ISCM链

链上生活启航者

Wihite Paper v1.0

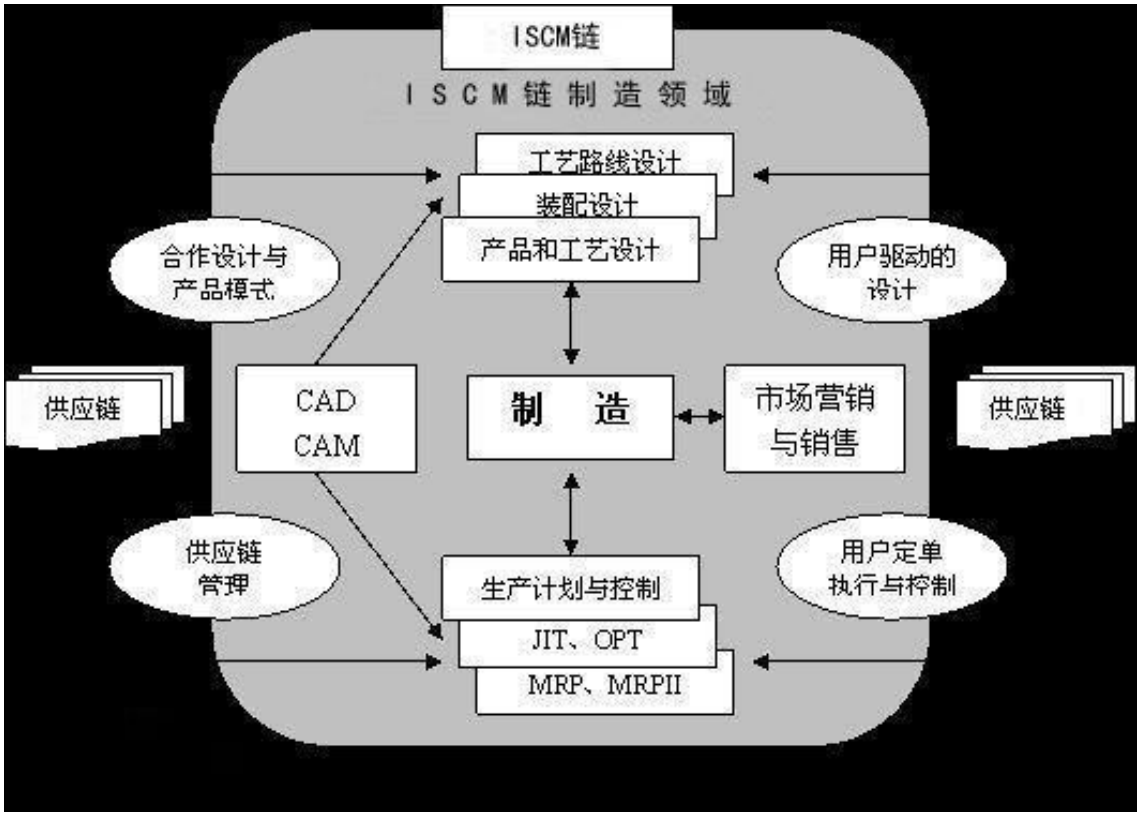
2018.9

摘要

ISCM链是一个多链、多系统融合的链群结构，除了ISCM链本身的框架可以支持实现不同治理模式下的区块链体系，也可与来自不同业务领域、不同地区的不同链，通过ISCM链的 各类协议进行协作，形成各类异构区块链和传统信息系统的跨链、跨系统交互映射。因此，ISCM链被称为ISCM链链群或ISCM 链链网，即区块链之间的互联网。

ISCM链又是一种可生成和共享交易活动数字账簿的数据结构，其核心设计思想是系统中的每个网络节点都参与全网公开账簿记账。这种分布式总账结构保证了所记录信息的不可篡改和可追溯特性，创造出一条“去中心化”的、牢不可破的网络“信任链”。

分布式账本是ISCM链底层存储的重要基础设施。分布式账本技术的去中心化、共同维护、不可篡改等特性是ISCM链实现分布式多方信任的关键。分布式账本包括共识、智能合约体系在内的实现，并为分布式信任框架、上层应用提供共识、存储和智能合约支持。ISCM链和分布式账本技术采用解耦设计，默认使用核心账本，也可以支持NEO、以太坊等其他区块链作为底层。在账本层，我们创造性提出共享数据合约模型，将数据存储和业务逻辑解藕，由不同的智能合约来实现不同的业务逻辑，使整个架构具备更好的伸缩性及灵活性。



在ISCM链中，提出包括身份标识协议、多维实体认证协议、用戶授权协议、分布式数据交换协议等一系列的协议标准。各类协议的实现都兼容了国内外主要的协议标准和体系，如身份标识协议全面兼容W3C 的 DID方案；数字签名协议同时支持国密标准、RSA、ECDSA 等算法；在分布式数据交换体系中，兼容通用授权协议 OAuth、UMA 等，既使得架构满足开放性和标准性，亦可支持后续更广泛的生态合作与拓展。对于应用服务提供来说，ISCM链会做好“最后一公里”的支持，应用开发者无需具备底层的分布式系统开发能力，就可以直接基于ISCM链提供分布式服务。简而言之，ISCM链提供一系列应用框架，包括 API、SDK 以及各种应用功能组件，让各行各业的应用服务提供方开发自己的dApp，做到 dApp as a Service(DAAS)，让区块链真正的好用起来。

目录

1. 项目背景

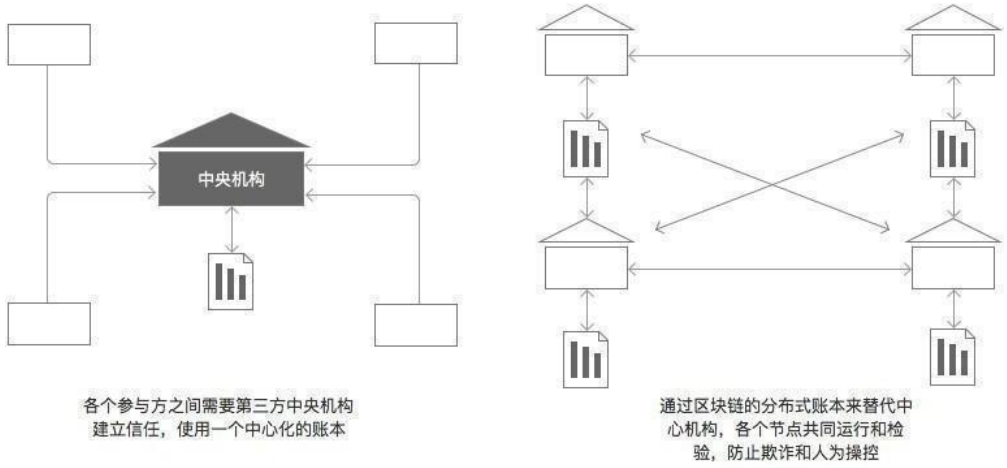
1.1 区块链时代前景

ISCM链是由以太坊技术团队协会创始，实现了公司化和中心化的智能化供应链模式，ISCM链定义为“是围绕核心企业，从配套零件开始到制成中间产品及最终产品、最后由销售网络把产品送到消费者手中的一个由供应商、制造商、分销商直到最终用户所连成的整体功能网链结构”。ISCM链是一个包含供应商、制造商、运输商、零售商以及客户等多个主体的系统。供应链管理就是指对整个供应链系统进行计划、协调、操作、控制和优化的各种活动和过程，其目标是将顾客所需的正确的产品，能够在正确的时间，按照正确的数量、质量和状态送到正确的地点，并使这一过程所耗费的总成本最小。

在人类社会化进程中，社会以优胜劣汰的形式进步和更迭。从远古石器时代到如今的互联网、共享经济时代，每一次核心技术出现，都会极大解决当下社会中生产、经济、沟通等问题，推动社会进步。

随着社会飞速发展，科技进步，生活节奏几何倍增，信息不可靠、信用资源缺失的情况愈发严重，政府、企业、个人之间的信任体系愈发脆弱，沟通和交易成本增加。

我们认为ISCM链在这个经济快速发展的时代，以其去中心化，防篡改，高度透明等特性，会成为继PC 互联网、移动互联网后又一个革新人类社会的技术，将会让社会各种关系的信任变得更加简单。基于密码学、分布式共识协议、点对点网络通信和智能合约等技术保障，使用区块链账本系统的多个参与者，无需额外的第三方担保机构，即可构成多方交易的信任基础。进而实现低成本、低延迟的信息交换和交易处理，实现数字价值的高效流通。



1.2 ISCM链是什么

ISCM链（ISCM链）是一个多链、多系统融合的链群结构，除了ISCM链本身的框架可以支持实现不同治理模式下的区块链体系，也可与来自不同业务领域、不同地区的不同链，通过ISCM链的各类协议进行协作，形成各类异构区块链和传统信息系统的跨链、跨系统交互映射。因此，ISCM链被称为ISCM链链群或ISCM链链网，即区块链之间的互联网。

我们希望通过ISCM链，帮助原有生活工作中缺乏中心化信任体系的场景，自由搭建去中心化的业务模型，从而解决社会中个体与商业体之间的信任矛盾。基于ISCM链，我们将提供丰富的模块化组件，使用者可自由选择共识、存储、合约、仲裁、账户系统，匿名策略、权限等模块，组装成为适合自己需求的子链。子链不限于公链，亦可以是私链或者联盟链。

1.3 ISCM链的设计使命

经过市场调研和分析，我们发现区块链发展过程中存在一些问题，区块链技术人才稀缺、研发成本高昂的状况，在短时间内都不可能缓解；越来越多的应用场景需要ISCM链的支撑；现有区块链性能受限，不同链之间无法通信；机构会倾向使用联盟链、私有链，而二者去信任不完全。ISCM链可为此提供一个可靠的解决方案。

- **灵活易用的区块链基础设施**

ISCM链为开发者和用户提供完整的基于图灵完备的模块化开发。开发者和用户无需研究密码学、共识机制、存储方式等底层技术细节，使用简单快捷的可编程环境直接对接商业应用，从而降低区块链商用成本。

◆ **适配海量的区块链应用场景**

在应用层面，可以预期区块链将作为机构甚至个人在工作、生活多方面的底层基础支持，ISCM链通过模块化、多链并行、智能合约等运行机制，为智慧城市、精准扶贫、“一带一路”建设、ISCM链产业、跨境电商

ISCM链千城万店、ISCM链山村万店、ISCM链千乡万店等应用场景和区块链底层的不同需求提供支撑。

◆ **高性能驱动区块链商用落地**

商业应用对性能的要求极高，ISCM链致力于解决现有区块链的性能受限问题，采用平行扩展技术， 通过链网结构、多链并行的运行机制，以满足千万级 TPS 需求。

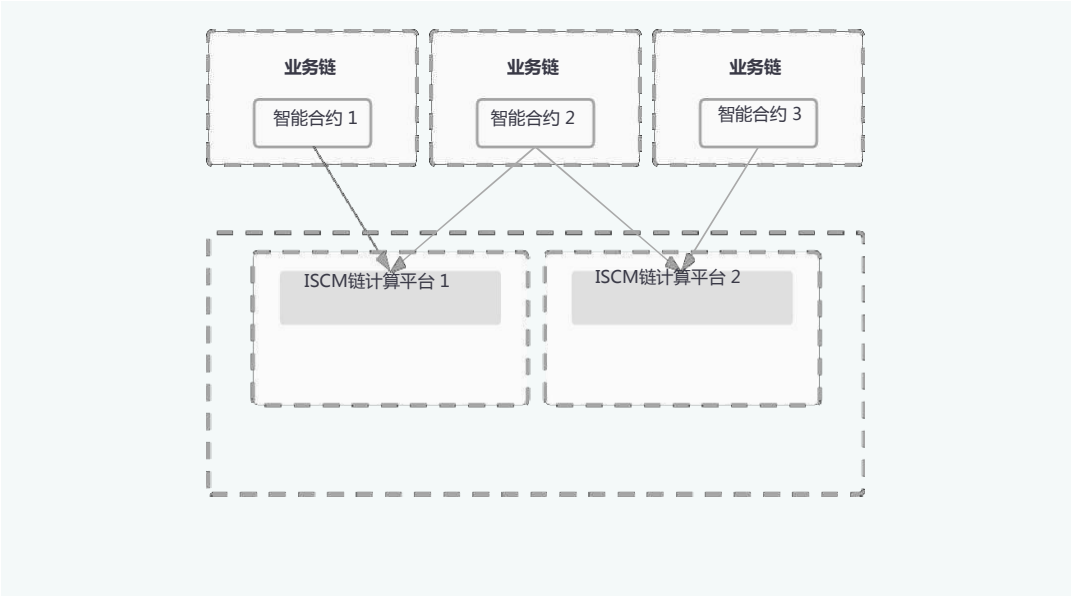
◆ **数据透明与商业保密的平衡**

对于机构而言，数据保密性和安全性极其重要，而区块链的公开透明特性却让机构有所顾虑。ISCM链通过对框架的合理建设以及用技术支撑多种协议的方式，让业务数据保密性和安全性得到保障，解决数据透明与商业保密的平衡问题。

2. 链网结构

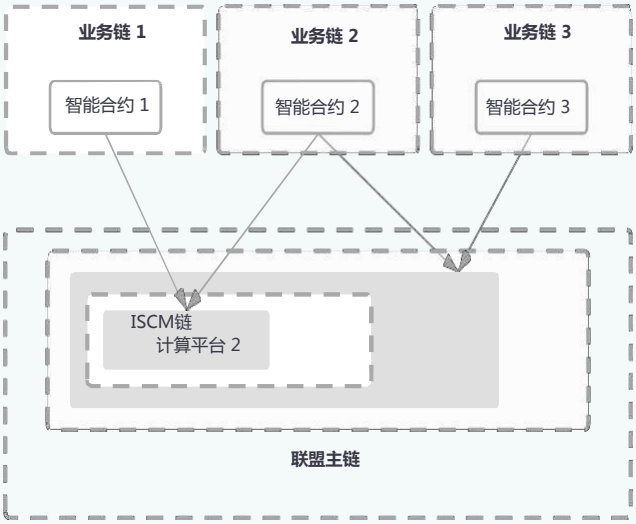
ISCM链的目标是建立起现实社会和分布式数字体系的连接桥梁，由于现实社会中业务的多样性、复杂性和特殊性，出于对性能、可扩展性和业务适用性的考量，仅使用一条公有链/联盟链难以支撑所有的应用场景。实际应用中是由不同的链来运行不同的业务逻辑，以不同的准入方式以及不同的治理模 式，来满足不同场景的需求。同时，很多应用在现实当中并不是独立存在的，而是需要与其他应用进行多样化的交互 协作。因此在这些不同的链之间，又需要具备多种交互协议，以支持应用间的流程协作。

基于以上需求和模式，ISCM链提出了一个矩阵式立体网格架构 超融合链网结构。在横向的领域，可以有一条或多条提供基础性通用服务的公有链，如实体映射，或进行数据交换通用协议支持，以及 提供通用性智能合约服务体系的多个公有性服务链。在一条或多条公用服务链的基础上，各个行业、地域和不同的业务场景，可以有自己独有的业务链，以满足不同场景下的准入要求、合规要求、治理要求及共识要求等。这些业务链，又可以使用公有服务链提供的基础性服务，如实体认证、数据 交换协议等，也可以通过公有链在一些行业共性流程上进行协作。ISCM链白皮书除了与通用性的公有服务链交互，业务链还会与很多行业或业务性质相关的链之间进行协作。



业务链通过ISCM链计算平台进行跨链信息交互

不同的协作场景会涉及不同的业务链，或者业务链上的不同业务点。因此可以有一些小型的专用公有/ 联盟业务服务链，按照特定的业务规则，协同一条或多条业务链或业务点。这样在纵向的领域，存在多条业务协同链，对某些特定跨链业务的智能合约、业务逻辑服务等功能提供专项协同支持。



在ISCM链计算平台基础上构建专用交互链，满足特定的协作需求

这样的矩阵式网格架构，可以形成一张具有弹性的网，成为一个真正自治运作的下一代互联网，不同的业务场景都将以各自的展现方式在其中寻找到合适的服务模式，并且可以很方便地进行大范 围、跨领域的协作。

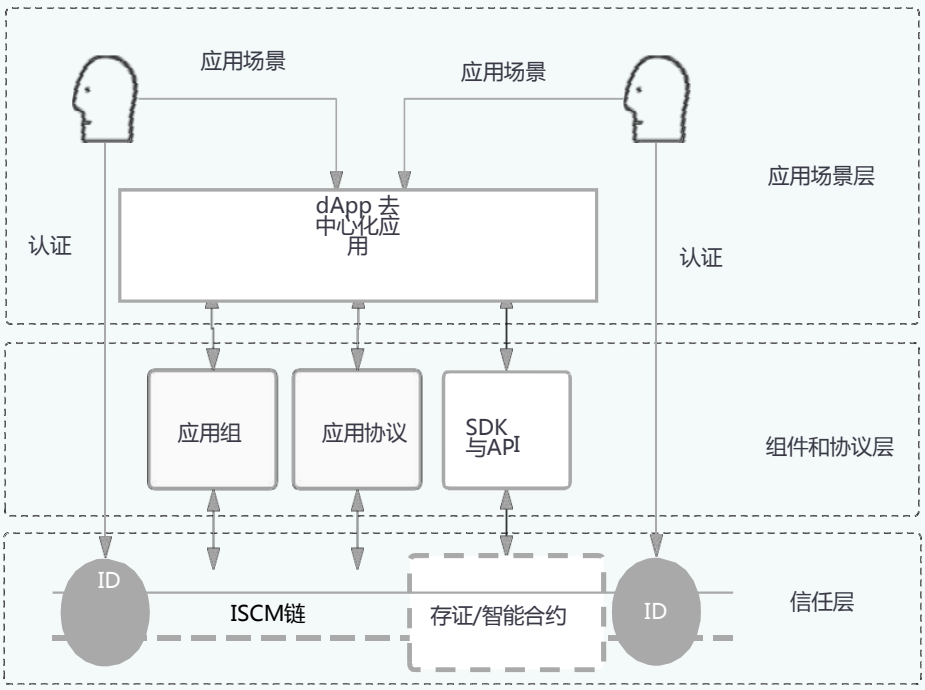
ISCM链中的各类协议，并不是一成不变的，会根据不同的业务场景、行业特点、监管要求及治理要求， 选择和发展不同的交互协议。因此在ISCM链当中，协议是一个不断发展的过程，但一个大的原则是：尽最大可能兼容和采用现有的各类协议与标准，在同一场景下，也尽可能多地支持更多不同协议，以使ISCM链具有更好的兼容性和扩展性。

ISCM链会基于ISCM链分布式账本框架，实现一条或多条满足不同场景的可配置区块链。同时ISCM链的分布式账本框架还可以用于定制特定业务场景下的业务链（如不同的准入机制、治理机制、共识机制、存储模式等）。此外，ISCM链也可以通过交互协议与现有的其他区块链体系进行协同。传统的IT 系统在支持了特定协议后也可与ISCM链对接。

3. ISCM链应用框架

3.1 应用框架模型

ISCM链应用框架提供了一系列丰富的应用层协议和组件，帮助应用开发者快速构建出去中心化应用，使其不用花精力关注底层分布式账本交互的复杂性。ISCM链应用框架具有高度的可扩展性， 可以根据实际场景的需要，不断进行扩展。



应用框架模型示意

- **信任层** ISCM链通过去中心化的身份体系、存证、智能合约交易等实现了分布式信任；
- **组件和协议层** 通过应用组件、应用协议、SDK 和 API 帮助上层场景更好的使用ISCM链网络；
- **应用场景层** 各种场景dApp 重点关注场景开发、用户服务等，信任问题交给ISCM链来解决。

3.2 数据交易市场

未来是一个数字化的世界，未来的数据交易市场也将不仅限于对数据所有权的转移，数据的可信协同计算也将成为重要的协作模式。数据交易市场中的商品包括数据产品、数据预测、数据计算资源等，参与角色包括数据的使用方、提供方，还包括数据的加工方，比如利用深度学习等 AI 技术处理大数据的服务商，这些角色共同构成了数据协作生态。复杂的数据协作生态需要与之匹配的基础设施提供支撑。ISCM链提出的分布式交换协议 DDEP、数据交易组件DDM 及一系列密码学组件共同构成了完备的分布式数据交易和协作框架，确保满足面向全球级的交易规模以及跨交易市场的交易需求，支持基于SCMI链的服务全球用户的各类 dApp 应用。上层数据交易服务商可以在此基础上实现各类别、各领域的数据交易市场。

3.3 数据交易组件

数据交易组件（Data Dealer Module，DDM）基于分布式数据交换协议实现，是ISCM链重要的基础应用组件。无论是 dApp 开发者还是数据交易参与方都可以通过组件快速实现基于ISCM链的数据交易应用。该组件提供 RESTful 接口、RPC、SDK 等，可支持不同类型协议。

数据交易组件包括多种类型：数据交易服务端、单用户客户端、多用户客户端、轻钱包客户端。不 同类型的组件适合不同的应用场景。组件的功能主要分四大模块：ISCM链身份管理、数据资源管 理、智能合约交易、点对点通讯。

数据交易组件的设计具有以下主要优势和特点：

- **组件与访问控制模块解耦** 组件只管理数据资源与数据资源所有者权限控制服务器的绑定关系，不

参与访问权限配置与验证，既维护数据拥有者的隐私保护权益，也增强卖方信用度，避免不必要的纠纷。

- **保护数据隐私** 组件不存储实际数据，交易数据可加密，消除卖方担心数据沉淀等顾虑。
- **需求方除了检索数据** 还可通过广播需求订单通知数据提供方。
- **按照“单一模块单一功能”原则** 和密码学安全组件、用户授权组件配合，将很容易支持灵活多变的场景需求。

3.4 密码学及安全组件

3.4.1 安全多方计算

在数据协作场景中，协作的两方甚至多方，它们既希望能够完成协作任务，又希望保留源数据所有权和控制权，而仅仅向对方开放有限的数据使用权。目前传统做法无法满足需求， 比如，要使用机器学习算法的应用开发商 A，传统的做法是，提供数据给算法提供商 P，由P 在A 提供的数据上运行其算法，得到的结果再返回给 A，但这种传统方式已将 A 的数据泄露给 P。

对于这种典型场景，我们采用多方安全计算技术（Multiparty Secure Computation, MSC）来处理。最早的 MPC 技术是由姚期智提出的，其方法可以解决著名的“百万富翁问题”：两个百万富翁希望比较谁更有钱，但是又不希望对方知道自己的真实财产是多少。在 n 个协作方的场景中，我们假设他们各

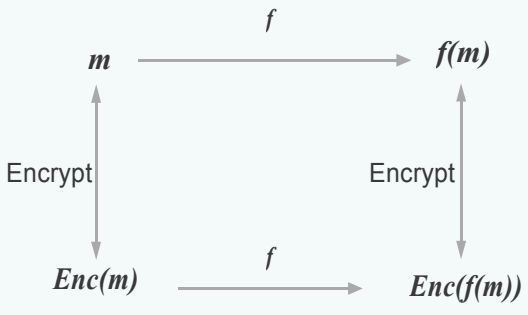
自持有数据 xi，协作的目标是计算关于这 n 个数据的函数值 目标是所有人最终只知道该函数值，任意

一方数据的其他信息都没有泄露。

MPC 技术主要分为两种，一种是基于姚期智提出的混淆电路，另一种是基于秘密分享。这两种技术路线各有优缺点，会根据场景进行选择。

全同态加密

在许多数据交易场景中，数据提供商仅仅希望提供数据的使用权，而不是将数据直接就转让给买方。提供对企业数 据的隐私保护是极为迫切的需求。全同态加密技术提供了一个很好的解决方案。企业首先利用自己的公钥，使用全同态加密算法对数据 加密，将密文C提供给算法提供商，对 C进行加法或者乘法运算（以及由加法和乘法合成的复杂运算），经过这些运算之后，得到密文C'并返回给企业， 企业使用其私钥恢复出明文结果f)。
一个全同态加密算法除了包括基本的加解密算法，还有密文相加 CAdd 和相乘 CMul 算法。假设C1和C2分别是明文M1和M2的密文，那么



在密文上作同态运

3.4用戶授权控制组件

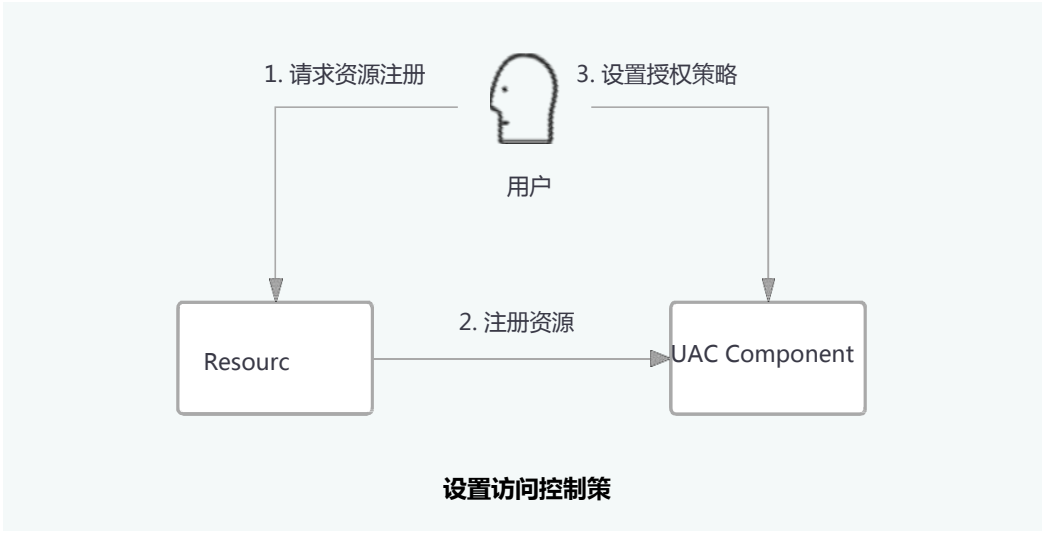
用戶授权控制组件 UAC 基于用戶授权协议实现。UAC 组件实现授权主体对自己数据的多维度颗粒状的授权访问细化控制，任何涉及到授权主体相关数据的交易，都会通知授权主体，得到授权后才可进行数据交易。

大块功能：

- 用户数据授权访问策略设置；
- 用户数据授权访问控制。

3.5.1 授权访问策略设置

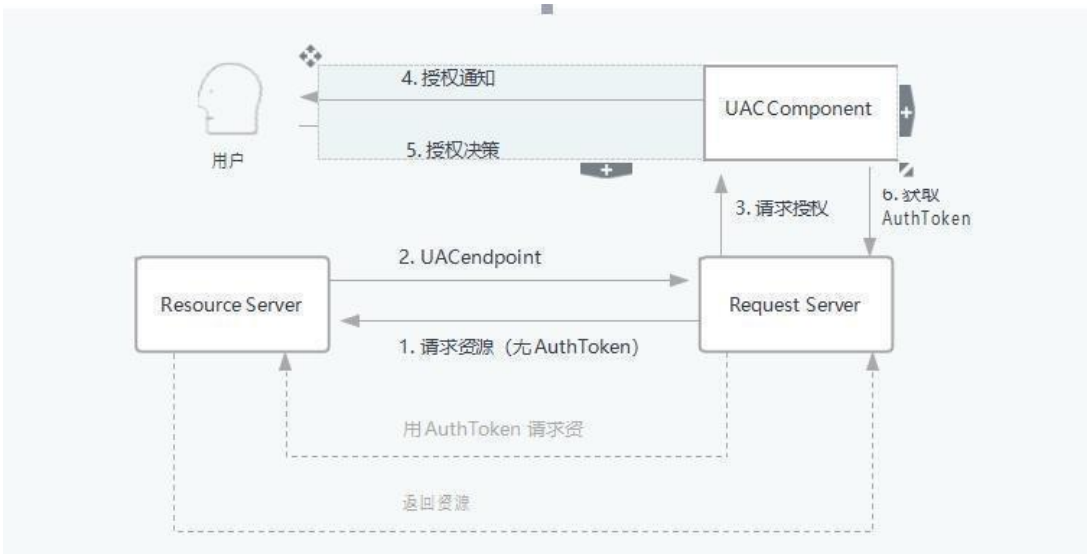
用戶要求资源提供方通过 UAC 组件提供的 REST ful API 对用戶的数据进行资源注册，注册成功后用戶通过UAC 组件便可查看、搜索自己的已注册数据，并对自己的数据进行细化的访问控制策略设置。且针对一些频繁访问的隐私级别不太高的数据，用戶可在 UAC 组件设置授权托管。



设置访问控制策

3.5.2 授权访问控制

作为用戶数据的保护方，在数据交易流程中，当涉及到用戶数据时，非托管模式下 UAC 组件会通知用戶进行授权决策，由用戶自行决定是否允许请求方访问自己的数据。托管模式下，UAC 组件代用进戶行授权决策，并提供授权回执给用戶。两种模式下用戶都能清楚的知道是谁，在什么时候，对自己的哪些数据，要做什么操作。



3.6 声明管理组件

对于ISCM链的信任锚来说，可验证声明管理是重要的功能组件。声明管理组件按照分布式信任体系要求开发。组件对外提供 REST ful API，支持使用关系型数据库（Mysql 或 Oracle）。其组件主要功能包括但不限于：可验证声明签发、验证、查询和注销。

4. 全局事务数据库

全局事务数据库 GlobalDB 是一个可插拔的 Key-Value 分布式数据库界面。它的底层是基于 Google Spanner/F1 的设计实现的开源分布式NewSQL 数据库 TiDB。

GlobalDB 是为区块链/分布式账本以及 IPFS高度优化的数据库组件。GlobalDB 提供了 SQL 兼容、存储分片、分布式事务、水平线性扩展、故障自动恢复的能力，可应用在区块链与大数据、区块链与人工智能等计算相关的场景。

GlobalDB 具备**分布式事务、存储分片、负载均衡**以及 **SQL on KV** 四大特性。

4.1 分布式事务

GlobalDB 可以提供完整的分布式事务，为状态分片和 o -chain 业务提供支撑，事务模型基于 Google Percolator 的基础上做了一些优化。

GlobalDB 的事务模型采用乐观锁，分布式事务只有在真正提交的时候，才会做冲突检测。传统的方式如果有冲突，则需要重试，这种模型在冲突严重的场景下，会比较低效，而乐观锁模型在大部分场景下具备较高的效率。

由于分布式事务要做两阶段提交，并且底层还需要做一致性复制，如果一个事务非常大，会使得提交 过程非常慢，并且会卡住下面的一致性复制流程。为了避免系统出现被卡住的情况，我们对事务的大 小做 了 限制：

1) 单条KV 记录不超过6MB；
2) KV 记录的总条数不超过300,000；
3) KV 记录的总大小不超过 100MB。

存储分片

GlobalDB自动将底层数据按照 Key 的范围进行分片，每个分片是一个[StartKeyE,ndKey)区间。分片中的 Key-Value 总量超过一定阈值，就会自动分裂。

4.2 负载均衡

负载均衡器（PD）会根据存储集群的状态，对集群的负载进行调度。调度是以分片为单位，以 PD 配置的策略为调度逻辑，全部过程自动完成。

4.3 SQL on KV

GlobalDB自动将 SQL 结构映射为 KV 结构。简单来说，GlobalDB 做了两件事：

- 一行数据映射为一个 KV，Key 以 TableID 构造前缀，以行ID 为后缀；
- 一条索引映射为一个 KV，Key 以 TableID+IndexID 构造前缀，以索引值构造后缀。

可以看到，对于一个表中的数据或者索引，会具有相同的前缀，这样在 TiKV 的 Key 空间内，这些 Key-Value 会在相邻的位置，GlobalDB 会配置相应的脏数据管理策略，使得数据读取达到较高的性能。GlobalDB支持高度可配置，可同时适配 on-chain 业务与 o -chain 实时高性能业务。它将作为ISCM链

ISCM链的核心组件为底层账本平台提供坚实支撑。

5. 插件化实现RAFT 共识算法

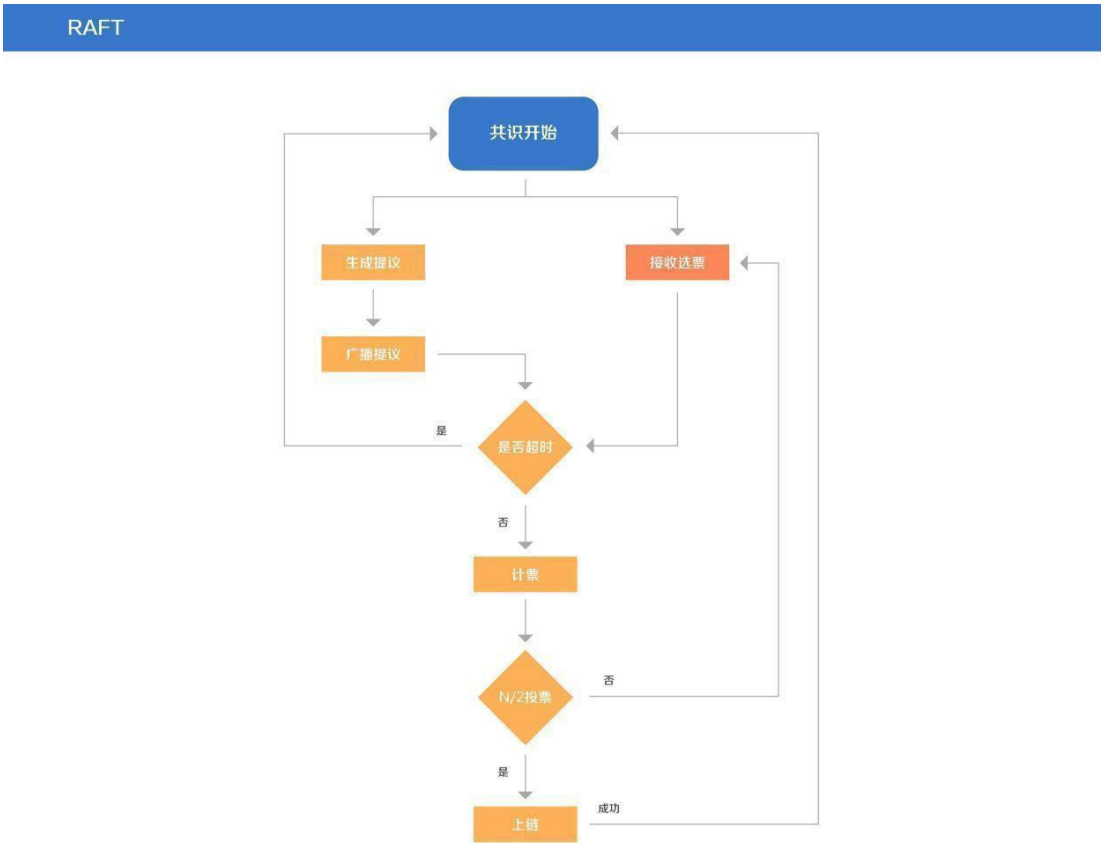
共识机制不但是计算机之间的算法和数据共识，也是合作伙伴之间进行协作的共识，共识机制使区块链的参与者通过约定的方式进行共同记账，确保合作者之间的记账正确性、一致性、持续性，避免少数出现故障的节点影响网络运行，并防御少数故意作恶者的破坏。

公有链如比特币、以太坊等使用的共识算法通常为工作量证明或权益证明等，可以根据投入权益和记 账的行为，对记账者制定奖励和惩罚制度。公有链上的共识算法一般确认时间较，或需要较多的算 投入。

RAFT 共识算法

ISCM链所使用的 RAFT 共识算法特性包括：

- ✓ 共识节点达到出块条件，即把当前块作为候选区块发起选举，所有共识节点具有同等选票权重，体现了参与者的对等性；
- ✓ 候选区块超过半数赞成票才提交到区块链中，保证高一致性；
- ✓ 如果超时没有收集超过半数的回复票，则重新发起选举，保证系统的容错恢复能力；
- ✓ 秒级出块，可以配置为 1 秒或多秒出块；
- ✓ 支持 1/2 节点容错，整个系统中少于 1/2 数量的节点出现故障，均不影响共识进行；
- ✓ 在选举过程和区块同步过程中严格校验签名，保证数据的安全性。



RAFT 共识机制

RAFT 共识具有较高的效率、高一致性和高可用性。与PBFT 共识的拜占庭容错特性对比，适用于互信程度较高的各种链型。

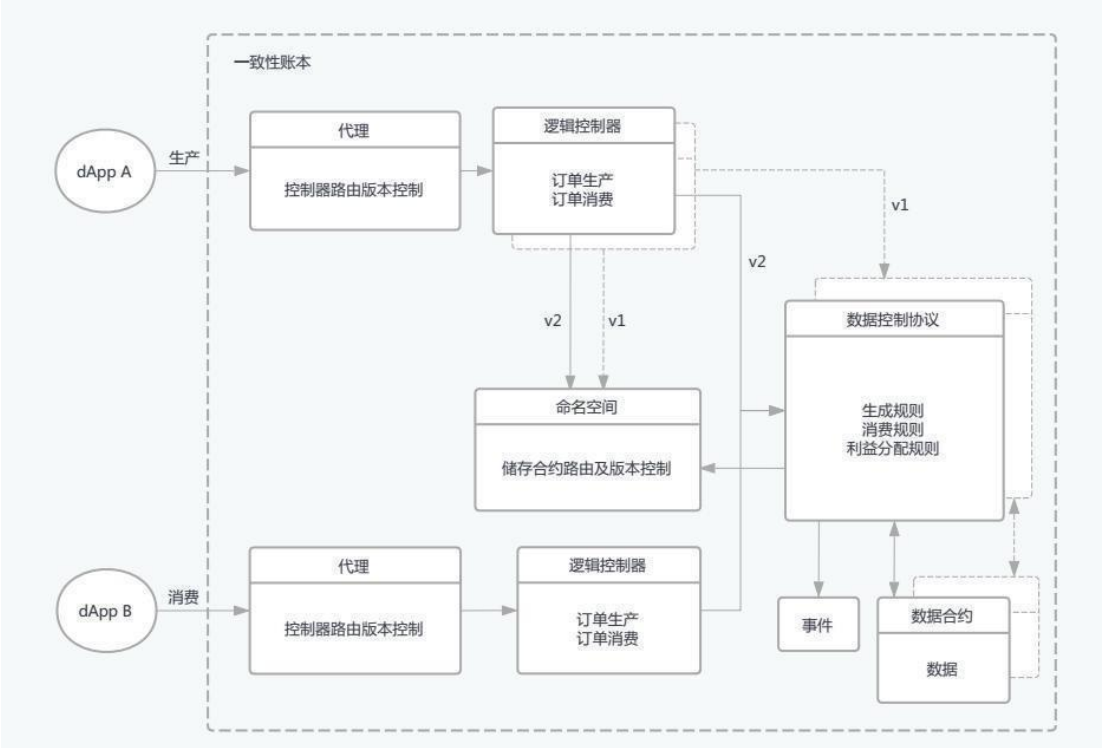
联盟链的共识算法在节点总数不多、网络规模不太大时，可以提供较高的交易并发处理能力。但随着节点数量增多，比如达到几百个共识节点的规模时，由于需要共识节点之间交换较多的信息，会出现明显的性能下降。所以在联盟链中

一般会通过协商，在保证公平公开的前提下，控制参与者共识的节点数量，以保证共识算法的效率。

ISCM链的共识算法根据不同的区块链要求的身份对等性、交易响应时间、并发能力、以及服务器计算能力和网络带宽等进行深入优化，可提高计算效率，减少重复工作，降低带宽消耗。在保证高并发的同时，可保证交易在短时间内能得到确认，且一旦确认后，在联盟链里即达成共识且不可篡改。

6. 共享数据合约模型

ISCM链上层应用对于分布式账本的需求主要包括以下两个功能：数据结构的定义及存储、业务逻辑的处理及与外部系统的交互。为了通过解耦使之具备更好的伸缩性及灵活性，我们设计了一种模型将这两部分分开，由不同的智能合约来实现，一部分负责数据存储（数据合约）；另一部分负责处理业务逻辑（控制器合约）。通过使用多个不同的控制器合约来共享同一份数据合约的架构我们称之为共享数据合约模型。



该模型包括以下设计功能组件：

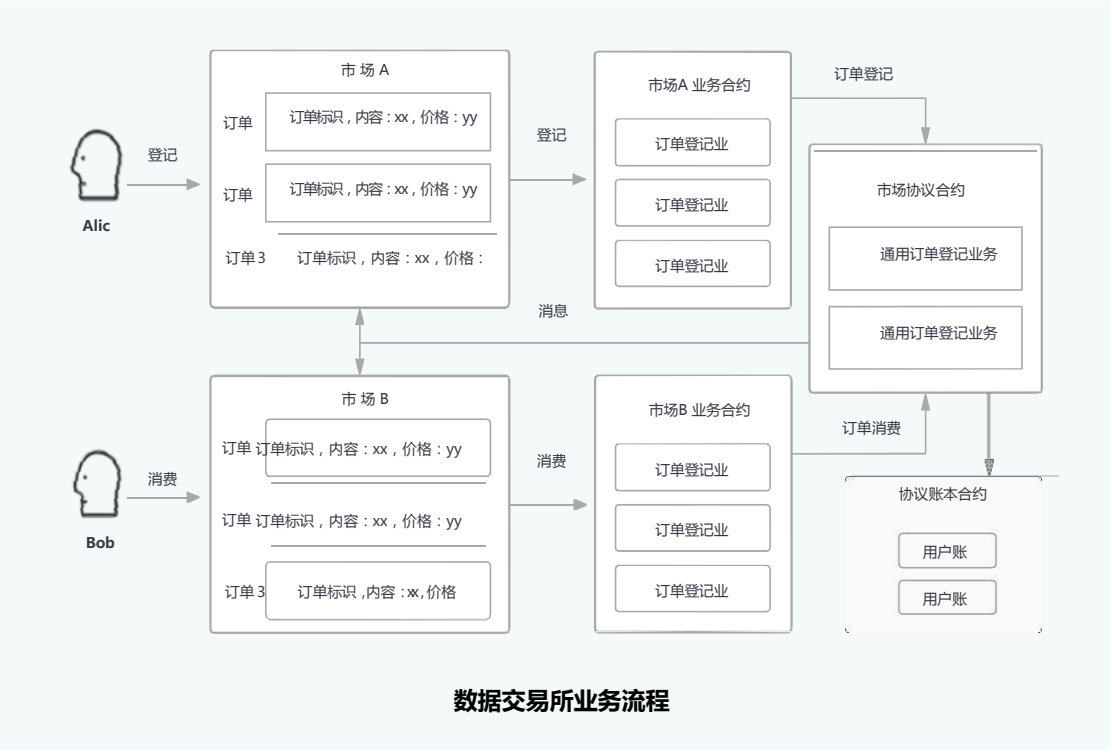
- 代理控制器：面向dApp，提供外部 dApp 确定的合约入口，保证即使合约升级，也不会引起外部调用的不一致性；
- 逻辑控制器：业务逻辑控制；
- 命名空间：支持在不同dApp 不同版本下，数据合约地址的映射。确保数据结构的升级不影响业务逻辑，并且能支持不同版本间的数据回溯；
- 数据合约：提供基本的数据结构及存储接口。类似DAO，提供GET/SET方法。
- 数据控制协议：由各业务关联方制定的通用业务规则，数字化为协议控制器。这个协议控制器包括以下部分：

  - 连接该逻辑控制器的权限控制；
  - 与外部系统的交互接口；
  - 通用的业务逻辑；
  - 通用业务核心账本的控制逻辑；
  - 事件通知机制；

- 消息事件：是在智能合约的执行过程中，把一些需要广播的内容推送出来的一种机制，各方在同步账本的过程中，均能通过本地重放分布式账本区块的方式获得当前合约的交易消息。消息实际上也是分布式账本的一种廉价存储机制，不关心这个合约的节点可以选择不执行这个合约，当然也就不会收到这个消息事件了。而关心这个合约的节点可以通过合约的执行，获得跟此合约相关的事件。 因为链上不存储实际的交易内容，这样就可以极大地减少各节点的存储压力。

这种设计模式意味着即使上层业务不同，只要基于通用的业务协议，就可以实现数据共享，优势互补，让跨界协作也变得更加简单。

以数据交易所 dApp 为例。如图所示，业务逻辑包括订单登记和消费（交易）两个流程。



数据交易所业务流程

登记流程：

1) Alice 向市场A 发起订单登记请求；
2) 市场A 检查完Alice 的订单之后，按照分类，往该分类协议合约登记订单；
3) 市场协议合约检查市场 A 的权限及其提交的订单内容，满足规则则将订单登记到该协议核心账本；
4) 登记成功以后，协议合约广播订单登记消息，并返回结果；
5) 市场A 业务合约向Alice 返回最终结果。

交易流程：

a. 市场B 通过同步区块获得所有交易；
b. 市场 B 通过执行区块中的交易获得市场 A广播的订单登记消息；
c. 市场B 通过订单登记消息中的订单信息在市场B 中展示；
d. Bob 向市场B 发起交易行为，对象为上面Alice 所登记的订单；
e. 市场B 检查完Bob 的交易请求后，按照分类，向该分类协议合约发起交易；
f. 协议合约检查市场B 的权限及交易请求信息，满足规则则处理 B 的交易请求并做最终结算；
g. 协议市场广播订单交易完成信息，并向市场 B 返回处理结果；
h. 市场B 向Bob 返回最终结果；
i. 市场A 监测到协议合约的交易完成广播信息，并向Alice 推送交易完成信息。

7. 核心协议标准

7.1 多源认证协议

多源认证不同于以往的单一身份认证体系，ISCM链可以为实体提供融合了外部身份信任源认证及链中实体间背书的多源认证体系，不但可以为实体提供“我是谁”的基础身份认证，还可以为进一步为实体提供诸如我拥有什么、我喜欢什么、我经历过什么等多维度的身份信息，进而形成 Who amI

/ What is it 的多源认证 package。

多源认证协议包括以下两种模式：

- **外部信任源认证** ISCM链以自签可验证声明的形式给接入信息绑定外部信任源，任何实体都可以通过验证 ID 绑定的外部信任源来验证实体的身份。实体身份认证的可信任程度由已绑定的外部信任源公信力和认可度决定。
- **ISCM链实体间的身份认证** ISCM链中的实体还可以通过ISCM链中其他实体签发声明的方式实现身份认证。

7.1.1 外部信任源认证

外部信任源认证支持自我导入和信任锚 Trust Anchor 导入两种方式。

7.1.1.1 自我导入

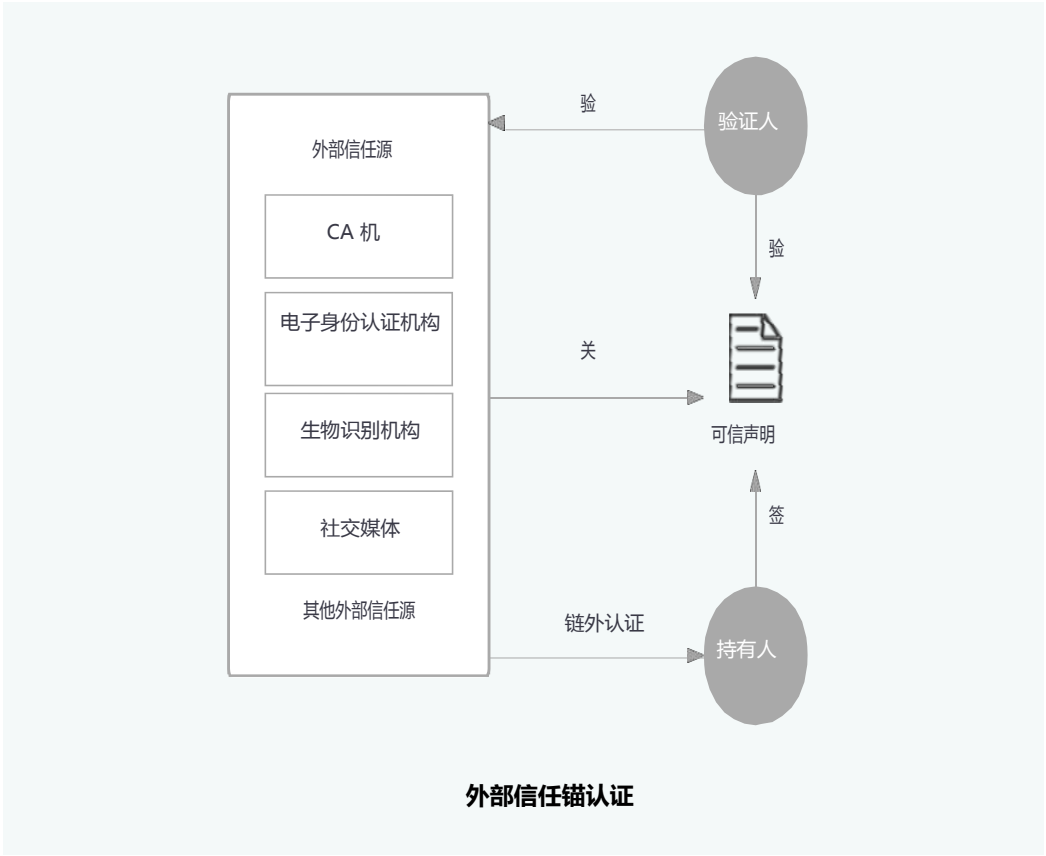
用戶通过社交媒体、银行UKEY 签名等方法来绑定现实信任，该模式利用了现实世界已有的信任（如微信、Facebook、银行等等）。原理实际上很简单，首先用戶在 ONT 上添加一个外部信任源的证明地址，用戶接着在该证明地址上提供一个可验证声明，包含如下内容：

- **声明创建与过期时间**
- **声明内容** 包含声明的类型，ID，社交媒体类型，社交媒体的用户名等；
- **签名** 需要指定使用的公钥，必须是 ID 描述信息中已包含的公钥列表中的一个。

当第三方需要验证用戶的外部身份时，首先在ISCM链中读取到用戶信任源的证明地址，然后到这个地址去获取可验证声明，最后验证该可验证声明即可。正常来说，用戶的社交媒体账戶基本只能由其本人方可以进行管理，也就是说只有其本人才能够发表一个可验证声明。

7.1.1.2 信任锚导入

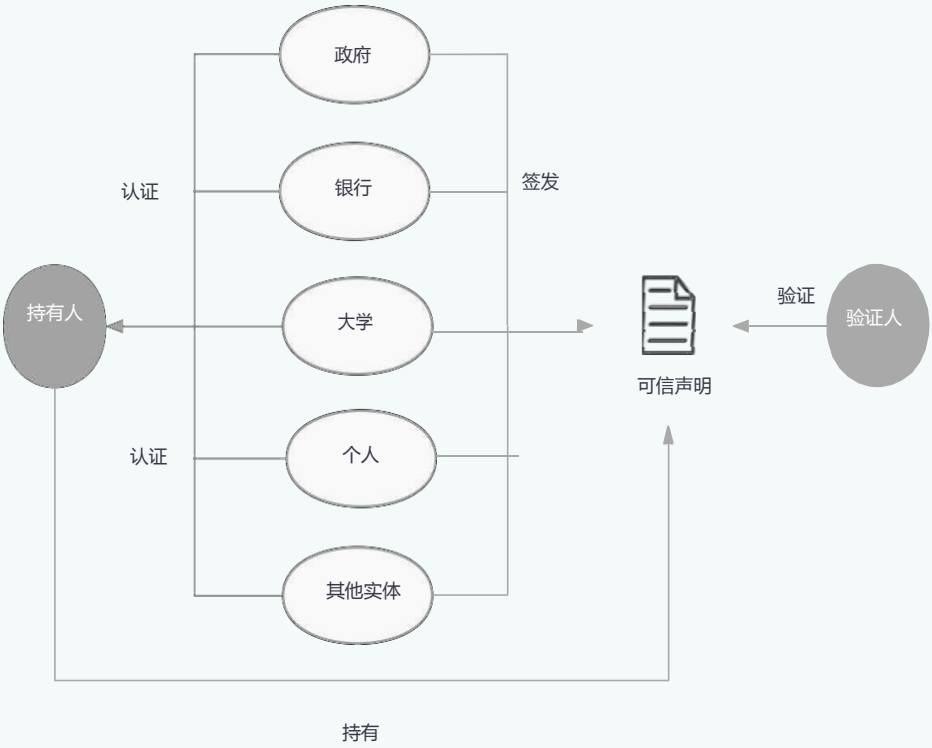
信任锚通常是那些经过了实名认证，且在社会中由一定公信力或声望的政府单位、企事业单位、非盈利组织以及社会名人等。成为信任锚需要遵守ISCM链链委员会发布的一系列标准。信任锚使用自 有的认证方式对被认证实体进行认证后，对被认证实体签发一个可验证声明。声明中不需要包含被认 证实体的真实身份信息，仅记录实体及认证服务的ID，作为该服务的认证结果证明即可。其认证模型如下：



外部信任锚认证

7.1.2 ISCM链实体间的身份认证

ISCM链中的实体还可以通过ISCM链中已通过身份认证（外部信任源）的实体来认证身份，如图所示，用戶不仅可以通过学校、银行等实体做身份认证，还可以通过个人等其他方式获得身份认证。 正是由于可验证声明的开放性，使得ISCM链中任何实体可以对任何另一实体就任何事情发布声明，这使得ISCM链中的身份认证远远超过传统的身份认证概念。通过收集来自政府机构、学校、医院、银行、企业以及家人、朋友、领导、同事、老师、合作伙伴等的声明，可以证明“我们是谁”、“我们拥有什么”、“我们经历过什么”、“我们掌握什么技能”，甚至是“我们有什么兴趣爱好”等。这种多角度、多方面的认证相比传统的单一认证更准确、更全面。



实体间身份认

7.2 用戶授权协议

在ISCM链中，用戶对自己的数据有绝对的掌控权。任何涉及到用戶主体的相关数据访问、交易都 需要得到所有者的授权。为此，我们设计了一套用戶授权协议来保护用戶的数据隐私。协议利用可 验证声明技术完成异步、可验证的授权，同时支持授权托管以及细粒度的访问控制策略制定。

7.2.1 角色定义

在用戶授权协议中涉及的主要角色有：

- **用户** 对资源拥有所有权的实体，能够对资源作访问控制；
- **资源需求方** 需要获取数据等资源的请求方；
- **资源提供方** 提供资源的服务方；
- **授权服务** 提供资源授权服务，接收用户对资源的访问控制策略及对资源请求进行权限认证。

7.2.2 授权流程

用戶授权协议根据应用场景,主要分为三个阶段:

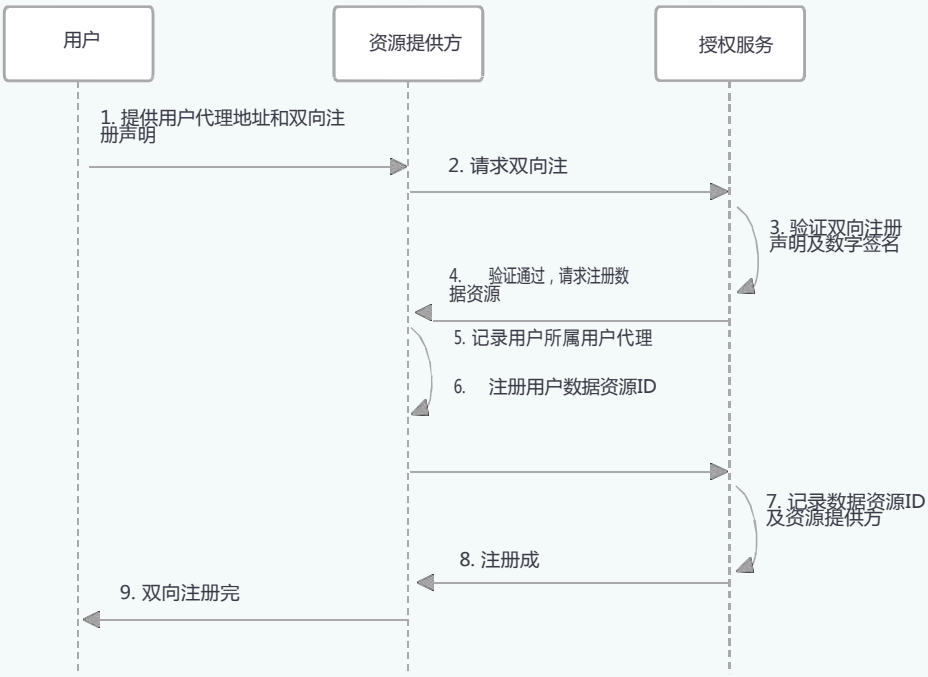
1) 双向注册：用户授权资源提供方将指定资源注册到授权服务，同时授权服务向资源提供方注册自己的地址；

2) 设置访问控制策略：双向注册完成后,用户可以访问授权服务设置资源的访问控制策略；

3) 授权：需求方向授权服务发起访问授权申请，若满足授权条件则会收到授权证明，用于向资源提供方请求数据。

7.2.3 双向注册

双向注册是指授权服务向资源提供方方注册自自己己的地址，以便资源提供方方在处理资源访问请 求时，给资源需求方方返回授权服务的地址；同时，资源提供方方也需要向授权服务注册自自己己 的地址， 以便用用户对数据进行行行访问控制。
在进行行行授权操作之前，用用户需要协同资源提供方方和授权服务，完成双向注册流程。双向注册流程如图所示：



双向注册流程

1) 双向授权过程由用户启动，用户自签发一个双向注册声明，包含资源提供方的 ID 和地址，及授权服务的ID 和地址；

2) 资源提供方使用双向注册声明与授权服务进行握手，双方验证数字签名；

3) 资源提供方记录授权服务的访问地址；

4) 授权服务记录资源提供方提供的用户数据资源ID。

7.2.4 访问控制策略

利用基于属性的访问控制，所有者能够设定灵活的访问控制策略，限制特定的资源能够由满足特定属性条件的请求者访问。访问控制策略可以描述为一个布尔表达式，如三个属性条件组合成的策略A∨(B∧C)。请求者在申请授权时需以可验证声明的形式提供满足策略要求的属性证明。

7.2.5 授权证明

授权服务接收到授权请求后，通知用户进行授权操作。对于满足授权条件的资源访问者，用户为其签发授权证明。在证明的有效期内，资源需求方可以重复访问数据而而无需再次申请授权。

7.2.6 授权托管

授权服务可以为用户托管授权操作。用户在授权服务中设置好自己的访问控制策略，后续的授权请求全部由授

权服务处理并签发授权证明。用户需要为授权服务签发授权托管声明，以证明其授权结果的有效性。

7.3 分布式数据交换协议

针对目前中心化数据交易所的痛点如：数据缓存、隐私数据未经用戶授权、数据版权无法保护等问题 ，

ISCM链提出分布式数据交换协议 DDEP，该协议对实体之间的数据交易行为定义了一整套协议规范。

7.3.1 角色定义

在分布式数据交换协议中主要的角色有：

- **数据需求方**

需要采购数据的机构/企业/个人；

- **数据提供方**

提供数据的机构/企业/个人，数据可以是源数据，也可以是加工数据，数据提供需要完全满足当地政府的法律法规；

- **用户代理机构**

负责和用户交互，以满足数据交易环节中需要用户的授权，

用户代理机构形式可以多样（可以是企业OA 系统、互联

网平台甚至仅是简单的短信网关），但需要完整实现应用

协议框架中定义的用户授权协议；

- **数据所有者**

即数据主体，可以是机构/企业/个人。

7.3.2 用戶授权机制

数据交换体系中，由于交易的数据需要通过数据所有者的授权，授权流程完全遵守用戶授权协议，其协议定义参考用戶授权协议。

7.3.3 担保交易模式

通过智能合约实现的担保交易协议，为交易行为提供了去中心化的第三方保证服务，最大程度保证“一手交钱，一手交货“的交易过程，保护买卖双方的权益。

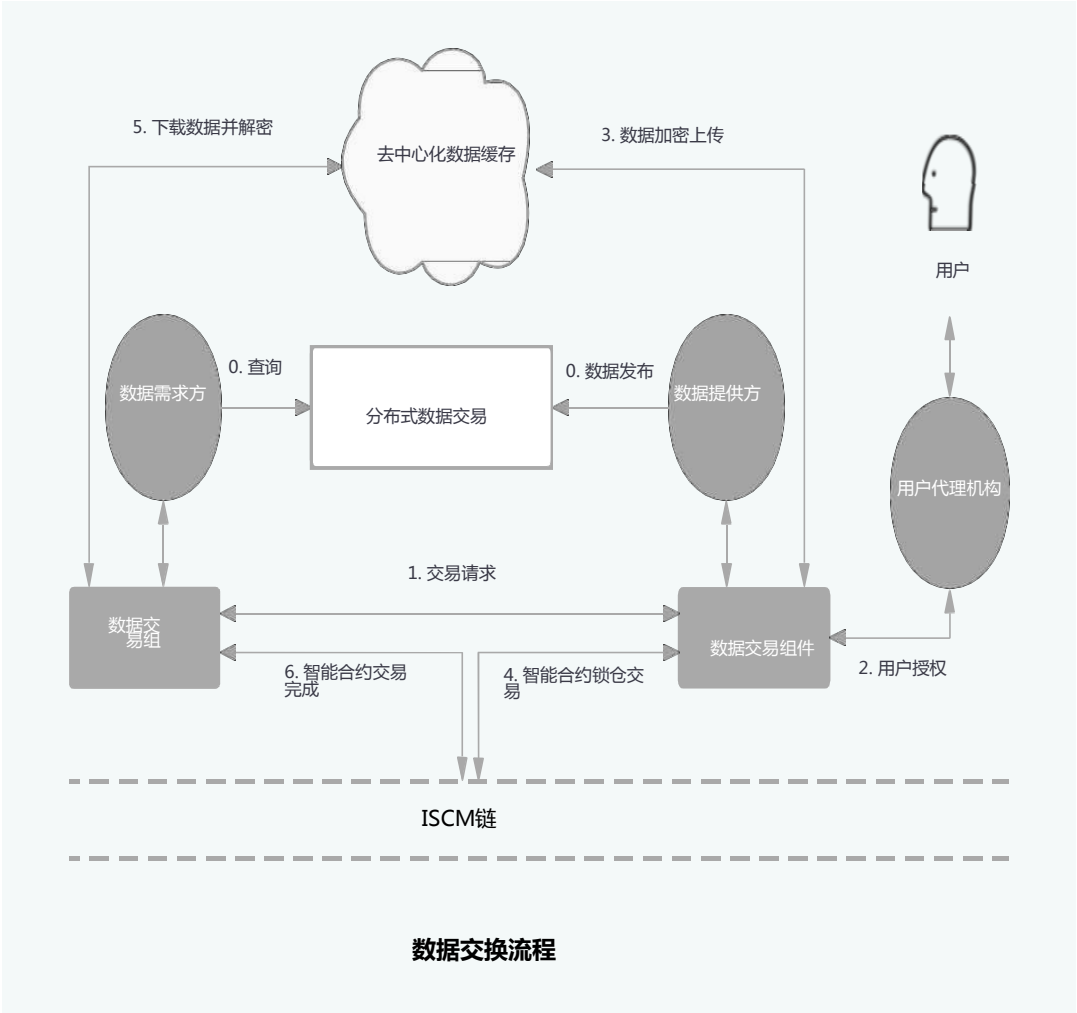
a) 若检查未通过，则向转入者反馈错误，返回等待交易状态；

3 数据提供方提供数据后，向合约进行确认，并设置有效期。若有效期结束时仍未执行其他操作，则合约自动进入结算过程（步骤 5）；

4 数据需求方收取数据完成后，向合约进行确认；

5 合约将资金转到数据提供方账户，返回等待交易状态。

7.3.4 数据交换流程



数据交换流程

前置步骤 交易前准备

数据产品发布

数据提供方将数据元信息在交易市场中发布，数据需求方可在交易市场中浏览、搜索数据信息，选择自己需求的数据发起交易。元信息中应包括但不限于：数据资源介绍、关键字、数据资源哈希、合约收款地址等信息。

- **授权双向注册**

数据产品如果需要数据所有者的授权，数据提供方在发布数据之前，首先需要和用戶指定的用戶代理机构之间进行双向注册，详　双向注册部分。

1）交易请求

需求方在上架的数据产品中查看到想要购买的数据后，通过ISCM链验证数据提供方的身份，具体参考多源认证协议。在交易请求发起之前，需求方首先向合约地址存入一笔资金，向提供方发送购买数据请求，并附带用戶授权所需要的信息。该请求包括不限于：交易信息、身份信息等。

2）申请授权

数据提供方方收到需求方的请求之后，访问用户代理理，发起授权申请。此时，用户代理可以通过联网络认证需求方的身份，并根据数据所有者事先提供的访问策略略进授权处理。如果所有者没有设置访问策略，用户代理理通知其进行授权操作。如果未能获得的授权，则交易终止。

3）上传数据

数据提供方根据请求方支持的对称加密算法，生成一次性会话密钥，使用会话密钥加密交易的数据和

数据特征值，将密文上传到中间存储服务（如 IPFS）。

4）智能合约锁仓

数据提供方通过智能合约锁仓，合约在检查资金金数额正确后，锁定数据需求方账户，直到交易完成或取消。同时使用需求方的公钥加密会话密钥，通过安全通道发送给需求方。

5）收取数据

数据需求方接收到智能合约事件通知后，从中间存储服务收取数据，并使用会话密钥解密数据密文，然后计算明文的特征值进行比对验证，确认无误后，执行第六步。

6）交易确认

数据需求方向交易合约确认交易完成，合约中的资金转到数据提供方账户。异常处理机制：异常处理机制可以根据业务场景进行定制实现，比如可以实现：如果超过一定时间，数据需求方还没有确认的话，数据提供方可以调用合约解锁资金，或者智能合约自动触发解锁资金。

7.3.5 对交易者的隐私保护技术

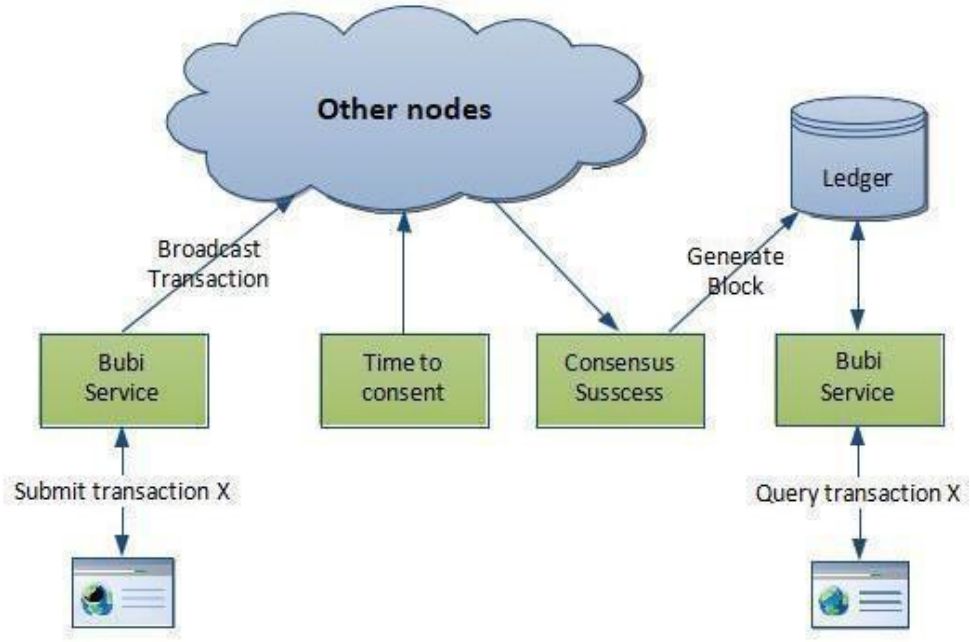
在部分交易场景中，交易者需要隐藏自己真实的交易记录信息，我们使用用隐形地址技术来模糊交易易收款与真实身份 ID 之间的关联。具体方法是数据需求方根据数据登记中的收款地址生成一个隐形地址，该隐形地址的私钥只有数据提供方才能够掌握。

需求方进而向地址 E 转账，并附加信息 R。仅数据提供方利用可计算出隐形地的私钥

8. 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，ISCM链区块链在性能方面可达到：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。

8.1 性能方面
快速交易验证



通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，ISCM链可

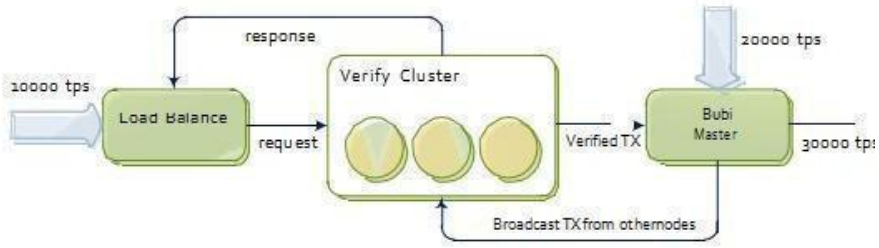
以实现秒级的快速交易验证。满足绝大部分区块链应用场景的用户体验。

海量数据存储

区块链复式记账的模式，在系统长时间运行下，历史数据不断累积；ISCM链区块链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）。

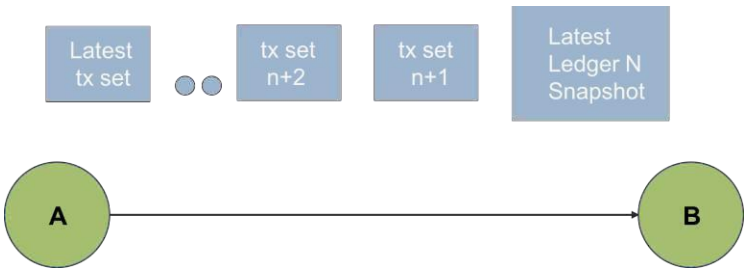
高吞吐量

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，ISCM链区块链的处理性能已经能满足万级 TPS 的需求。如果再引入Off-Chain 等机制，还能进一步大幅提高交易吞吐量。



节点数据快速同步

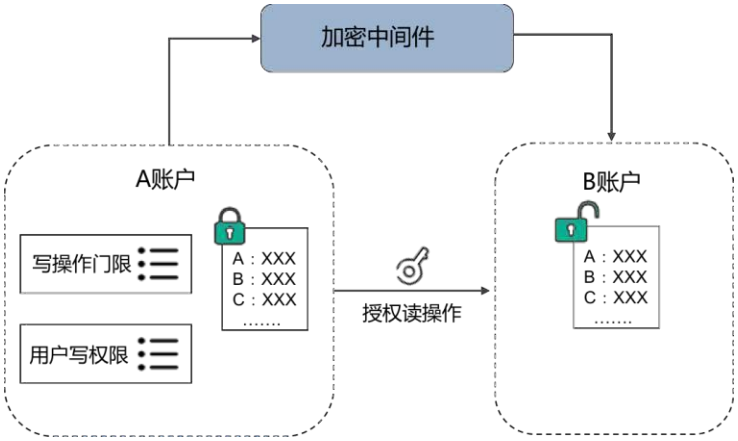
ISCM链支持镜像(Snapshot)机制，可以定期对本地账本制作镜像，实现便利的回滚机制，在统一共识下，可以指定镜像标签进行回滚；同时，缩短新加节点加入运转的周期，仅需同步最新镜像及少量近期交易集合，即可融入网络并参与共识验证。



8.2 扩展性方面

权限控制策略

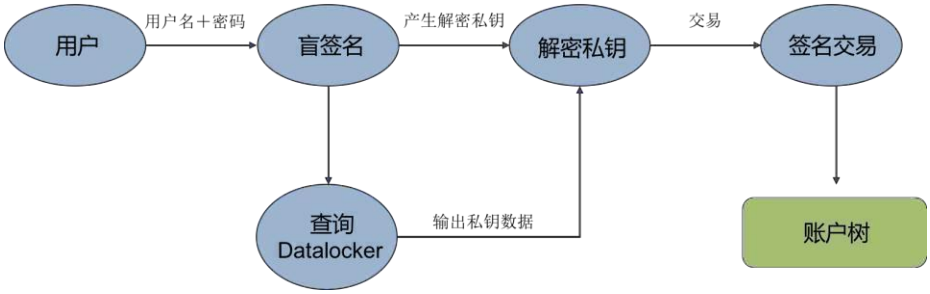
提供数据信息写入与读取两类权限控制策略。数据信息写入权限，同一账户下设置多个使用户，并针对不同的操作设置相应的权限，满足多方签名控制的使用场景。数据信息读取权限，用户可以授予和撤回单用户或用户组对数据的操作权限，用户组可以由用户灵活配置。数据包括用户账户信息，交易信息等，粒度可以细化到交易或账户的各属性字段。



8.3 安全方面

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，ISCM链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。



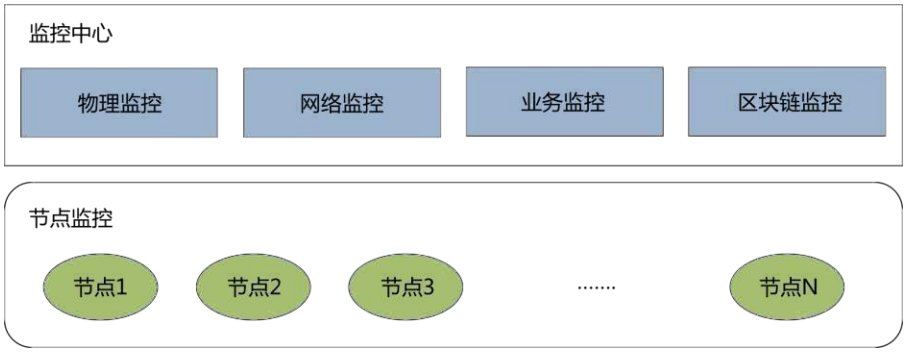
8.4 运维方面

全平台部署

ISCM链的所有代码均可跨平台编译运行，平台相关代码均封装成基础库，业务逻辑独立于ISCM链平台。除了 PC 及服务器的方式编译，同时支持交叉编译方式，如 ARM、MIPS 平台，方便在移动便携式系统部署，为区块链物联网化做预备支撑。同时，ISCM链已与国内几家知名云平台达成战略合作，可以实现在云平台上快速部署。

可视化运维

提供运维管理所需的可视化工具。区块链节点上部署的系统监控服务（MonitorAgent）：支持业务（区块、交易、合约、共识等）、网络（组网、时延、吞吐量等）、系统层面（CPU、内存、磁盘等）的数据信息监控；同时提供完备的日志、告警与通知机制，便于商用系统的维护。



低成本接入方式

ISCM链抽象出适用于多种业务场景的 API 接口，如：资产、溯源、存证等，供这些场景相关的业务直接使用。在新的业务场景下，ISCM链可以基于现有的框架为用户快速定制接口，满足业务功能需求。同时提供已封装的支持多种主流开发语言（JAVA、C++、node-js、PHP）的 SDK 软件开发包。

目前ISCM链服务主要有两种：一种是搭建一套区块链底层，提供一套标准化的 API 并开放，然后由开发者自己对接应用；另外一种是配合上层应用解决一些行业痛点，将分布式账本内嵌到已有的应用系统中。区块链是一项新兴技术，只有不断的满足业务需求，才能走向成熟，所以我们通过对底层分布式账本的封装，降低上层应用使用的门槛，在对接和使用的过程中，不断地优化和完善底层分布式账本和共识算法，使之更加贴近商用诉求。

8.5 隐私

私密性不是独立的功能，它在本文中许多其他方面都有描述，本节总结了各处描述的私密功能。ISCM链利用多种技术来提高分布式账本系统中用户的私密性。

部分数据的可见性 事务不像其他系统那样在全局范围内广播。

事务分离 交易的结构像Merkle 树，可以有个别子组件透露给参与方，它已获知Merkle 树的根哈希值。此外，它们可以在不知道对方的情况下就签署交易。

密钥随机化 库生成和使用都有一个随机密钥，它和没有相应证书的身份标识不关联。

图修剪 涉及流动资产的大型交易图可以“修理”，它要求发行人使用一个新的参考字段重新发行资产到账本。这个操作不是原子化的，但能有效地把资产从旧版本链到新版本，这意味节点在验证期间不会尝试探索原始的依赖图。

ISCM链已考虑未来整合额外的隐私技术。在所有潜在升级中，有三个特别值得一提：

安全硬件

虽然我们将数据传播的范围缩小到只需要查看数据的节点，
在一个去中心的数据库中，“需要”还可以
是一个直观的概念，数据往往只需要进行安全检查。我们已经成功地在安全飞地保护JVM 下，使用英特尔 SGX™ 试验了运行合约验证。安全硬件平台允许在一个不可调试、防篡改的环境中执行计算，对于在该环境中运行的软件，只能获得仅对该实例访问的加密密钥。对于在互联网上的软件第三方远程证明，

它确实运行在安全状态。通过节点远程证明对方在一个地区运行智能合约的逻辑验证，这让一个事务在一个密钥下被传送到一个对等加密的节点成为可能。

安全硬件开启了潜在的单击隐私模型，这将极大地简化写智能合约的任务。然而，它仍然需要将敏感数据发送到对方，然后对方可能试图攻击硬件或利用侧通道，从加密的容器内提取商业信息。

混合网络

有些节点可能知道与它们无直接关系的交易，例如公证人或监管节点。即便使用了随机密钥，节点仍然可以获得有价值的身份信息，如通过简单地检查源IP 地址或该节点发出的用于公证的认证证书。对这个问题的传统加密解决方案，是混合网络。最著名的混合网络是 Tor，但更合适的设计将是一个自我匿名转信站。在混合网络中，使用一小组随机选择的节点所拥有的密钥，消息像洋葱般的方式被反复加密，洋葱中的每一层包含下一“跳”的地址。一旦消息传递到第一跳，它将解密以获知未来的加密层并转发过去。返回路径以类似的方式运行。向ISCM链协议添加混合网络将允许用户选择升级隐私， 代价是较高的延迟和更多的失败网络节点暴露。

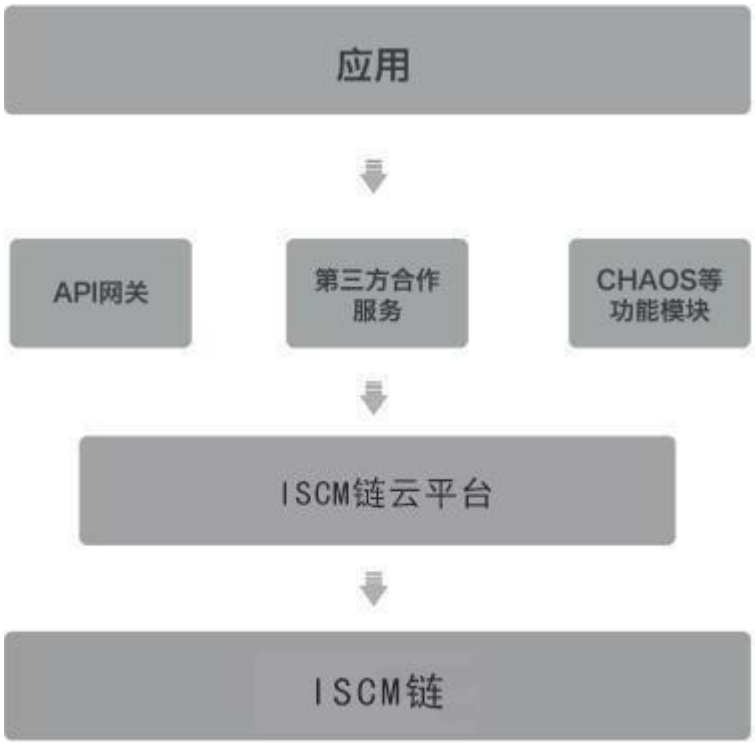
零知识证明

在去中心化数据库系统中，解决私密问题的圣杯是使用零知识证明去说服对方一个交易是有效的，而不向它们透露交易的内容。虽然这些技术还未实际用于通用智能合约的执行，但近年来我们已取得了巨大的进步，我们已经设计了数据模型假设，希望将有某天迁移到使用简洁的非交互式参数的零知识证明方式（zkSNARKs）。这些算法允许计算一个固定大小的数学证明，利用混合公共和私有输入来保证程序的正确执行。程序可以直接表示为一个低级多元多项式编码的代数约束系统，或通过简单的模拟CPU(vn Tiny RAM)执行，它本身作为一个大的预计算的约束集实现。由于程序共享了认同功能（即智能合约）与私有输入数据的组合，这足以验证正确性，只要证明的程序可以递归地核实其他证据， 即输入事务的证明。BCTV zksnark 算法依赖于对 vntinyram 组成的操作码执行递归证明，所以这不是一个问题。与ISCM链最显著的整合需要紧密地编写通用智能合约（如现金）的汇编语言版本，这需要手写并和 JVM 版本保持一致。不明显但更强大的整合将涉及 vntinyram 后端及提前 JVM 字节码编译器，如Graal，或者 Graal 的图直接编译为系统约束。根据最近的研究，SSA 形式直接编译器编译的约束和“可扩展的概率可验证明”是最好的集成，这是一个开放的研究问题。

9. 应用及拓展

ISCM链的技术团队通过一段长时间的努力，已经设计出较为完善的合作框架，其中不乏和全球知名企

业合作开发的落地应用。ISCM链的应用架构如下：ISCM链在底层的区



个便于合作伙伴及客户一键部署的区块链云平台用户只
需要选择自己做处的行业，所需要的解决方案，很方便的部署属于自己的区块链节点、智能合约、生成相对应的 API 配置。

ISCM链的应用架构还包括自主开发的分布式加密数据库服务 CHAOS、用户私钥管理、智能合约授权管理等，这种模块化的服务模型使得不管是客户还是服务提供商的开发更佳便捷和灵活。同时打算以这 些成功案例为模版，进行快速的扩张和延展，让更多的企业、更多的商业活动运行在ISCM链的平台之上， 并且逐步的在这些商业活动之间建立进一步的连接，同时通过开发相关的商业智能合约来推广

ISCM链 代币的流通，将ISCM链的分布式生态逐步完善和扩大。

ISCM链技术的应用情况

在金融领域已经有大量的应用

- ISCM链，这是一个由全球金融机构支持创建的使用区块链技术的交易平台;
- 纳斯达克等交易所使用区块链技术来开发股票上市系统;
- 澳大利亚股票交易所(ASX)选择使用比特币背后的区块链技术，作为其清算和结算系统的替代品。
- 支付网络和服务提供商使用区块链来开发P2P转账平台;
- ISCM链，使用区块链技术来协助跟踪保险欺诈。

除了金融领域，ISCM链技术在其他领域也已经有大量的应用，如合同和协议、知识产权，防伪，博彩，物联网等，并有大量的风投进入。

9.1 助力一带一路

“一带一路”对于中国整个经济的发展起到了至关重要的作用，据深交所发布的信息显示，截至 2016 年末，深市 1870 家上市公司中有 284 家以不同方式参与“一带一路”建设，产品出口规模超 900 亿元人民币，工程建设规模约 1500 亿元人民币。 “一带一路”正在快速发展，但规模的扩大也带来了一些问题，如货币风险、信用系统有一定局限性、知识产权无法得到有力的保护等，这些问题将会在一定程度上制约“一带一路”发展的步伐，而ISCM链，却注定它将解决了一些以往无法解决的难题。

ISCM链能解决“一带一路”中不少难题，概括说来，它的作用突出体现了以下几个方面：

ISCM链 作为新型交易方式

国际货币结算广泛采用美元，不但成本较高，还容易遭受汇率波动风险、信用风险和贬值风险等风险。要减缓或避免这些影响，通过ISCM链内置的 Token-ISCM链 的发行，为其运作的有效性、安全性提供了可靠的依据，该系统可以为“一带一路”沿线国家提供一个可靠的虚拟资产通道，进行以货易 货的交易方式。

全新信用系统

ISCM链将“一带一路”沿线国家中一些拟出售的农业、能源、资源等被投资者的资料数字化，通过相关技术一方面把相关讯息广泛地、迅速地向包括中国企业在内的全球投资者传播，供潜在的投资者参考。另一方面，则是通过ISCM链高安全性、互相监察验证和公开透明等的优势作信用背书， 可以增强投资者和被投资者的互信基础，方便投资者作出投资选择及签订具有信用背书的合同，而无须担心遭遇欺诈问题。

近年来，ISCM链技术在全球范围内得到了越来越广泛的认可，世界各主要经济体及重要国际组织均在对区块链技术进行积极的探索和推进。在中心化机构运营和管理的情况下，ISCM链的运行多年以来一直十分稳定。

资产数字化

在盛产石油的阿拉伯国家，跨境电商的潜力不可估量。可以将这些国家拟出售的能源，或者包括农产品和其他资源，以及中国的过剩产能都数字化，通过ISCM链搭建交易平台，将这些贸易需求公布给全球潜在投资者。ISCM链的全民审查验证、不可篡改和公开透明等特性为潜在贸易提供了信用背书，能够增强贸易和投资双方的信任基础，减少欺诈风险。同时，区块链上的点对点交易，也减少了跨境贸易和投资所需要的交易和营销成本，提高了便捷性。

升级物流

在“一带一路”发展过程中，物流是非常重要的一环，但是在物品流转的过程中会遇到损耗、步骤繁琐、报关手续时间较长等问题。但ISCM链的出现却可以完美的解决这些问题，如在货物流转时可以先登记好产品，之后上链，由于区块链不可篡改的特性，这个信息可以保证绝对的真实，之后在流转的过程中发生任何事都实时的反馈到链上，这些数据可以提供给这个货物相关人员，帮助货物在流转的过程中缩减物品损耗和时间。

提高旅游业利润

“一带一路”得到国际社会的高度关注和有关国家的积极响应。3 年多以来，旅游业从不断深入的“一带一路”建设中获益良多，“一带一路”已然成为旅游业的超级IP，为旅游企业带来新的机遇。但不可否认的是，旅游业的发展过程中遇到了一定的瓶颈，这些瓶颈在区块链未出现之前并没有很好的解决方案。ISCM链拥有的特性却可以突破这些瓶颈，其可以在常旅客积分计划、认证旅行证件、旅游保险和住宿等方面发光发热。可以通过使用ISCM链建立整个旅游地区的虚拟等价物交易结算系统，为旅游业提供全面立体的支持，可以大大提升“一带一路”整个旅游产业的服务效率，立体式闭环将使旅游业获得更大收益。

全过程记录

有利于金融机构精细化的操作和养老群体的细分。金融机构会跟踪你和你的家庭成员的健康状况，你的资产负债状况，你的消费行为和交通行为，并适时对你的人寿险保费、车险保费进行调整，减少或提高你的消费贷款的利率，他们还会不遗余力地为你的子女做教育成长金融规划，做你的慈善信托和家族信托等。

数据加密

1) 自己掌握着私钥，可以保护自己的隐私，不让与己无关的金融机构或别有用心者获得数据
2) 通过数据加密保证数据不能更改，避免私人和金融机构内部人员串通，产生任意减免保费、降低利率等舞弊行为
3) 保证追溯，让接入ISCM链的养老机构更好地了解你过去的行为习惯，以便提供更具针对性的养老方案和护理方案。

ISCM链 代币激励

对于养老机构和养老金融机构的补贴可以利用ISCM链实施定向追踪，并用 ISCM链 实施奖励。还将有助于“以房养老”金融产品的推广，在代币制度下，可采取售后回租、收拢后统一出租等多种方式，使得国家养老金和养老机构补贴能够以多种形式发放。

9.2供应链下的产业链

ISCM链是由以太坊技术团队协会创始，实现了公司化和中心化的智能化供应链模式，ISCM链定义为“是围绕核心企业，从配套零件开始到制成中间产品及最终产品、最后由销售网络把产品送到消费者手中的一个由供应商、制造商、分销商直到最终用户所连成的整体功能网链结构”。ISCM链是一个包含供应商、制造商、运输商、零售商以及客户等多个主体的系统。供应链管理就是指对整个供应链系统进行计划、协调、操作、控制和优化的各种活动和过程，其目标是将顾客所需的正确的产品，能够在正确的时间，按照正确的数量、质量和状态送到正确的地点，并使这一过程所耗费的总成本最小。

ISCM链又是一种可生成和共享交易活动数字账簿的数据结构，其核心设计思想是系统中的每个网络节点都参与全网公开账簿记账。这种分布式总账结构保证了所记录信息的不可篡改和可追溯特性，创造出一条“去中心化”的、牢不可破的网络“信任链”

极强的可靠性

ISCM链 平台将供应链的产业信息存储在分布式数据存储空间中。为了防止数据的丢失，连续生成和维护备份数据，对于被记录的数据，其哈希值将被记录在区块链中以验证数据的完整性，当数据被强行变更或伪造时，将使用备份数据来恢复原始数据。

高度的透明性与互操作性

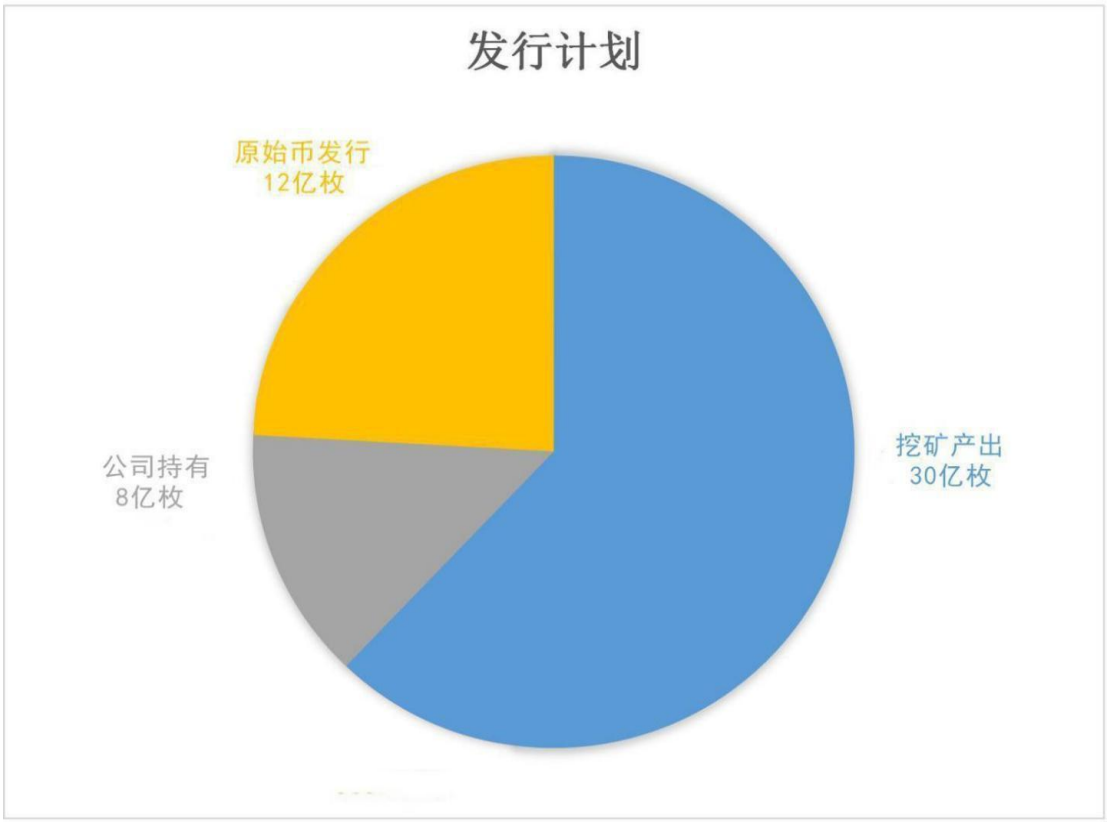
ISCM链 平台是不可破的网络“信任连”，上面所有产品信息、个人记录和他人查看信息的过程都会被记载在区块链上。以平台上存储的数据和信息为媒介可以和各种应用程序自由连接。

10. 发行计划

发行代币名称:ISCM 发行

总量：50亿枚发行计划：

（如图）



11. 创始团队

CEO：Martti Malmi

Martti Malmi来自俄罗斯伯明翰，毕业于剑桥大学政治经济学院，获得经济、MBA和会计荣誉学士学位，并拥有HR硕士学位;在以太坊协会区块链研究十余年，国际知名区块链专家，曾参与开发以太坊多个区块链项目。

COO:（Nick Tomaino）

Nick Tomaino 是ISCM链的联合创始人和首席运营官，为区块链初创企业提供量身定制的解决方案，从种子募款到市场营销和社区建设， 到众包传导和最终交易所上市。Nick Tomaino拥有强大的跨文化技能和商业联系人和合作伙伴网络，自 2012 年以来一直在以太坊协会， 并从此作为投资者和顾问参与了众多项目。

James Brandon

高级技术师，宾夕法尼亚大学高级系统软件工程师，精通多种计算机软件，区块链应用讲解方案，擅长应用密码学、安全协议、云计算安全等。曾就职于 Apple Inc，在嵌入式软硬件开发及管理有 9 年经验。

Nikolai Petrov

俄罗斯人,毕业于圣彼得堡大学,精通多种计算机软件，区块链应用讲解方案，擅长应用密码学、安全协议、云计算安全等。曾就职于 Apple Inc，在嵌入式软硬件开发及管理有 6 年经验。

附录

风险提示

在ISCM链的开发、维护和运营过程中存在着各种风险，这其中很多都超出了ISCM链开发者所能控制的范围。除本白皮书所述的其他内容外，请参与者充分知晓并同意接受了下述风险：

市场风险

ISCM链价格与整个数字货币市场形势密不可分，如市场行情整体低靡或存在其他不可控因素的影响，则可能造成ISCM链本身即使具备良好的前景，但价格依然长期处于被低估的状态。

监管风险

由于区块链的发展尚处早期，在全球没有有关募集过程中的前置要求、交易要求、信息披露要求、锁定要求等相关的法规文件。并且目前政策会如何实施尚不明朗，这些因素均可能对项目的发展与流动性产生不确定影响。区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体插手或施加影响则ISCM链可能受到其影响，例如法令限制使用、ISCM链有可能受到限制、阻碍甚至直接终止ISCM链应用和发展。

竞争风险

当前区块链领域项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力。ISCM链项目是否能在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、战略规划等方面挂钩，也受到市场上诸多竞争者乃至寡头的影响，存在面临恶性竞争的可能。

人才流失的风险

ISCM链汇聚了一支活力与实力兼备的人才队伍，吸引到了区块链的资深从业者、具有丰富经营的技术开发人员。在今后的发展中，不排除有核心人员离开、团队内部发生冲突而导致ISCM链整体受到负面影响的可能性。项目技术风险密码学的加速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给ISCM链平台，这可能导致ISCM链的数据丢失。项目更新过程中，可能会出现漏洞，漏洞发现后会及时修复，但不能保证不造成任何影响。目前未可知的其他风险除了本白皮书内提及的风险外，此外还存在着一些创始团队尚未提及或尚未预料到的风险。此外，其它风险也有可能突然出现，或者以多种已经提及的风险的组合的方式出现。请参与者在做出参与决策之前，充分了解团队背景，知晓项目整体框架与思路，理性参与。

免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在ISCM链及其相关公司中出售股票或证券的任何买卖建议、教唆或邀约。本文档不组成也不理解为提供任何买卖行为，也不是任何形式上的合约或者承诺。鉴于不可预知的情况，本白皮书列出的目标可能发生变化。虽然团队会尽力实现本白皮书的所有目标，所有购买ISCM链的个人和团体将自担风险。文档内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。本文档仅供主动要求了解项目信息的特定对象传达信息使用，并不构成未来任何投资指导意见，也不是任何形式上的合约或承诺。

ISCM链明确表示不承担参与者造成的直接或间接的损失包括：

a. 参与者一旦参与ISCM链分发计划，即表示了解并接受该项目风险，并愿意个人为此承担一切相应后果。项目团队明确表示不承诺任何回报，不承担任何项目造成的直接或间接损失。

b. 本项目涉及的ISCM链是一个在交易环节中使用的虚拟数字编码，不代表项目股权、收益权或控制权。

c. 由于数字货币本身存在很多不确定性(包括但不限于：各国对待数字货币监管的大环境、行业激励竞争,数字货币本身的技术漏洞)，我们无法保证项目一定能够成功，项目有一定的失败风险，本项目的ISCM链也有归零的风险。

d. 虽然团队会努力解决项目推进过程中可能遇到的问题，但未来依然存在政策的不确定性，大家务必在支持之前了解区块链的方方面面，在充分了解风险的前提下理性参与.团队将努力实现文档中所提及的目标，但基于不可抗力的存在，团队不能做出完全承诺。在适用的法律允许的最大范围内，

对因参与所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失，本团队不承担责任。