

云智未来<sup>9th</sup>

第九届中国系统架构师大会  
SYSTEM ARCHITECT CONFERENCE CHINA 2017

# 区块链与数据时代

海纳云CTO 邹均

SACC  
2017

北京·新云南皇冠假日酒店

IT168.com

ChinaUnix

ITPUB

# 目录

- 1：数据时代介绍
- 2：数据时代挑战
- 3：区块链与数据时代
- 4：案例
- 5：小结



# 数据主义意识的产生

## • 人类主流意识的改变

- 从人文主义向数据主义转变
  - 《未来简史》尤利瓦尔

## • 数据主义观点

- 宇宙由数据流组成，任何现象或实体的价值就在于对数据处理的贡献；
- 生化算法和电子算法合二为一
  - 生物体都是生化算法
  - 图灵机电子算法
- 电子算法将全面超越生化算法
  - 大数据处理能力
  - 人工智能



# 数据革命推动数据时代的到来

- 历史发展阶段

- 农业革命
- 工业革命
- 信息革命
- 数据革命

- 数据时代的到来

- 马云的DT时代
  - 商业与数据挖掘、处理、分析息息相关
- 基于数据管理一切
- 大数据处理能力需求飞速增长
  - 超越生化算法能力
  - 越来越依赖电子算法



# 不同时代的生产力和生产关系

- **农业革命、工业革命时代**

- 生产力是获取物质资料的能力；
- 生产关系注重物权

- **信息革命时代**

- 科学技术是生产力；
  - 信息处理成为生产力水平标志
- 生产关系关注点
  - 从物权延伸到知识产权

- **数据革命时代**

- 生产力标志
  - 获取数据、处理数据的能力
- 生产关系关注点
  - 数据权益
    - 所有权
    - 使用权



# 目录

- 1 : 数据时代介绍
- 2 : 数据时代挑战
- 3 : 区块链与数据时代
- 4 : 案例
- 5 : 小结



# 如何保障数据权益？

- **信息革命时代的知识产权**
  - 商标、专利、版权、商业秘密
  - 权属人
    - 通过脑力劳动生产出来
    - 或者通过合法购买获得
- **数据革命时代的数据权益**
  - 所有权
    - 个人数据
      - 权属属于个人，与生产者无关；
      - 权属不可转让；
    - 非个人数据
      - 权属属于数据采集、生产者；
      - 权属可转让
  - 使用权
    - 所有人授权他人使用



# 如何保护个人数据？

## • 国际主流国家

### – 立法保护个人数据

- 隐私保护法

- 未经个人同意，他人不能擅自使用个人数据

- 银行业PCI DSS

## • 国内隐私保护

### – 没有专门立法

- 隐含于民法、刑法

### – 现状

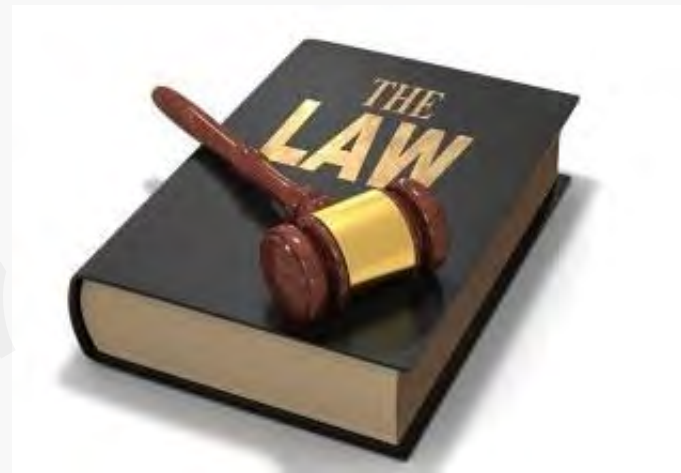
- 大平台垄断用户数据

- 大平台垄断数据主权

- 用户数据被滥用

### – 发展趋势

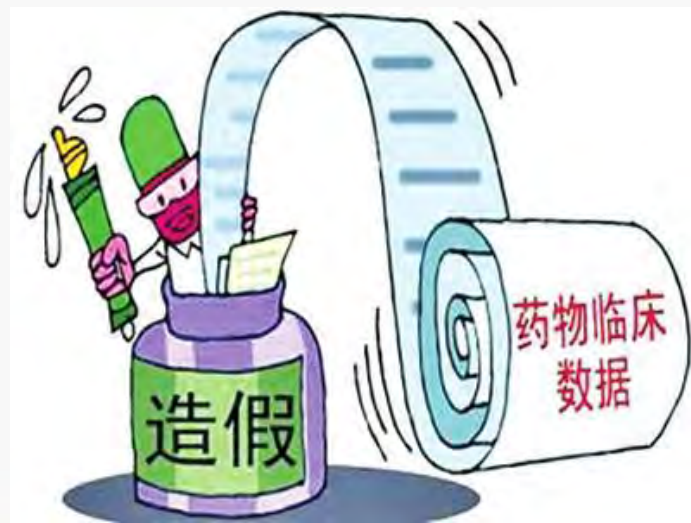
- 与国际接轨





# 如何确保数据真实性？

- **数据真实性含义？**
  - **数据来源真实性**
    - 数据提供者身份验证
    - 数据传输环境没有经过第三方篡改
  - **数据的真实性程度**
    - 正确性
      - 数据与其描述对象吻合
    - 客观性
      - 数据没有受主观因素影响
- **如何确保数据真实性？**
  - **权威机构（Oracle）**
    - 专业、资质
  - **透明化**
    - 众智
  - **技术手段**
    - 减少人为环节



# 如何形成数据权益定价机制？

- **目前机制**

- **数据交易所**

- 交易量少

- **点对点交易**

- Ad-hoc

- **目前机制问题**

- **缺乏透明性**

- **数据权益缺乏流动性**

- **缺乏评价体系**



# 目录

- 1 : 数据时代介绍
- 2 : 数据时代挑战
- 3 : 区块链与数据时代
- 4 : 案例
- 5 : 小结



# 区块链技术和其它主流技术的不同

- **风口上的技术**
  - 大数据
  - 人工智能
  - 物联网
  - 5G
  - 区块链
- **技术风口提升生产力**
  - 自动化替代人工
    - 提升效率
    - 降低成本
- **区块链改变生产关系**
  - 改变行为
  - 改变组织架构



# 区块链技术的核心 – 去中心化信任机器

## • 去中心化信任建立

### – 区块链信任的含义

- 真实性
  - 私钥签名保证交易不能伪造；
- 透明性
  - 交易记录在交易相关方公共账本
- 溯源性
  - 账本交易可追溯；
- 不可篡改性
  - 账本只能追加，不能删改；
- 客观性
  - 账本状态是共识结果
  - 推翻共识结果成本高昂
- 权益确定性
  - 私钥决定数据权益
- 唯一性
  - 价值权益只可转移，而不可复制



# 区块链是改变生产关系，改变行为和组织架构的技术

## • 后信息革命时代面临的矛盾

- 数据产权不清
  - 用户数据被平台侵占
- 数据使用权混乱
  - 隐私数据被滥用
- 价值交换不能保证原子性
  - 企业普遍存在的应收账款问题，彰显价值交换的不确定性和不公平性

## • 数据时代生产关系的要素

- 数据权益的确立
  - 数据所有权
  - 数据使用权
- 数字资产权益保障
  - 数字资产权益唯一性
  - 数字资产价值转移安全性
- 价值交换的确定性和公平性
  - 交易双方价值交换的及时性、公平性和确定性

## • 区块链带来的改变

- 去中心化组织
  - 把人为因素、主观行为去掉，代之以自动执行的客观契约
- 数据确权
  - 数据链上确权
  - 数据使用链上追溯
- 数字资产价值安全转移
  - 从信息互联网到价值互联网
- 价值交换的原子性保障
  - 智能合约解决应收账款问题



# 数据权益的保护需要颠覆性的商业模式

## • 中心化商业模式的限制

### – B2C商业模式

- 商业运营的基础决定于是否占有用户数据
- 数据垄断即核心竞争力

## • 去中心化商业模式

### – C2B商业模式

- 由用户提需求，商家提供个性化服务
- 用户授权决定 - “我的数据我做主”
  - 什么数据可供商家使用；
  - 怎么使用；



# 数据时代数据权益保障的前提

- **区块链技术推广**
  - P2P架构、分布式信任构建
  - 确立数据主权
  - 数据使用权追溯、审计
  - 数据价值的平等交换和转移
- **商业模式创新**
  - 去中心C2B模式
- **数据价格体系**
  - 数据市场价格体系的形成
- **法律跟进**
  - 明确数据权属
  - 隐私保护立法





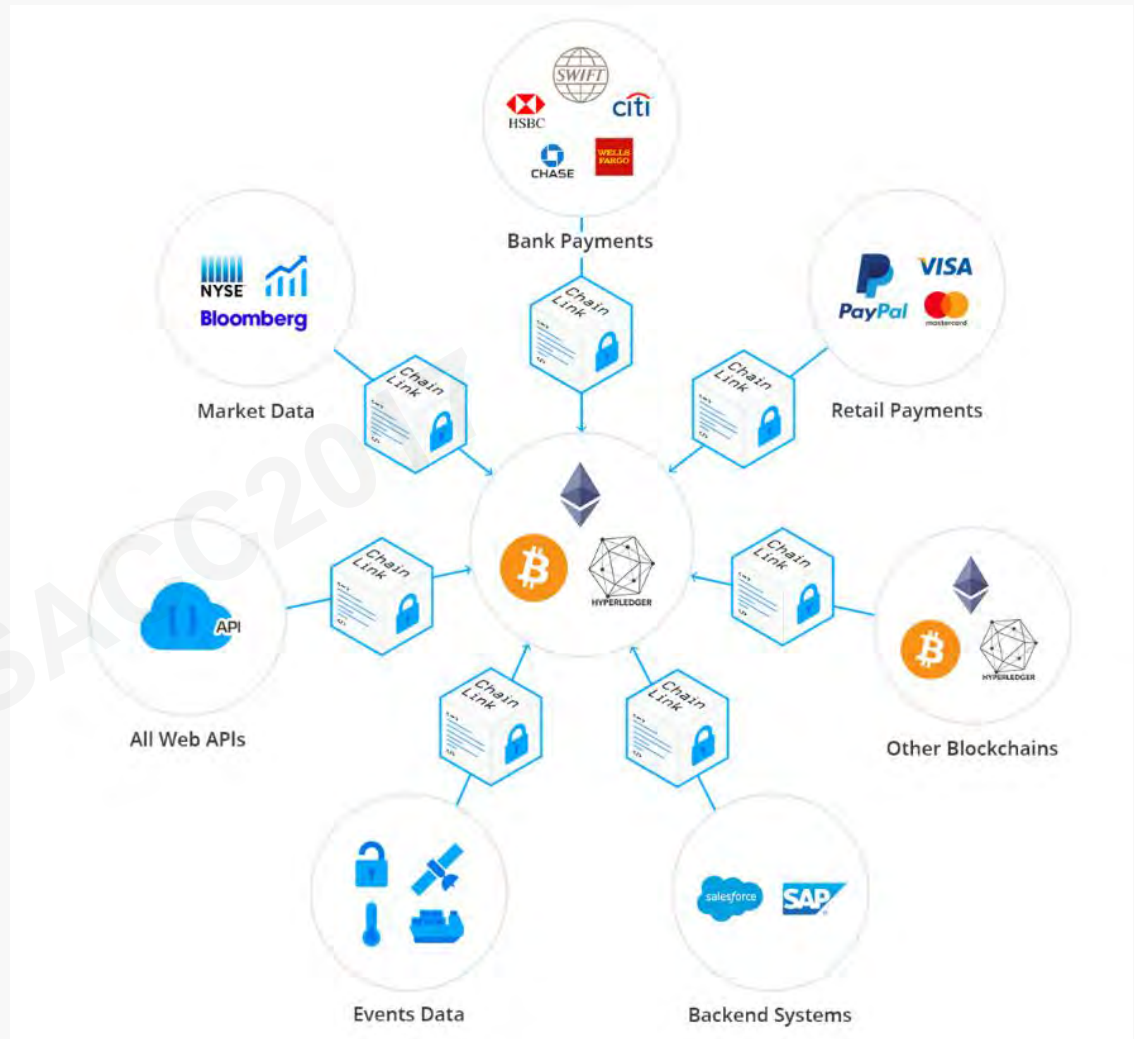
# 目录

- 1 : 数据时代介绍
- 2 : 数据时代挑战
- 3 : 区块链与数据时代
- 4 : 案例
- 5 : 小结



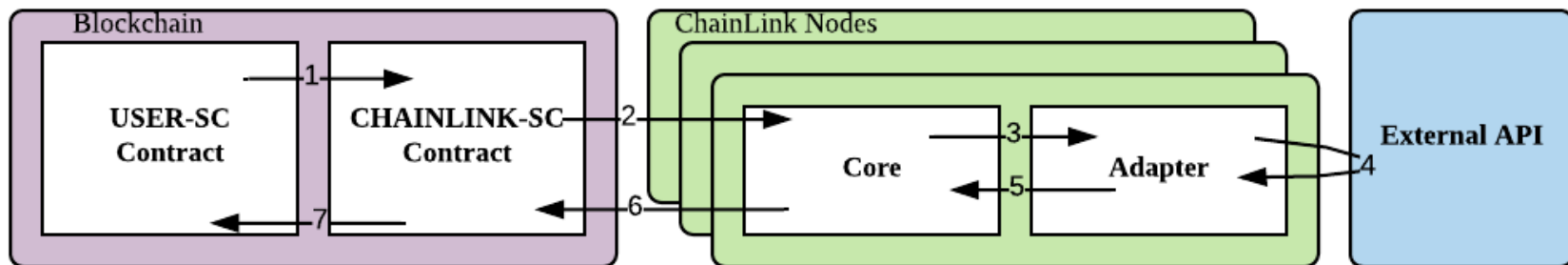
# 国外案例 – SmartContract

- SmartContract
  - 智能合约公司
  - Garner 2017 Cool Vendor
- 方案
  - 提供去中心化Oracle网络 - ChainLink
  - ChainLink 网络提供数据，支付信息给智能合约，同时提供API



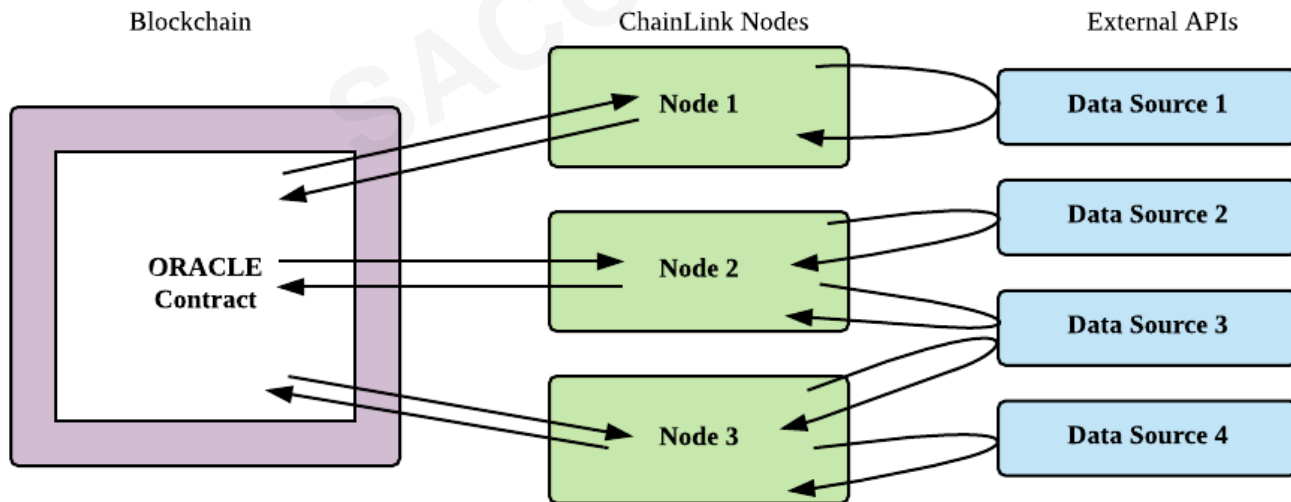
# SmartContract ChainLink workflow

- 1) USER-SC 链上调用ChainLink 合同CHAINLINK-SC
- 2) CHAINLINK-SC 为Oracle将事件做日志
- 3) ChainLink 核心读到事件，把请求路由给适配器。
- 4) ChainLink 适配器调用外部API来执行请求
- 5) ChainLink 适配器处理回复并发回给核心
- 6) ChainLink 核心把数据返回给CHAINLINK-SC
- 7) CHAINLINK-SC 把所有返回数据整合后一次性的返回给



# SmartContract ChainLink如何保障数据真实性？

- **采用分布式数据源**
  - 选用半数以上多数的数据
- **分布式Oracle**
  - 采用Commitment Scheme以防Oracle串通
  - 拜占庭容错
- **采用可信硬件**
  - Arm TrustZone , Intel SGX



# 国内案例 – Scry.Info无域开源项目

## 项目目标

- **SCRY是一个灵活而具备可扩展性的开源协议**
  - 为搜集、整合、群策分析、预测真实数据验证的区块链智能合约广泛使用创造条件。
- **开发者/个人以及任何自由组织通用区块链社区授权的开源协议**
  - 开发者可以通过SCRY协议官方登陆系统创建使用数据服务集合的API接口；
  - 可以选择有趣的数据源加入SCRY进行集群智慧数据验证工作；
  - 可以查找到所有真实的区块链数据源信息文件。



## 底层创新

- **SCRY作为全球验证真实数据区块链合约的开源协议**
  - 开发者和个人都可以在SCRY中寻找来自交通、气象、金融、体育、娱乐、农业等数据源
  - 鼓励全球更多的社区开发者、跨国组织、黑客、公司和个人写入数据源参与到区块链数据节点的集群智能认证中。
- **SCRY提供一个完备的图灵优化数据辨识协议层**
  - 参与者可以在SCRY上开发自己的区块链数据应用产品
  - 所有的数据均来自SCRY协议节点认证签名的数据智能合约。

# Scry.Info核心技术

## 1 数据查询

对scry底层数据链的数据进行索引，查询等。

## 2 Scry Service

提供了对SCRY CABSI的部分封装,为上层平台/应用提供的方便的调用API. 可以方便的发起委托供应协议;进行公证投票。

## 5 ScryDB

将大的数据放置到外部去中心化用户数据存储的链中,把外部存储的索引保存在数据合约/注册合约内部。

## 4 数据公证

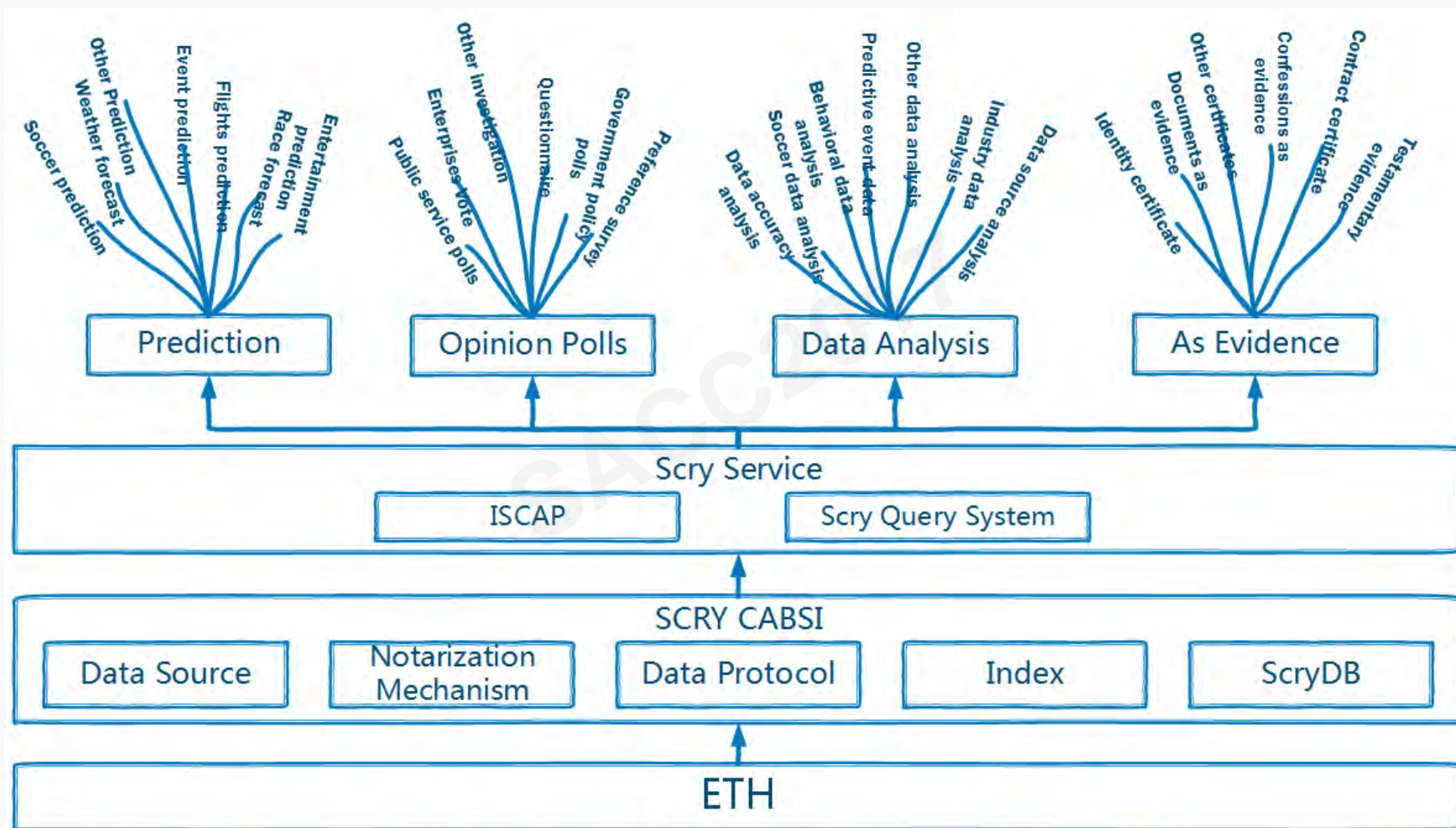
对数据提供者的数据进行盲投。公证人参与数据盲投，核实数据的真实性。

## 3 数据协议（合约）

数据写入者创建供应协议；数据需求者创建委托供应协议；数据公投入公共协议等。

SCRY.  
INFO  
应用

# Scry.Info底层架构



# Scry.Info核心模块 -CABSI

- **CABSI**

- Certification Agreement Based Swarm Intelligence
- 是一个集群认证的基础规则模型
- 提供对Ethereum smart contract访问和操作

- **CABSI组件**

- 索引:
  - 主要用于查询相关
- 认证:
  - 使用盲投的形式对数据的真实性进行公证
- 数据源:
  - 数据的录入形式:直接调用Scry.info相关接口进行录入;
  - 从第三方数据源录入等
- ScryDB
  - 对数据录入后的相关存储操作
- Scry Data Protocol
  - 包含了对真实数据进行存证的几种模型的具体操作实现



# 支持上层应用-Scry Service

- **Scry Service**
  - ISCAP(Implemented by SCRY CABSI Automation providers)
    - 提供了对SCRY CABSI的部分封装；
    - 为上层平台/应用提供的方便的调用API
  - SQS(Scry Query System)
    - 通过索引信息，来直接给出一个方便的查询系统  
(含可视化界面)

# Scry.Info 特点

- **Scry.info开源协议层**
  - **方便区块链应用开发**
    - 封装并提供了上层应用接口；
    - 方便了上层调用者对Ethereum的操作；
  - **提供去中心化数据真实性验证**
    - 提供数据供应协议标准和接口API；
    - 基于群体智慧投票验证数据真实性；
  - **提供数据供需方聚合平台，形成数据定价机制**
    - 有偿数据验证、调用、查询
  - **构建数据行业生态**
    - 基于Scry.info的提供数据协议模型可以快速构建出基于真实数据的相关应用；
    - 任何个人和公司可以实现自己的协议和数据存储等相关行为,并接入到Scry.info系统中

# 目录

- 1：数据时代介绍
- 2：数据时代挑战
- 3：区块链与数据时代
- 4：案例
- 5：小结



# 小结

## ● 数据革命的开启

- 后信息革命时代 -- 数据时代初级阶段
  - 挑战
    - 数据权益的归属？
    - 数据真实性如何保障？
    - 数据定价机制？
  - 区块链是改变生产关系的技术
    - 信任构建，数据权益确权，数据价值安全转移，数据使用权追溯

## ● 数据时代数据保障的前提

- 区块链技术的推广
- 商业模式创新
- 数据价格体系的形成
- 法律体系的跟进

## ● 案例

- 国外--SmartContract
  - 分布式数据源、分布式Oracle保障数据真实性
- 国内- Scry.Info无域开源项目
  - 开源协议降低区块链数据应用开发门槛
  - 构建数据行业生态
  - 采用群体智慧保障数据真实性
  - 提供数据供需聚合平台形成数据定价体系

# 附：《区块链技术指南》

《区块链技术指南》新书介绍本书和其他描述应用场景的书不同，重点介绍各类区块链技术的特征和开发方法，包括比特币、以太坊、超级账本、共识算法、闪电网络、比特币开发技术、以太坊智能合约开发等等。对区块链技术感兴趣的朋友，请参考邹均博士、张海宁先生、唐屹博士、李磊博士和陈晖先生等作者合著的新书：《区块链技术指南》，机械工业出版社



扫描二维码购买

京东购买链接：

<http://item.jd.com/12007317.html>

THANKS

The background features a dark, almost black, space filled with numerous small, bright blue particles. These particles are arranged in several distinct, curved paths that sweep across the frame from the bottom left towards the top right. A bright, white-to-blue gradient light source is positioned behind the word 'THANKS', creating a lens flare effect that illuminates the surrounding particles and the text itself.