

宇链科技

基于区块链的 隐私计算探索与实践



宇链科技
滕海明
2021/05/28

目录 CONTENTS

01 背景

02

隐私计算相关技术

03

探索与实践

04

展望

01. 隐私计算-政策背景

- 美国



2019年12月发布《联邦数据战略与2020年行动计划》，将数据作为战略资源开发

- 欧盟



先后出台《迈向繁荣的数据驱动型经济》、《建立欧洲数字经济》;2020年2月发布《欧盟数据战略》

- 英国



2020年9月发布《国家数据战略》，提出释放数据的价值是推动数字部门和国家经济增长的关键

- 中国



2020年4月19日，十九届四中全会《关于构建更加完善的要素市场化配置体制机制的意见》

数字经济的核心生产要素是数据



01. 隐私计算--数据安全背景

数据采集

- ① 数据采集要符合相关法律法规和监管要求
- ② 明确数据采集的目的/用途/方式/范围/采集源/采集渠道
- ③ 只采集经过授权的数据并进行日志记录

数据销毁

存储介质销毁(不可逆销毁)

数据使用

- ① 数据交换/共享
- ② 数据导入导出
- ③ 监控审计

数据
共享

实体交换

价值交换

数据传输

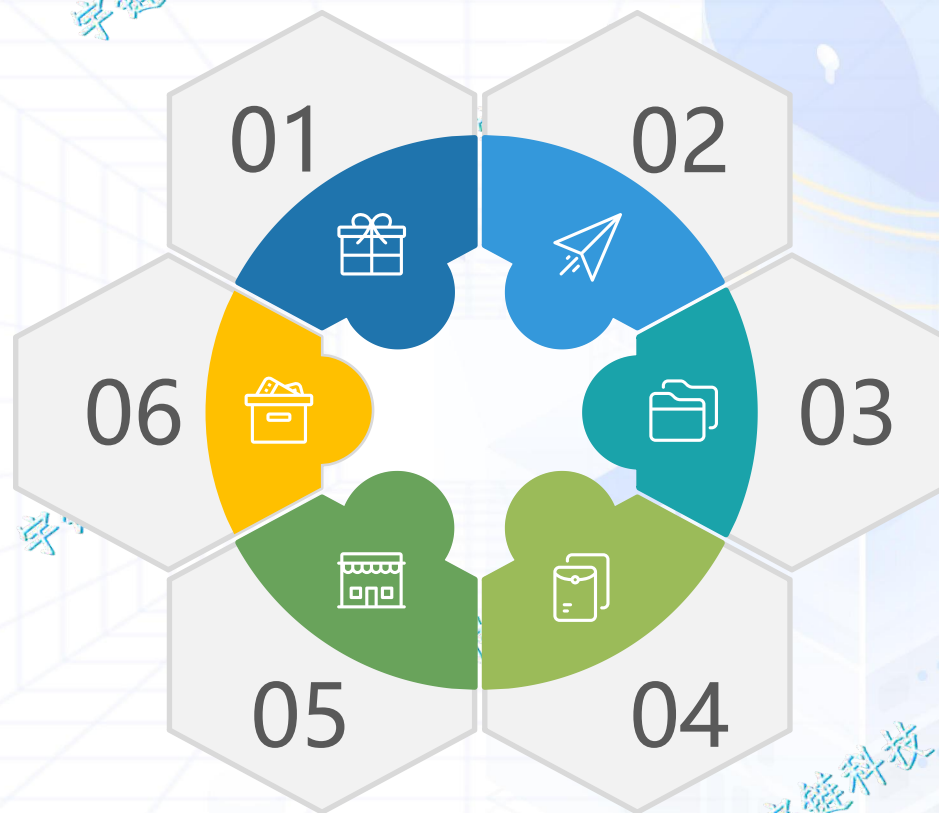
传输通道加密,TLS1.3/国密相关的算法

数据存储

- ① 行业监管要求一些数据落盘加密
- ② 容灾备份

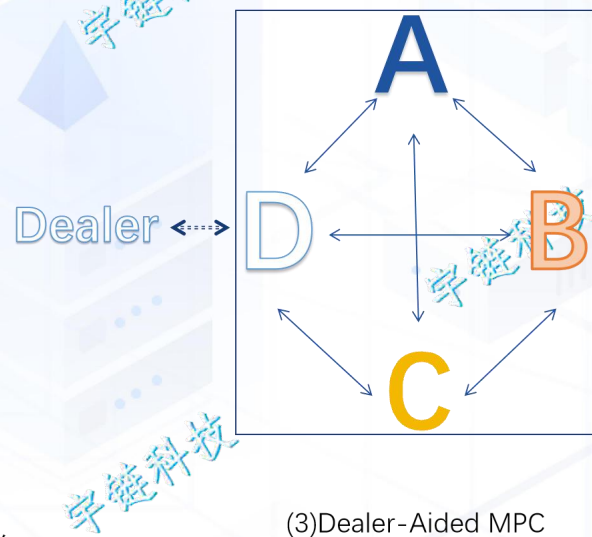
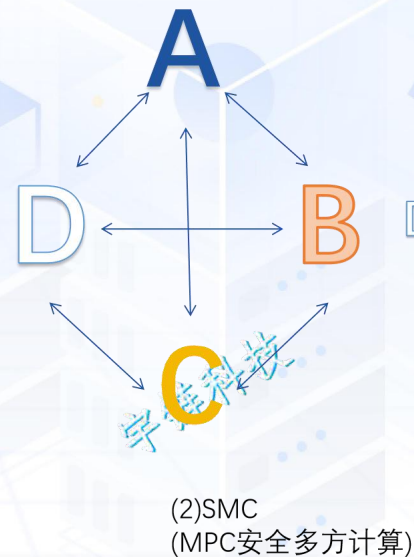
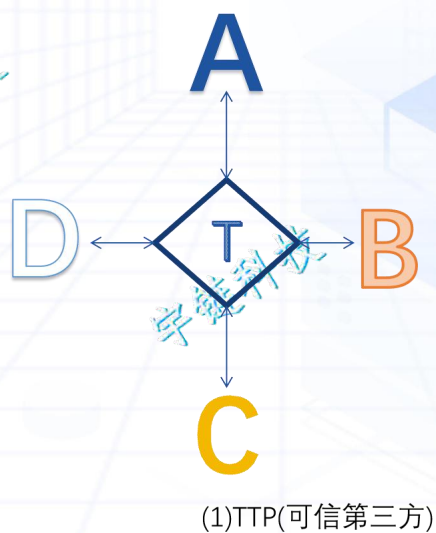
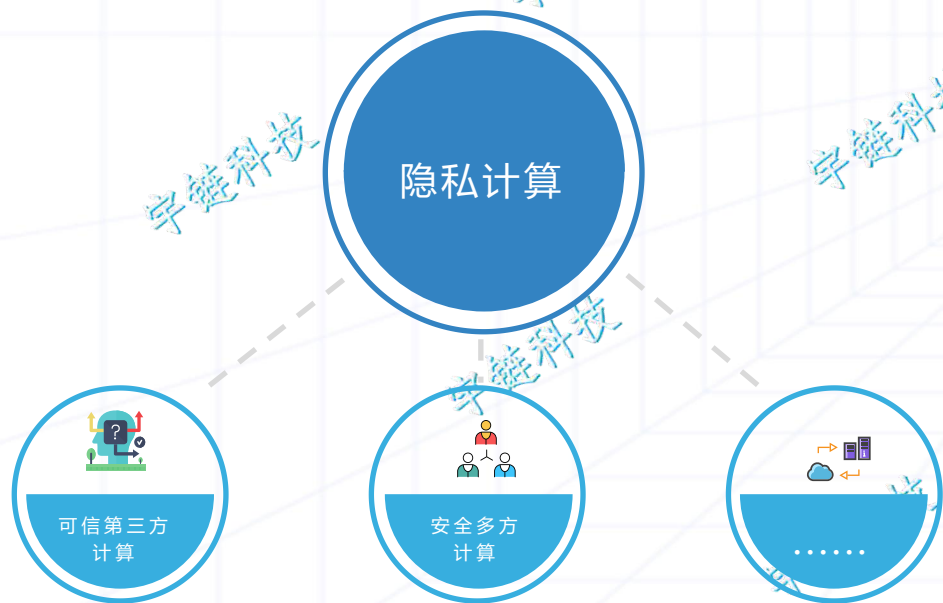
数据处理

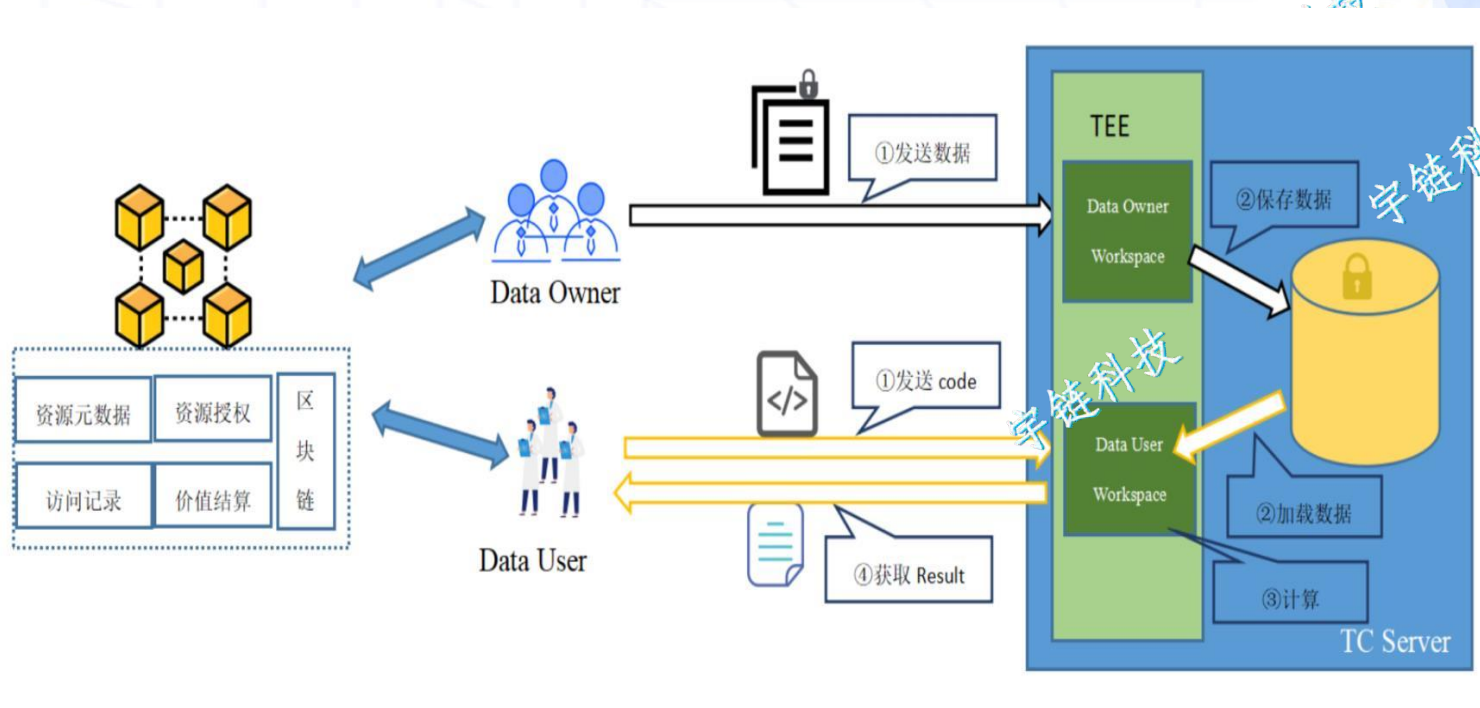
针对业务场景进行脱敏处理



隐私计算:在提供**隐私保护**的前提下,实现数据**价值挖掘**的技术体系。

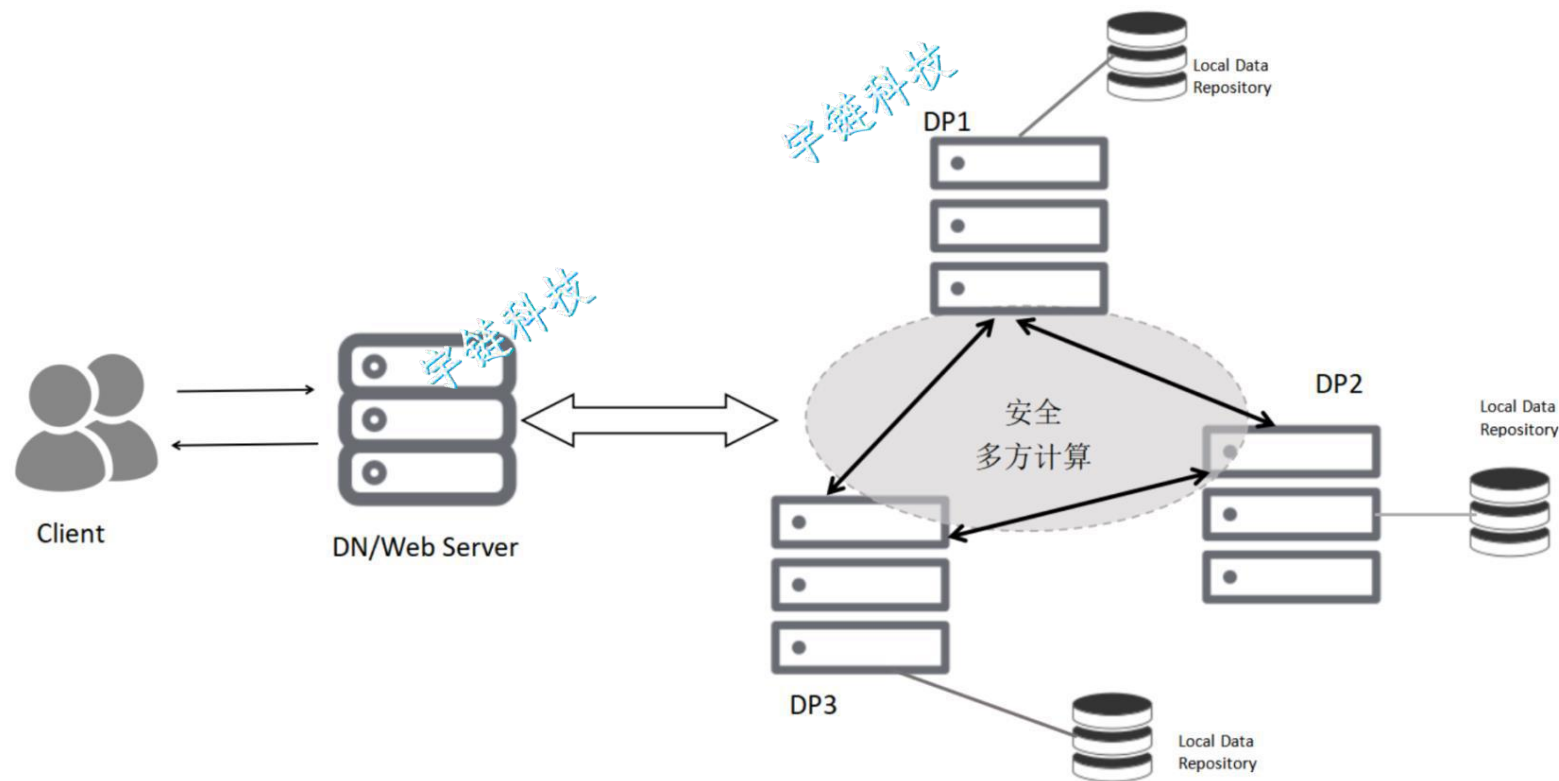
- 隐私计算并不是一种单一的技术包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体现。
- 隐私计算能够保证满足数据隐私安全的基础上,实现**数据价值**和**知识的流动与共享**,真正做到数据**可用不可见**





- 身份/权限校验(CA证书/PKI/智能合约权限管控)
- 数据元信息上链, 隐私数据加密落盘存储(确权)
- 数据传输过程通过硬件保证过程可信(身份)、可靠(TLS/DH/链上哈希校验), 数据全流程加密。
- 数据分析过程, 模型审核/远程证明RA/可信执行环境TEE, 确保“数据可用不可见”

02. 隐私计算相关技术-SMPC



- 运用领先的技术手段，保障巡检的真实有效
- 实现可信的实时监管能力，降低管理成本,提升管理效率
- 保障数据不可篡改、可追溯、可审计，形成可信大数据
- 协同具有公信力的机构，证明巡检过程的有效性
- 可信消防巡检大数据，带来无限价值

运用

- 区块链芯片
- 区块链分布式账本
- 区块链密码学技术
- 多方安全计算
- 智能安全合约
- 区块链浏览器

03. 探索与实践——可信大师（四位一体）

人

通过人脸识别技术，对巡检人的身份进行确认，保障了巡检人员的真实性。巡检任务部署、排班管理、人员管理模块的运用，使得管理方、监管部门可以第一时间掌握巡检的情况。

时间

通过区块链技术的赋能，所有巡检数据都会在区块链上存证，并附有时间戳，且无法被篡改（包括技术提供方），保障了时间的真实性，杜绝了时间造假、事后补录的漏洞。

地点

在巡检点位安装“区块链可信巡检盒”，巡检开始、巡检结束，都需通过巡检盒打卡，实现了只有达到巡检盒所在的地点才能打卡作业，杜绝了远程巡检作假的可能。

全过程

运用全球领先区块链的技术，将巡查人、时间、地点、过程存证在区块链上，形成完整的全过程链条，可回溯、可审计；一旦发生事件和纠纷，可迅速界定责任，追溯事故发生的原因。

- 四位一体巡检全流程监管体系
- 巡检全过程区块链实时存证
- 人/时间/地点/内容均不可篡改
- 数据全链路无损回溯
- 巡检大数据实时分析、实时告警

消防巡检

消防柜、仓储、消防疏散通道

安全生产巡查

油气管网、危化企业、危化运输船舶

特种行业巡检

特殊经营场所、易制毒易制爆企业

食品安全巡检

餐厅后厨、连锁餐饮、学校食堂

文物古建筑巡检

灵隐寺、古建筑景区

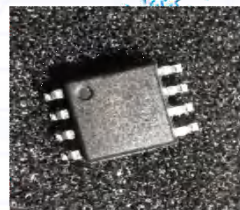
智慧社区/园区巡检

配电房、水务房、电瓶车充电站

区块链可信巡检盒

Blockchain inspection box

运用

内置
区块链芯片

如何使用?

1. 区块链巡检盒安装在巡检点位固定(如消防柜、强电箱等)
2. 打开可信巡检小程序,验证人脸以确定巡检人身份
3. 通过小程序查看巡检任务,确认巡检路线、时间、地点等
4. 到达巡检点位,与巡检盒通信,确认巡检标准与流程,开始作业,并记录巡检结果、照片、视频、定位等,巡检结束后,在与巡检盒近场通讯后,完成该点位巡检。

巡检盒有哪些创新技术?

1. 区块链巡检盒内置宇链自主研发的区块链芯片,内置特殊指令集和硬件级别的加密算法,实现区块链不可篡改的算法,确保芯片不被破解。
2. 宇链区块链芯片拥有独一无二的“指纹”,对应区块链上全球唯一的“身份ID”,从而实现了不同巡检盒无法相互掉包、替换,保障了设施设备的唯一性,保障了巡检的有效性。

地下室没信号怎么办?

1. 在有网络信号的地方打开可信巡检小程序,在无信号的地方巡检时,支持离线填单和提交功能,到有信号的地方,系统会自动上传,保障巡检过程有效性。

03. 探索与实践--可信大师整体框架



市市场监督管理局餐饮食品安全门店重点部位检查系统大屏

区块链数据统计

出块节点	区块链硬件总计	总处理量
126	64	1141
同步节点	每秒处理容量	TOSS存储量
1152	23678	99.77 GB

近期事务处理历史



最新链上事务处理

区块...	交易哈希	来源	创建时间	确认
3055	0d1e68f...	rec...	2021-02-02 07:5...	已上链
2986	f3ff1a44...	rec...	2021-02-01 22:2...	已上链
2964	b207b8...	rec...	2021-02-01 09:0...	已上链
2890	27fe1cf...	rec...	2021-01-31 20:2...	已上链

最新区块

区块...	区块哈希	来源	创建时间	已确认
3055	9ceb37...	rec...	2021-02-02 07:5...	已上链
2986	a72ab2...	rec...	2021-02-01 22:2...	已上链
2964	d5fd5e...	rec...	2021-02-01 09:0...	已上链
2890	aaeca02...	rec...	2021-01-31 20:2...	已上链

覆盖点位

64

巡检总计

141

巡检人员

209



点位14日巡检次数统计



点位数据统计

点位总数: 64



每日巡检详情

区域	已安装数量	已巡检	未巡检
温县	5	2	3
武陟县	5	2	3
修武县	5	2	3
博爱县	5	1	4
沁阳市	5	2	3

最新巡检记录

记录	县(市)区	巡检场景	主要负责人	手机号码	巡检状态	巡检时间
●	山阳区	蜜雪冰城丹尼斯店	王月琳	13*****719	一切正常	2021-02-02 18:2...

03. 探索与实践——医疗区块链



一、建立联盟链与准入机制

- 建立医疗区块链，在浙江省某专科医院、全国各专科分院、国家相关部门等，建立区块链节点。区块链以联盟链的方式部署，并建立准入机制，建立权限与数据逻辑控制体系，引入国家监管部门作为区块链节点，最大程度保证联盟链数据的可信。

二、提供可信的数据共享交换

- 医院内部的信息化系统、医疗系统、医疗研究数据、医疗设备获取的医疗数据等通过本地的区块链节点上链存证，并提供数据整合、数据处理、数据交换、数据共享等功能，形成联盟链内的数据可信共享交换能力。

三、提供灵活的数据控制

- 各区块链节点可设计灵活的数据管理权限和分享策略机制。多点控制数据或个人拥有数据的主权时，超细粒度的权限控制和管理机制，可面对不同专科医疗应用场景进行灵活变换。

03. 探索与实践--医疗区块链(框架图)



医疗上层应用

与原有应用融合开发

专科医疗大数据可视化

病情数据分析应用

分院数据管理

数据共享管理

机构考核管理

积分贡献机制管理

更多应用定制

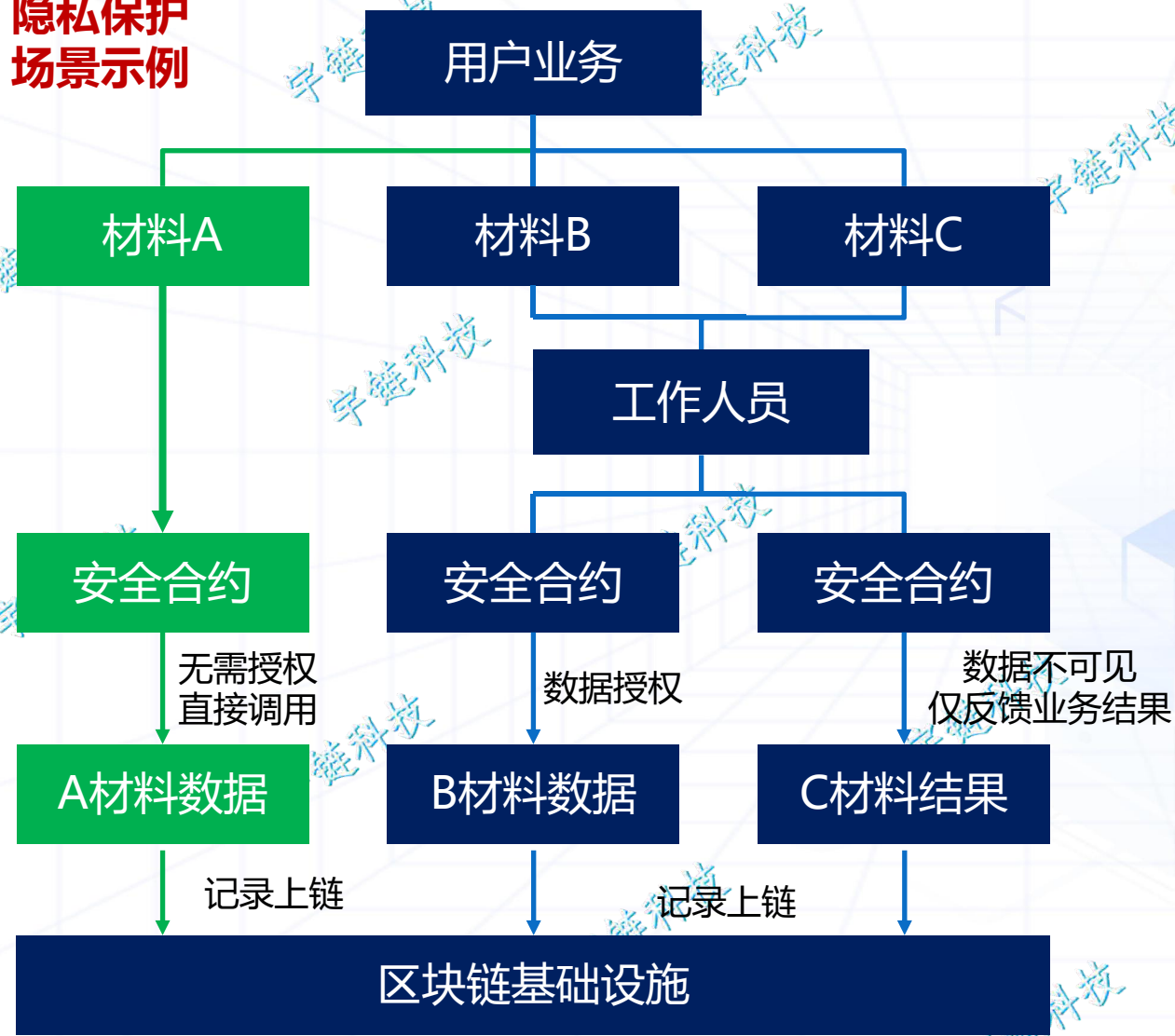
共享一二级数据，三级数据原则上不共享;二级数据最小化授权

分类(企业管理域划分)

- 研发数据域(研发设计数据/开发测试数据)
- 生产数据域(控制信息/工艺参数)
- 运维数据域(物流数据/产品售后服务数据)
- 管理数据域(设备信息/客户与产品产品信息)
- 外部数据域(与其他主体共享)

分级(影响严重程度)

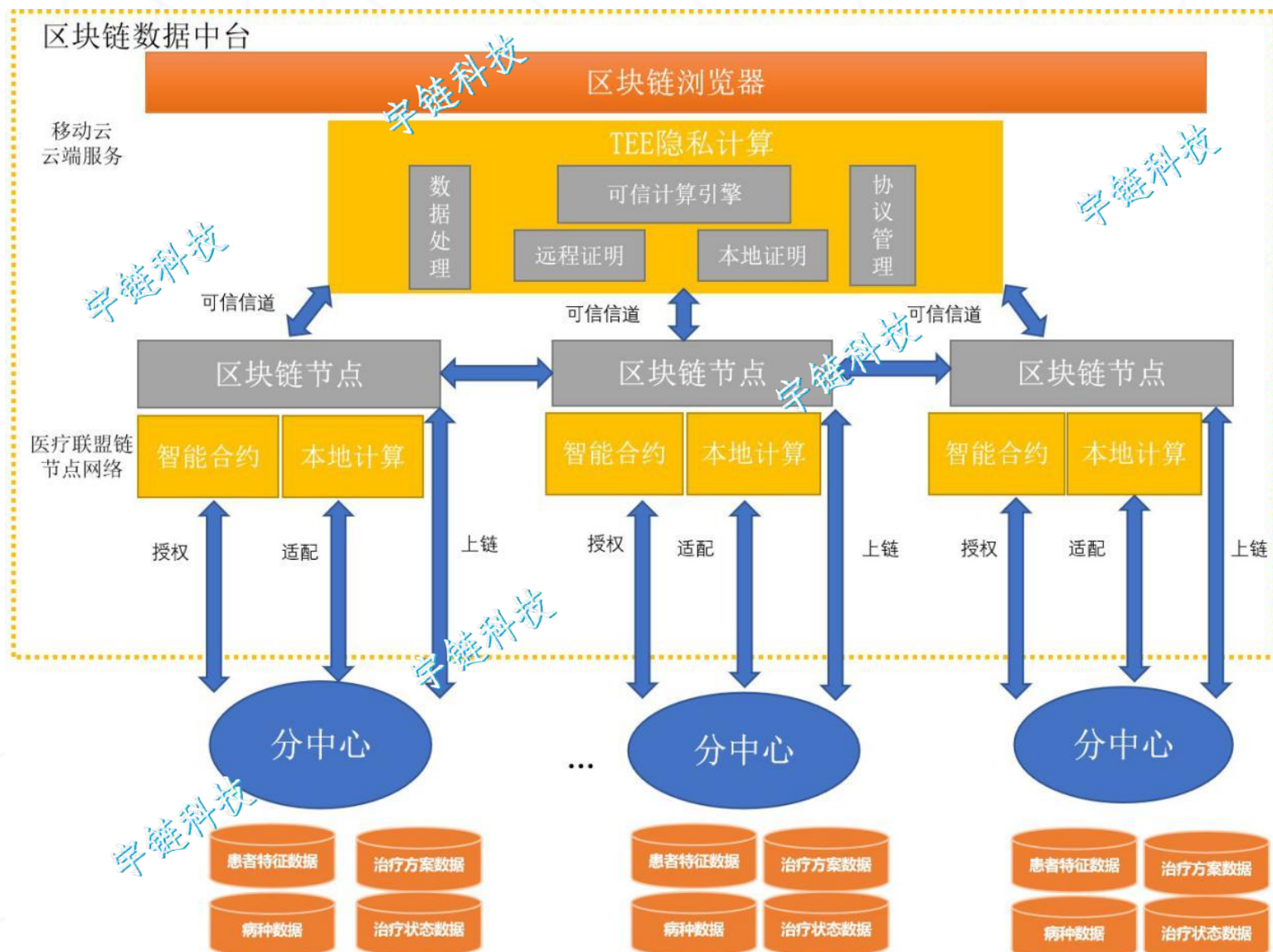
- 一级:负面影响较小/直接经济损失小/恢复数据代价小/受影响的用户和企业数量较少, 持续时间短
- 二级:引发较大安全事故, 给企业造成较大负面, 直接经济损失较大/持续时间长, 波及范围广
- 三级:引发重大安全事故, 造成直接经济损失特别大/国家安全

隐私保护
场景示例

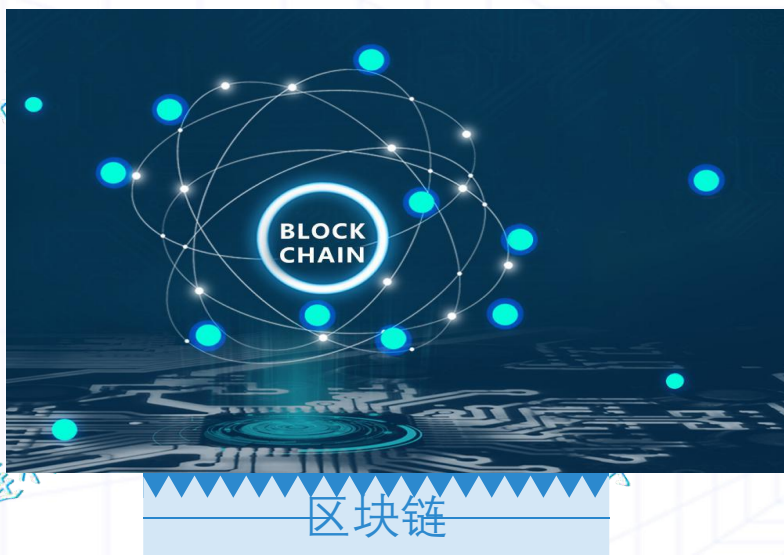
三级隐私保护管理

- 可公开的业务材料（材料A）：将在用户发起业务申请后直接调用材料数据，调用的记录将在区块链上进行存证。
- 低密级的业务材料（材料B）：将由相关业务单位的工作人员完成数据调用申请后数据授权使用，遵循授权最小化原则，每个数据字段需要单独授权。
- 高密级的业务材料（材料C）：高密级业务数据不可查询数据原文件，仅在业务工作人员完成数据申请后进行隐私计算，返回业务结果，实现业务数据“可用不可见”。

03. 探索与实践--医疗区块链(可信计算)



- ①数据提供方发布共享数据的元数据信息(哈希/用户公钥/数据积分), 且数据加密后存储在本地
- ②数据需求方查看共享元数据
- ③数据需求方通过智能合约向数据提供方申请授权
- ④数据提供方授权数据需求方使用数据
- ⑤数据需求方发起计算任务, 并数据提供方发布本地计算模型
- ⑥数据提供方审核模型后, 同意加入
- ⑦数据需求方发起任务, 并传输计算模型
- ⑧通过可信信道传输适配数据
- ⑨可信计算环境内数据与模型计算, 输出结果



区块链



医疗



企业

- 防伪溯源
- 价值结算/积分激励
- 数据可信(可信硬件IoT/可信上链)
- DID分布式数字身份(去身份标识)
- 数据确权/授权/共享

感谢聆听！！

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技

宇链科技