密文计算下的数据可信流通与应用

演讲人：李朋林　　同态科技 CEO

01 数据可信流通现状

02 密文计算带来新机遇与挑战

03 应用实践与场景落地

一、数据可信流通现状

数据要素政策导向，法规配套逐步完善

- 《中共中央 国务院关于构建更加完善的**要素市场化配置**体制机制的意见》 2020/3/30
- 《中共中央 国务院关于构建**数据基础制度**更好发挥数据要素作用的意见》 2022/12/2
- 《中共中央办公厅 国务院办公厅 关于加快**公共数据资源开发利用**的意见》2024/10/9

强化已有数据共享平台的支撑作用，开展**数据加密、可信流通、安全治理**等关键技术研究和攻关，推进跨层级、跨地域、跨系统、跨部门、跨业务政务**数据共享**和**业务协同**。

结合实际采用**整体授权、分领域授权、依场景授权**等模式，授权符合条件的运营机构开展公共数据**资源开发、产品经营**和**技术服务**。推动数据利用方式向**共享汇聚和应用服务能力**并重的方向转变。

要建立数据产权制度
推进
公共数据
企业数据
个人数据
分类分级确权授权使用
建立
数据资源持有权
数据加工使用权
数据产品经营权等
分置的产权运行机制
健全数据要素权益保护制度

我国数据要素流通的主要模式

业务视图下的数据流通机制

一对一流通许可

+

一对多流通许可

+

多对多流通许可

基于各参与方之间的业务关系形成的数据流通机制，主要分为点对点模式、星状网络模式以及融合模式。

数据可信流通的现状与对策

- 市场标准不健全

➢ 不同渠道来源的数据开发利用与融合应用存在困难，**影响数据价值释放效果**；
➢ 在数据流通安全的严格规定下，应加速推进数据可信流通**技术标准和行业应用规范**的发展，有利于健康可持续的数据生态发展。

- 产业链多方协同

➢ 不同行业/企业之间的数据融合有助于发现新的商业机会和价值，但目前**基础设施不足、多方协同推进进展缓慢**，尚未形成良性循环。
➢ 推动建立多方参与的协作机制、开放高效的数据生态，更有利于提升数据服务、产品的质量与效益。

- 技术实施难题

➢ 传统安全策略难以将“**安全贯穿数据要素价值创造和实现全过程**”；
➢ 数据应用的个性化需求、数据安全的严格要求都使得密文计算在应用上存在**高门槛**，实施时的算法选择、性能优化、系统兼容性等存在**技术难点**；
➢ **以行业云平台为着力点**，提升“可控可计量”数据可信流通服务效能。

数据可信流通的主流技术路径

[实现数据“可用不可见”]

	性能	通用性	安全性	可信方	整体描述	技术成熟度
多方安全计算（MPC）	低~中	低	高	不需要	面向具体场景需定制化安全协议计算和通信开销大、安全性可证明	未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，开发与部署难度大，依赖信任硬件厂商支持	快速增长的技术创新阶段
联邦学习（FL）	中	低	低	均可	定制化模型开发、推理，综合运用MPC、DP、HE多种技术方法	快速增长的技术创新阶段
同态加密（HE）	高	高	高	不需要	计算开销适中，通信开销小，安全性高、可独立应用，也可用于联邦学习或MPC的结合	快速增长的技术创新阶段

- 密态计算开销
- 海量数据+多元化场景
- 系统处理可扩展性
- 技术应用规范

二、密文计算带来新机遇与挑战

开放环境下的数据流通与应用新挑战

授权链条覆盖全周期

数据处理的合法性

明确所有权与使用权

计算结果的归属

安全验收确保“不可逆”

结果合规性

个人信息安全影响评估

业务流程不变，对个人权益影响不变

技术方案的安全性

安全性可证明

降低数据敏感度

不针对个人特征

审计与监督

保留密文计算过程作为凭证

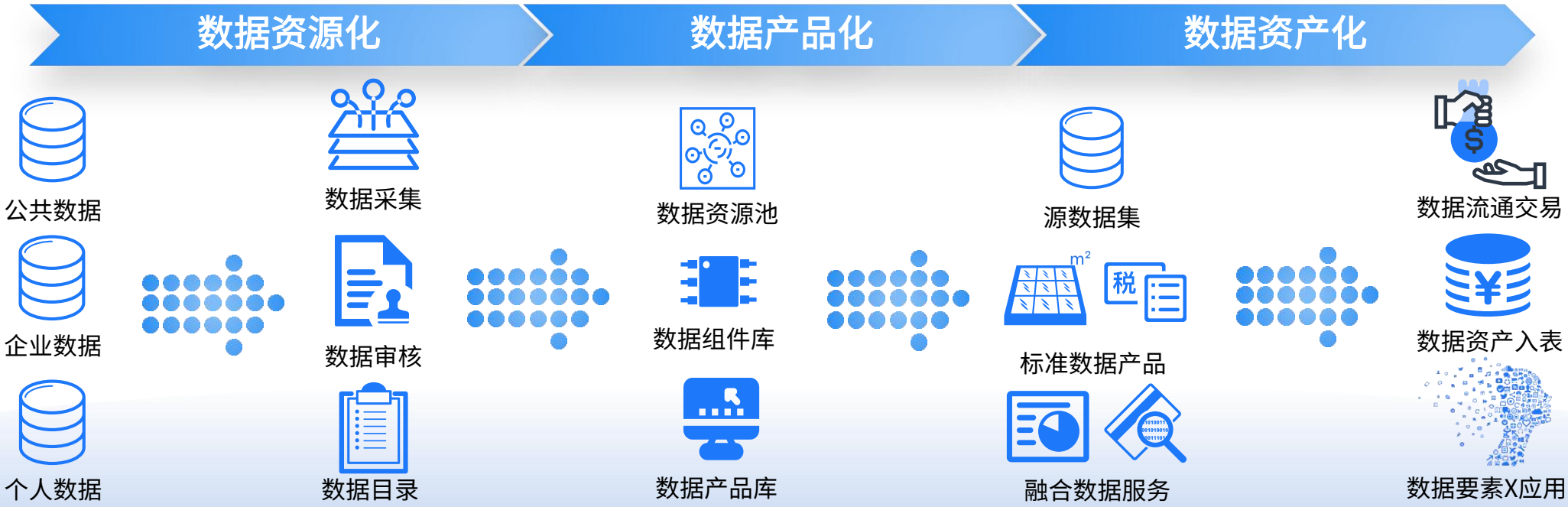
数据全生命周期安全过程域

数据采集安全	数据传输安全	数据存储安全	数据处理安全	数据共享安全	数据销毁安全
PA01 数据分级分类	PA05 数据传输加密	PA07 存储媒体安全	PA10 数据脱敏	PA14 数据导入导出安全	PA18 数据销毁处置
PA02 数据采集安全管理	PA06 网络可用性管理	PA08 逻辑存储安全	PA11 数据分析安全	PA15 数据共享安全	PA19介质销毁处置
PA03 数据源鉴别及记录		PA09 数据备份和恢复	PA12 数据正当使用	PA16 数据发布安全	
PA04 数据质量管理			PA13 数据处理环境安全	PA17 数据接口安全	

区块链 · 数字水印 · 同态加密 → 传输加密 → 数据签名 · 透明加密 → 区块链 · 密文计算 → 联合建模 · 密文应用 → 授权销毁

多元化数据产品，多样化应用场景

释放数据流通价值，推动高水平应用



数据封装节点

数据权限管理

同态构型加密

密钥管理

SM 2/3/4

商用密码加密

明密文计算

数据组件/产品设计

资源/资产管理

模型计算

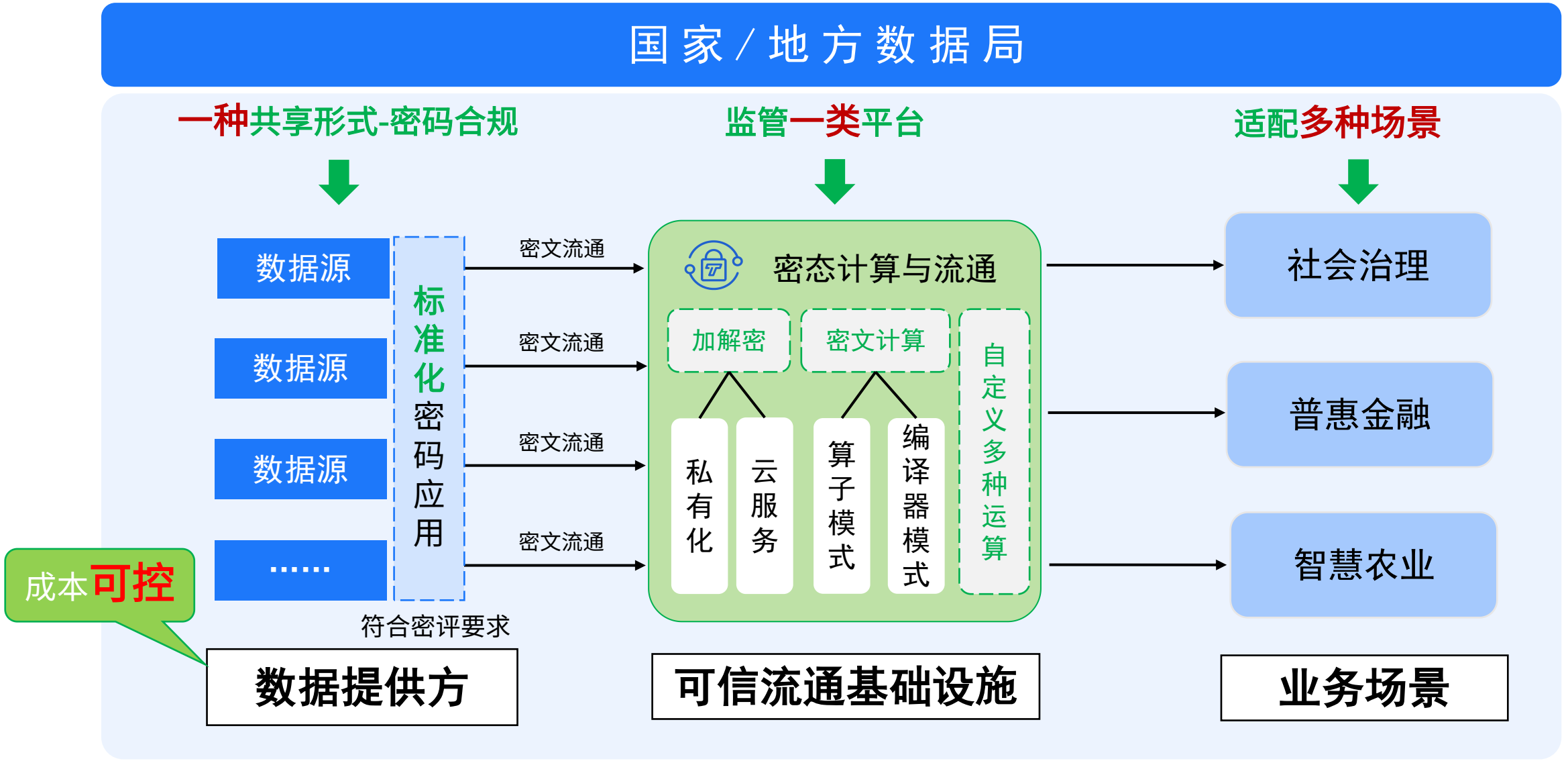
数据组件/产品加工

登记/入表管理

数据工坊业务处理平台

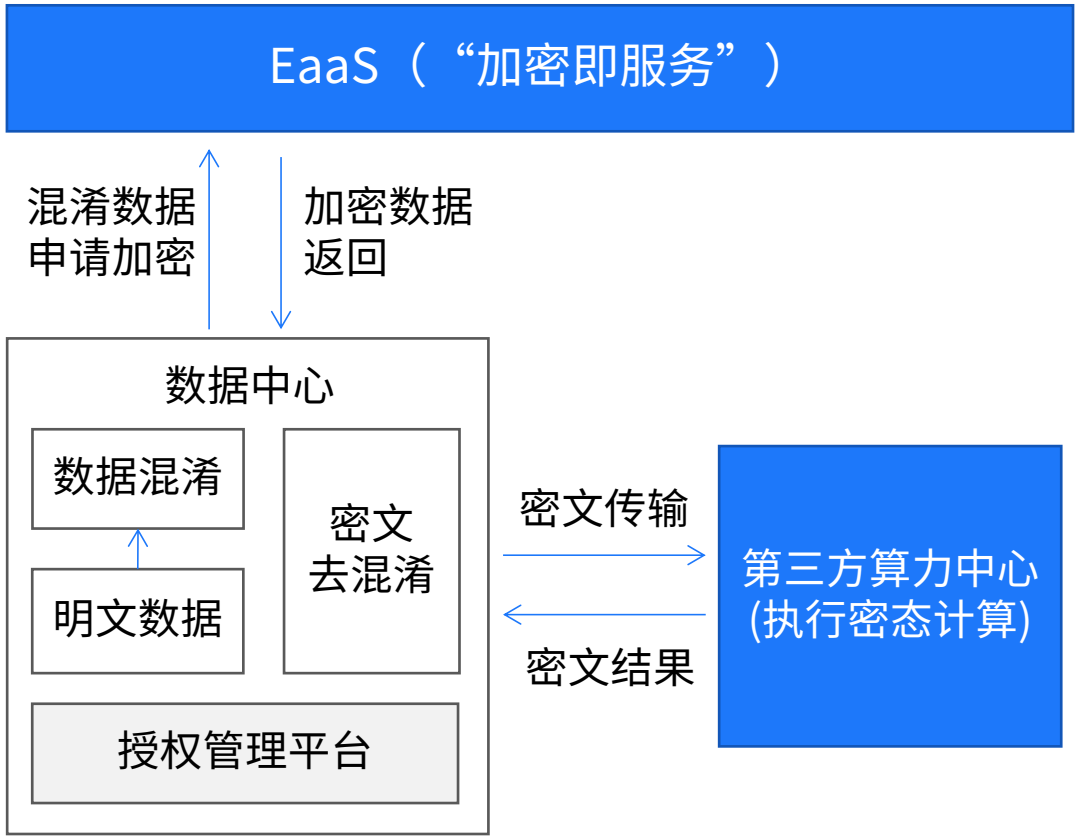
数 据 可 信 流 通 域

基于密文计算构建的数据可信流通体系



开放式数据可信流通服务——EaaS

- 充分利用同态加密特有的数学性质，提供了开放式加解密及密文计算服务。
- 用户能够对密钥进行安全可靠的管理，也能使用多种加密算法对业务数据进行可靠的加解密运算。




团 体 标 准
云计算中同态加密技术应用要求

1、牵头国内首个云计算中同态加密应用标准

积极参与并牵头制定云计算技术与密态计算结合的相关标准，并推动工业制造、能源等领域的试点项目落地。

2、促进高效率、低成本的产业链信息共享

采用云端+链式密文计算，确保数据流通可管可计量，提升产业链共享意愿，减轻企业硬件配置与维护等重复成本，保障各方利益。

3、降低企业研发、运维压力

EaaS提供多种对接形式（API、SDK），满足传统研发人员轻松开发、快速对接的需求，降低业务改造成本和开发人员学习成本。

4、具备高性能、高可靠、高并发优势

作为全托管式的服务，实现多个企业在不同地域、不同需求、不同资源下，支持资源的横向扩展，满足客户对底层设施的扩容/缩容要求，加快形成规模经济。

以技术革新创新密码服务新模式

1. 自主研发能力提升，技术性能不断优化

自主可控的底层能力支撑，数据场景与流通模式创新，更好地满足实际应用需求。

2. 生态逐步完善，催生新产业新业态新模式

完善规范建设，推动不同产业间的协同耦合，充分发挥数据的渗透性、覆盖性、创新性。

3. 应用场景不断拓展

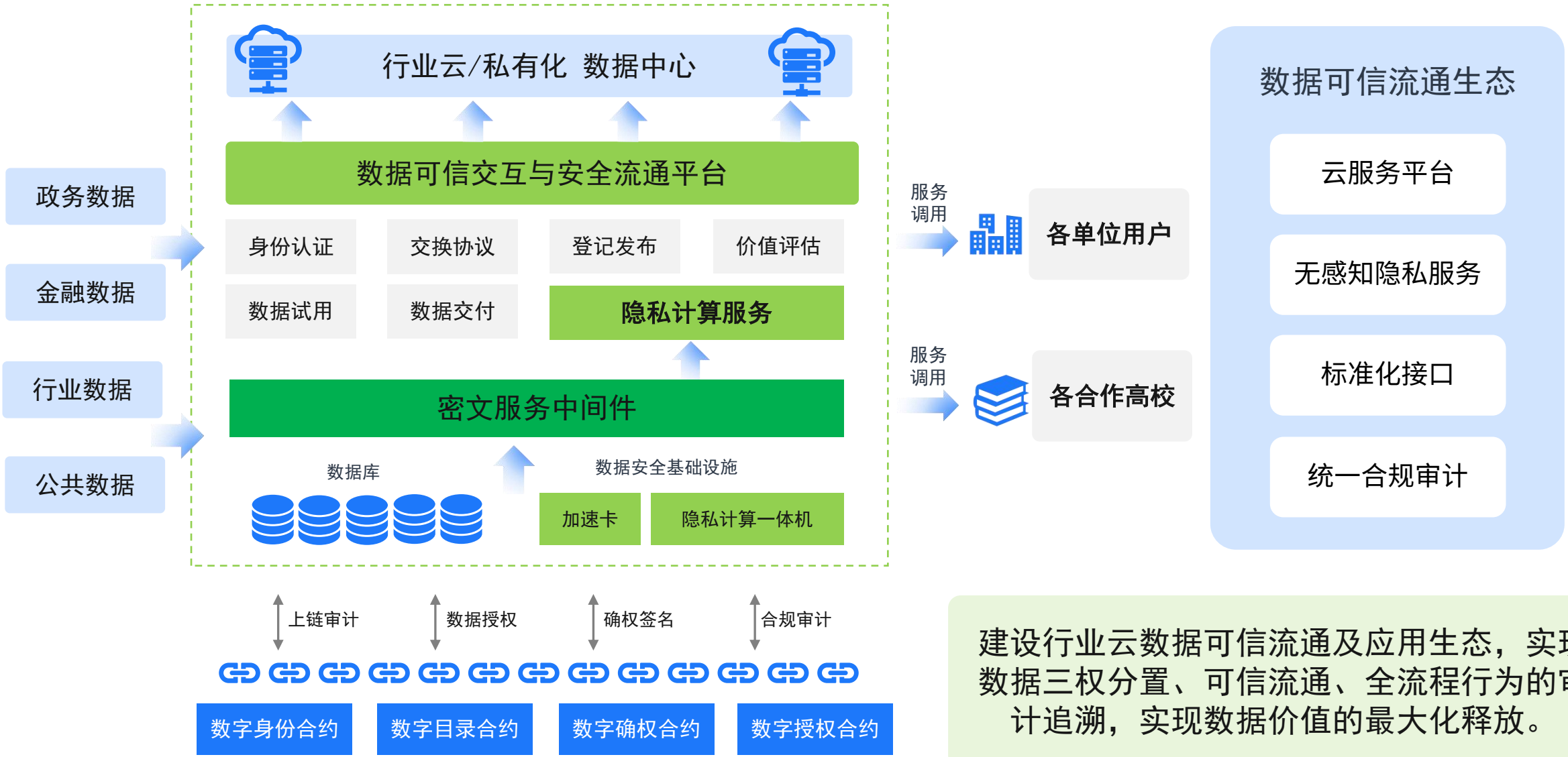
在政务、金融、工业等多个领域得到了广泛应用，并取得了良好的效果。

EaaS

- Web3.0 → NFT、数据资产、DeFi
- 区块链 → 无人药房、智慧城市、产品溯源
- 云计算 → 在线会议、金融云、教育云等
- 边缘计算 → 穿戴式医疗设备、智能工厂等
- 大模型 → 智能客服、智能问诊等
- 物联网 → 自动化物流、智能家居等

三、应用实践与场景落地

行业云数据可信流通应用



建设行业云数据可信流通及应用生态，实现数据三权分置、可信流通、全流程行为的审计追溯，实现数据价值的最大化释放。

能源数据云上外包计算

项目痛点

（1）电力数据具备**体量大、增长快、实时性强、价值密度高**等特点，对数据开放共享安全保障的**技术能力要求高。**

（2）在云与新型电力系统融合的发展趋势下，电网企业亟需具备能有效支撑新模式下的电力大数据安全运算的能力，打造标杆项目。

技术路径

（1）“匿名化”身份认证，为应用系统构建可靠的**信任基础**；

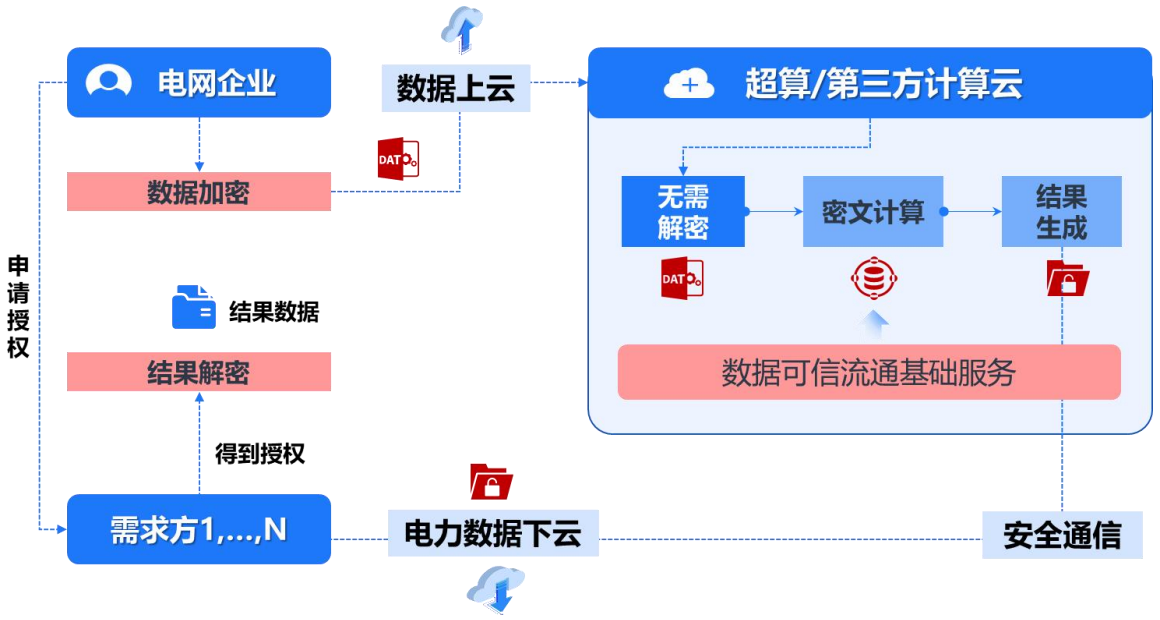
（2）利用**可计算的加密数据特性**，解决数据在超算平台计算环境、第三方平台计算环境以及数据在应用全过程中的隐私保护问题；

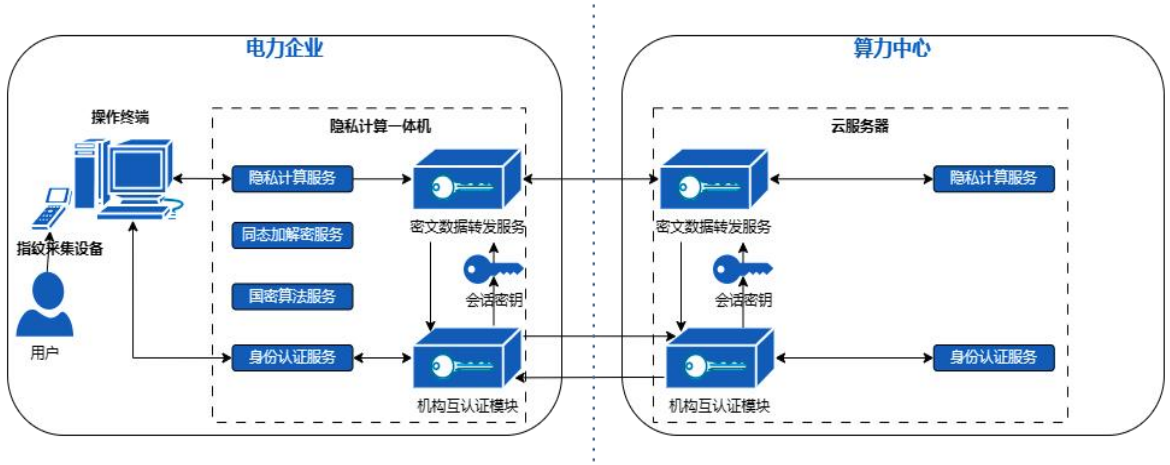
价值收益

1）在整个电力数据多源协同共享过程中，电力数据全流程保持“可用不可见”的高效流通、云上安全计算、数据增值服务；

2）形成网状的安全协同共享模式，基于前沿安全技术避免新型安全威胁，综合安全成本降低30%以上。

3）应用于深圳市电费计价服务，目前正在上海、新疆等地电网推广。





拓展行业级云平台的用户体验

安全保障

EaaS的安全体系设计包含了网络安全、身份认证、数据使用策略、可存证运行环境、远程认证、应用层虚拟化等方面。组合应用后能够实现不同场景下对应安全级别的执行环境要求。

弹性边界

EaaS提供私有化和行业云部署两种模式。私有化服务可以提供保障数据主权的计算和交换边界点；行业云结合EaaS能够实现跨域数据融合的产品级输出，并分别维持原有数据供给协议要求的正常执行。

隐私保护

EaaS提供开放接口允许集成多种业务系统，通过统一的经典与新型商用密码的组合开发，在密文状态下整合处理高度敏感和异构数据，输出分析结果或可视化效果，帮助形成领域知识。

流通服务

EaaS保障了数据主权、实现了数据的合规流转，将治理好的多源融合数据资产进一步转化为可参与生态流通的数据产品，并可通过行业云平台的数据市场、或互联网公开门户同时进行供需对接信息的发布。

部署和初始化 | 数据产品的定制化开发 | 实现场景智能化 | 实现数据产业生态化

THANK YOU!