

# 数瑞技术白皮书



北大数瑞  
B D W A R E

# 目录

1.	前言.....	1
2.	价值定位.....	2
3.	数瑞技术架构.....	3
3.1.	总体架构.....	3
3.1.1.	生态参与者视图.....	3
3.1.2.	技术架构.....	4
3.2.	主要模块设计.....	6
3.2.1.	可信图式账本设计.....	6
3.2.2.	可信合约引擎设计.....	9
3.3.	部署架构设计.....	13
4.	数瑞技术特性与优势.....	16
4.1.	可信图式账本技术特性与优势.....	16
4.2.	可信合约引擎技术特性与优势.....	17
5.	典型案例.....	19
5.1.	政务数据可信共享开放.....	19
5.2.	政府社会数据可信统筹.....	21
5.3.	数据资产可信流通平台.....	23
5.4.	海量非结构化数据可信存证.....	25

# 1. 前言

数据资源，是驱动数字经济发展的核心力量，也是提升信息社会智能水平和运行效率的关键要素，被视为决定未来竞争能力的战略资产。如何将政府、企事业单位在运行过程中形成的庞大数据资源资产化，使之成为支撑数字经济崛起的“新石油”，是数字经济发展的关键挑战。

国务院日前印发《促进大数据发展行动纲要》指出，要加快政府数据开放共享；推动产业创新发展，培育新兴业态，助力经济转型；强化安全保障，提高管理水平，促进健康发展。习近平总书记在中央政治局第二次集体学习中指出，要构建以数据为关键要素的数字经济，运用大数据提升国家治理现代化水平，运用大数据促进保障和改善民生。

数据资产价值的发挥是一个让数据“动起来”的过程。高质量、高可用、高有效数据资产的安全可信流动、加工融合是支撑大数据分析、流通与应用变现，从而推动数字经济发展的基础。政府企事业单位拥有大量高价值核心数据，有效保障数据资产安全可信的共享流动和融合使用，防窃取、防滥用、防误用，是数据可信流通过程中关键问题。

## 2. 价值定位

北大数瑞依托北京大学软件研究所雄厚的科研实力和科技孵化成果，立足大数据领域，研发数瑞数据智能可信操作系统，打造数据智能生态，致力于实现数据的可信流通与全生命周期管控。“瑞”的含义是美好，北大数瑞的愿景是创造数据可信流通的美好数字世界，实现数字世界的价值传递。

北大数瑞以保障数据资产安全可信的共享、流动、开放、融合变为抓手，研发数瑞可信图式账本、数瑞可信合约引擎两项核心产品。通过可插拔的产品模块，实现数据全生命周期过程监管，使数据采集、预处理、分析、可视化，全过程可信、可管、可控。北大数瑞秉持开放心态，所有产品均支持与已有系统进行对接、整合和升级。可信图式账本、可信合约引擎为原有大数据平台新增数据可信流通的技术特性。

北大数瑞团队专注于底层技术，为平台集成及应用开发合作伙伴提供稳定的数据可信管控技术支撑，与各方合作伙伴合力打造数据智能生态。

## 3. 数瑞技术架构

### 3.1. 总体架构

#### 3.1.1. 生态参与者视图

数瑞生态的主要参与这有三大类：数瑞技术团队、平台开发商、应用开发商。生态的用户视图如所示。

表格 1 数瑞生态参与者视图

参与者角色	对应的人或系统	职责任务	拥有的权力和能力
数瑞技术团队	北大数瑞核心技术团队、生态其他开发团队或个人	提供稳定的底层技术，支撑数据流通可信可管可控	获取技术服务费
平台开发商	集成开发商,开发数据共享交换平台、开放平台、数据交易平台等,为最终客户提供服务	围绕客户的业务场景，基于数瑞技术开发可信平台系统，为客户提供整体解决方案	可信管理数据。通过平台可以实现数据全生命周期管理，获取集成开发和解决方案费用
应用开发商	应用开发商,开发数字政府、智慧城市、数字社会、工业互联网等应用，	基于数据可信平台，围绕应用场景，开发具体的数据应用	可信使用数据。通过应用解决客户实际场景中的问题，获取应用开发和产品销售

	解决客户痛点		售费用
--	--------	--	-----

### 3.1.2. 技术架构

北大数瑞的总体技术架构图如所示，包括物理层、网络层、可信存储层、可信计算层、数据接入层、平台层和应用层。

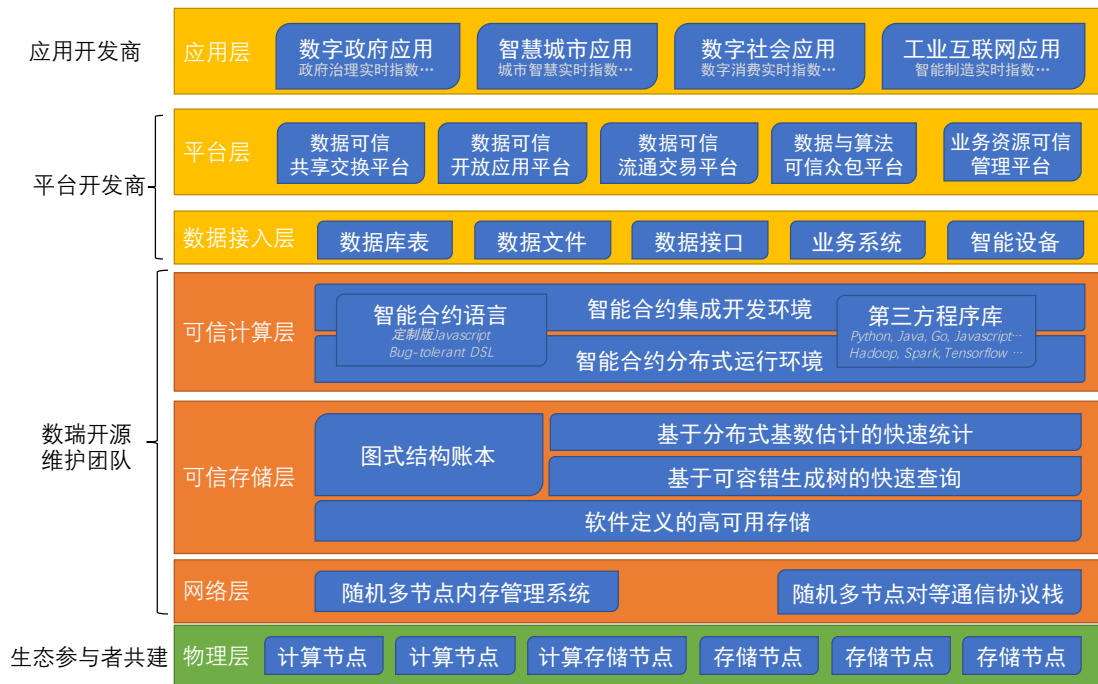


图 1 北大数瑞技术架构图

1. 物理层。物理层由数瑞生态参与者共建，各方提供数瑞节点形成网络，保证数瑞的存证真实可信。物理层可以是物理机或者虚拟机，根据节点的推荐配置安装不同的数瑞软件，可分为计算节点、存储节点、计算存储节点。

2. 网络层。网络层由数瑞技术团队研发维护，由随机多节点内存管理系统、随机多节点对等通信协议栈构成。网络层的功能是实现对物理层节点的管理，主要内容包括对存储节点的随机调度和节点间的

对等通信协议。

3. 可信存储层。可信存储层由数瑞技术团队研发维护，完成数据可信上链、不可篡改的软件实现。图式结构账本模块采用有向无环图结构，实现数据的高性能写入；快速统计模块和快速查询模块实现图式账本的高性能读取。可信存储层对上层暴露读写接口，可以在智能合约中、或程序代码（现已支持 Java/GO 两种语言，可根据合作伙伴需求增加编程语言支持）中调用相关接口实现数据的高性能可信存证。

4. 可信计算层。可信计算层由数瑞技术团队研发维护，实现随机多节点相互校验的可信计算，并支持调用可信存储层的接口将合约执行的过程信息存证到可信存储层。数瑞定义了可信计算的编程语言和框架，并对上层提供编写说明和远程调用接口，按照框架编写程序即可实现可信计算并存证。围绕智能合约语言，可信计算层提供合约开发环境、运行环境和其他编程语言的第三方库调用模块。

5. 数据接入层。数据接入层由平台开发商将原有的数据通过智能合约调用或者可信存证 SDK 接口调用的方式，接入数瑞生态中。全面支持数据库表、数据文件、数据接口等多种接入方式。特别地，对于已有的业务系统、智能设备等，数瑞提供业务系统数据接口重构服务，形成与业务对应的数据接口，并接入数瑞数据智能生态中。

6. 平台层。平台层由平台开发商基于数瑞构建的可信数据流通机制，结合客户的需求，为客户开发的大数据平台及相关解决方案，可应用于数据共享交换、数据开放服务、数据流通交易、数据与算法

可信众包、业务资源可信管理等场景。数瑞团队不参与平台的研发或销售工作，只提供底层可信技术支撑。

7. 应用层。应用层由应用开发商基于可信数据平台，针对客户的数据应用场景需求，开发相应的可信数据应用，无需关注底层数据可信细节，只需要按照关注场景和应用，底层的大数据和可信技术由平台开发商和数瑞技术团队来保证，降低数据应用开发技术门槛。

## 3.2. 主要模块设计

下面主要介绍可信图式账本和可信合约引擎两个数瑞主要功能模块的设计与实现。

### 3.2.1. 可信图式账本设计

围绕数据智能场景，可信图式账本创新采用有向无环图结构，构建大数据区块链操作系统，满足大数据场景的超高数据吞吐量。创新采用 nRW 随机见证共识算法，见证节点、共识节点、交易节点分级部署管理。功能结构组成

可信图式账本是面向大数据的区块链操作系统，与通常的“比特币”、“以太坊”等区块链技术，不同的设计理念在于，由于数据是一种可以被无限复制的无形资产，可信图式账本承载的大数据共享交换业务无需解决现有代币交易系统的“双花”问题，因此采用了有向无环图的结构与 nRW 随机见证共识。可信图式账本包括图式账本联盟链、共识算法、图式账本集成 SDK、图式账本管理系统、图式账本统



计看板等功能模块。可信图式账本的功能结构图如下图所示。

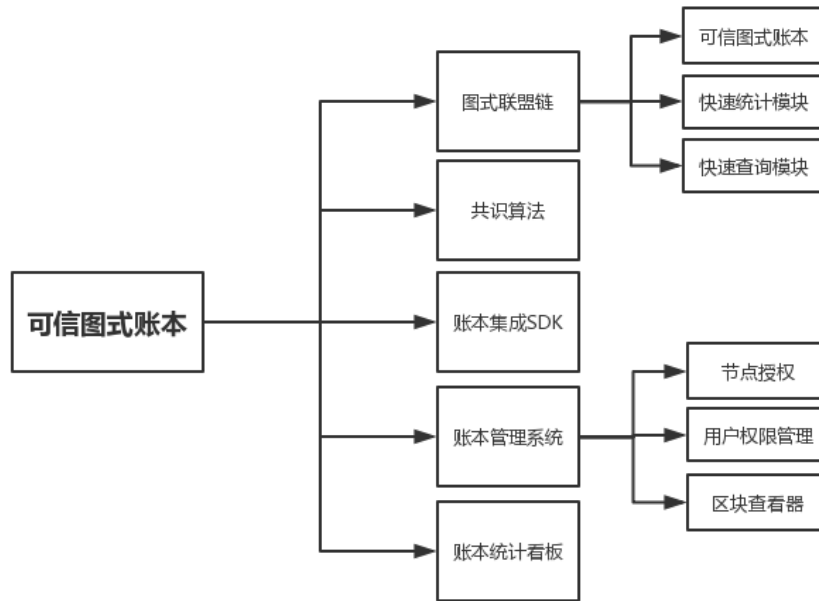


图 2 可信图式账本功能结构图

### 3.2.1.1. 主要功能模块

#### 1. 图式账本联盟链

图式账本联盟链由可信图式账本、快速统计模块、快速查询模块组成。

(1) 可信图式账本。可信图式账本采用有向无环图结构，实现数据全生命周期状态存证监管。数据链实现了超高的吞吐量，并且随着节点数目的增加，可信图式账本的吞吐量线性扩容，能够满足大数据业务的大规模吞吐量。

(2) 快速统计模块。数瑞实现了基于分布式基数估计的快速统

计。

(3)快速查询模块。数瑞实现了基于可容错生成树的快速查询，采用树形广播和结算的可扩展查询算法，通过对高容错和负载均衡的树形结构进行广播和汇总，保证在节点数量和存证吞吐量增加的情况下，快速查询的可扩展性。

## 2. 共识算法

创新采用 nRW 随机见证共识算法，对于每笔交易，由随机 3 个见证节点进行见证，每个见证节点再随机挑选 3 个共识节点进行共识，加快分布式账本共识速度。

## 3. 图式账本集成 SDK

通过图式账本集成 SDK，实现可信图式账本与已有产品的灵活结合，在系统中需要数据监控与溯源的点调用数据集成 SDK，即可完成数据的上链。在合约中可以也可以调用图式账本集成 SDK 将合约执行过程在可信图式账本上进行可信存证。

图式账本提供多种上链方式，供不同场景下使用。原始数据上链方式，适合高价值数据上链；原始数据不上链，调用记录和数据 HASH 值上链方式，适合共享交换场景大量数据交换、校验、审计。

## 4. 图式账本管理系统

图式账本管理平台用于图式账本系统的节点授权、用户权限管理、区块数据查看等功能，方便平台管理者对图式账本进行管理。

## 5. 图式账本统计看板

全面展示图式账本全网数据统计情况,实时反应图式账本节点部署、区块数目、共享交换频率、数据吞吐量等信息,进行相关数据的可视化呈现。

### 3.2.2. 可信合约引擎设计

可信合约引擎通过运行时计算反射技术,将合约执行的过程进行全程监管控制,可以实现对数据字段操作权限控制、数据访问者身份核验,并将合约执行监控结果使用区块链技术可信存证,保证数据在共享开放过程中的可信、可管、可控。通过对合约进行静态分析和动态分析,完成对数据的溯源和血缘分析,实现数据全生命周期可追溯,以及共享开放效果的定性评价标准。

#### 3.2.2.1. 功能组成结构

可信合约引擎包括在线合约代码编辑调试 IDE、合约代码解释器、合约反射运行环境、合约分析模块、北大数链可信存证模块等功能模块。可信合约引擎的功能结构图如下图所示。



图 3 可信合约引擎功能结构图

### 3.2.2.2. 主要功能模块

#### 1. 合约代码编辑调试 IDE

提供合约代码的在线编辑及调试功能。主要包括以下几个功能：

(1) 用户认证。通过生成或上传密钥完成用户的身份认证，在合约审核和执行过程中，通过验证密钥来确定是否对该用户开放合约调用权限。

(2) 新建合约。用户可以在 IDE 上新建一个合约，并在系统中完成该合约的注册。

(3) 编写调试合约代码。支持在线编写调试合约代码，用户可以在合约代码中对数据进行数据分析等操作，并支持使用数据提供方的小规模测试数据对合约代码进行测试。

(4) 运行合约。在满足数据使用权限的情况下，在线执行合约代码，合约在数睿节点中执行，无需将原始数据返回给数据需求方，只将合约代码对应的分析结果返回。

(5) 搜索合约。对于在系统中注册的合约，可以通过搜索功能进行检索。

## 2. 合约代码解释器

(1) YJS 脚本语言。北大数睿大数据资源一体化平台的合约代码由 YJS 脚本语言编写。YJS 是一种类似 js 的脚本语言，方便用户迅速上手，合约代码解释器可以将 YJS 高级语言转译运行。

(2) 支持跨语言操作。解释器支持 Python、Java、C/C++ 等多种语言的跨语言操作，让用户可以直接调用其他语言现有的数据分析类库，方便用户进行数据分析。

## 3. 合约反射运行环境

在合约反射运行环境中，通过计算反射等技术，实现对数据字段的用户访问控制和操作权限限制。在代码执行过程中检查用户是否被

授予相应的权限访问数据的特定字段，如果发现异常，则拒绝代码执行。

结合合约代码中数据字段的操作权限申请审批等制度，保证数据的使用方式与数据需求方申请数据时填写的理由和对数据字段进行操作的权限相一致，防止数据被滥用。

#### 4. 合约分析模块

通过对合约的静态分析和动态分析实现对合约的数据字段操作权限检查报警，以及数据的流转过程监控。

(1) 静态分析。通过合约的静态分析，得出合约代码对数据字段的操作权限。操作权限由高到低分为原始数据开放、算数运算开放、控制依赖开放、不开放四个等级，如果数据需求方申请数据时填写的字段操作权限低于合约代码实际的操作权限，则静态分析模块会产生警告，防止数据安全问题发生。

(2) 动态分析。通过合约的动态分析，监测合约每一次执行过程中的条件输入、关键执行路径、返回结果等信息，并且可以将数据的流转过程进行可视化呈现。动态分析的结果可以用于数据的全程溯源以及血缘分析等功能。

#### 5. 北大数链可信存证模块

将合约执行的关键点通过北大数链进行存证。包括合约的调用者、调用时间、运行节点情况、合约输入、合约关键点、合约返回值等。

通过可信存证，不可篡改，监控数据流转的全生命周期，使数据可信流通可溯源，数据共享开放过程可信、可管、可控。

### 6. 随机多点同步执行模块

通过随机多点同步执行，一方面保证多个节点之间可以相互校验，保证执行结果的可信行；另一方面避免了全网同步执行效率低的问题。采用 PBFT 定序算法，实现多个节点之间的状态同步；在有节点发生异常的时候，有相应的内存同步机制和状态恢复机制，保证合约执行的准确性。

## 3.3. 部署架构设计

数瑞平台存在存证节点、计算节点和管理节点三类。这三类节点之间，通过数瑞的 P2P 层进行连接，同时，这三类节点对外提供了 GRPC、Websocket 和 Http 等不同形式的访问接口。

1) 管理节点（图中绿色节点）：负责节点之间的准入管理、分发可验证的私钥，管理节点往往仅有一个。

2) 计算节点：提供计算服务。运行了可信计算层的智能合约引擎。支持对数瑞合约的启、停、调用等操作。同时，也可以对合约的 I/O 状况、合约的执行状态进行监测。

3) 存储节点：提供可信存证服务。运行了可信存储层的图式账本，提供高吞吐量的写入、快速统计与查询的服务。

下图以数据开放平台为例，展示了典型的数瑞部署结构：

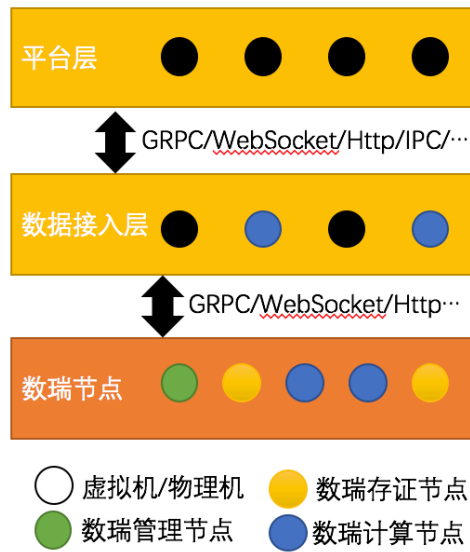


图 4 数瑞节点架构

图中的每个圆圈为一个虚拟机/物理机。实际上计算节点与存储节点也可运行于同一虚拟机/物理机之中。基于数瑞进行开发的应用平台的开发者通过调用计算节点与存储节点提供的服务,实现上层应用的某些功能逻辑的可信、可管、可控。因此,这些开发者还会有运行自己本身逻辑的一些节点(图中黑色节点)。上图以数据开放平台为例,在数据接入层,在一些节点运行了数据库程序、API管理程序(黑色节点),这些提供数据的节点不直接给平台层提供服务,而是通过开发者通过开发接入原始数据的合约,实现对数据的接入(即数据接入层的蓝色节点)。

数瑞的管理节点、计算节点和存证节点的主要程序逻辑为Java与Go语言开发,节点的程序均支持各版本Linux(CentOS、Ubuntu、中标麒麟)和Windows等操作系统。



下表为数瑞管理节点、计算节点、存证节点的推荐配置：

表格 2 数瑞节点部署推荐配置

节点类型	推荐配置	备注
管理节点	4 核（3GHz），4GB 内存，1GB 硬盘	支持一万个节点管理
计算节点	4 核（3GHz），8GB 内存，1GB 硬盘	
存证节点	双核（3GHz），2GB 内存，至少 40GB 硬盘	视存证需求可增加硬盘、蓝光存储

## 4. 数瑞技术特性与优势

### 4.1. 可信图式账本技术特性与优势

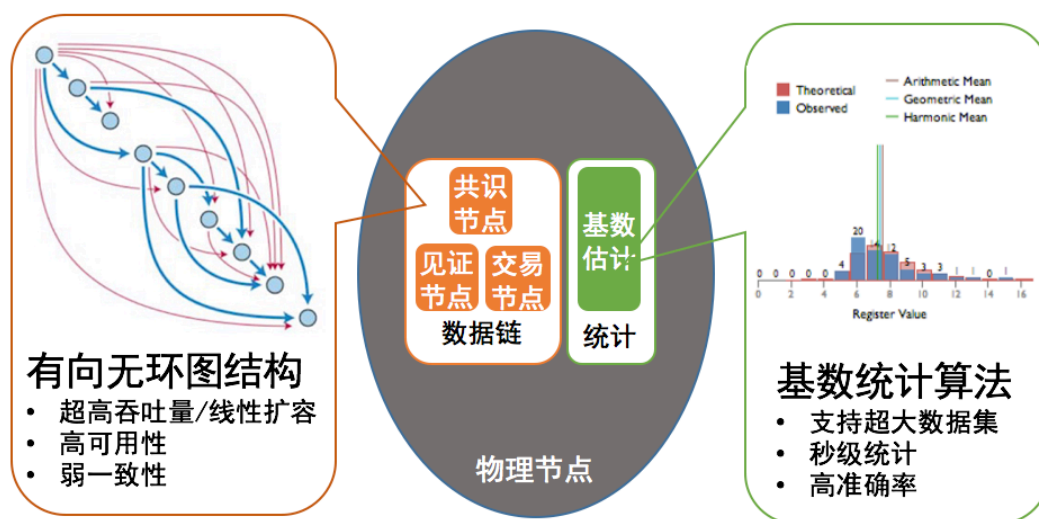


图 5 可信图式账本结构图

可信图式账本是北京大学技术团队针对大数据场景自主研发的区块链存证系统。通过可信图式账本，对数据全生命周期的使用过程中产生的“指纹”进行可信存证，防止记录被篡改，并支持指纹溯源。

使用方需要在环境中部署数瑞节点，并且可以根据自身业务需求动态调整节点数量，适应业务吞吐量。相比于传统的区块链，数瑞可信图式账本针对大数据使用场景进行了设计和优化，有以下技术特性：

- (1) 支持大数据场景超高吞吐率，单节点吞吐率超过 100TPS
- (2) 吞吐率随节点数增加线性扩容，根据交易量需求弹性配置
- (3) 实时存证，不使用“伪链”缓存，高可用性

(4) 分布式基数估计算法，实现秒级统计；高容错生成树，实现快速查询

(5) 支持分级存储，利用蓝光存证冷数据成本节省 1000 倍

## 4.2. 可信合约引擎技术特性与优势

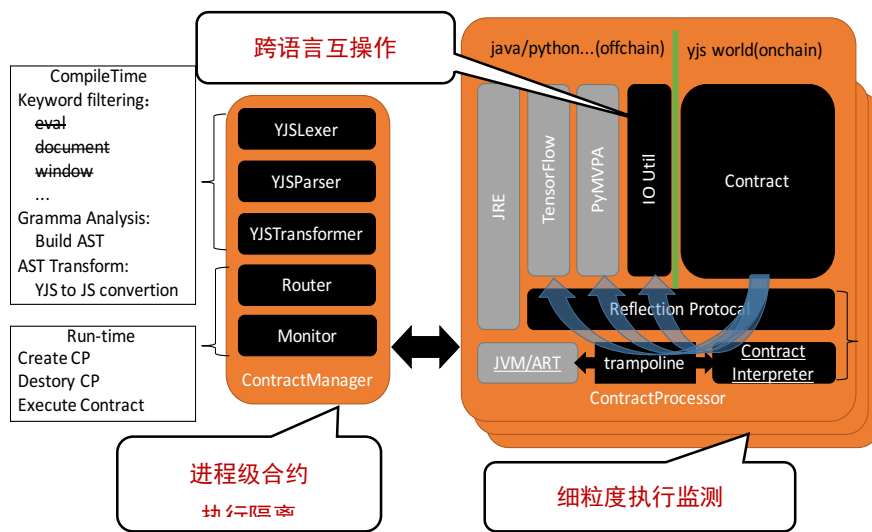


图 6 可信合约引擎结构图

可信合约引擎对现有的大数据平台业务进行可信监管补充，通过合约算法的可信执行实现原始数据不脱离数据提供者的物理控制，只将分析结果返回给数据需求方的数据可信分析过程，解决了数据使用场景与申请理由不一致、数据脱离所有者物理控制后被滥用等问题。

可信合约引擎由合约代码编辑调试 IDE、合约代码解释器、合约反射运行环境、合约分析模块、图式账本可信存证等模块组成。在可信图式账本的和可信数据管道支撑下，可实现以下能力：

(1) 灵活支持数据库、数据接口、数据文件等多种方式的可信数据接入；

(2) 通过运行时计算反射，实现数据字段操作权限控制，全程监管合约代码对数据的操作情况，形成不同源数据分析融合过程血缘分析；

(3) 基于三节点同步验证机制，核心数据不动、完成对合约代码的静态分析和动态分析，形成数据生命周期的“指纹”并上链。

(4) 支持合约执行全过程信息上链，进行指纹溯源，保障不可篡改。

(5) 支持合约代码编写过程中调用多种编程语言的类库，如 Tensorflow、Hadoop 等，可以接入其他语言实现的已有人工智能算法；

## 5. 典型案例

### 5.1. 政务数据可信共享开放

案例介绍：某直辖市政务数据可信开放服务平台试点

为了发挥大数据促进经济发展、服务改善民生、完善社会治理的作用，培育壮大战略性新兴产业和加快构建数字经济和智慧城市，某市颁布《促进大数据发展应用条例》，并建设政务数据开放平台，将政务数据开放给社会企业和个人使用，促进当地数字经济发展。

政务数据关系国计民生，有着巨大的社会价值，在数据开放过程中，如何防窃取、防滥用、防误用，保障数据安全是关键的问题。政务数据开放过程中，流转各方的责权效不清晰，导致其面临如下问题：

1. 数据提供方不敢提供数据。数据需求方在申请数据时填写的使用场景可能与实际的使用情况不一致，将部门数据与其他数据进行碰撞，可能会造成难以控制的后果。直接将数据提供给数据使用方，难以保证对方不会将数据转手给其他人使用。数据安全关系到政府部门的责任，数据提供方不敢将有价值的数据放到开放平台上，没有真正发挥数据开放平台的作用。

2. 数据提供方不愿提供数据。由于缺乏合理的技术手段记录数据的使用过程，难以衡量数据提供方在数据应用建设过程中起到的作用，缺乏合理的激励措施和手段，数据提供方没有足够的动力将自身的数据贡献出来给别人使用。

3. 平台方责任问题。如果发生数据安全问题，难以说清楚在哪个环节发生了滥用、误用的问题，平台方作为数据的中介方，在很多情况下不得不承担保护数据安全的责任，在事故发生后，缺乏合理的手段对数据使用过程进行溯源。

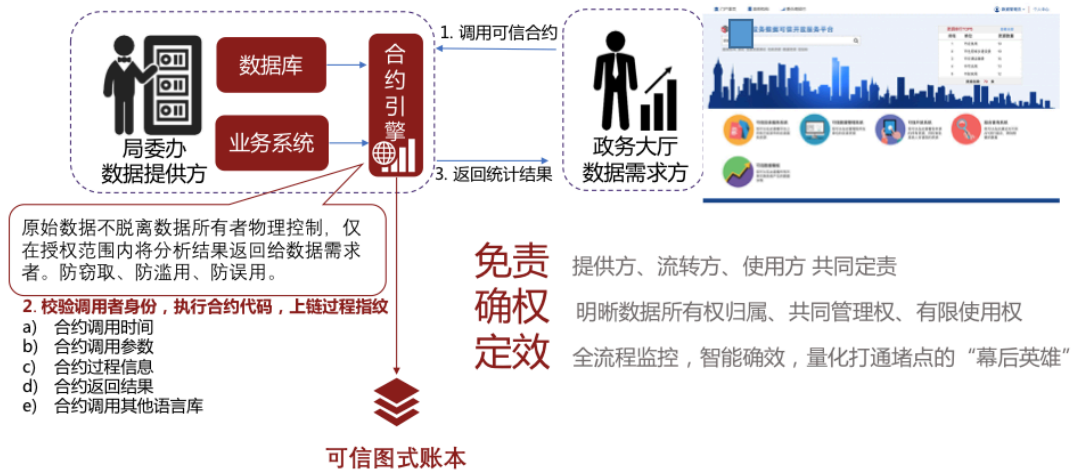
解决方案：

使用数瑞可信图式账本和可信合约引擎对已有的政务数据开放平台进行改造，使政务数据开放过程可信、可管、可控。

1. 优化数据申请审批流程。数据需求方将对数据的操作过程以合约代码的形式提交给数据提供方审核，数据提供方通过代码审核确定数据需求方对数据的操作与申请理由一致，从源头防止数据被误用。

2. 数据使用全生命周期监管。按照合约代码在可信合约引擎中执行数据操作过程，数据在可信环境中，不脱离数据所有者物理控制，仅将数据分析结果返回给数据需求方。在执行合约代码过程中，对数据全生命周期进行监管，将关键环节形成“数据指纹”，使用可信图式账本进行可信存证，不可篡改。

3. 数据指纹溯源。通过可信图式账本，对数据指纹进行溯源，校验数据开放过程中申请、审批、数据使用全过程，形成数据血缘分析和贡献度报告，明确数据开放中各方的责权效。



应用效果:

对已有政务数据开放平台进行改造, 实现 11 个委办局、103 项数据的可信开放试点, 实现数据开放过程中的免责、确权和定效, 让数据资源成为真正的数据资产, 探索数据可信开放利用、高效协同融通, 进一步支撑地方大数据生态的建设与发展

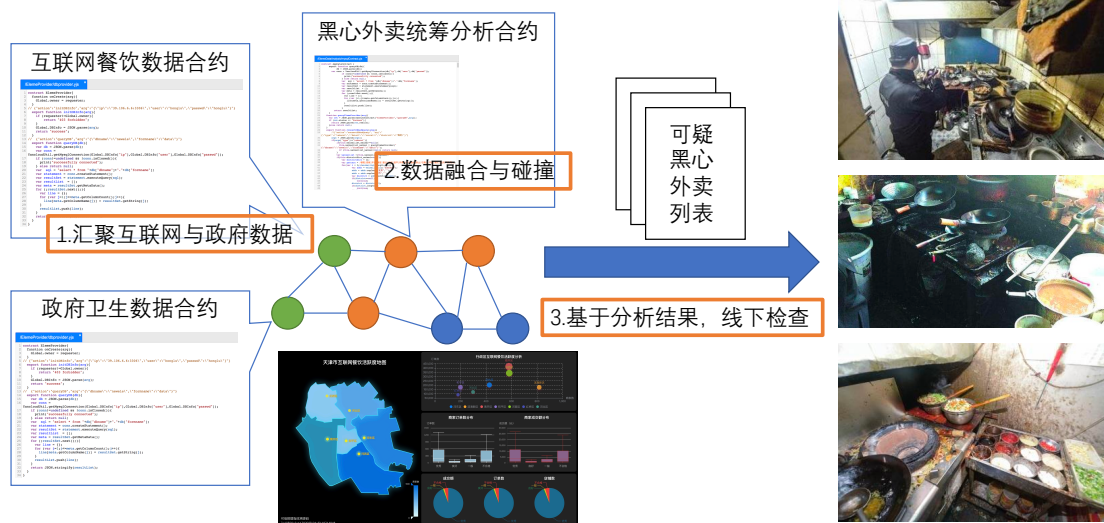
## 5.2. 政府社会数据可信统筹

案例介绍: 某直辖市社会数据统筹可信开放应用示范

企业在为社会提供服务的同时积累了大量高价值的数据, 地方政府如何打造区域性数据平台, 鼓励企业将数据通过平台进行流通、变现, 与政务数据或其他企业的数据相融合, 打造一批地方数据应用, 是地方数字企业发展的重要机遇, 也是发展数字经济的重要抓手。

然而数据提供方在提供数据时仍有很多顾虑, 一是担心企业数据被滥用, 威胁企业的经营和业务发展; 二是没有合适的激励机制和计价方式让企业的数据被他人使用后, 可以反馈给企业足够的经济收益。

解决方案：



结合企业的互联网餐饮数据和政府的卫生评级数据，进行社会数据统筹可信开放应用示范。

食品安全民生工程是某市政府的一大重要民生工程。当前互联网餐饮火爆，一方面降低了食品行业的准入门槛，另一方面也增大了食品安全的隐患。例如，新闻报导某地区黑心外卖作坊猖獗，而食品药品监督管理局因为人力有限等原因，很难通过全市线下巡查的方式落实。通过将互联网餐饮数据和政府卫生评级数据进行关联分析，可以迅速定位卫生有隐患的餐厅，并进行定点排查。

企业和政府分别部署数瑞节点，将其所有的数据配置为可以数据合约，提供数据格式和样本供他人参考，并编写合约代码。第三方开发者通过可信合约引擎完成数据载入、预处理、关联分析、可视化流程。通过企业和政府相关部门的审核后，可以在数瑞可信节点中进行数据处理的全过程，全过程数据不脱离提供方的物理控制，只将分析结果生成图片，将图片返回给数据需求方。



应用效果：

通过数瑞可信技术支撑的开放应用平台，让企业和政府部门放心地将数据配置到数据合约中，第三方编写合约代码，互联网餐饮数据与政府食品卫生评级数据进行关联分析。第三方无需拿到企业和政府的原始数据，只需提交代码，系统将分析过程在可信环境中完成，并将结果返回给第三方进行应用，提供可信的安全卫生信息服务，保障人民食品安全，提高政府公共服务能力。

### 5.3. 数据资产可信流通平台

案例介绍：上海某金融公司智能数据投研系统

上海市某企业在进行投融资业务过程中，积累了大量高质量的数据，并希望通过数据流通交易开辟新的商业模式。但是担心其他竞争对手在获得其数据后开展与他相似的业务，或直接转卖数据，使其丧失数据方面的优势和业务的竞争力。由于缺少合适的技术方案帮助其解决数据流通中的信任问题，一直无法开展新的业务。

解决方案：



数睿支撑某公司数据资产可信流通平台

数瑞提供底层技术，支撑其建设智能数据投研系统，进行数据资产可信流通。企业只需提供数据资产的元数据和样例，数据需求者提交数据处理代码进行审核，该企业确定数据需求方的业务范围与其不重合，并且没有将原始数据直接拿走后，批准需求方对数据的使用。数据需求方无法获得原始数据，只能在该公司的数据上进行双方约定的数据处理、分析工作，并获得数据分析的结果；最后根据数据的使用情况进行计费。

应用效果：

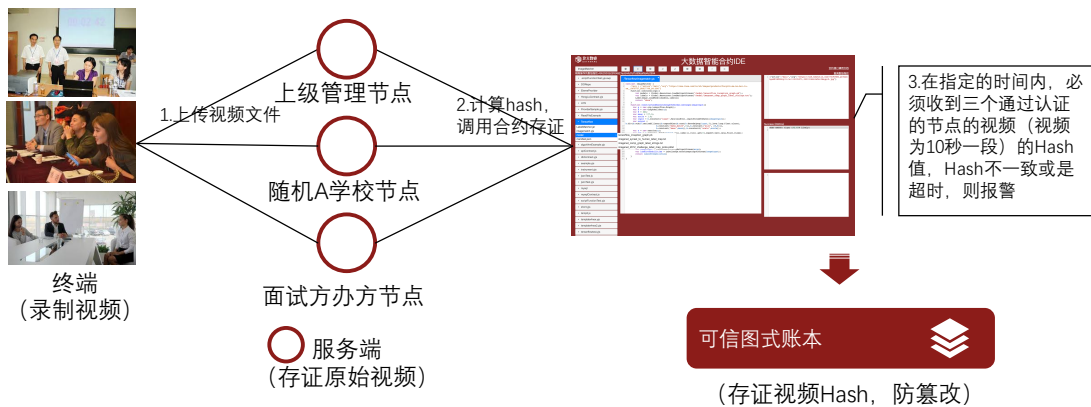
所有的数据处理过程都通过可信合约引擎的计算反射技术监控，并由可信图式账本记录，可以进行全程溯源。数瑞支撑该公司开辟了全新的数据可信流通交易的商业模式和业务场景，已成为该公司的重要业务与盈利增长点。

## 5.4. 海量非结构化数据可信存证

案例介绍：阳光面试

某高校自主招生面试、研究生面试过程中，为了避免黑箱操作，希望将面试过程中的视频存证。如果视频按传统的方式进行单点存证，容易被人篡改，失去了视频存证的意义。若使用普通区块链进行存证，则需要在全网存储数量庞大的备份，存储和共识开销太大。

解决方案：



使用数瑞可信计算引擎实现了一个哈希校验合约。该合约对外提供两个方法调用：1) 实时哈希上传；2) 哈希校验。首先，在实时录制视频的过程中，每 10 秒便会由视频录制终端计算这段视频的哈希值，并通过合约存证，防止了视频录制时造假。接着，原始视频录制完成后，会上传到三个节点上进行备份：1) 上级管理节点；2) 该校的主办方的节点；3) 随机一个参与单位（学校）的节点。这些节点在收到了这个视频的时候会每隔 10 秒计算一个哈希值，并进行哈希校验。这防止了视频录制完成在上传之前篡改。最后，当三个节点都校验通过之后，这个视频就是完成了存证的整个过程。当有人想恶意

篡改这个视频的时候，不仅需要可信图式账本上的哈希数据进行篡改，还需要对多份的原始视频数据篡改。通过这种方式，基本杜绝了篡改视频数据的可能性。

应用效果：

三个视频存证节点与可信图式账本上的 HASH 值可以相互校验，保证数据的真实性，防止视频被篡改。通过数瑞的随机见证机制，既保证了海量非结构化数据可信存证，杜绝修改数据的可能性，也大大降低了存储开销。