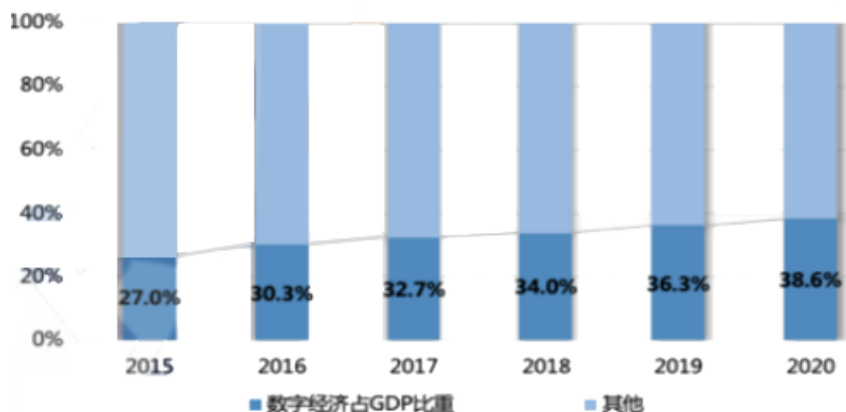


# 区块链可信计算平台

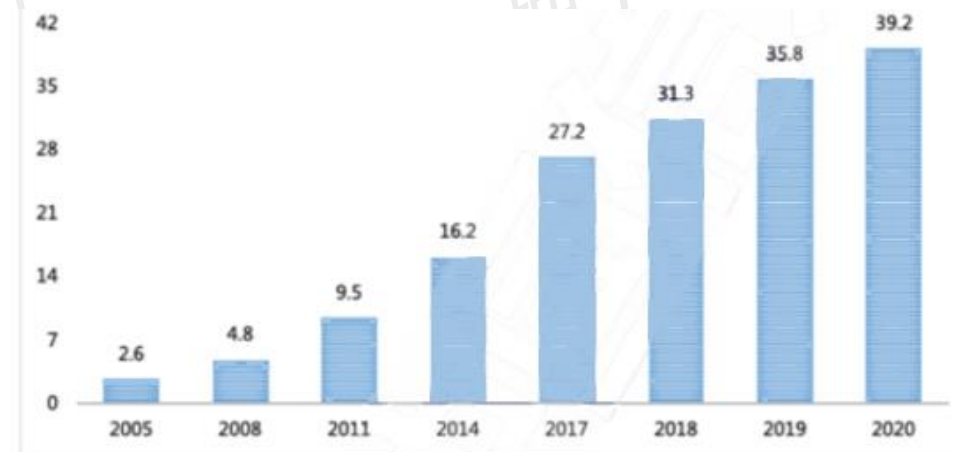
v2.1.3

# 数字经济发展的趋势

## 数字经济占GDP比重



## 数字经济规模 (万亿元)



随着经济活动数字化转型加快，数据对提高生产效率的乘数作用日益凸显。数据变得像其它生产要素一样可参与分配和流通：

### • 数字产业化

- 包括电子信息制造业、电信业、软件和信息技术服务业、互联网行业等

### • 产业数字化

- 即传统产业应用数字技术所带来的产出增加和效率提升部分，包括工业互联网、两化融合、智能制造、车联网等

### • 数字化治理

- 以“数字技术+治理”为典型特征的技管结合，以及数字化公共服务等

### • 数据价值化

- 包括数据采集、数据标准、数据确权，数据标注，数据定价，数据交易，数据流转，数据保护等

数字经济规模逐年上升，到2020年，整体规模已达39.2万亿元，占GDP的38.6%。

# 数据相关政策法规



加快培育数据要素市场。把数据与土地，劳动力，资本，技术并列，成为时代新的生产要素提升社会数据资源价值，构建各领域规范化数据开发利用的场景

加强数据资源整合和安全保护，研究根据数据性质完善产权性质。制定数据隐私保护制度和安全审查制度

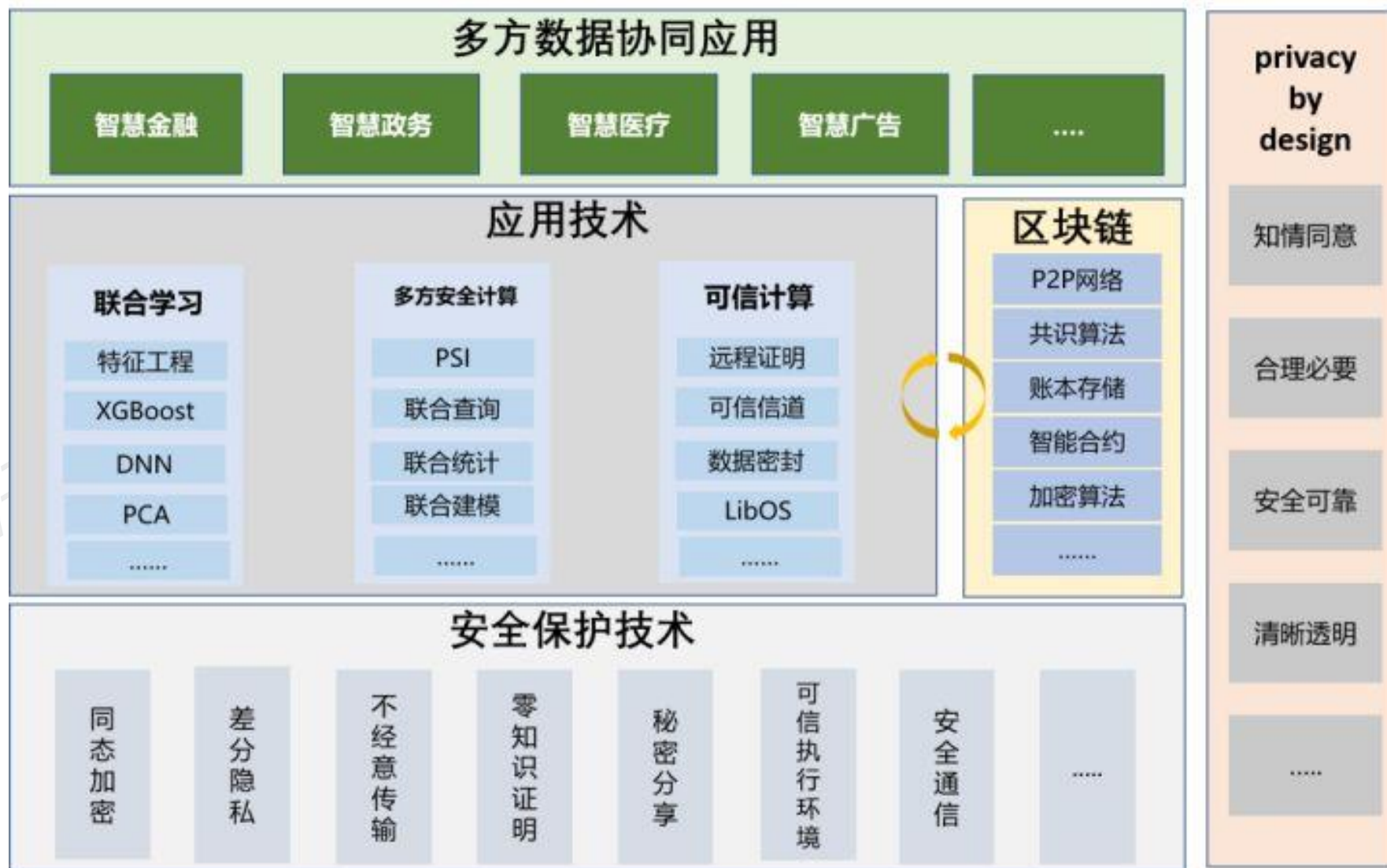
国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展

国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场

自然人的个人信息受法律保护,任何组织、个人不得侵害自然人的个人信息权益



# 隐私计算体系架构



## 隐私计算:

是指通过技术手段实现在保护数据隐私的前提下,完成对数据的安全处理。

数据可用不可见  
保护数据安全  
打破数据孤岛  
促进数据流通共享

# MPC、联邦学习、同态加密、零知识证明等概述

## 多方安全计算

是指在无可信第三方的情况下，多个参与方共同计算一个目标函数，并且保证每一方仅获取自己的计算结果，无法通过计算过程中的交互数据推测出其他任意一方的输入数据(除非函数本身可以由自己的输入和获得的输出推测出其他参与方的输入)。

## 可信执行环境

使用硬件隔离技术构建出安全可信区域，加密后的数据在此区域内运算，而不会暴露给系统的其他部分。

## 联邦学习

是实现在本地原始数据不出库的情况下通过对中间加密数据的流通与处理来完成多方联合的机器学习训练。

## 同态加密

是指能实现在密文上进行计算后对输出进行解密，得到的结果和直接对明文计算的结果一致。

## 零知识证明

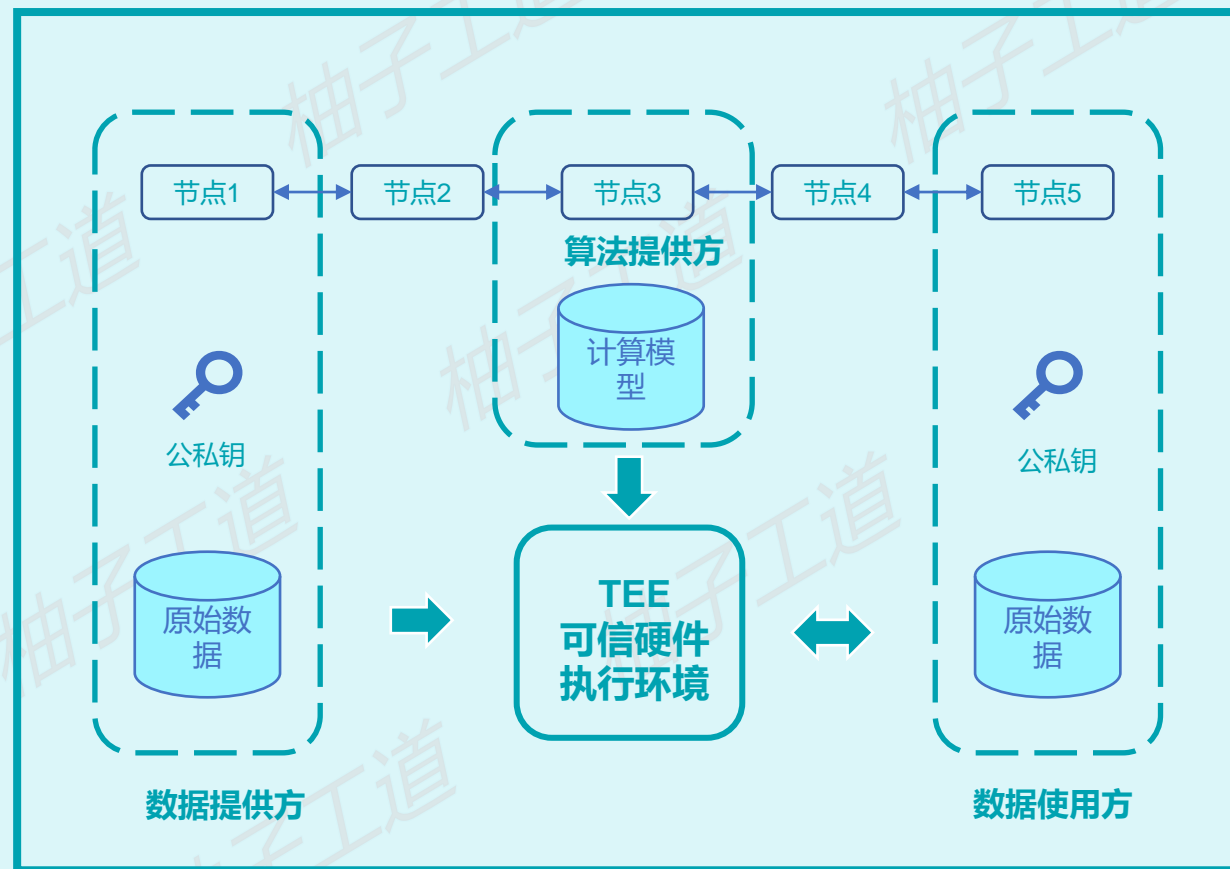
指的是证明者能够在不向验证者泄漏任何有用信息的情况下，使验证者相信某个论断是正确的。

技术	性能	通用性	安全性	可信方	整体描述	技术成熟度 <sup>5</sup>
多方安全计算（MPC）	低~中	高	高	不需要	通用性高、计算和通信开销大、安全性高，研究时间长，久经考验，性能不断提升	已达到技术成熟的预期峰值
可信执行环境（TEE）	高	高	中~高	需要	通用性高，性能强，开发和部署难度大，需要信任硬件厂商	快速增长的技术创新阶段
联邦学习（FL）	中	中	中	均可	综合运用 MPC、DP、HE 方法，主要用于 AI 模型训练和预测	快速增长的技术创新阶段
同态加密（HE）	低	中	高	不需要	计算开销大，通信开销小，安全性高，可用于联邦学习安全聚合、构造 MPC 协议	快速增长的技术创新阶段
零知识证明（ZKP）	低	低	高	不需要	广泛应用于各类安全协议设计，是各类认证协议的基础	快速增长的技术创新阶段
差分隐私（DP）	高	低	中	不需要	计算和通信性能与直接明文计算几乎无区别，安全性损失依赖于噪声大小	快速增长的技术创新阶段
区块链（BC）	低	中	中	不需要	基于带时间戳的区块链式存储、智能合约、分布式共识等技术辅助隐私计算，保证原始数据、计算过程及结果可验证	逐渐接近技术成熟的预期峰值

# 产品概述

## 区块链可信计算平台

- 本系统主要包括数据共享区块链配置、TEE可信计算框架、TEE客户端SDK组件、分布式数据共享流通子系统等模块组成。
- 系统利用区块链技术，连接数据使用方、数据提供方和算法提供方等，实现数据合作联盟管理、可信计算集群管理、数据管理、计算模型管理、项目管理、计算任务管理、可信计算等操作，从而保障数据流通的有序性，安全性。



# 产品定位

“让数据融通，让安全可及，让价值可见”



## 数据生态构建

- 数据流通管道
- 数据供需撮合
- 数据应用协同



## 数据治理延展

- 分布式数据治理
- 数据确权、鉴权
- 数据隐私保护
- 数据可信追溯



## 数据价值挖掘

- 数据应用场景挖掘
- 数据联合建模
- 数据资产交易

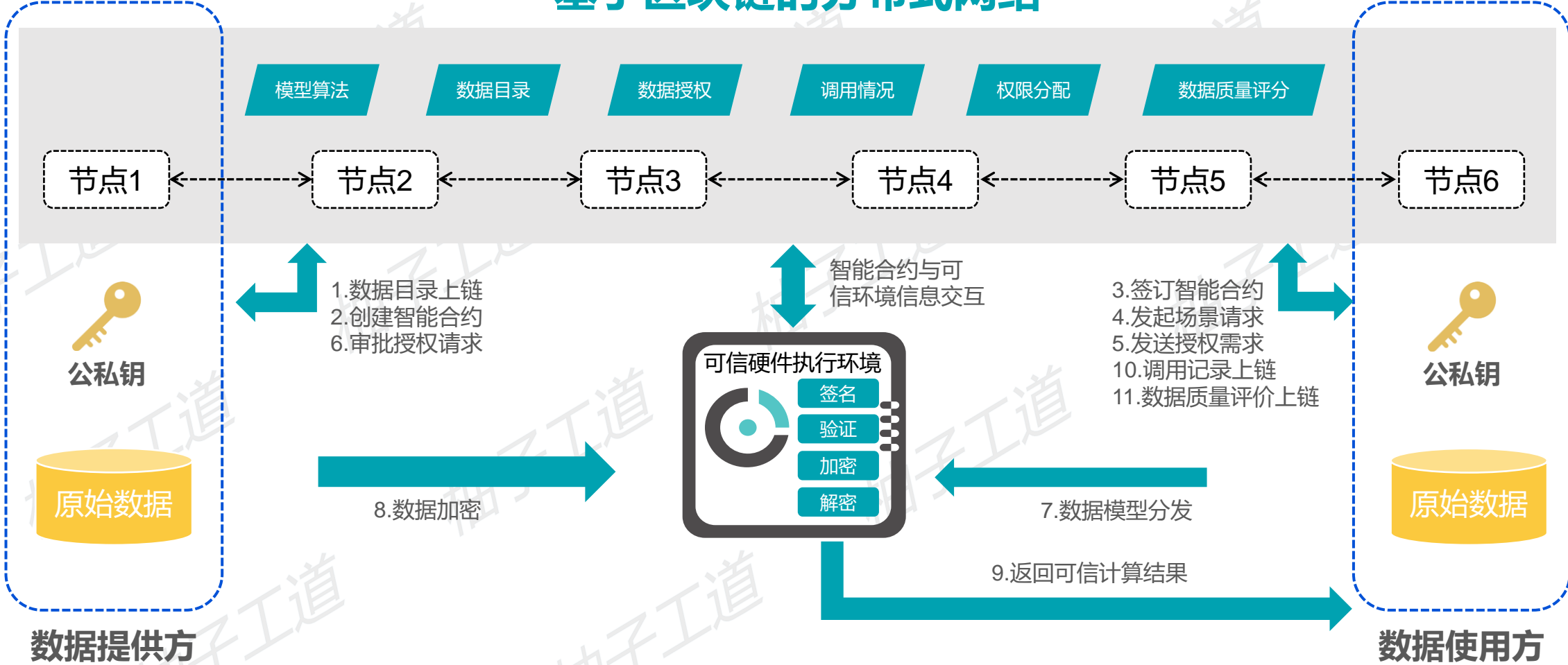
# 产品定位

数据确权溯源，确保真实可信

数据可用不可见，保护数据隐私

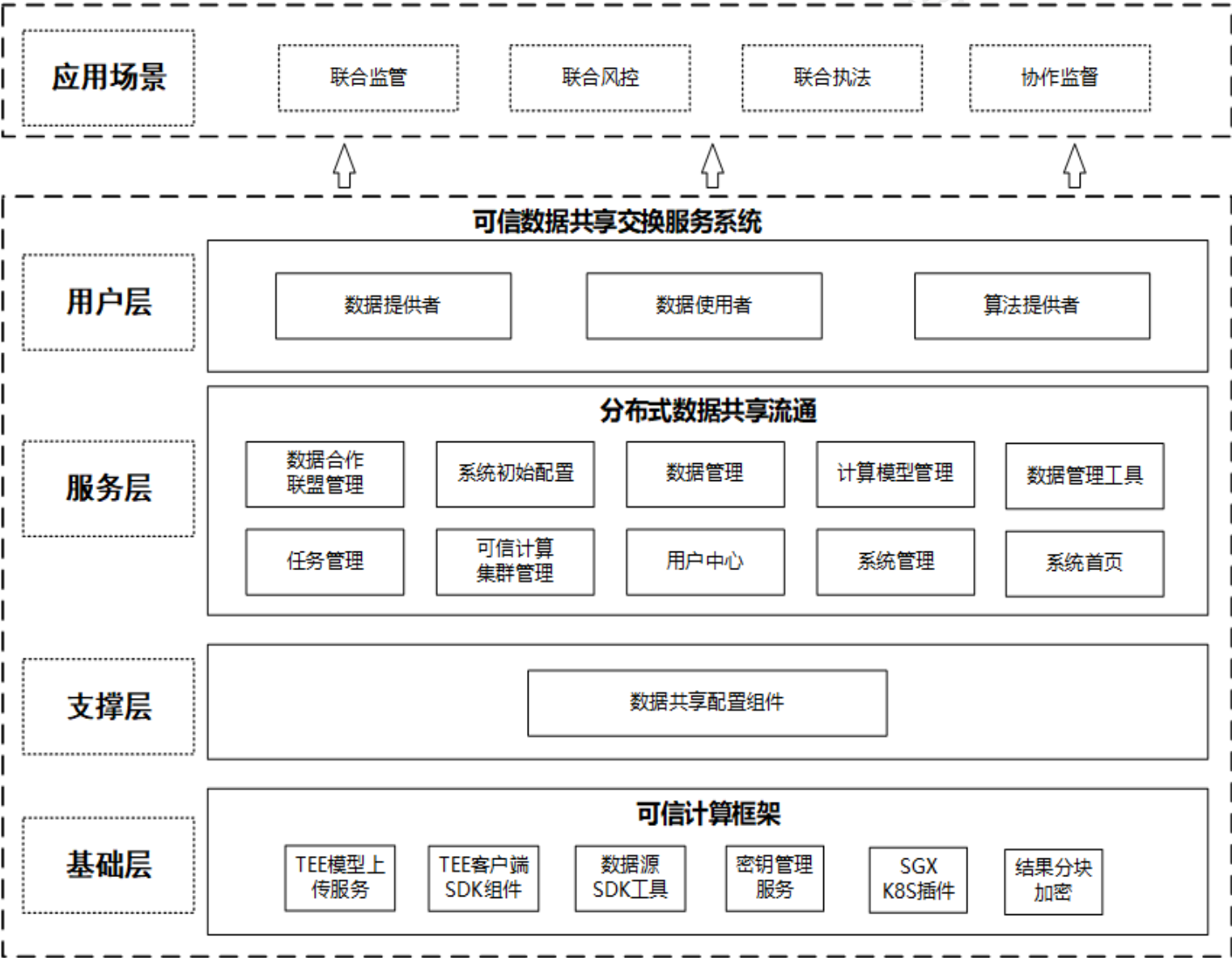
打破数据孤岛，共享数据价值

## 基于区块链的分布式网络





# 平台架构图



平台采用分层分端架构设计，不同的参与方可以完整的拥有独立应用端，可方便的与其业务系统进行数据对接，系统主要分层如下：

## 1.基础层

可信计算框架主要针对底层可信安全硬件资源进一步进行封装，对上层提供统一的对接标准及可信资源控制，为构建可信应用场景提供框架基础。

## 2.支撑层

为解决上层服务与特定区块链平台耦合太紧密问题，数据共享关联组件是作为支撑上层服务的组件，主要为上层服务提供快速、方便的对接BaaS。

## 3.服务层

服务层主要面向应用侧，是分布式数据共享流通子系统的后端服务，让用户可以通过相关服务功能完成跨组织的数据协同。服务层也包括数据管理工具，实现数据提供方根据需要对数据的管理、发布、授权等功能，对数据使用方或算法提供方来说，可以向数据提供方申请数据，在授权后查看数据，满足数据对接和业务协同的需求

## 4.用户层

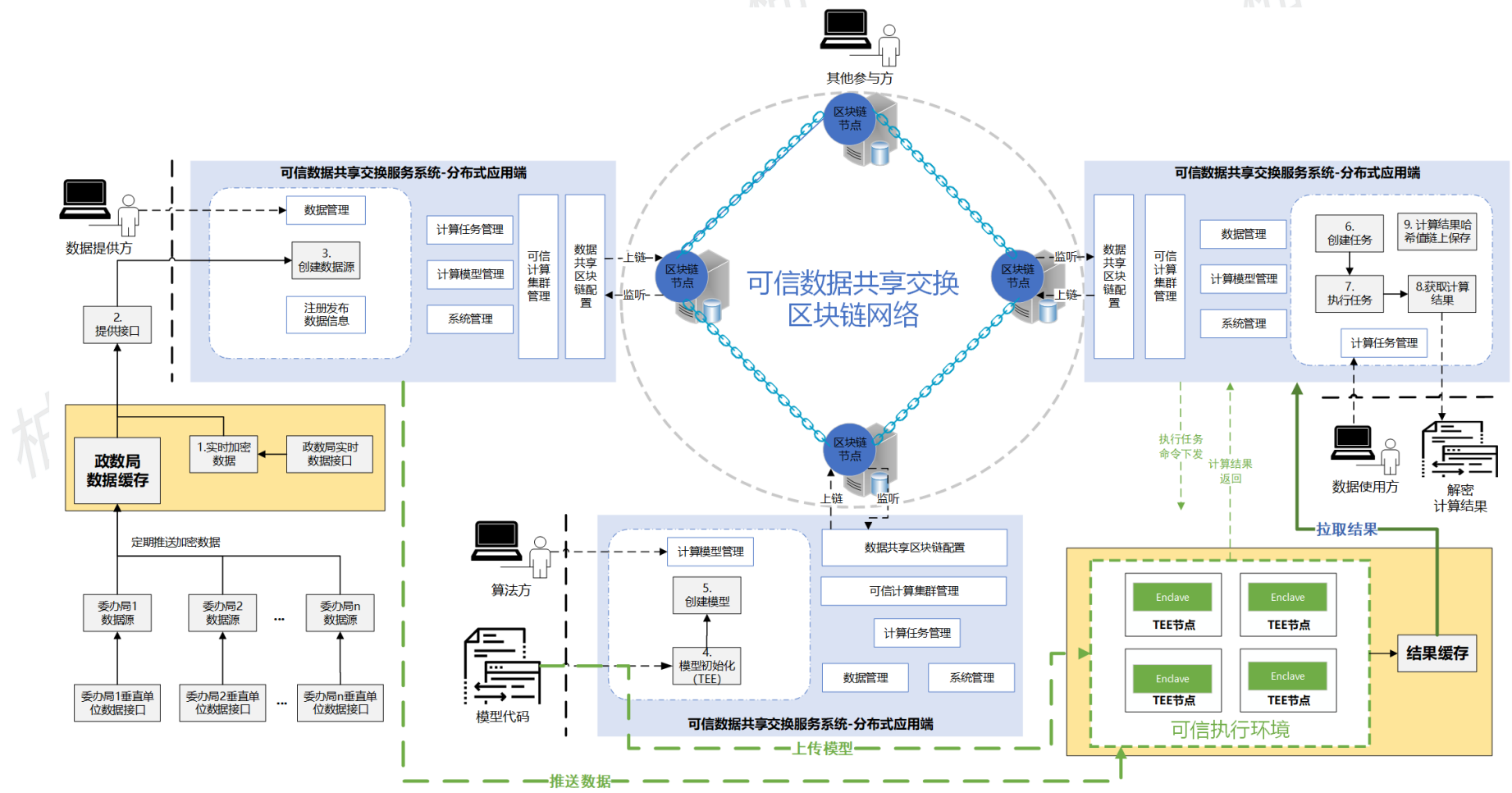
为用户提供系统操作界面支持，是分布式数据共享流通子系统的前端展现，用户可进入系统发起可信计算任务。

## 5.应用场景

为可信数据共享交换服务系统可支撑的应用场景，主要有联合监管、联合风控、联合执法、协作监管等。

# 可信计算流程示意图

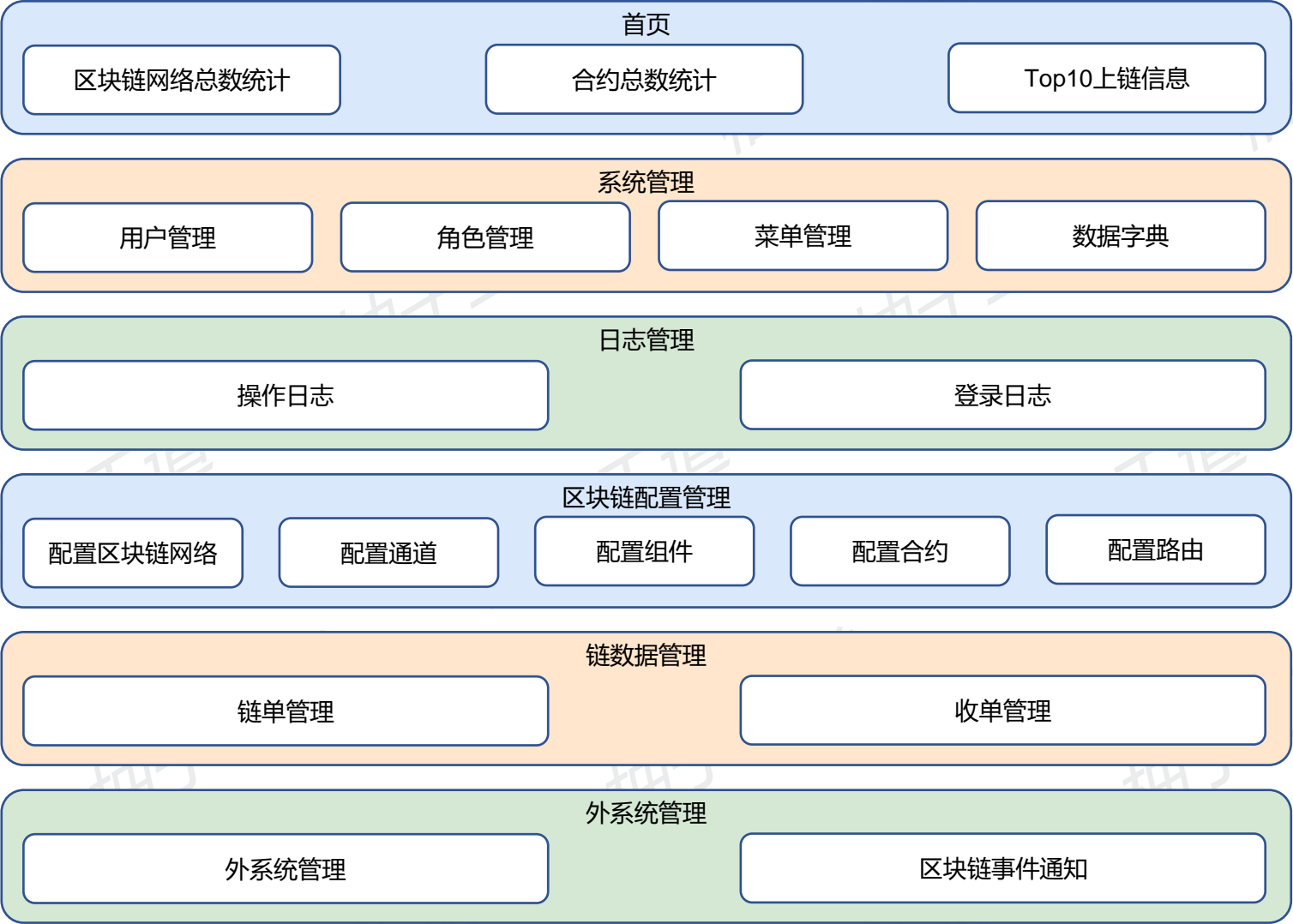
基于区块链的可信计算平台，不同场景下其多方参与的主要业务过程如下



- 数据提供方对原始数据进行加密并完成数据的获取方式配置；
- 算法方进行模型代码开发，并部署模型到TEE环境中，并在完成模型创建；
- 数据使用方发起数据共享协同计算的请求，创建计算任务后并执行任务；

系统通过预先设计并建立好的数据可信计算模型，向数据提供方（如企业、政府、金融机构等）请求加密后的原始数据；任务执行完成后，计算结果加密上链；数据使用方（如水务局）获取计算结果后进行解密，实现数据共享交换业务场景（如联合监管、联合执法、信用画像、协作监管、联合营销、联合风控等）。

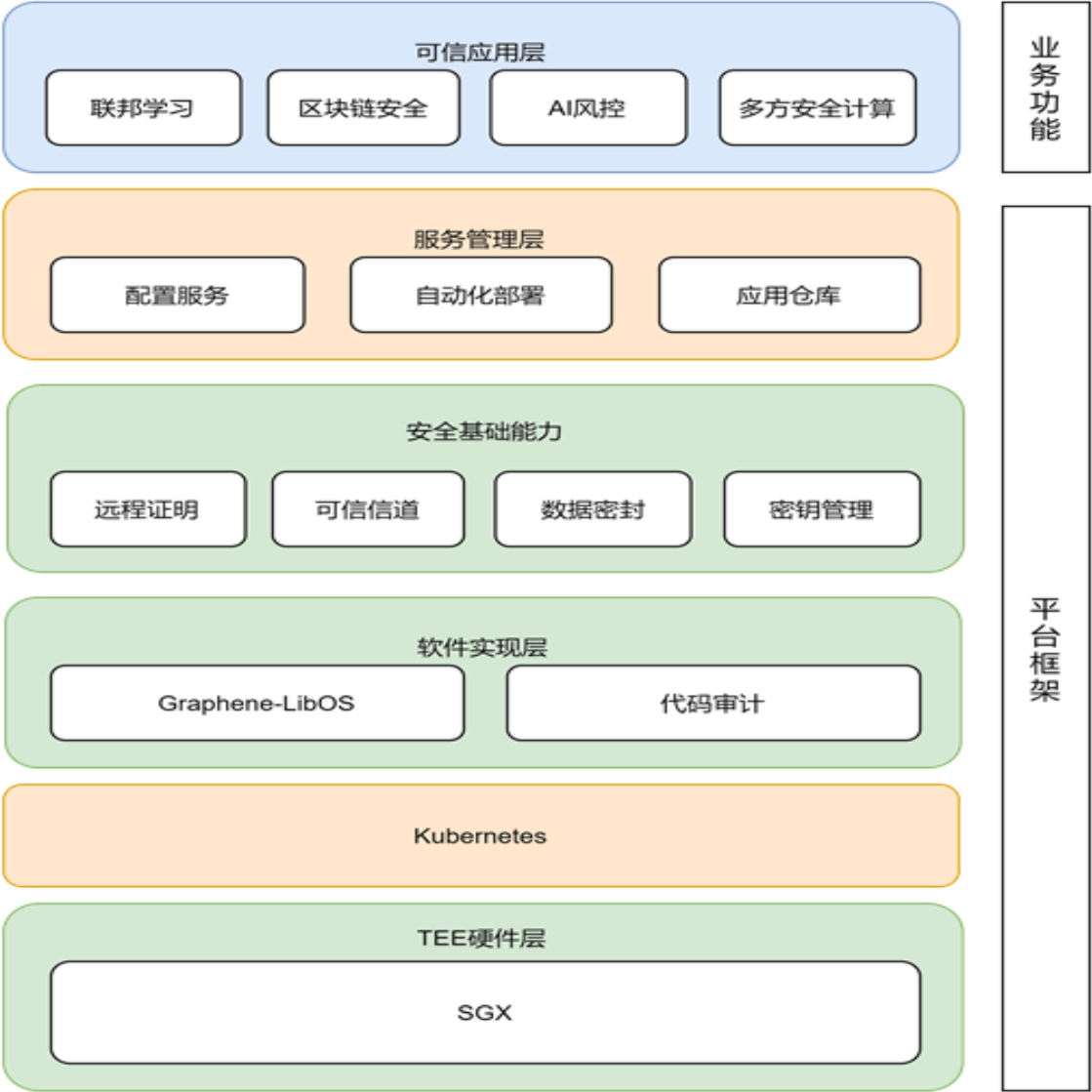
# 功能介绍（一）数据共享区块链配置



## 数据共享区块链配置

是用于配置与BaaS创建的区块链网络等信息进行绑定的支持系统，提供分布式数据共享流通子系统与BaaS区块链基础服务平台之间的快速对接，并对区块链网络成员管理数据下发和业务数据上链等操作提供相关接口服务。

# 功能介绍（二）TEE可信计算框架



## TEE可信计算框架

基于硬件中的可信计算区域，进行多方数据计算，保护数据隐私，功能主要包含配套服务、远程证明、代码审计、密钥管理、可信通道、自动化部署等功能。

- TEE硬件层采用Intel SGX技术。
- Kubernetes层为TEE程序提供集群化能力。
- 软件实现层采用LibOS，并提供代码审计功能。
- 安全基础能力层提供远程证明、可信信道、秘钥管理、数据密封等功能。
- 服务管理层提供配置服务、自动化部署、应用仓库。
- 可信应用层对功能开发和业务提供支撑。

# 功能介绍（三）TEE客户端SDK组件

## TEE客户端SDK组件

是TEE框架客户端对一些复杂操作以SDK形式进行封装，提供用户可调用的SDK API与TEE服务端进行交互，包括发起远程证明，调用业务逻辑等功能。

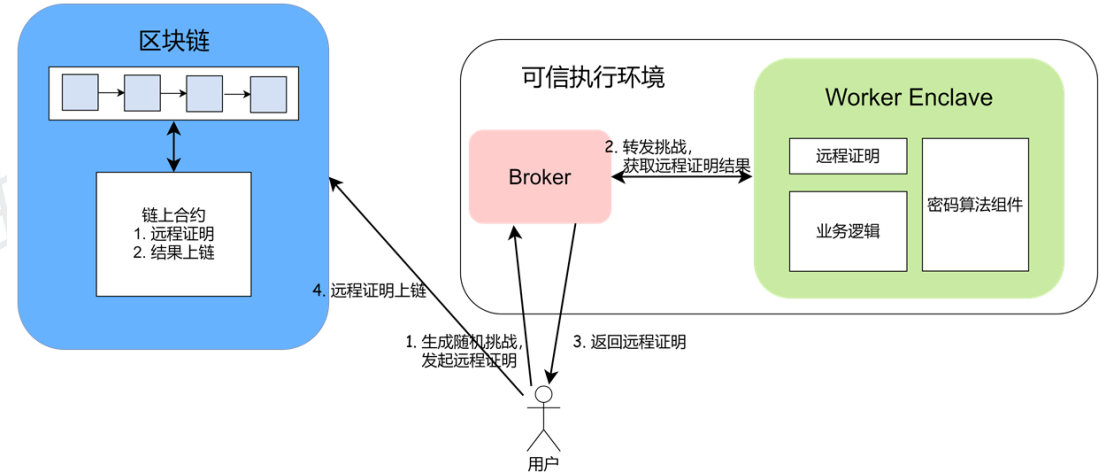


图1：远程证明流程

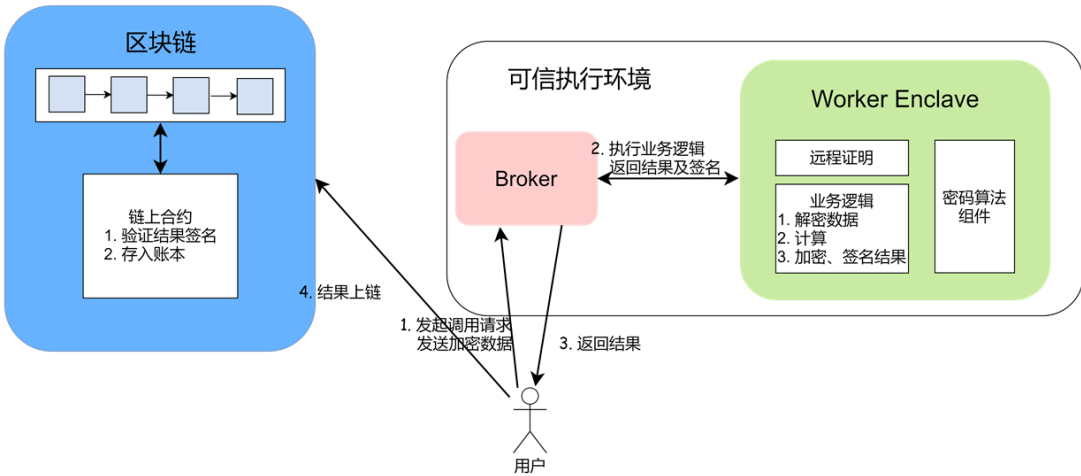
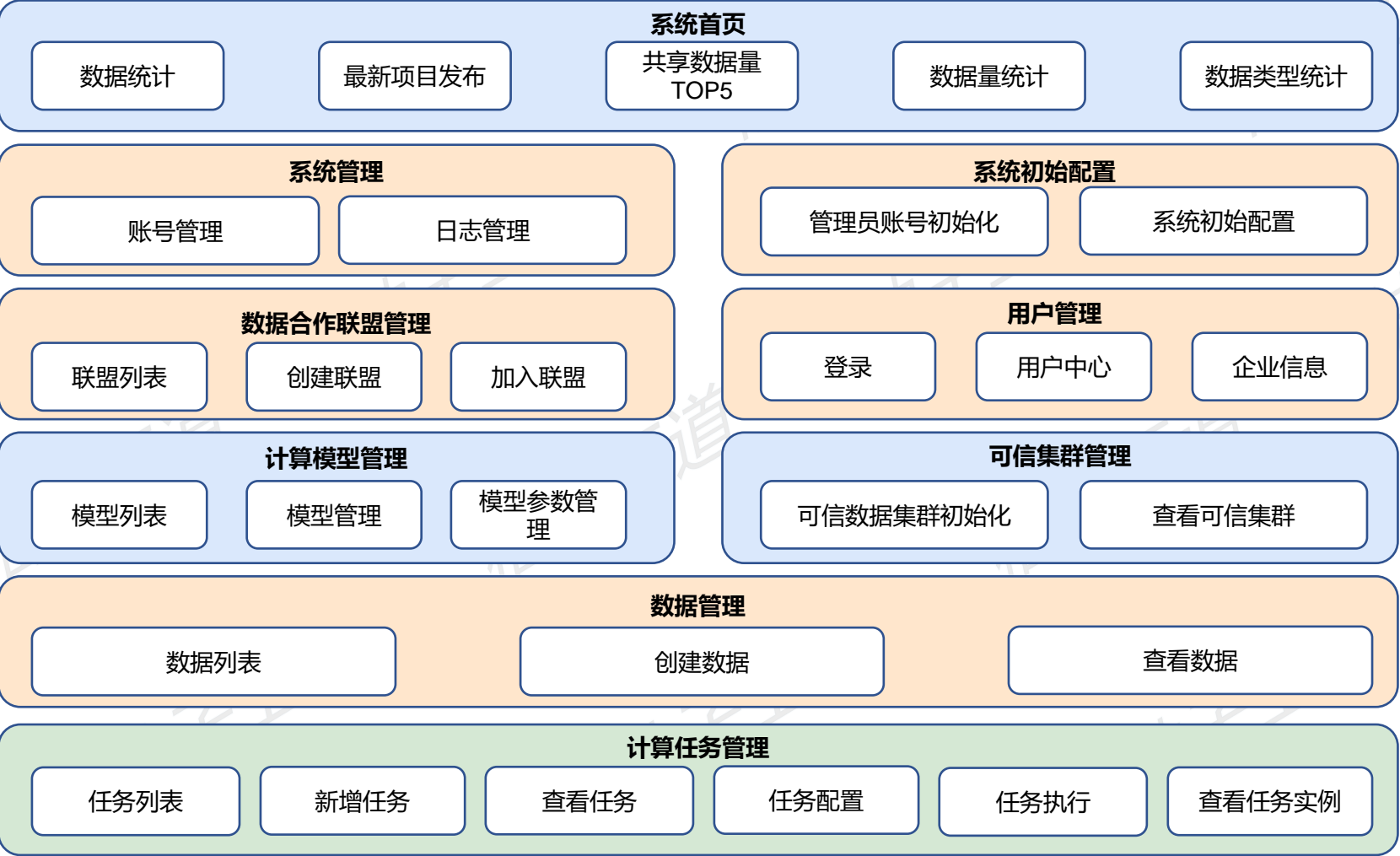


图2：处理隐私数据流程



# 功能介绍（四） 分布式数据共享流通子系统

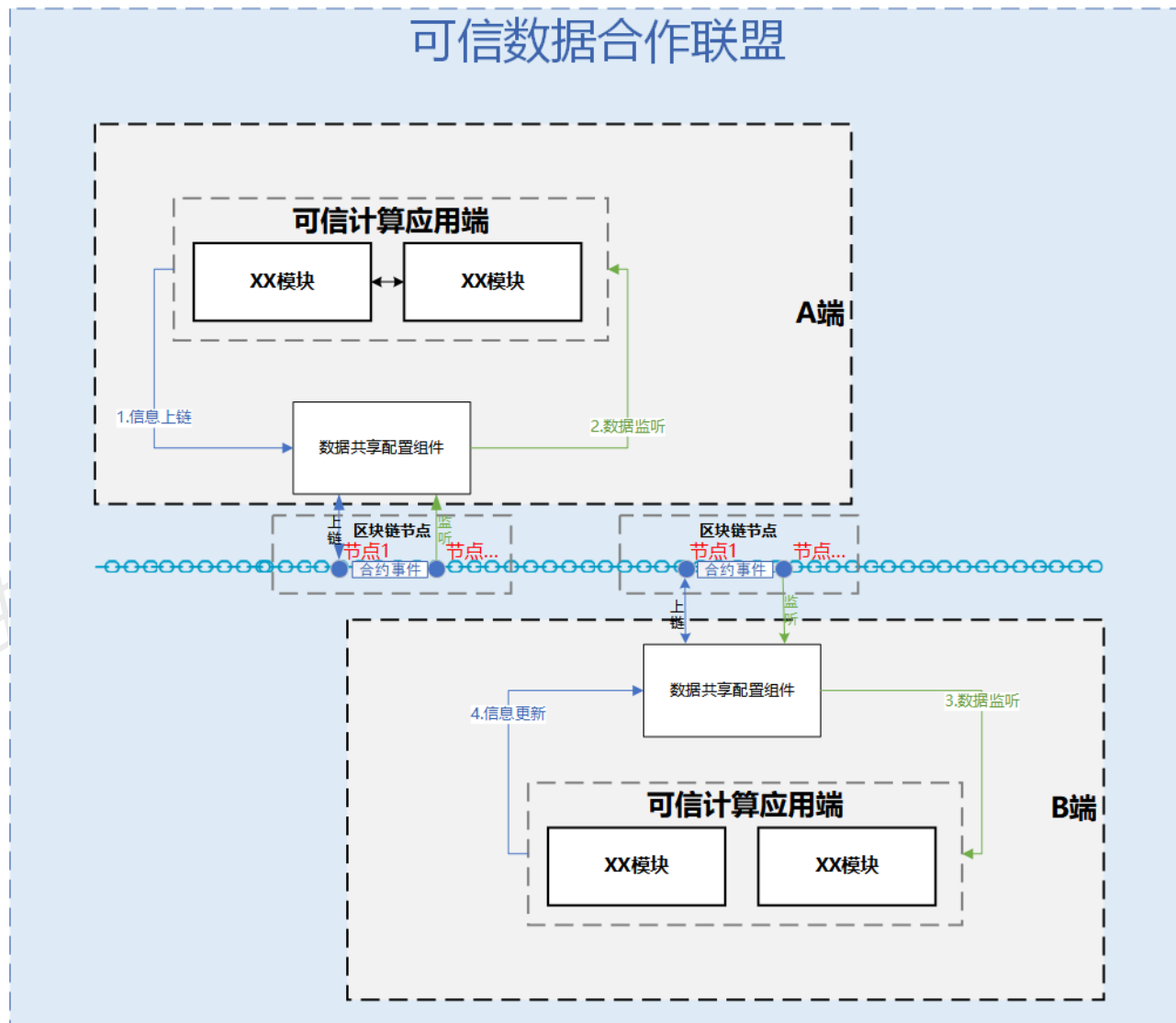


## 分布式数据共享交换子系统

实现数据提供方，数据使用方和算法提供方的三权分置，对数据共享业务流程的可视化操作，还包括对系统各个资源的创建和使用情况的展示。

通过该系统，数据提供方可以对拥有的数据信息、数据的调用方式进行管理；模型提供方提供数据计算需要用到的计算模型；数据使用方在看不到数据的前提下得到数据的计算结果。

# 产品核心理念（一）分布式分端

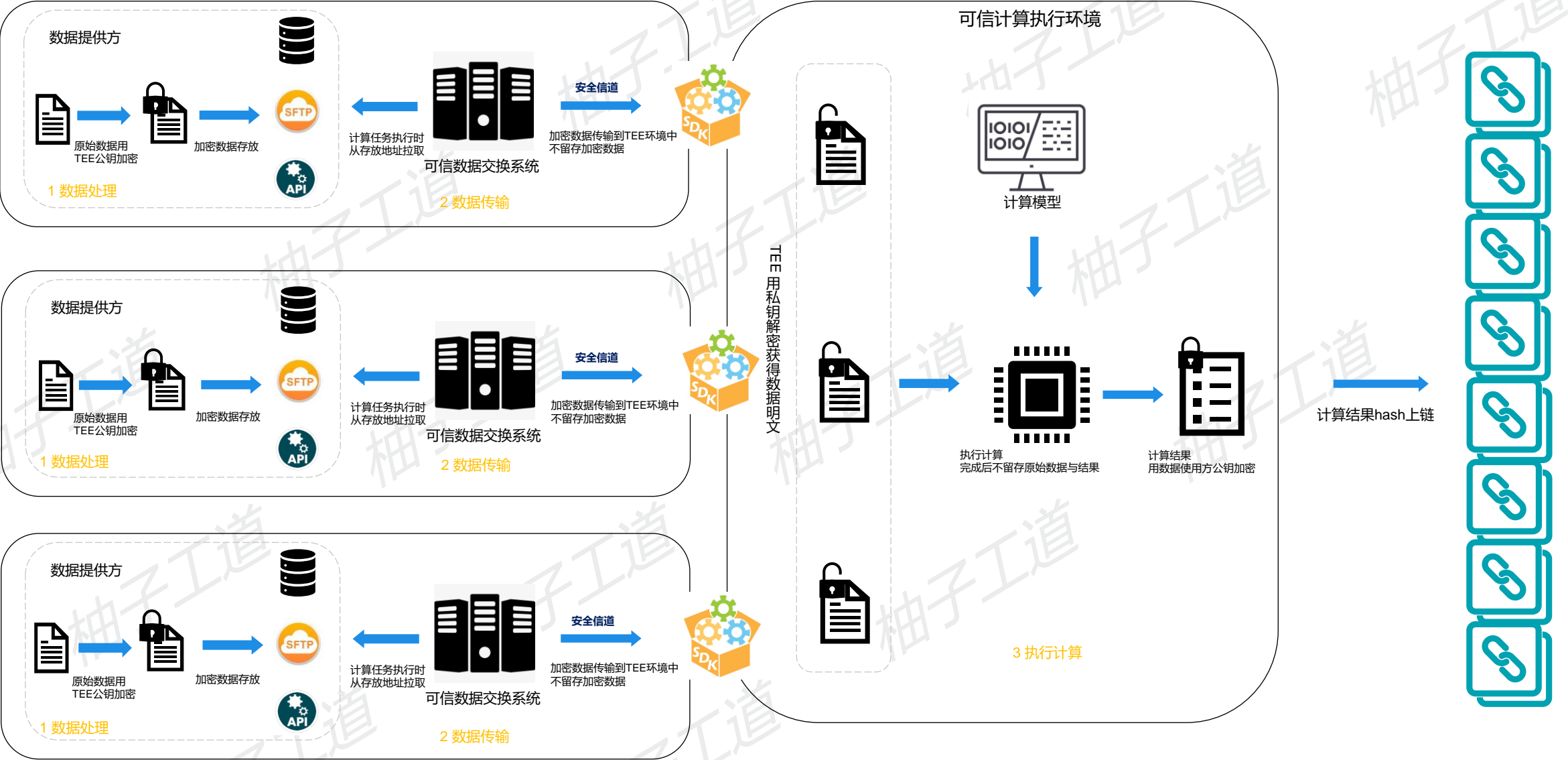


可信计算平台采用分布式分端设计，分端互操作的逻辑主要依赖区块链网络，多方通过其持有的区块链节点进行读链写链操作，其他方的节点通过同步账本后触发合约事件获取到其互操作数据，其应用端进行本地数据更新，其主要设计逻辑如下：

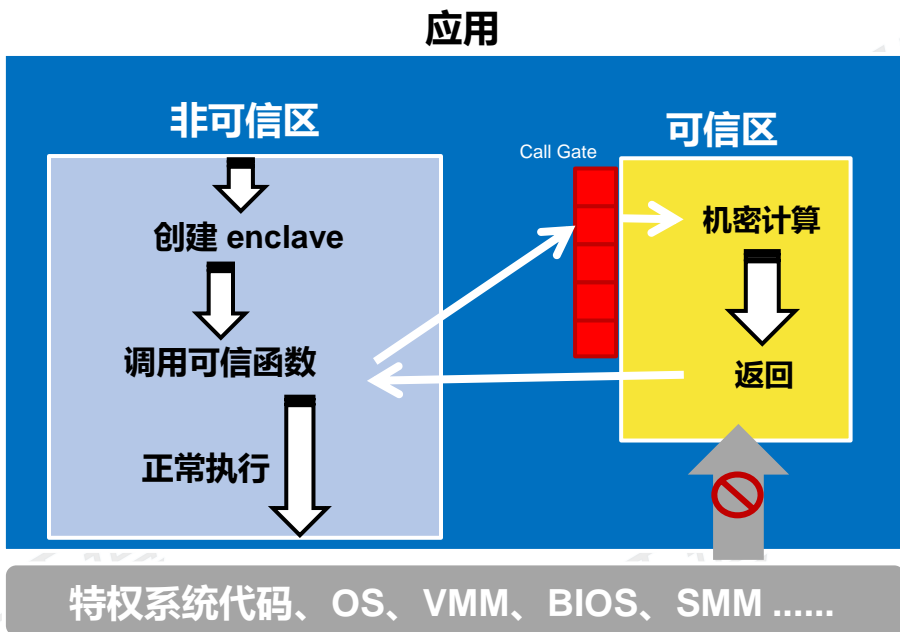
1. A应用端进行数据操作，通过其数据共享配置组件进行调用区块链节点进行数据上链操作；
2. B端对应的区块链节点同步账本，进行合约交易执行，触发合约事件，其事件被B端的数据共享配置组件监听到，其把事件数据给到应用端；
3. B应用端对收到的事件数据进行本端处理，若B端进行业务操作，其数据同理可通过其数据共享配置组件进行上链数据更新；
4. A端可收到数据更新智能合约触发的事件，进行本端业务处理。

通过上述逻辑，其A、B端就可通过区块链完了分端的分布式业务协同。

# 产品核心设计理念（二）数据隐私安全



# 产品核心理念（三） — TEE可信环境逻辑



TEE（可信执行环境）是实现“数据可用不可见”的关键，所有数据只在TEE中才解密计算，保证了数据提供方的原始数据不出本域。

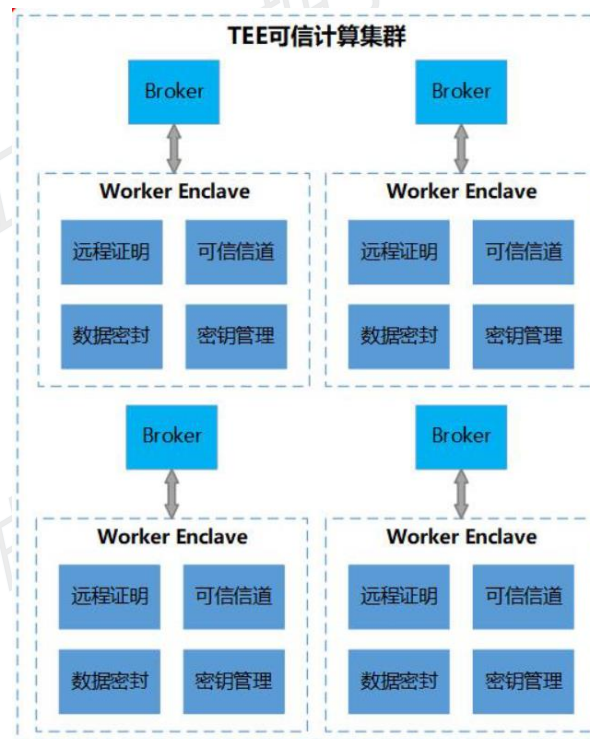
区块链可信计算平台，使用Intel SGX技术作为TEE。SGX 全称 Secure Guard Extension，是在应用程序内建立 TEE（称为 enclave）的处理器拓展指令集。程序在 TEE 内运行时的数据和状态只对 CPU 可见，TEE 外的操作系统、VMM（虚拟机管理器）等均无法看到这些数据和状态

单节点：实现计算任务的动态安全

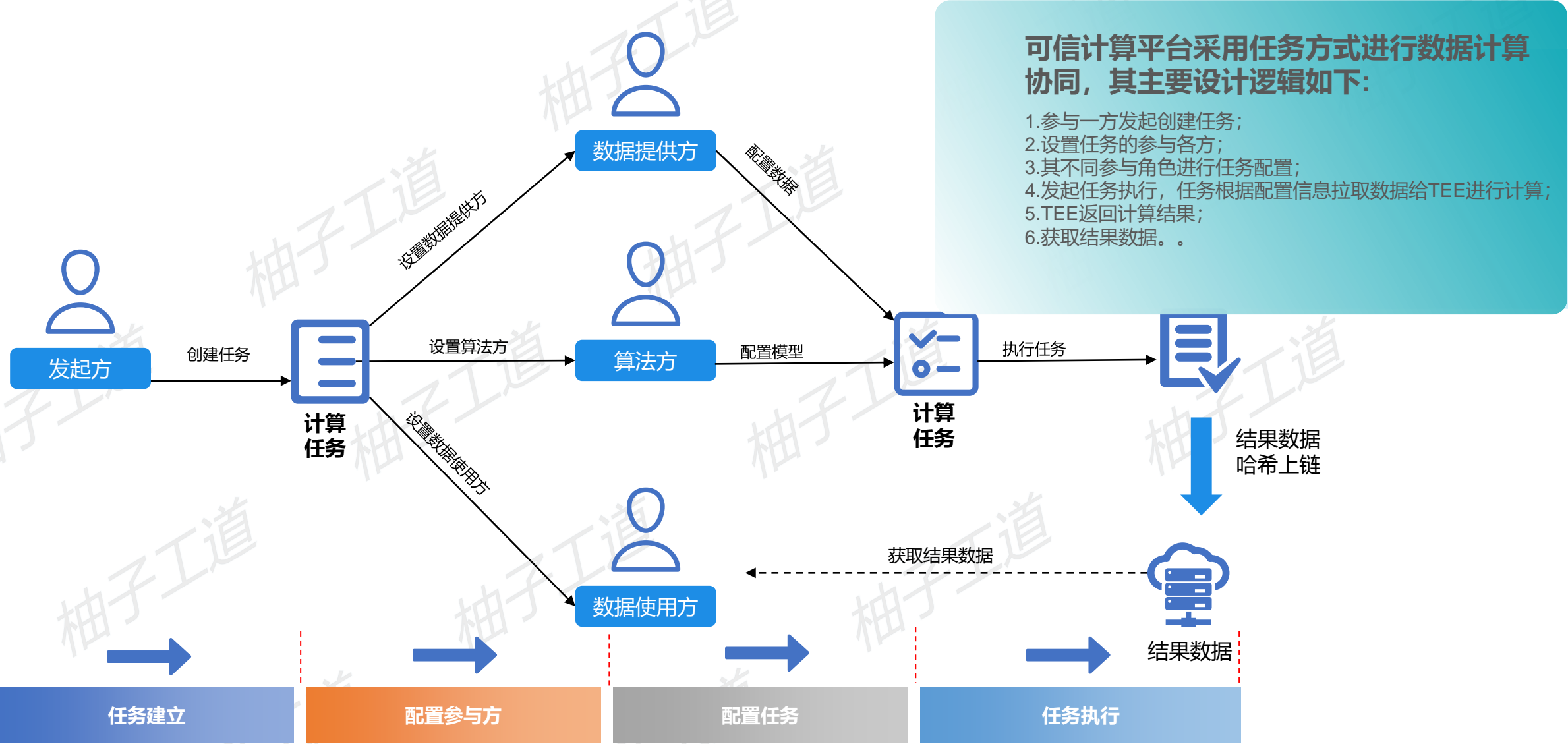
- 模型上传、自动打包
- 远程证明、数据密封
- 可信信道

可信计算集群：基于k8s集群实现计算任务的自动调度

- 密钥管理服务
- 数据分块加密、解密



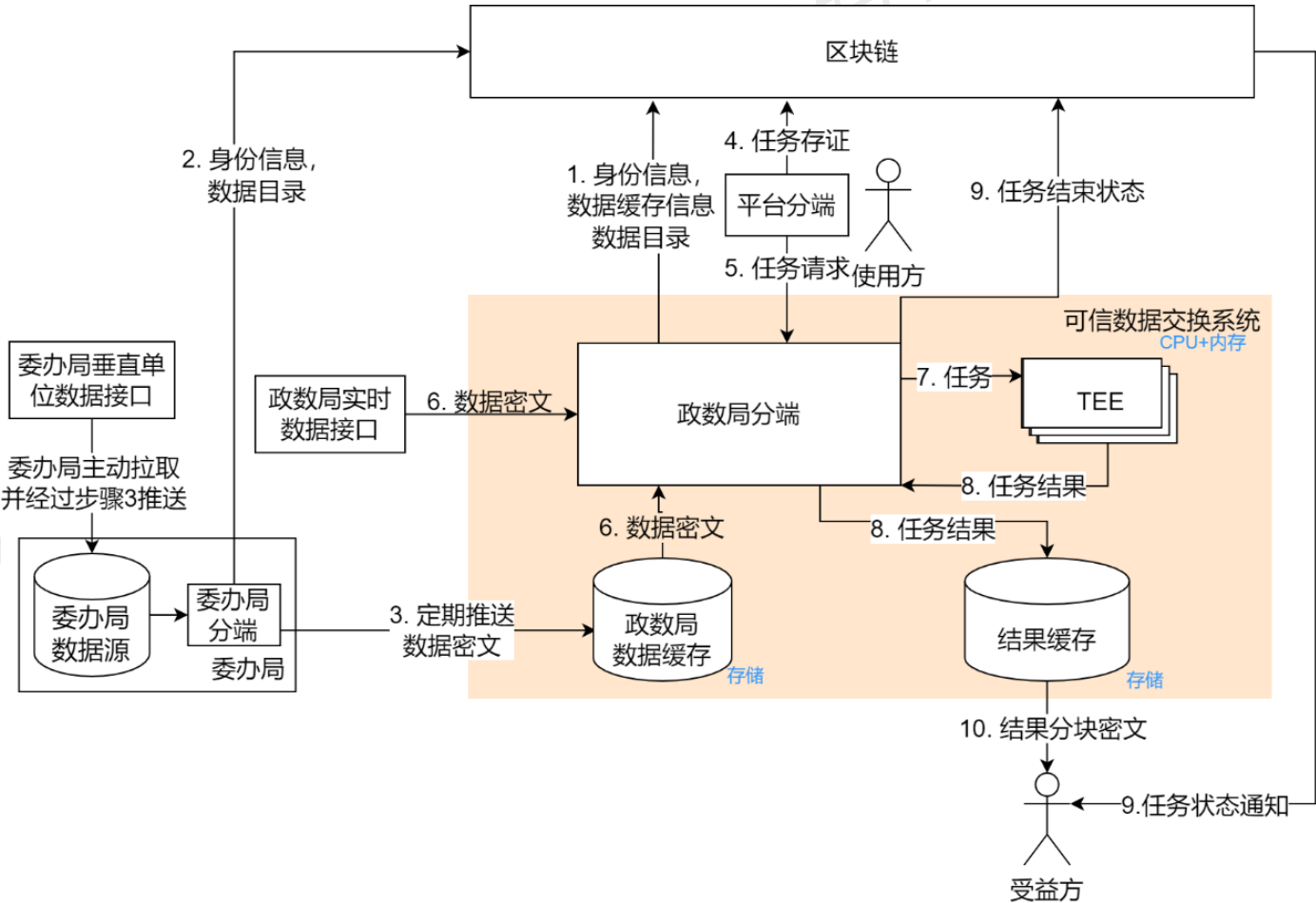
# 产品核心理念（四）任务协同逻辑





# 产品核心设计理念（五）——业务逻辑

某政数局可信计算框架业务流程图



## 特点

- 1、为避免对客户的生产数据库的影响，政数局的各委办局采用定期推送加密数据到数据缓存
- 2、对结果分块加密，可实现一次计算结果，分别满足多个数据使用方
- 3、支持任务定时执行，计算结果可放在结果缓存，可通过接口异步获取，多次获取
- 4、对任务实时监控，对运行时间过长的异常任务可强制中断，释放宝贵的计算资源
- 5、所有数据发布、审批、任务执行的环节均存证在区块链上，保证数据的可审核追溯。

# 产品优势

## 数据隐私保护

数据实时运算，数据内容或结果加密上链 链上授权与链下权限实现无缝结合 国密算法满足金融级加密要求

## 支持联合建模，可信安全计算

联合数据计算建模，满足业务需求 可信执行环境确保安全计算

## 实现数据内容和数据价值的流通

无需中心化归集，避免数据垄断 保护数据所有权，降低多方博弈成本 降低数据流通成本，提高数据使用效率

## 操作可追溯

授权链条完整，易于执行 操作行为上链，透明可监督 支持事后审计，保障多方权益

## 对数据进行一致性表达

支持多种数据描述方式，包括 数据目录、数据描述、数据样例等 数据表达链上可获取



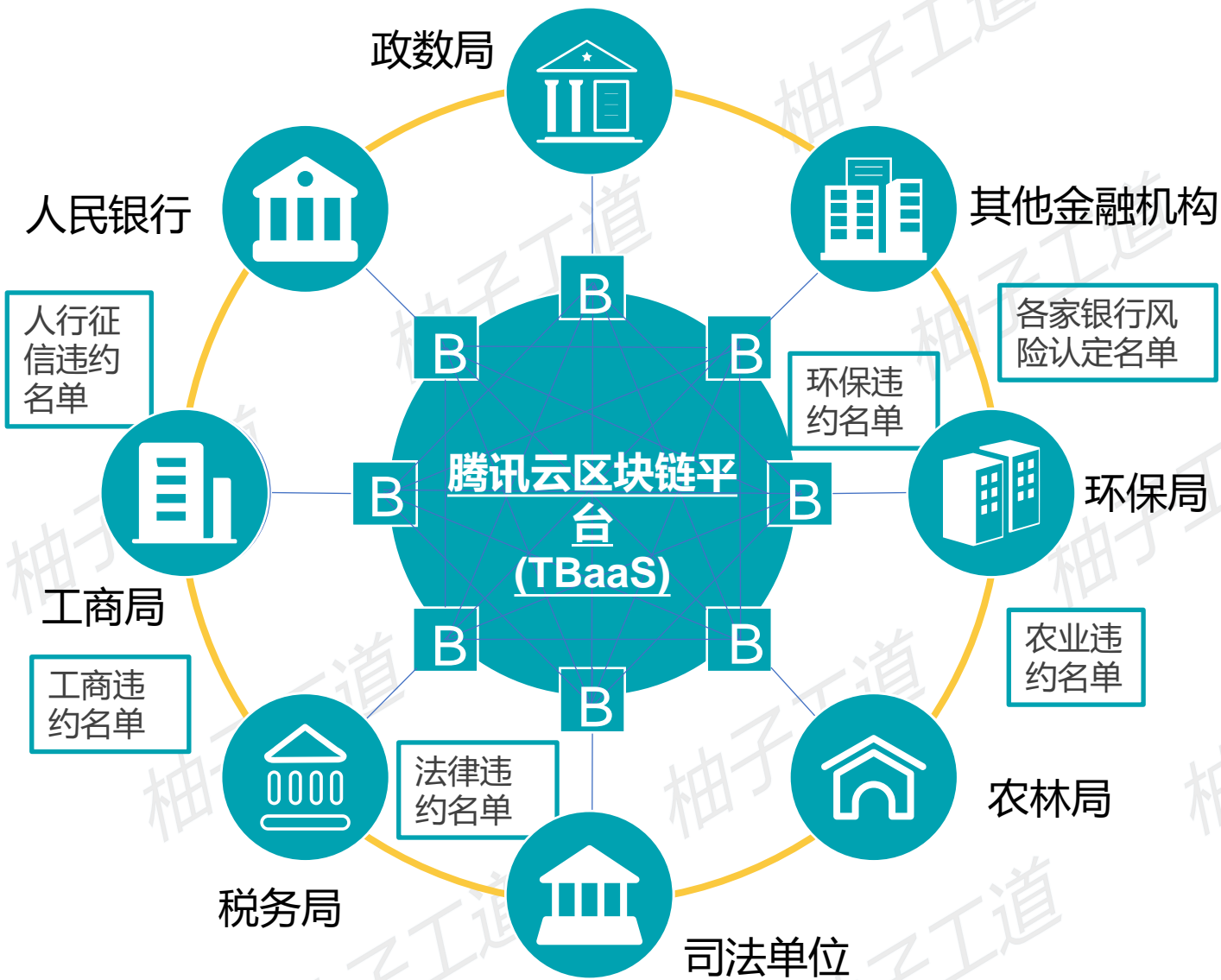
区块链  
可信计算平台

# 区块链可信计算平台——应用场景

可信计算应用场景广泛，可支持金融、医疗、政务等领域的相关数据交换，也可打通不同行业领域间的阻碍。支持联合监管、联合执法、联合营销、联合风控、协作监管等多类应用场景



# 案例1：某省不良企业名单信息共享区块链解决方案



## 构建信息索引

各个单位将共享信息的上链，同时提供数据的导引上链，并进行数字签名



## 数据访问授权

数据信息作为资产进行管理，通过授权人的密钥，访问者对需求数据进行访问



## 大数据为核心

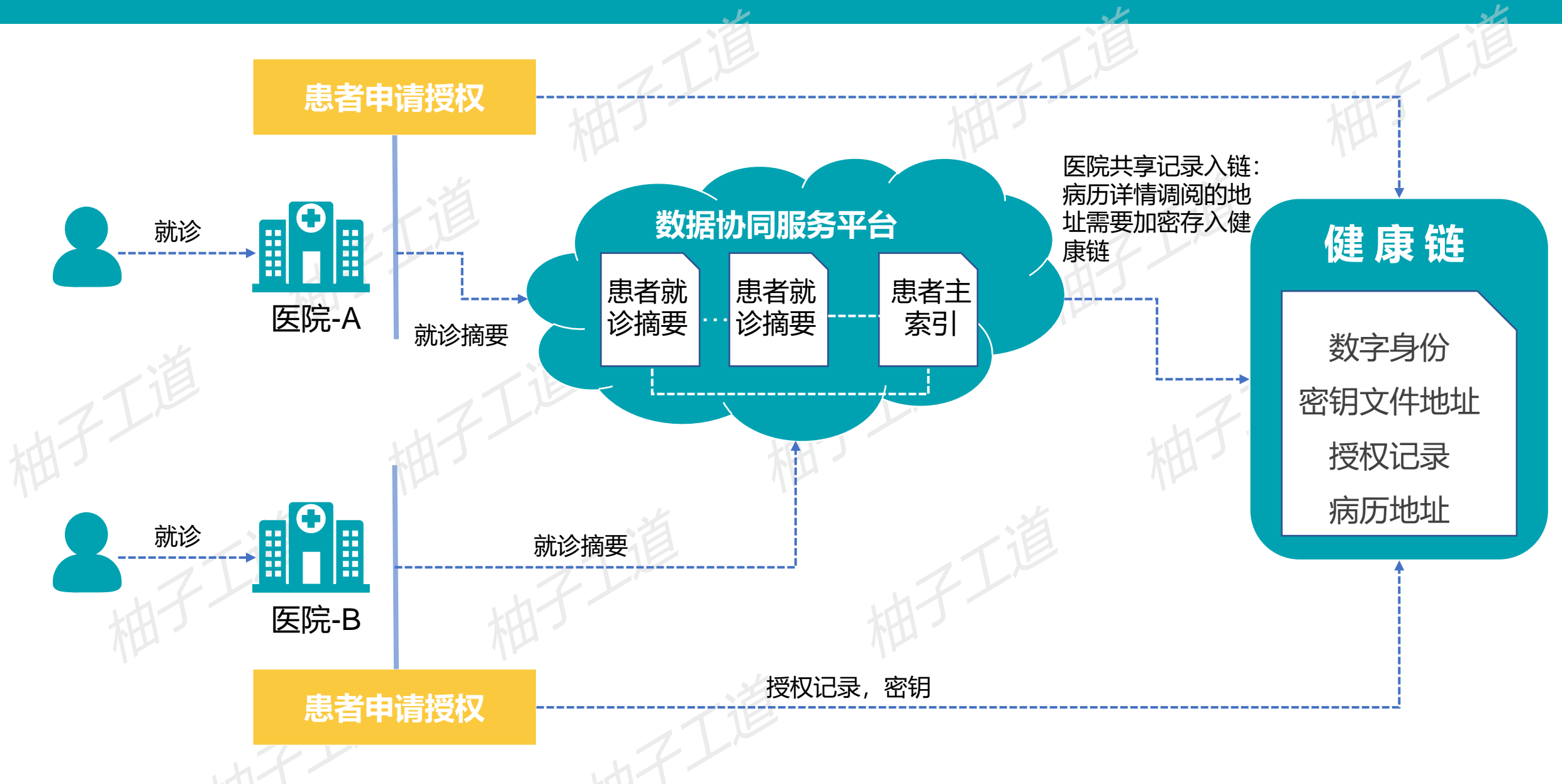
政数局作为发起方和平台承建方，集成各方接入区块链，通过区块链作为信息交流的平台



## 共享黑名单信息

共享各个单位、各个组织之间所掌握的违约信息，不同纬度的违约内容、违约事件、违约是否处理完毕、违约程度

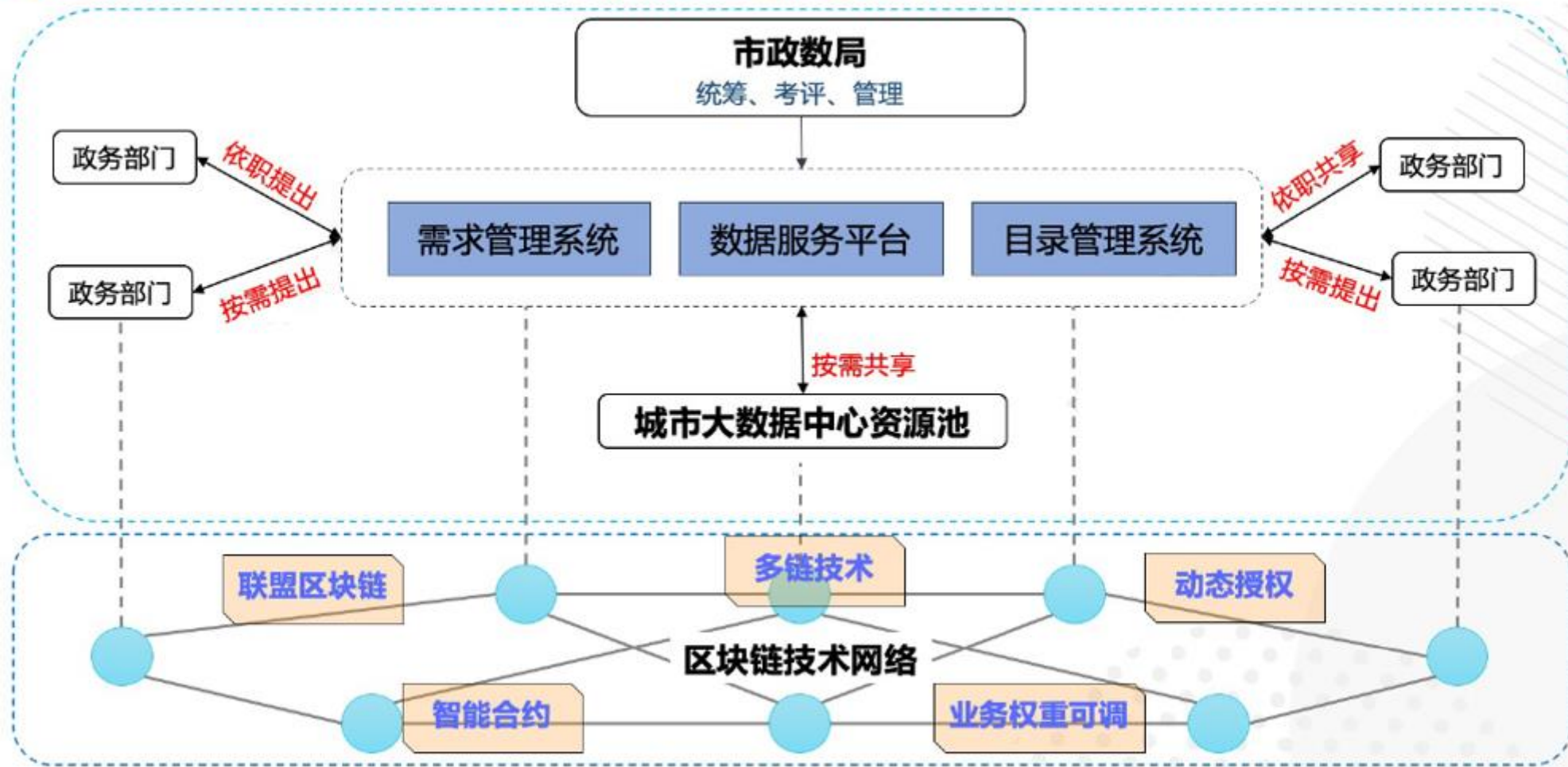
# 案例2：支持医疗数据流转的区块链解决方案



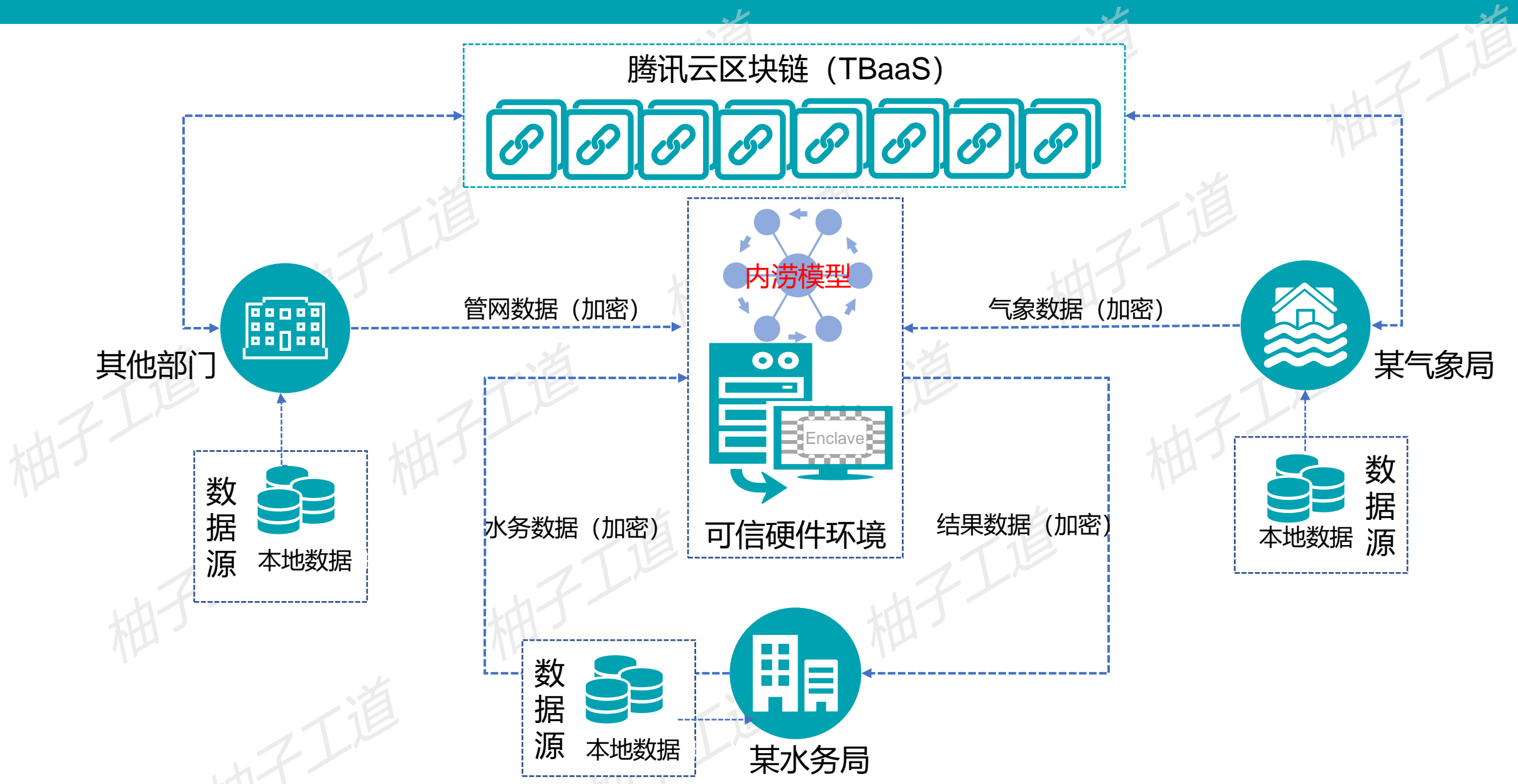


# 案例3：某市政数局数据共享交换链--解决数据共享难题

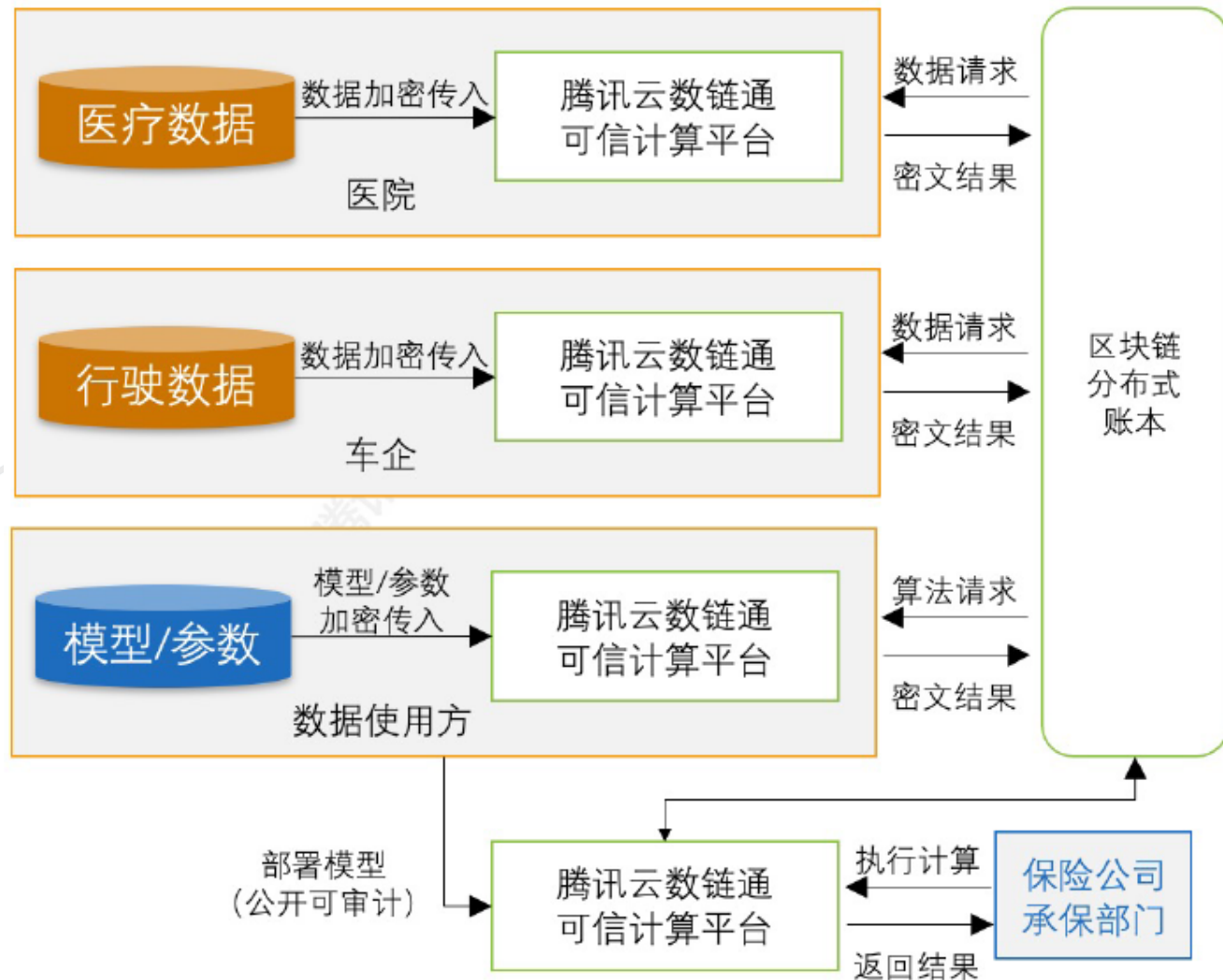
基于区块链技术，完成目录上链、供需授权上链、服务记录上链，实现共享全流程可追溯、不可抵赖



# 案例4：某区委办局内涝模型分析预测



# 案例5：某保险公司多方数据可信计算



- 数据使用方：提供数据算法模型
- 医院、车企等数据提供方：提供评估所需数据，处理为中间数据后加密上链
  - 医院可提供投保人、被保人的健康状况数据
  - 车企可提供投保人、被保人的驾驶行为数据
- 保险公司相关部门：将基于各类数据的评估算法模型部署到可信计算平台
- 保险公司承保或理赔时，通过智能合约取用链上投保人、受保人中间加密数据，输入可信平台进行评估
- 保险公司以此评估结果，可实现比如快速的理赔，灵活的车险定价等，降低运营成本，以及提高保险产品竞争力。
- 整个过程不会泄露医院、车企等机构的原始数据，使各机构间的数据合作成为可能。

# 产品截图



产品截图

首页

数据合作联盟

项目管理

数据管理

计算模型管理

计算任务管理

任务列表

可信集群管理

系统管理

任务列表

成员管理

任务执行

任务配置

新建项目

新增成员

任务名称:

所属项目名称:

查询

重置

新增

任务名称	所属项目	创建者	创建时间	操作
水利信息数据交换	水利信息	水利局	2021-08-02 18:36:11	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:35:08	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:34:36	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:34:16	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:33:55	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:32:09	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:31:42	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:30:53	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:30:34	查看 任务配置 查看实例 执行
水利信息数据交换	水利信息	水利局	2021-08-02 18:30:00	查看 任务配置 查看实例 执行
公共资源信息	公共资源信息	政务局	2021-08-02 18:18:08	查看 任务配置 查看实例 执行
公共资源信息	公共资源信息	政务局	2021-08-02 18:17:45	查看 任务配置 查看实例 执行
公共资源信息	公共资源信息	政务局	2021-08-02 18:17:07	查看 任务配置 查看实例 执行
公共资源信息	公共资源信息	政务局	2021-08-02 18:16:50	查看 任务配置 查看实例 执行
公共资源信息	公共资源信息	政务局	2021-08-02 18:16:31	查看 任务配置 查看实例 执行
采购信息数据交换	政府采购信息	政务局	2021-08-02 18:15:56	查看 任务配置 查看实例 执行
采购信息数据交换	政府采购信息	政务局	2021-08-02 18:15:11	查看 任务配置 查看实例 执行
采购信息数据交换	政府采购信息	政务局	2021-08-02 18:14:50	查看 任务配置 查看实例 执行
采购信息数据交换	政府采购信息	政务局	2021-08-02 18:14:04	查看 任务配置 查看实例 执行
采购信息数据交换	政府采购信息	政务局	2021-08-02 18:13:10	查看 任务配置 查看实例 执行

共40项

20条/页 < 1 2 > 前往 1 页



# Thanks!



上海柚子工道物联技术有限公司  
上海市虹桥商务区申长路988弄万科中心T8-905  
(86) 021-54378925 | [www.uzigood.com](http://www.uzigood.com)

构建可信数字世界 