶段：

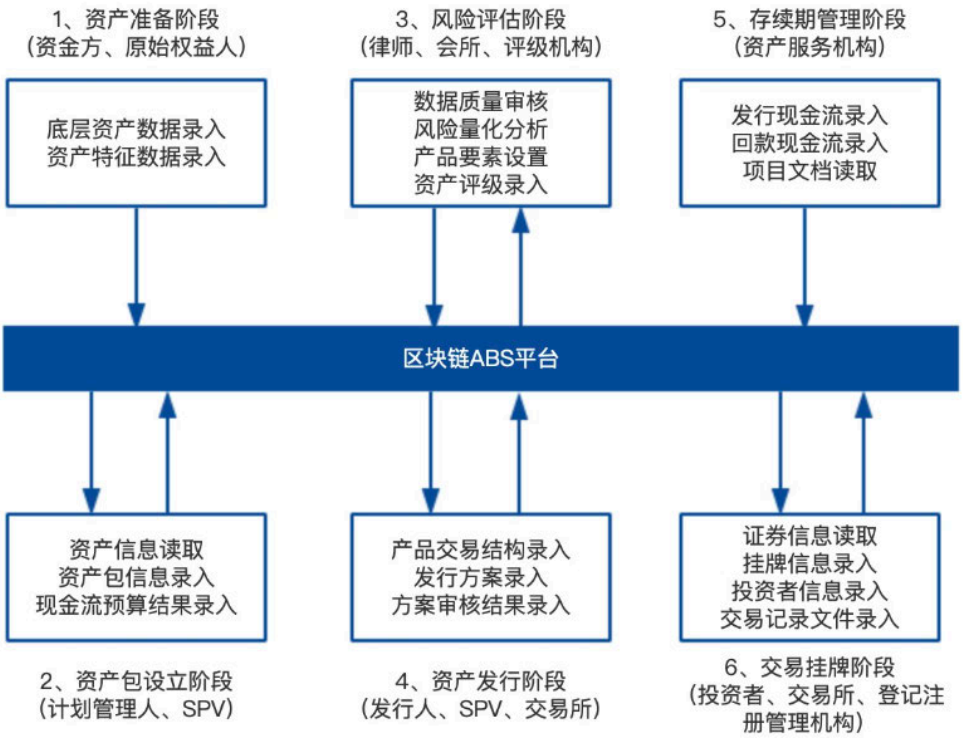


图 6.7 资产证券化流程

在前期的资产池数据、现金流预算结果、风险评级录入阶段，应用区块链技术可以实现更加精确的资产洞察、现金流管理、数据分析和投后管理；到准备期的产品设计发行阶段，交易结构和评级结果由评级公司和券商确认后再共识入链；中期投资人注册登记环节阶段，投资人可以从链上获取数据，以及上传数据至区块链；在存续期管理阶段，回款数据、循环购买数据、资产赎回、置换和回购数据均可入链，并可生成资产服务报告。

**受益角色：**

- **投资者：**通过底层资产逐笔穿透监控，可对资产历史信息、实时表现进行全程监测，缓解了金融资产信息不对称的难题。
- **资产发行人：**产品设计全流程的透明化，动态实时的信息验证渠道能提升投资者信心，有助于降低操作及合规成本。
- **资产管理人：**帮助资产管理人从资产生成、筛选组包、资产分析、产品设计、展示上架、投资兑付、资产监控到监管报送在内的全流程智能化管理。

## 6.8 积分商城

方案应用区块链技术，构建公开、透明的积分商城。商城可发行区块链积分，并支持多商铺多积分模式，构建“电商+积分+区块链”生态系统。旨在利用区块链积分技术，优化传统积分商城方案，解决传统积分存在的问题，打造一个公开透明、灵活配置、有效提升各方效率、助力商户突破营销瓶颈的区块链积分商城。

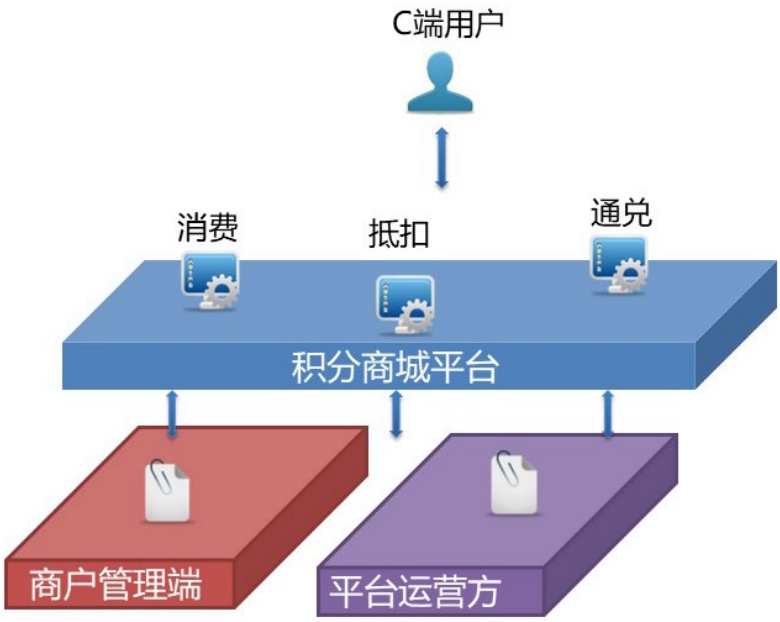


图 6.8 区块链积分商城平台

区块链积分商城是分析传统积分商城痛点并结合市场需求后而设计，可有效解决积分发行不透明、通兑过程繁琐、流通率低等问题。

应用了区块链技术的积分商城，在包含了传统电商平台功能以外，支持运营方和商户发行属于自己的区块链积分，并设计适合自身业务的积分发行、使用规则。运营方可设定联盟中的通用积分，商户间可自行规定积分通兑规则，实现积分在联盟内自由流转、通兑，提升消费者粘性，实现共享会员。记录在

区块链上的积分规则，消费者可随时查看，不必再担心商户暗箱操作，消费者可在系统内按规则通兑积分。

**受益角色：**

- **运营方：**积分商城平台运营方可对各方信息进行整合，利用区块链技术的特点对联盟数据进行统一管理，优化运营结构、提升运营效率。
- **商家：**区块链积分助力商家进行更加公开可信的营销活动，商家间亦可互相引流、共享会员，突破现有营销瓶颈。
- **消费者：**公开透明的积分体系可保障消费者权益，并且，消费者可统一管理联盟发行的积分，并在联盟商家之间自由通兑积分，实现积分价值最大化。

## 6.9 安全生产监管平台

通过搭建联盟链来整合计划进行安全监管覆盖的生产运营相关的所有单位和机构，以及产业各上下游相关成员。联盟成员之间达成安全监管模式下的互信关系，所有数据操作执行可溯源，同时能够及时的进行快速的各个节点数据同步，特别是监管机构单位全节点的同步实现。通过联盟链联合各方生产关系成员共同推动行业内相关单位各个生产运营环节的安全监管，实现了安全作业的事中存证和事后溯源，严格的存证监督，在很大程度上规范了作业人员开展合规的安全作业。

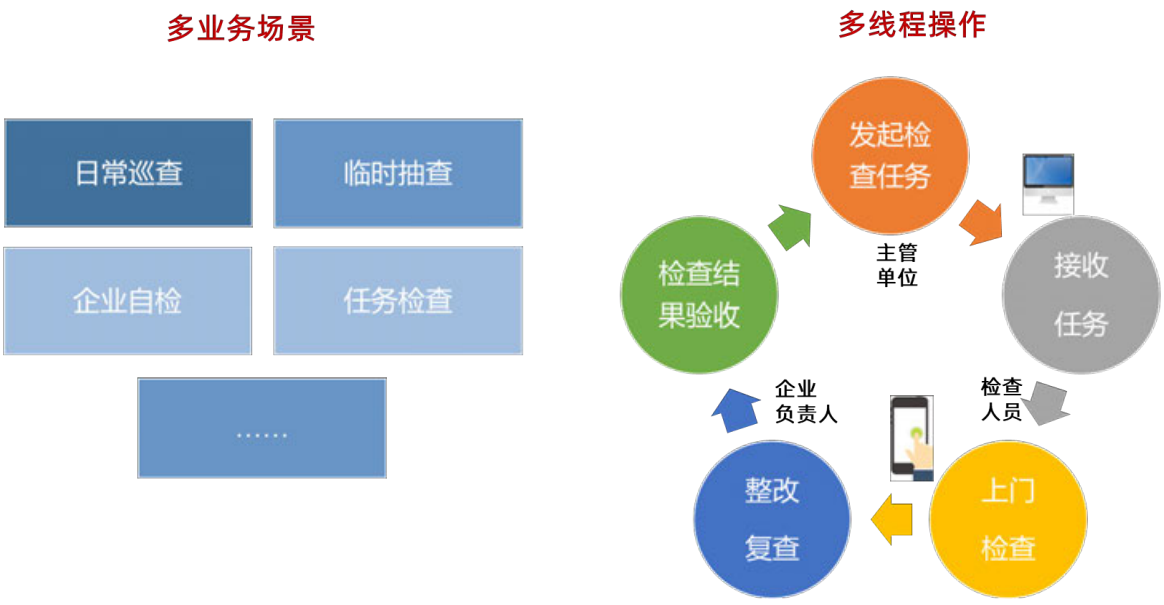


图 6.9 业务场景及多线程操作

**受益角色：**

- **管理部门：**通过平台可对安全生产监管总体情况迅速掌握，清晰掌握监管现状，并对具体监管进展精准掌握；通过平台分析对安全生产监管存在的重点及共性问题进行及时预警，为管理部门及时调整监管策略和防控决策提供依据，打造常规管理更加精准，应急管理更加及时以及防控更加有效的新型管理模式。
- **被管理单位：**通过平台保证监管内容、标准的透明和可信；监管过程可追溯，责任明确，保证监管效率和监管操作的合规性；监管流程清晰可见，明确监管进度；及时接受监管指令，并采取有效措施，保证响应的及时性。

## 6.10 档案管理平台

区块链电子档案管理平台联合监管部门、政府部门、档案局、各级档案馆等机构建立联盟链，以电子档案数据为操作对象，支持档案利用接待、借阅管理、档案出入库、移交接收的全流程线上操作，将档案原始数据固化，永久封存并不可篡改。实现电子档案生成、存储、流转、验证、使用等全过程管理，保证了电子档案全生命周期数据的真实性、可信性、安全性，有效运用于新时期下的档案管理工作。

图 6.10 电子档案管理平台

**受益角色：**

- **监管方：**档案数据真实有效、公开透明，可实时监管档案出、入库记录，减轻监管负担。
- **档案局：**降低运营成本，缩短档案利用接待流程，提升协同效率，实现档案的全生命周期管理。

- **企事业单位：**公开透明的档案体系可保障数据的一致性，避免档案追回过程中可能出现的信息纠纷。

众享比特
PeerSafe

技术改变世界 创造更可信的未来

**北京众享比特科技有限公司**

http://www.peersafe.cn

010-84569800

北京市朝阳区将台西路18号皮革大厦7层