腾讯云 | DataFun.

区块链+隐私计算助力构建数据共享协作基础设施

刘江 腾讯云区块链隐私计算产品负责人

目录 CONTENT

腾讯云 | DataFun.

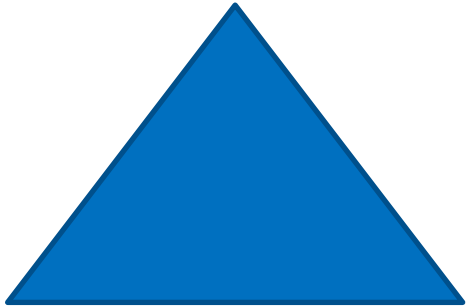
01

数据隐私安全背景介绍

数字经济时代企业发展面临的难题：数据共享、流通难

隐私保护与合规

隐私数据泄露和滥用



数据价值流失

数据拥有方担心数据价值流失，
数据使用方希望保障模型产权并
保障业务安全

数据提供方

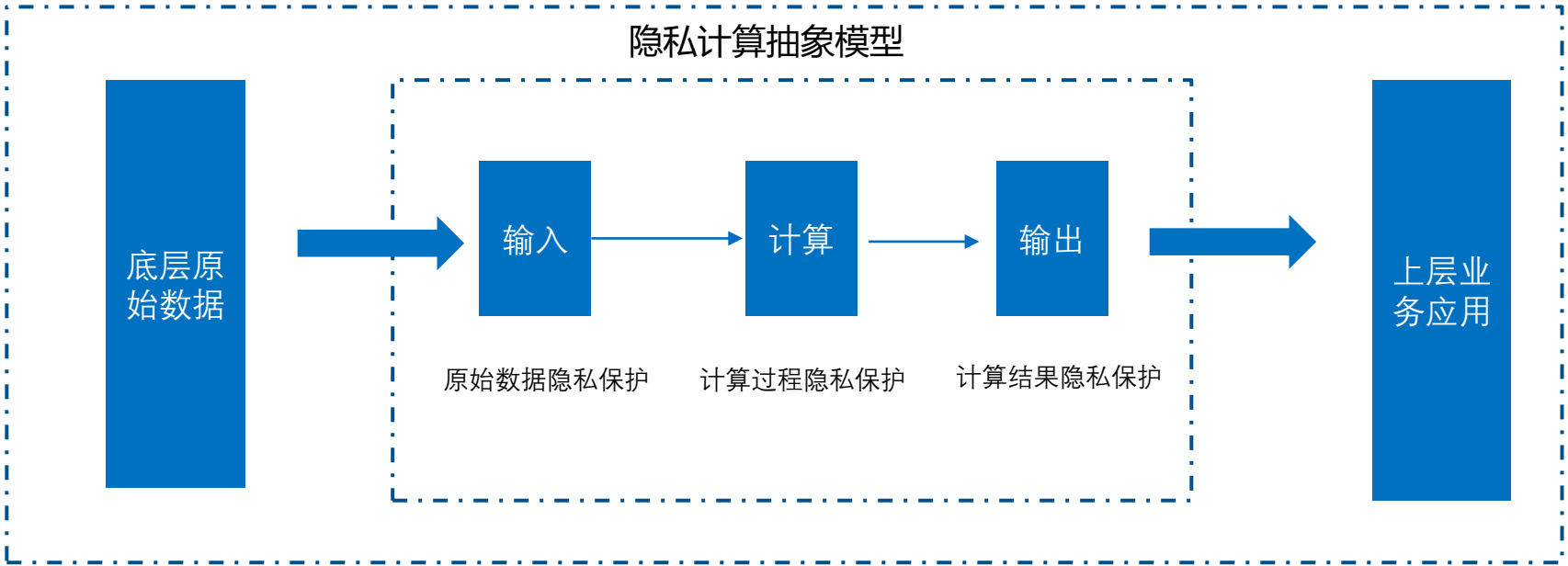
数据使用不便

数据合作基础设施不完善，标准
不统一，流程长，合作难度大，
周期长

数据使用方

隐私安全计算：当下数据隐私保护的最佳技术实现方式

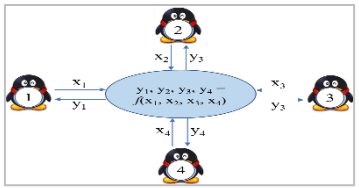
隐私安全计算是为应对数据安全流通挑战而量身定做的解决方案，其核心理念是“不共享数据，共享数据的价值。”



隐私安全计算技术路径:融合发展成为趋势

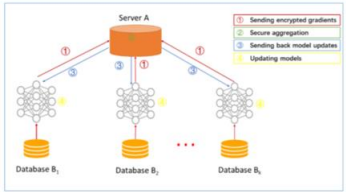
多方安全计算（Secure Multi-party Computation，MPC）

在无可信第三方的情况下，多个参与方协同计算一个约定函数，除计算结果以外，各参与方无法通过计算过程中的交互数据推断出其他参与方的原始数据



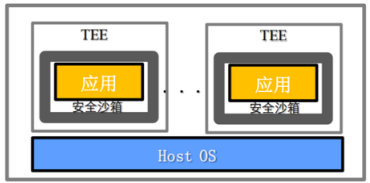
联邦学习（Federated Learning，FL）

由每一个拥有数据源的机构训练一个模型，而后将各自模型相关信息（模型的权重更新和梯度信息）采取加密的方式反复交互优化，最终通过模型聚合得到一个全局模型。已训练好的联邦学习模型不共享，分别置于各参与方，在实际使用时共同配合形成预测。



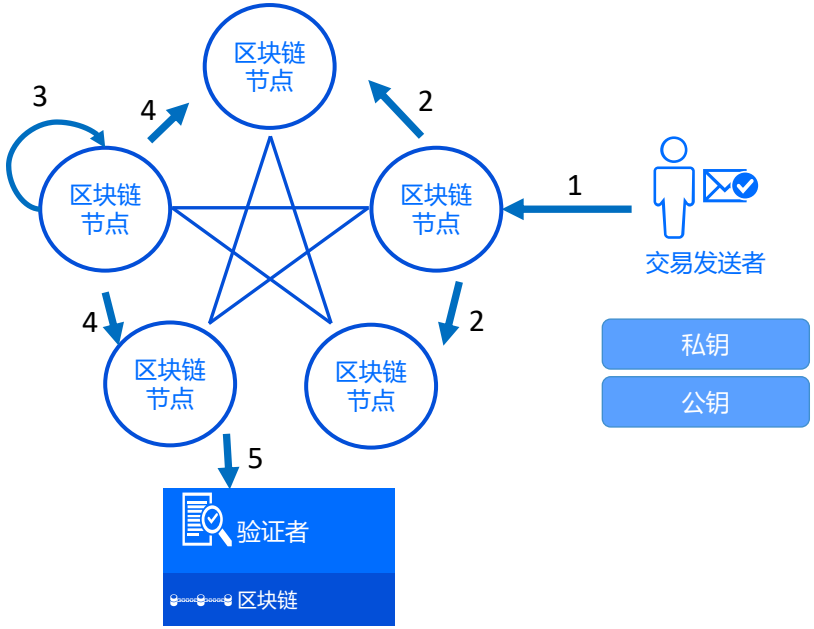
可信执行环境（Trusted Execution Environment，TEE）

通过软硬件方法在中央处理器中构建一个安全区域，保证其内部加载的程序和数据在机密性和完整性上得到保护



区块链核心逻辑：分布式、可追溯、多方共识

1. 交易的发起方通过应用程序（或者钱包）**构造交易**，并进行**签名**（数字签名），发送给其连接的节点。
2. 接收交易的节点通过P2P网络将交易发送给其感知的节点，以此类推，交易将会被发送到网络的**全部节点**。接收到交易的节点对节点进行验证，包括**签名是否有效。**
3. 区块链网络根据**共识算法**（DPOS、BFT），由一个节点**产生一个区块**，区块中包含这一时间段内的所有经过验证的交易。
4. 产生区块的节点将区块通过**P2P网络进行广播**，所有节点都会收到该区块。
5. 收到区块的节点，**独立验证区块和交易的有效性**，并通过共识算法确保块在全网的一致性。验证通过后，就会将区块**追加**到本地记录的区块链中。



去中心化，防篡改，可追溯，公开透明，数据可信

隐私计算融合区块链提升数据协作全流程保护能力

隐私计算

区块链

数据安全

计算安全

模型安全

服务安全

数据可信

模型可信

计算可信

服务可信

腾讯云 | DataFun.

02

隐私计算赋能数据要素流通

多方数据融合实现企业信用评估面临数据隐私安全问题

民政局A

USCI	score	year
959Q	22	2022
2638	21	2021
772C	20	2020

社保局B

USCI	score	num
959Q	50	100
2638	25	50
772C	35	70

税务局C

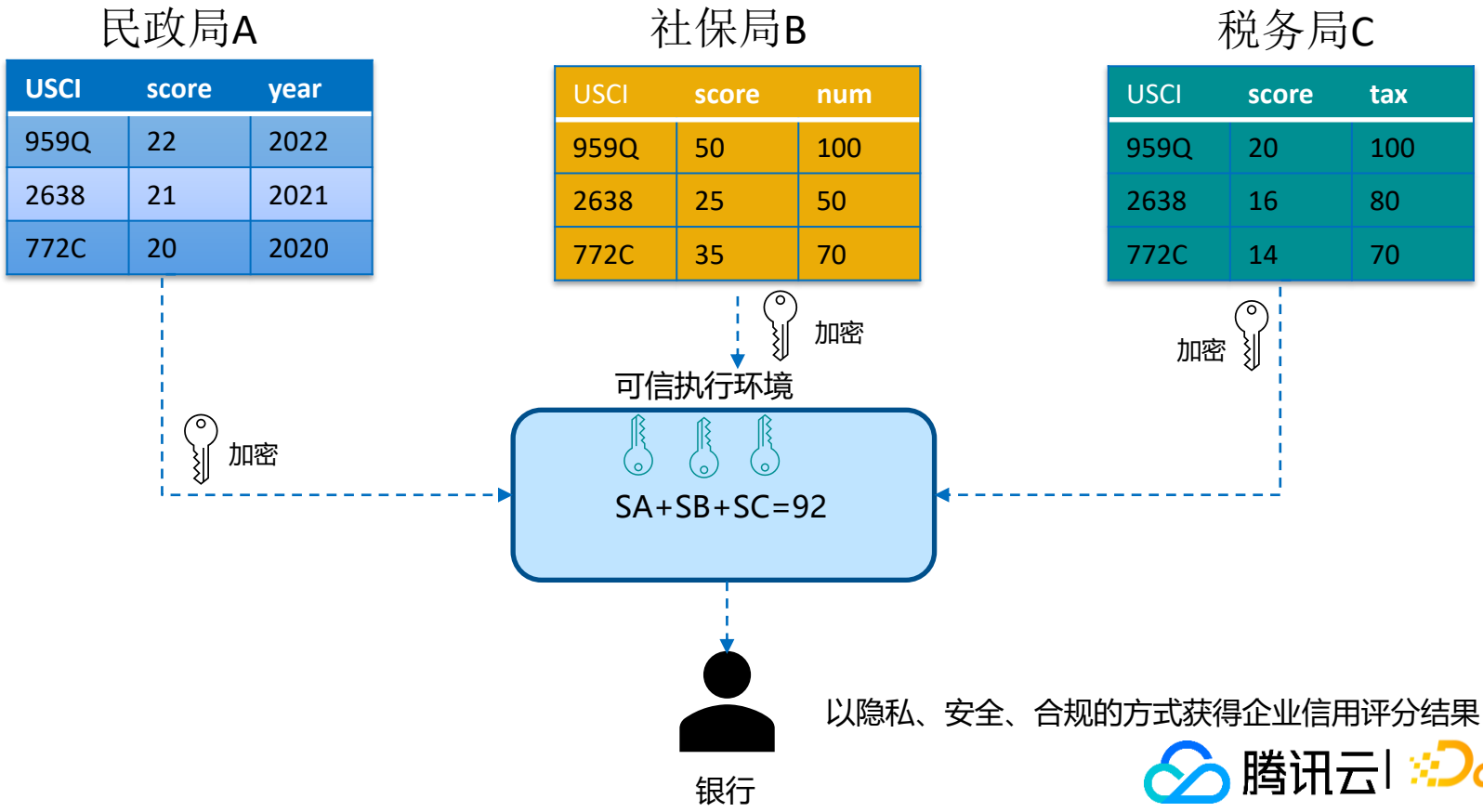
USCI	score	tax
959Q	20	100
2638	16	80
772C	14	70

银行

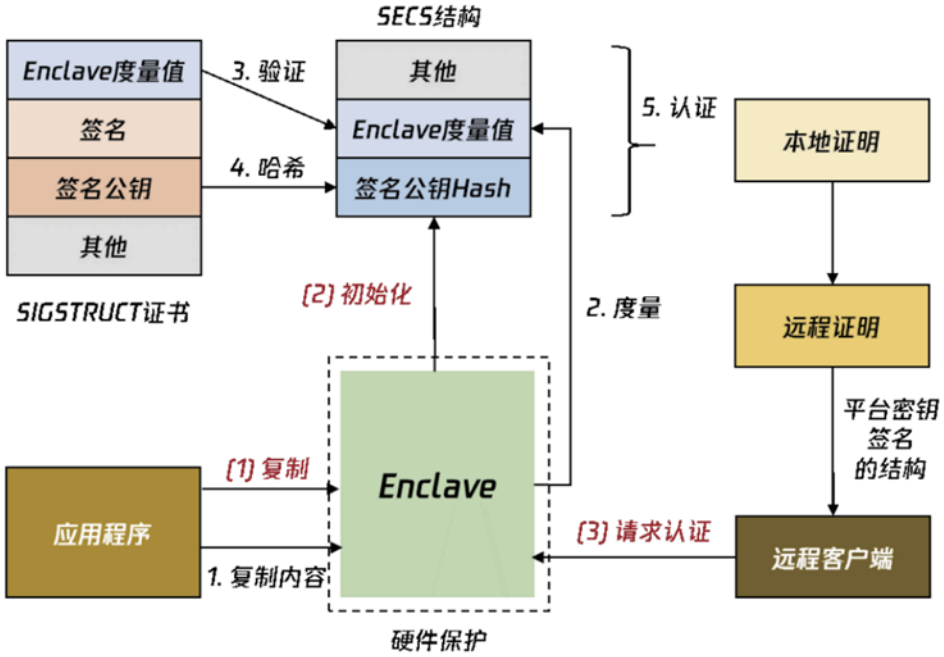
企业E信用评估=SA+SB+SC

如何实现对三个不同数据源的融合应用实现企业信用评估?

基于可信执行环境TEE的企业信用评估实现



TEE可信执行环境的核心能力

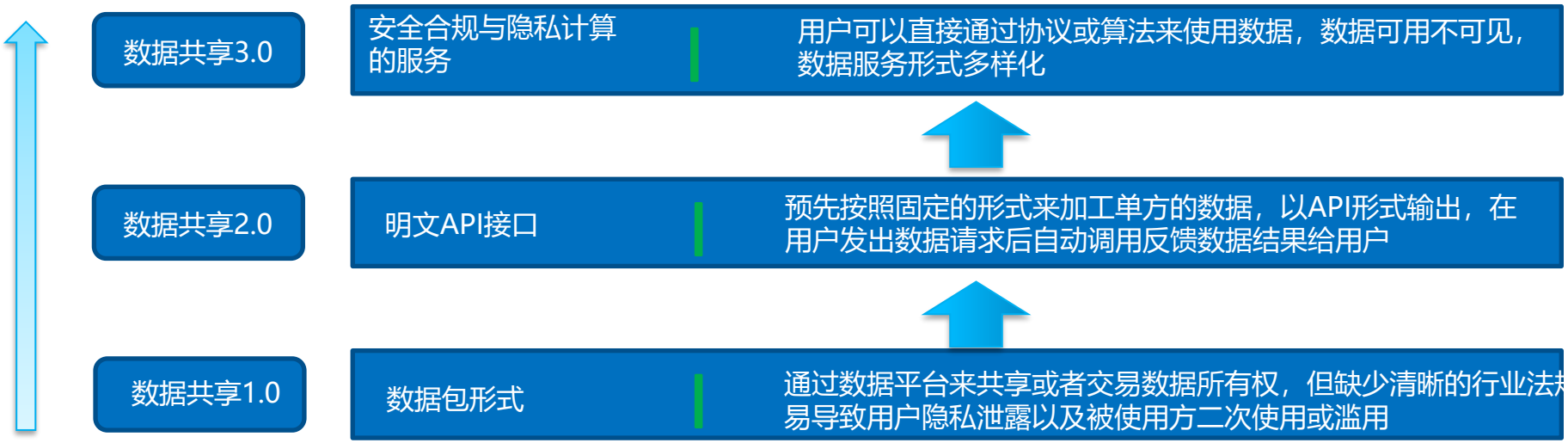


- 远程证明
- 可信信道
- 数据密封

可信执行环境TEE适用业务场景

- 计算逻辑相对复杂的计算场景
- 数据量大，数据传输和加解密的成本较高
- 性能要求较高，要求在较短时间内完成运算并返回结果
- 数据的传输与使用环境与互联网直接接触，需要防范来自外部的攻击
- 数据协作的各方不完全互信，存在参与各方恶意攻击的可能

可信执行环境TEE等技术让数据共享3.0成为现实



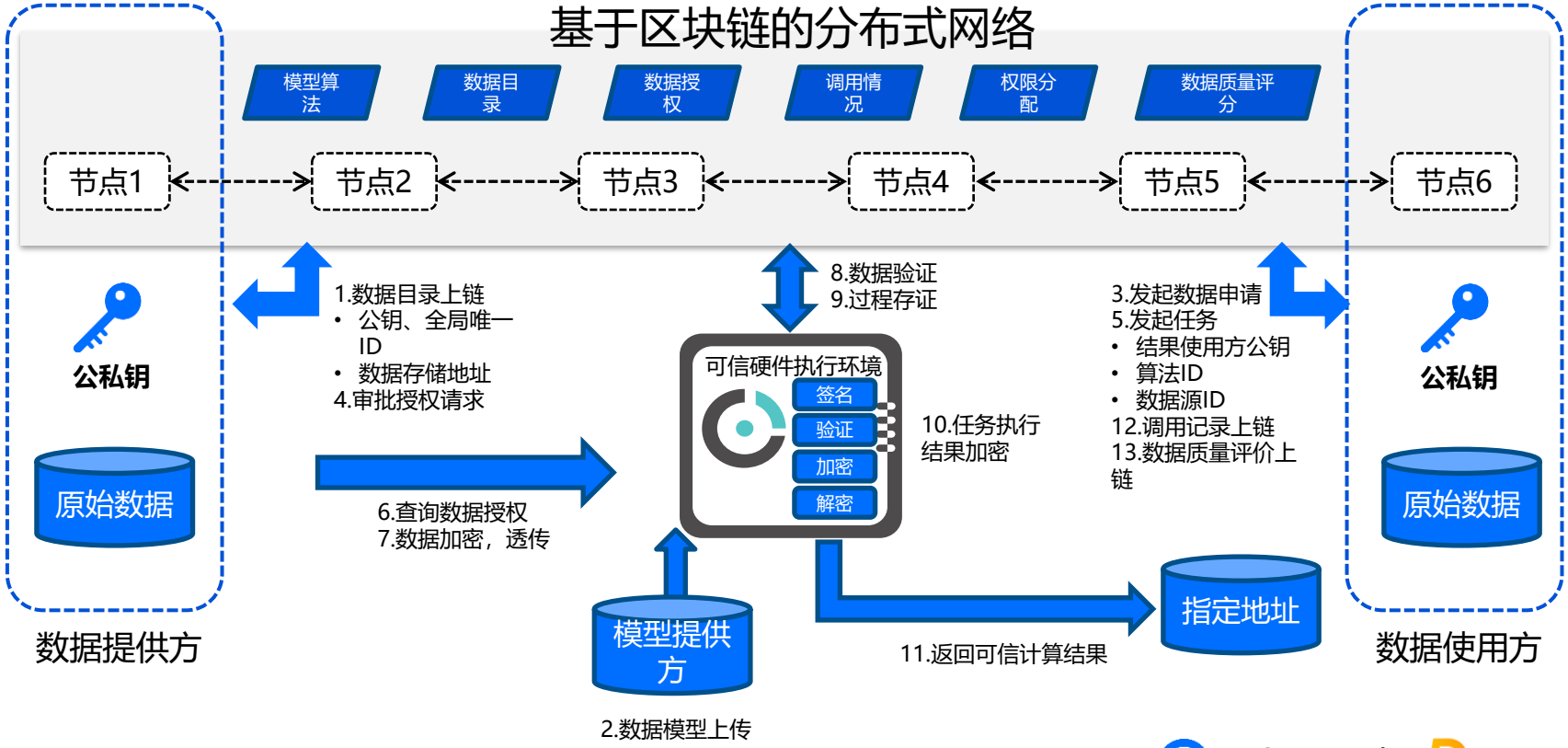
腾讯云 | DataFun.

03

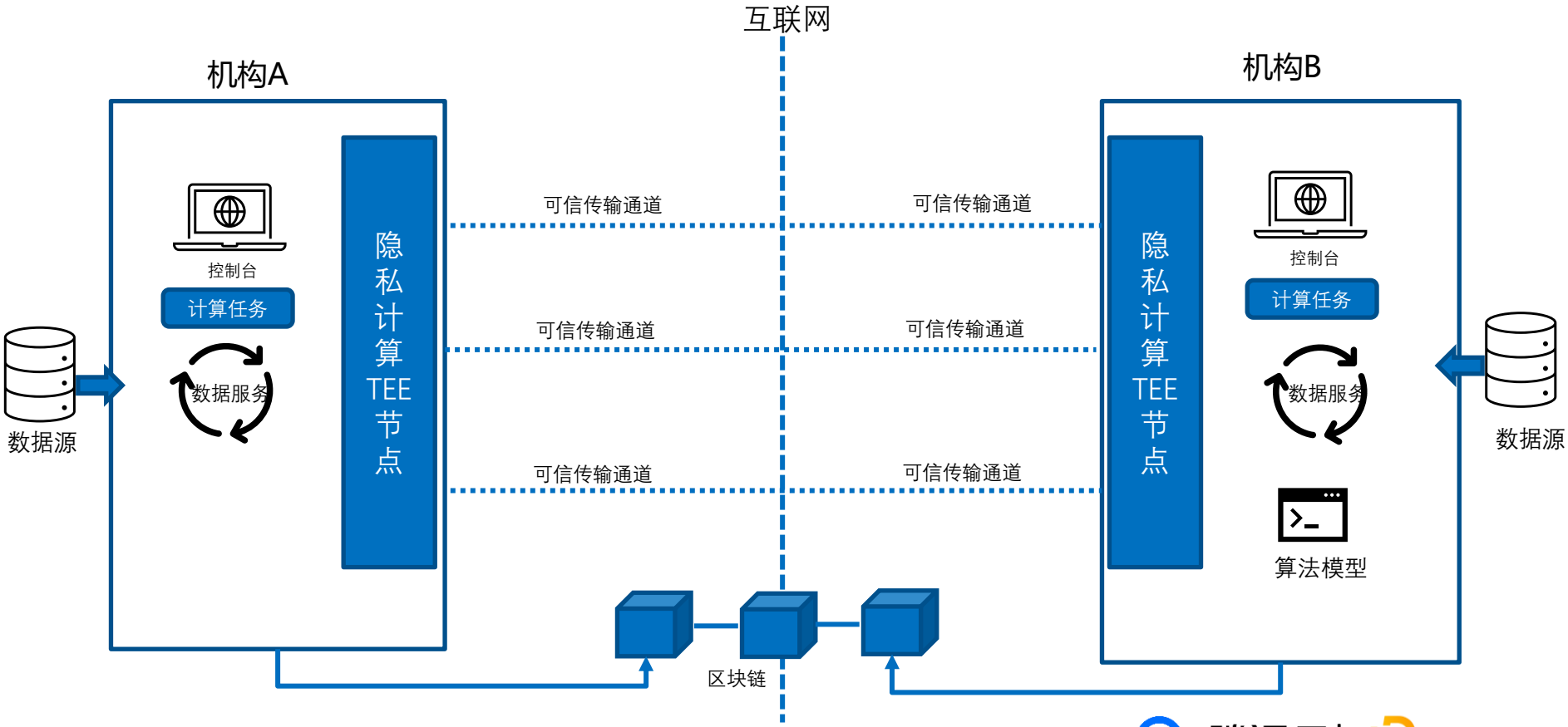
数据共享隐私计算平台打造

可信数据共享计算平台产品架构

可信数据共享计算平台实现数据可信协同共享



可信数据共享计算平台分布式数据交换网络部署实现



可信数据共享计算平台核心能力

数据目录	多场景任务	多级授权体系	多底层链支持	多种数据结构
• 支持组织-职责-数据三级目录体系 • 数据目录上链，不可篡改	• 支持普通任务自行，执行实时 • 针对大数据量的场景支持定时执行，按照制定时间点执行数据任务	• 数据使用前要针对数据进行申请授权 • 数据计算后数据所有方可以根据计算结果进行授权	• 通过配置后台配置不同的底层链 • 支持Fabric和长安链	• 结构化或半结构化 • 非结构化 • 接口类

可信数据共享计算平台的核心优势

安全可靠

原始数据不出域，数据输入、运算、结果输出全流程可信环境密态保护

性能优越

结合芯片级可信安全计算能力，能快速满足业务迭代变化能力，支持亿级海量数据计算

使用便捷

开发接入门槛低，支持主流数据源和数据服务，部署方便，使用简单

灵活扩展

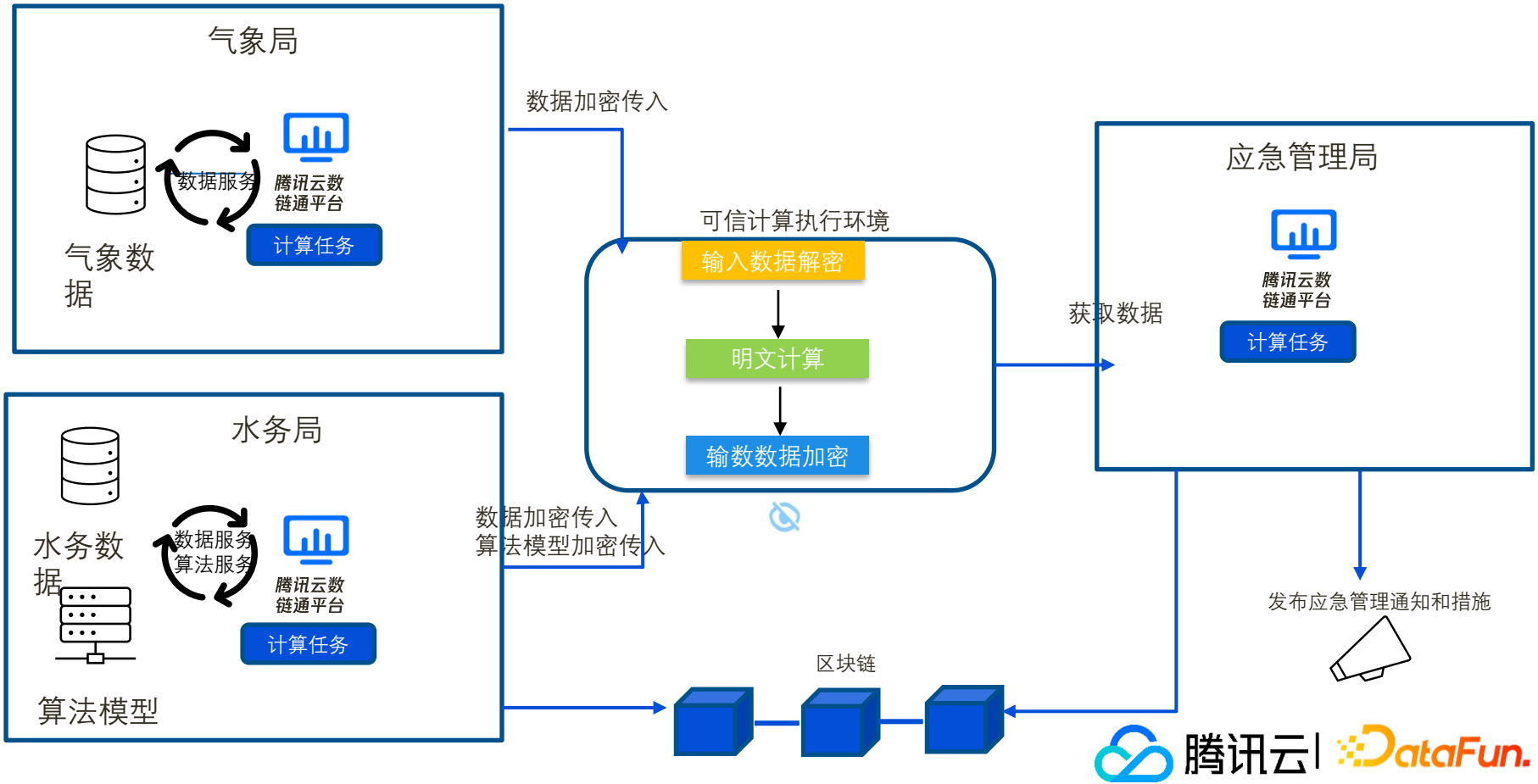
可根据不同业务提供模块化定制能力，分布式架构，可弹性灵活扩展

腾讯云 | DataFun.

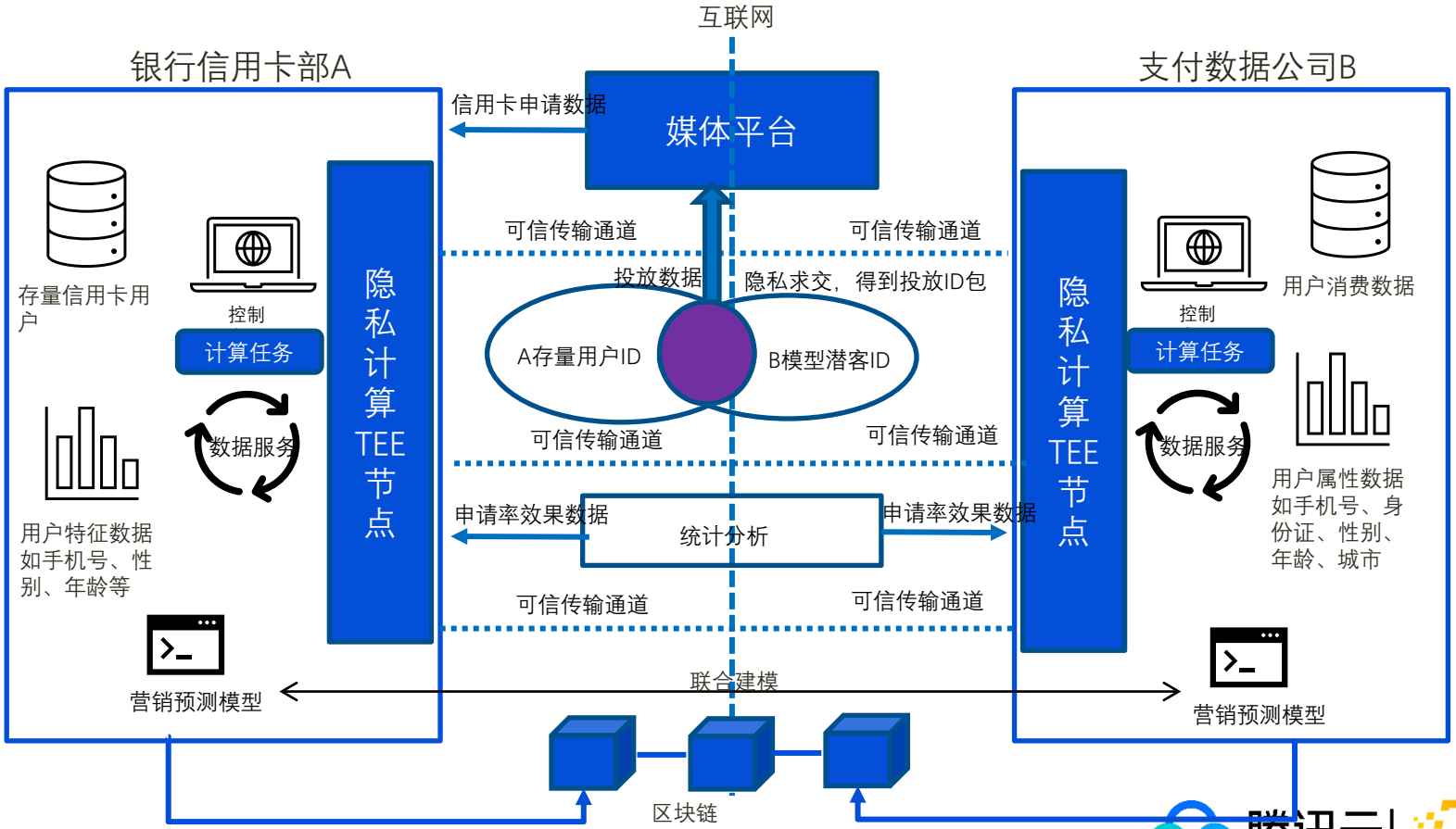
04

应用场景与实践

政数局政务数据可信共享协同内涝预测



金融机构基于多方数据实现精准营销场景



非常感谢您的观看

腾讯云 | DataFun.