主权区块链技术蓝皮书

（Sovereign BlockChain）

贵阳区块链技术与应用联盟

主编：夏琦 陈瑞东 董传晔 张小松

2017-5-27

目 录

1. 概述.....3
1.1. 核心优势.....3
1.2. 商业模式.....4
1.3. 主要目标.....5
2. 顶层设计.....5
2.1. 架构.....5
2.2. 模型.....7
2.3. 运营模式.....9
2.4. 价值估算.....10
3. 需求.....13
3.1. 实现区块链的主权特性.....13
3.2. 实现主权区块链生态体系.....13
3.3. 实现公平可信的数据交换平台.....14
3.4. 优先破解数据资源流通与安全保护难题.....15
4. 技术规范.....15
4.1. 技术规范.....15
4.1.1. 自由可扩展的区块链记账系统.....19
4.1.2. 主权区块链智能合约设计.....20
4.1.3. 安全监管智能合约支撑.....20
4.1.4. 资源共享的度量值设计.....21
4.1.5. 自主、可控的数据资产交易规范.....23
4.2. 技术指标.....24
5. 建设方式.....25
5.1. 数据区块链典型应用对接.....25
5.2. 区块链商业模式成功运营和推广阶段.....27
6. 实施要素.....27
7. 联盟现有典型应用.....30

7.1. 仓储/供应链/物流领域应用 30
7.2. 医疗领域的应用.....30
7.3. 数据交易领域的应用.....31
8. 蓝皮书修订过程 31

1. 概述

本文档旨在研究主权区块链的模型、架构、核心算法及运营模式等问题，提出在具体实施主权区块链过程中所应遵循的各项技术规范、量化指标、设计标准，以指导主权区块链的各项应用落地并形成区块链生态体系。

1.1. 核心优势

2016 年 12 月《贵阳市区块链发展和应用》白皮书发布。该白皮书从政府职能、产业聚合、业态趋势等角度分析出了区块链在“坚持主权原则，探索规则创新”的模式下如何发展区块链技术并和行业结合，与国外偏自由主义的“比特币、万向、以太坊”等技术平台相比，贵阳主权区块链强调在网络空间命运共同体间，尊重网络主权，在主权经济体框架下进行共有价值交付。因此，贵阳主权区块链在在“约束与自由”的辩证关系中更具有国际制高点，也是贵阳在大数据生态体系建设过程中形成区块链高地的核心优势。

基于上述原则来构建主权区块链生态体系，基于区块链的安全记账基础，**突破数据资产转移过程中的“脱链”难题**，结合国密标准与权益共识算法，形成自主研发、安全可靠的主权区块链基础设施与系列应用。

1.2. 商业模式

（1）共享经济商业模式

贵阳主权区块链生态体系用于为贵阳市区块链发展和应用提供技术规范和量化指标，针对所面向的不同行业和客户群体进行计算和存储能力的整合，只要是涉及主权应用场景下的区块链**记账服务、存证取证服务、审计溯源服务、真伪辨别服务、支付服务、物质资产化与转移服务、数字资产化与转移服务等**，都可以基于本体系进行平台研制、二次开发、私有链对接等多种共享模式。

（2）链上链下模式

白皮书中提到的“数字经济发展正成为全球经济增长的新引擎，而区块链推动和建立了可信安全和开放共享的数字经济”。贵阳主权区块链生态体系的功能作用从业务角度来看，其实质就是将“政权、金融、物流、医疗、公共安全、工业制造业等”一系列传统经济真正地进行“数字化”的历程。在过去 20 年的 Internet 发展中，人类只是通过简单的数字化完成了“可靠通信”业务，即使这样的 O2O 模式（Online To Offline）对传统行业所起到的加速作用都难以度量；而主权区块链将在保障社会稳定、行业规则的前提下，将实现可靠、安全、公信力的“**OnChain To OffChain**”的创新商业模式，对于传统难以数字化的资产、业务起到强力的推进作用。

1.3. 主要目标

- 通过技术定义来固化主权区块链的模型、架构、算法和运营的顶层设计，形成可有效指导主权区块链应用研发的方法论；
- 基于上述方法论对主权区块链的功能划分、场景描述、工程实现、应用对接、政策引导、商业模式等进行细化拆分，指导并评估形成可落地实施的贵阳区块链应用方案；
- 整合多方资源，形成对区块链硬件设施、软件平台等公共服务体系的建设，并在此基础上支撑 3 大领域 12 大典型应用；
- 最终促进贵阳主权区块链生态体系从原型、产品、应用、商业化运作的全过程建设，有效形成由政府扶持、企业牵头、行业锻造、商业推广的区块链大平台。

2. 顶层设计

2.1. 架构

贵阳以主权区块链为核心基础平台，在块数据和“绳网结构理论”指导下，形成跨区域、跨场景、跨部门应用的区块链立体空间。

图 1 贵阳主权区块链生态体系顶层设计

（1）主权区块链硬件基础设施管理平台、参与节点集群管理平台

如上图所示，贵阳主权区块链生态体系将利用贵州大数据硬件基础设施，结合覆盖全国的主权区块链参与节点（P2P 方式），形成主权区块链基础设施管理平台；该平台实现了由政府针对区块链业务的主管部门及相关区块链数据中心

（2）主权区块链调度平台

通过自主研制主权区块链调度平台，内部实现基于 POS 的共识算法来保障记账权的公信力及主权化，保证在涉及“社会稳定、公共安全、民生利益”等重大问题方面的账本信息的高度安全、高可用、稳定可靠。

（3）区块链记账平台

该区块链记账平台可以实现物质数字化记账功能和数据 2 次描述（元数据）记账能力。物质数字化记账采用 xml 标准的

KV 结构化描述物质的各种属性；而针对数据的 meta data 则通过“数据名、类型、内容摘要、数据流通量、数据敏感度、数据价值标定”等指标对“流动的数据”进行记账。

（4）数据区块链支撑平台

数据区块链支撑平台重点解决区块链记账过程中的加密、签名、密钥协商、摘要算法等部分的中国国家标准，以保证国家大数据区块链基础设施的安全；同时区块链参与节点在使用流通数据过程中，本支撑平台还有一部分用于实施数据防护功能，用于确保加入区块链的数据加工企业，在使用数据的过程中不会发生“数据脱链”，从而造成数据泄露所造成损失。

（5）区块链基础服务实现

区块链的应用于“金融支付、物流运输、公安存证、数据流通、个人数据管理”等多方领域，其对应的智能合约、区块链记账服务接口、可视化调用平台等都不相同；按照目前微服务（ESOA：增强型面向服务架构）的技术架构，将分离出“区块链记账服务、存证取证服务、审计溯源服务、真伪辨别服务、支付服务、物质资产化与转移服务、数字资产化与转移服务” 等上层应用平台，供各区块链 APP 应用实施。

2.2. 模型

（1）主权区块链理论模型： 主要包括块数据模型和“绳网

结构”模型。

首先，建立块数据模型，用于描述一个物理空间或行政区域形成的涉及人、事、物的各类数据的总和。其中，块数据模型又具体包括块数据的描述、存储和完整性保护模型，分别用于定义如何使用区块链上的数据来构建块数据，采用统一模型存储块数据，确保块数据所描述的数据与区块链上的数据正确和一致。

接着，基于块数据模型构建“绳网结构模型”，实现区块链的彼此连接，构建记录全网上的价值交付的所有历史数据的立体价值结构。提出在异构和跨越环境下，不同区块链彼此连接，区块链上具有统一属性数据的映射数学表达方法和映射模型。解决区块链上的数据如何关联，区块链如何彼此连接。然后，在块数据和“绳网结构”模型的指导下，形成跨区域、跨场景、跨部门应用的区块链立体空间。

最后，结合国密标准与权益共识算法，提出自主研发、安全可控的主权区块链技术，以此突破数据资产转移过程中的“脱链”难题。

主权区块链的应用模型支持 2 种类型的区块链应用对接方式：

（2）直接基于区块链服务接口进行 App 研发：这个方式最为简单，主要流程为“接入区块链基础平台 → 设置智能合约脚本（类 solidity 脚本）→ 设置区块链安全脚本（类 python 脚本）

→ 自定义可视化”。

图 2 主权区块链生态体系的应用模型

（3）采用公私链的对接方式：这个过程是将现有区块链应用平台作为私链直接对接（或插入）到主权区块链生态体系当中，这个过程则需要“定制锲链协议”，通常采用双向锚定（Two way peg）使得主权区块链生态体系中的主链（Main Chain）与其他行业区块链应用的侧链（Side Chain）相互连通，连通后可实现“实物资产或数据资产交换”过程中的信用共享、支付相互支撑的目的。

2.3. 运营模式

主权区块链生态体系涉及全市的区块链应用支撑和数据交付，其平台运维除了建设公司应为本地化企业提供技术支撑服务之外，还应建立相应的责任事业单位进行流程管理和规范化运作。

图 3 平台运维的机构设立与相应职责

按照主权区块链硬件基础设施管理需求，需成立区块链账本中心，管理该硬件平台对区块链海量大数据的稳定运营工作。

按照主权区块链应用过程中与金融、财会、固产、行政等领域的协调，以及负责的主权区块链参与节点的管理协调，分别成立区块链外联部和区块链备账管理中心。

对于公私链对接平台、以及区块链按照行业应用方式不同而进行的标准化工作，应成立区块链标准化工作组。

针对区块链记账服务、存证取证服务、审计溯源服务、真伪辨识、支付、物质资产化与转移业务、数字资产化与转移业务等服务，成立专门的区块链合约制定部，对不同业务的智能合约“依法、合法、合规、合理”进行制定和审查。

2.4. 价值估算

鉴于货币、货品等具有约定俗成的价值和价格计算方法。这

里将数据共享和交易做为案例，拟采用基于 AHP 溯源分析方法来定义数据流通过程中的价值规律，包括 **数据在特定时期内的价值初始认定、数据增值、数据价值回归等系列价值规律。**

算法集可确定数据流通过程中的初始定价和价格变化策略，将与数据资产有关的元素分解成目标、准则、方案等层次，在此基础之上进行定性和定量分析，最大的优点是遵循了数据资产本身具有的层次结构，它使得买方能够认真地考虑和衡量指标的相对重要性，同时在增值后将数据增值信息体现其增值过程，并实现价值回归。

```
{ // 本算法下的数据交易结构模型
 "id": "<hash of transaction, excluding signatures (see explanation)>",
 "version": "<version number of the transaction model>",
 "inputs": ["<list of inputs>"],
 "outputs": ["<list of outputs>"],
 "operation": "<string>",
 "asset": "<digital asset description (explained in the next section)>",
 "metadata": "<any JSON document>"
}
```

（1）建立层次结构模型。在深入分析数据资产评估问题的基础上，将有关的各个因素按照不同属性自上而下地分解成三个层次，最上层为目标层 O，最下层通常为方案层 D_i，中间为准则层 C_i，i=1,2,3。在本问题中，目标层为被评估的数据资产的评估值，准则层为资产价值评估应遵循的各原则，方案层为三种不同的定价策略。

（2）构造成对比矩阵。从层次结构模型的第 2 层开始，对

于从属于上一层每个因素的同一层诸因素，用成对比较法和 1-9 比较尺度构造成对比较阵，直到最下层。如：用a_{ij}表示C_i和C_j对 O 的影响之比,全部比较结果可用对比比较距阵表示。

$$A = (a_{ij})_{n\times n}, a_{ij} > 0 \quad (1)$$

由（1）给出的a_{ij}的特点,A 称为正互反矩阵。

（3）计算权向量并做出一致性检验等方法。对于每一个成对比较阵计算最大特征根及对应特征向量，如果得到的成对比较阵是一致阵,自然应取对应于特征根 n 的。归一化的特征向量(即分量之和为 1)表示诸因素 C_1，…，C_n 对上层因素 O 的权重，这个向量称为权向量。如果成对比较阵不是一致阵，但在不一致的容许范围内，建议用对应矩阵的最大特征根的特征向量（归一化后）作为权向量 w。而判断矩阵具有一致性的条件是矩阵的最大特征值要与矩阵阶数相等，据此建立一致性评价值为：

$C.I = \frac{\lambda_{max}-n}{n-1}$,其中 n 为矩阵的阶数。

则随机一致性比率 C.R 的值为：

$C.R = \frac{C.I}{R.I}$，其中 R.I 为随机一致性标准值。

计算 R.I 的过程是：对于固定的 n，随机地构造正互反矩阵 A'(它的元素a'_{ij}（$i < j$），从 1-9,1-1/9 中取随机值， a'_{ij} 为a'_{ji} 的互反数，a'_{ii}=1),然后计算 A'的一致性指标 C.I。可以想象到，A' 是非常不一致的，它的 CI 相当大。如此构造相当多的 A', 用他们的 CI 的平均值作为随机一致性指标。

3. 需求

3.1. 实现区块链的主权特性

以尊重网络主权背后的国家主权为前提，区块链技术发展必须在国家主权范畴下，在法律与监管下，从改进与完善自身架构入手，以分布式账本为基础，以规则与共识为核心，实现不同参与者的相互认同，进而形成公有价值的交付、流通、分享及增值，建立主权区块链。

主权应该至少体现出 3 项内容：

1）区块链上承载的网络和节点主权可控；

2）区块链上进行的业务流、策略合约主权可控；

3）区块链上流动的数据、货品等资产主权可控；

3.2. 实现主权区块链生态体系

目前国际范围内的区块链应用导致了基础设施的重复建设，容易导致以下问题：

1）公信力下降；

2）标准化程度低，后期资源整合困难；

3）直接的经费浪费。

贵阳建设的主权区块链生态体系，应是以通用记账平台、点对点分布式的高可用网络、区块链数据安全为共用设施的基础化

平台建设，其可以形成不同行业的区块链绳网结构，同时也可以形成具有国家级甚至国际公信力的基础区块链平台，避免了硬件资源的重复建设和后期运维，充分发挥贵州大数据产业生态的优势。

3.3. 实现公平可信的数据交换平台

从《华中大数据交易所、贵阳大数据交易所、中关村大数据交易所》等 2015-2016 近 1 年内的数据共享案例来看，政府来源的数据需求最为旺盛。从所出售数据的成交率来看，政府来源数据的成交率最高为 50%，企业来源数据的成交率最低为 18.3%。表明社会对政府来源的数据需求量较大，因此成交率相对较高。在一定程度上也折射出我国政府数据公开度不足，公共数据开放步伐有待加快。

但数据交易管理过程存在“漏洞”。尽管身份认证时需提供相应的机构代码、营业执照码、身份证号等身份证明，但在对会员单位认证的统计过程中发现，存在认证显示为政府但其内容简介却为企业的会员单位，如××科技、×梦××等。而且数据交易过程中还发现了数据在非授信情况下转移给第 3 方，而且难以取证和法律维权。

3.4. 优先破解数据资源流通与安全保护难题

我国在数据共享方面目前存在并将持续存在“共享不畅、数据‘打架’”等问题，在此条件下所进行的政务数据公开项目，极容易造成“数据关联”而最终形成大范围的“敏感信息泄露”，容易被诈骗分子利用这些敏感数据进行大规模化的诈骗；被反共、扰乱社会治安等团体进行信息关联和舆论引导、爆料。

数据开放后，数据使用的各方将这些数据据为已有，这个使用场景下政府作为数据的原始拥有者，非但没有途径去监管数据的价值发挥过程，甚至容易形成“争抢数据资源、囤货居奇”的局面，造成数据交易的恶意循环。

4. 技术规范

4.1. 技术规范

贵阳主权区块链生态体系，不同于目前比特币、以太坊等区块链平台，更不同于物流区块链、制造业区块链等 APP 应用体系，在技术和战略上属于现有区块链的盲区，同时也是 “数字经济”中最为困难的一项技术和工程，其技术规范如下：

1. 处于区块链基础操作系统层次：主权区块链需要可以满足块数据和绳网结构，形成跨区域、跨场景、跨部门应用的区块链立体空间，将突破国产区块链平台中“主权共识机制（俗称：

挖矿机制）、数据区块链难题、侧链支持”等尖端技术，形成符合我国经济发展形势状况的基础区块链核心平台。

2. 须支持独特的数据区块链：即需要通过区块链这种数字产品对“数据”进行描述，而不光是对“物流包裹、汽车部件、金融货币”等实物的描述。

3. 数据区块链的困难的克服：数据是一种易失、易变、异构的物质，这种物质本身又是对“物流包裹、汽车部件、金融货币”等客观物理世界进行描述的方式，这就造成了区块链的“2次记账困难”——即数据区块链用于记录“Data”，而 Data 又记录物理世界实体。

基于上述特殊性，应结合数据安全、网络安全、可用性 P2P 网络技术、终端数据芯片安全、侧链等一系列国际领先的核心技术，最终以满足实际需求。

总体架构设计如下图所示：

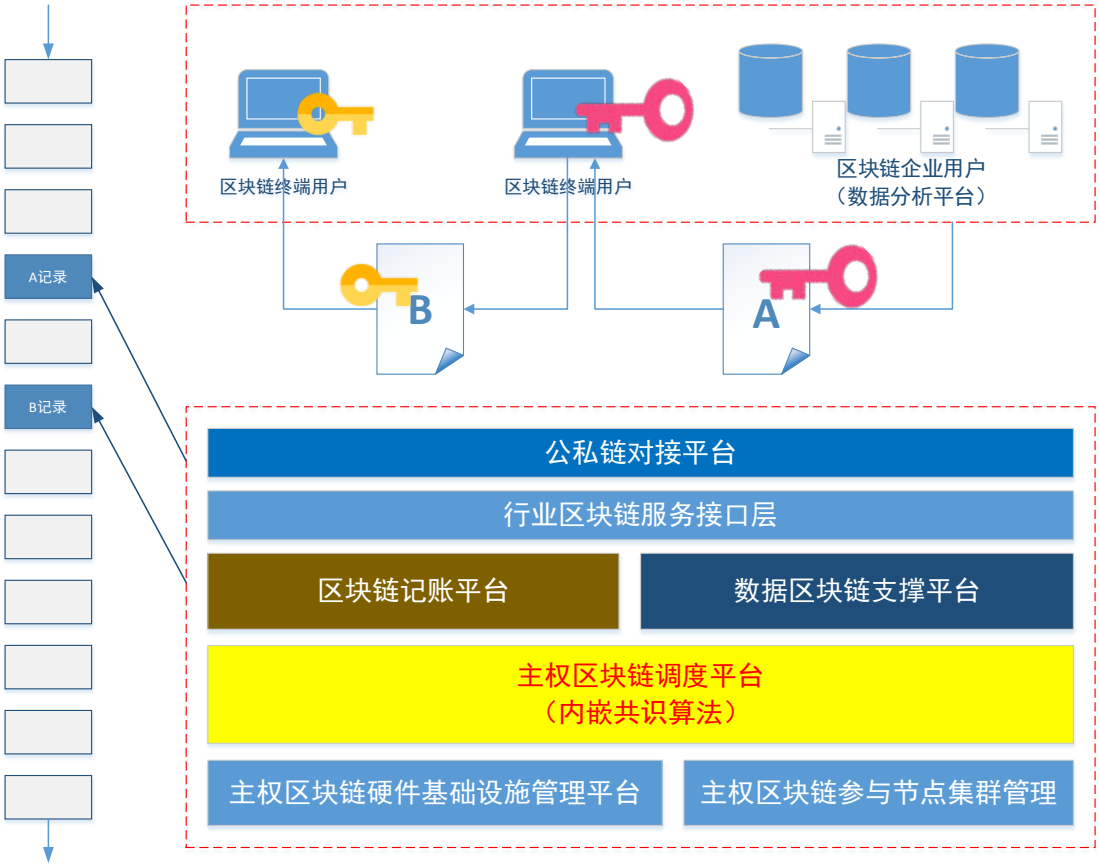

图 4 主权区块链生态体系技术规范图

贵阳主权区块链生态体系是面向异构、部门分散、行业百态的各类实体或数据资源的，应满足：

1）数据资源不流失，仍然在各政府、行业机构手中；

2）数据资源强保护，通过数据应用区块链安全基础芯片对数据进行保护，实现对政府数据更强有力的从“数据产生、数据流转、数据使用、数据终端拷贝和展示”等全方位的网络空间命运共同体的保护。

3）业务流通过程记账，实现的区块链应用记录了全网、全过程、全交易的实物或数据，并且所有数据被全网所有节点共同拥有，网络空间的信息更加透明、行为更加可追溯，从而实现全

网检查、全网监督和全网治理。通过智能合约，区块链能够自动化监控网络交易，实现更加自动化、智能化的互联网治理。

总体的技术框架如下图所示，其中涉及以下 3 个区块链子系统。公共链：对所有人开放，任何人都可以参与；联盟链：对特定的组织团体开放；私有链：对单独的个人或实体开放。

实物资产类型的区块链目前以太坊等方式已经逐渐开始落地实施，下面以常见的 3 个部门为例来说明数据区块链的实施方式，公安提供人口数据；社保提供居民社保数据；房管提供居民房屋不动产数据。这 3 个部门间进行数据共享交换过程中，采用区块链的安全交换方式如下图所示：

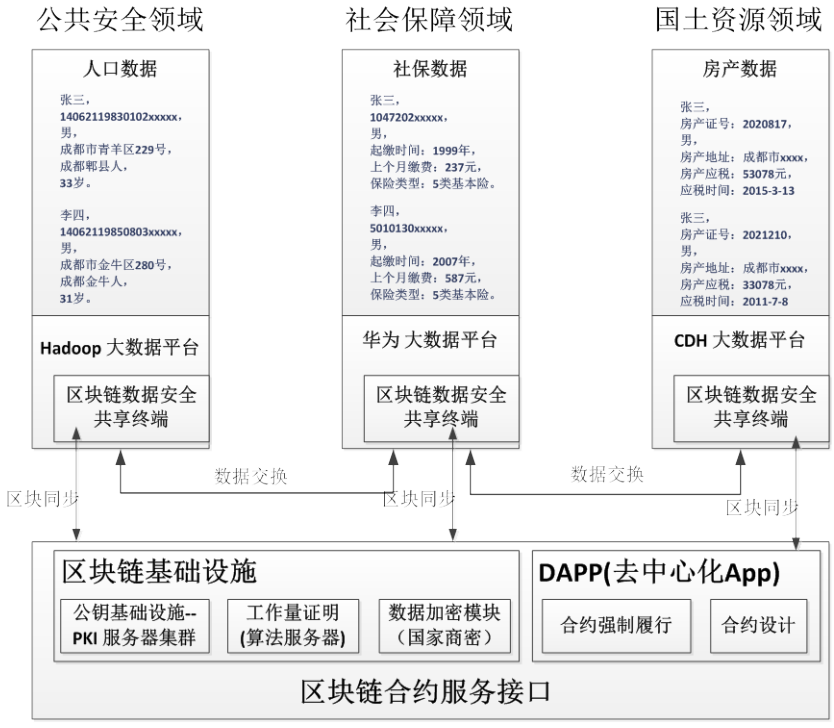

图 5 多方参与的主权区块链生态体系运行逻辑

通过区块链共享资源的首要任务是在云计算基础上形成安全可控的合约，鉴于合约涉及的法律范围不同，可形成例如“政

府各职能部门采用联盟链”、“政府公众服务平台与民众之间采用公共链”、“公安政法等涉密体系采用私有链”的混合区块链结构，进行应用链的发展与推广。

4.1.1. 自由可扩展的区块链记账系统

用于实现“A 单位向 B 单位资源共享”过程的记录，资源包括了多维世界的描述，其采用以下方式进行记录：

1）“资源共享源账号、资源共享目的账号”加密记录；

2）数据分组后进行 HASH 加密记录；

3）时间戳记录；

4）以 1 次“资源共享行为”作为 1 个事务，保证在事务开始和结束之间，参与方的身份是经过认证和授权的。

这种记账方式具有更加快速的数据记录能力，可以保障以下要点：

1）在数据和物质资产共享过程中，公共服务平台具有绝对的公信力；

2）政府对于数据和物质资产共享的过程具有“监管能力”，可以量化谁在进行数据共享、谁在使用数据、谁又将数据的价值发掘了出来。

3）整个事件具有密码学的理论依据，可作为具有法律效力的电子证据，具有存证取证能力。

4.1.2. 主权区块链智能合约设计

主权区块链生态体系中的资源共享智能合约是能够自动执行资源共享约定的可执行脚本。以政务数据共享开放为例，首先制定一套“数据共享开放合约条款”的计算机程序，该程序一直监视一个预先编好的条件是否被触发，智能合约将会执行相应的合同条款。

本系统将重点基于大数据管控技术来实现该智能合约的设计，按照《贵州大数据交易契约》规定的“数据安全防范公约”，其中具有以下重要的 2 项：

1）数据使用必须是联盟成员；

2）不允许私自传播交易数据。

以上 2 项重要公约不能光凭法律来保障，而是重点通过主权区块链智能合约来形成。其中智能合约部分将重点置于“数据安全管理”智能代理当中，用于在合适的时机拦截数据或者取回数据，而具有公信力的记账平台则重点是采用目前的区块链技术即可实现。

4.1.3. 安全监管智能合约支撑

安全监管智能合约中将实现三个子系统：数据认证授权合约、数据安全访问审计合约、数据平台下敏感数据泄露防护合约与代理组件，其各自的业务能力描述如下：

（1）数据认证授权合约

通过松耦合方式向多种 Hadoop 平台（如 Apache Hadoop、Cloudera Distribution Hadoop 及其他第 3 方定制的 Hadoop 平台）提供大数据认证授权管控能力，用于限制第 3 方应用向大数据平台的无认证授权访问，保障基本的大数据平台安全访问能力。

（2）数据安全访问审计合约

对大数据平台（Hadoop 及其他数据库）提供大数据平台用户（数据使用者）的访问过滤、访问异常分析审计等监测功能，满足管理员及时发现大数据平台中可能存在的安全风险点以及应用攻击行为的需求，强化应用安全管控，保证数据访问服务正常、安全、有序地进行。

（3）数据平台下敏感数据泄露防护合约与代理组件

基于对通信行业中涉及政府数据、个人用户、业务数据中敏感字段进行分类、分级处理结果，形成具有自动化的数据分类分级管理能力；基于敏感数据自动化检测与发现技术，实现对用户数据请求的返回结果的隐私保护处理；基于多形态和多业务需求的脱敏函数库，形成对涉及敏感数据威胁的数据集进行基于硬件级高速动/静态脱敏能力。

4.1.4. 资源共享的度量值设计

资源共享的度量值（下简称 GDTP-Value）将重点放在实物

或数据共享阶段的价值度量（Value）设计上，仍以政务数据共享为例，共享数据不是盲目的将数据接口提供给乙方，其共享安全过程中涉及以下要素：

- 共享前的数据用途；
- 共享过程中的容量；
- 共享后的业务效益；

综合以上 3 项不难发现，衡量以上 3 项在不同的政务数据共享业务场景中共享能力度量，只有使用资源共享的度量值（GDTP-Value）来实现；在支付领域，区块链系统通过代币来完成数字资产全自动移转，实现了非人工参与的打款行为；而 GDTP- Value 将实现自动化的物质资产合法转移。

GDTP-Value 的运行机制包括了 GDTP-Value 的防伪、公信力、表征对象（即共享的特定数据或实物）、以及为了促进数据良性共享而形成的激励机制。

良性的数据共享生态所对应的 GDTP-Value 应该满足：

1）良性的政务数据业务应用机构，将拥有更多的 GDTP-Coin，也将拥有更多的数据共享容量；——举例：A 机构的 GDTP-Coin 体量较大，将可以一次性申请大量政务数据；而 B 机构是新进入大数据领域的机构，则第 1 次所能申请的仅为少量样例数据。

2）其每次共享后的数据，随着数据引用次数及价值升值，可以不断提升 GDTP-Value；——举例：上述 A 机构通过一次民

生工程，将政务数据应用不断取得业绩，则其 GDTP-Value 将会按一定规律增加。

3）对于特定鼓励用途的业务，政务数据的申请与使用，可以获得额外的 GDTP-Value 补助。

4.1.5. 自主、可控的数据资产交易规范

目前，数据交易呈现“百花齐放”的局面，各种类型的数据资产，如虚拟货币、数字版权等如雨后春笋般不断涌现。然而，巨额的数据交易的背后，也暴露出一些严重的安全隐患。目前，传统的数据资产安全管理技术主要依赖可信第三方的支持，在开放互联的网络空间中使用受限，并且缺乏对数字资产的访问和使用过程的有效控制，频发出现非法使用数据资产等问题。

为了解决上述问题，主权区块链强调在尊重网络主权和国家主权的前提下，同时具备：可监管、分散多中心、和谐包容的共识算法和规则体系等特点，进行自主和可控的数据资产交易。具体包括：构建涵盖数据资产全生命周期的安全管理与交易模型，形成具有自主知识产权的数据资产安全管理和交易技术，实现虚拟货币、数字版权、游戏装备和网络域名等数据资产的安全存储、交易和追踪溯源，系统性地奠定数字资产的自主、可控和安全的管理和交易的方法。

4.2. 技术指标

- 主权区块链硬件基础设施管理规范

该指标用于描述由区块链账本中心负责运营管理的基础硬件平台的运维规范，形成对主权区块链基础平台的硬件、软件、网络、数据 I/O 的管理能力。

- 参与节点集群管理规范

由区块链账本中心负责运营管理，各建设公司应负责由各企业、志愿者节点参与的网络平台的接入、运营、监管等规范，重点对全民参与的区块链节点网络进行实时监管能力。

- 主权区块链调度技术规范

实现基于 POS 的共识算法来保障记账权的公信力及主权化的调度引擎和管理平台的相应技术规范。

- 区块链记账技术指标

该区块链记账能力，应可以实现物质数字化记账功能和数据 2 次描述（元数据）记账能力。尤其是针对数据的 meta data 则通过“数据名、类型、内容摘要、数据流通量、数据敏感度、数据价值标定”等指标对“流动的数据”进行记账的能力实现。

- 数据区块链支撑能力指标

应可以解决区块链记账过程中的加密、签名、密钥协商、摘要算法等部分的中国国家标准（SM 国密标准），以保证国家大数据区块链基础设施的安全。

- 数据隐私保护与防泄露指标

应可以解决基于区块链的数据交换过程中的可控共享，保障数据在数据导入、数据流通、数据分析、数据导出等阶段可能存在的泄露问题，实施数据防护功能以确保数据流通过程中不会发生“数据脱链”事件。

5. 建设方式

围绕区块链的主要建设目标，拟进行包括不限于以下内容的快速建设：区块链典型应用对接、区块链商业模式成功运营和推广等后续 2 个阶段的主权区块链行业应用。保障贵阳主权区块链生态体系从原型、产品、应用、商业化运作的全过程建设，有效形成由政府扶持、企业牵头、行业锻造、商业推广的区块链大平台。

5.1. 数据区块链典型应用对接

首先应建立数据区块链基础设施，从破解数据资源流通与安全保护难题入手加快推动大数据发展，构建一套经济社会发展以及人们生产生活各类活动的新的诚信体系、价值体系、秩序规则体系。

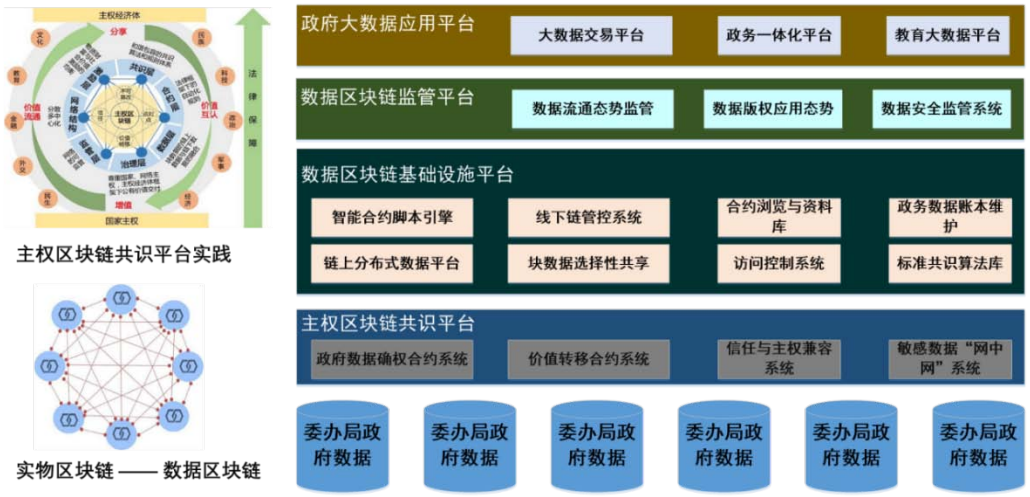

图 6 数据区块链架构设计

在该对接过程中，平台应用主要采用直接基于区块链服务接口进行 App 研发方式，主要流程为“接入区块链基础平台 → 设置智能合约脚本（类 solidity 脚本）→ 设置区块链安全脚本（类 python 脚本） → 自定义可视化”。

最终建立一整套面向政府大数据共享与开放业务的区块链基础设施典型应用，并达到以下平台指标，

（1）参与政府数据共享开放的各方都可在所属权限内使用数据，同时受大数据监管智能合约的约束；

（2）建立追溯与举证维权机制，保障数据不会轻易流失到其他领域；

（3）获得政府数据的第三方社会机构，将产生更大的数据应用价值。为获取更多新的政府数据，第三方社会机构也会积极拓展更多的数据应用方向，公开政府数据的应用价值，保证块数据资源源源不断的向贵阳汇聚。

（4）在国家网络安全法框架下，提供区块链维权与举证的法律保障。

（5）区块链的记账系统内容应通过法律权威部门鉴定，形成具有法律依据的电子证据；对于“使用数据、数据付费、数据资产评估、数据权属、数据溯源与追责”等方面形成支撑性电子凭证。

5.2. 区块链商业模式成功运营和推广阶段

这个过程主要基于区块链记账服务、存证取证服务、审计溯源服务、真伪辨识、支付、物质资产化与转移业务、数字资产化与转移业务等服务，对不同行业进行区块链合约制定、快速部署与运营管理。

对于采用公私链对接到主权区块链生态体系的方式，采用双向锚定（Two Way Peg）使得 主权区块链生态体系中的主链（Main Chain）与其他行业区块链应用的侧链（Side Chain）相互连通，连通后可实现“实物资产或数据资产交换”过程中的信用共享、支付相互承认的目的。

6. 实施要素

贵阳主权区块链生态体系与传统区块链系统的差异性，因此总体的建设过程通过主权区块链生态体系的研究，可以达到“辐

射 N 类数据区块链应用”的目标，即将本研究成果做为“数据与物质类型区块记账方案”的基础设施标准进行实施建设。

贵阳区块链发展是围绕数字经济、互联网治理和大数据发展中的价值实现，建立区块链在政用、民用和商用的应用场景，并培育和发展主权区块链系统的应用层、合约层、激励层、共识层、数据层和网络层，进一步发展区块链产业生态和商业模式，建设区块链发展和应用特区，组建区块链联盟，构建区块链等发展支持体系。

总体的建设过程重点依照“主权区块链”的构建模式进行，主权区块链的技术系统由自下而上的网络层、数据层、共识层、激励层、合约层和应用层组成。

- 网络层。基于点对点组网机制、数据传播机制和数据验证机制等,推进分散多中心的网络节点间形成主权区块链，与操作系统、网络、存储、计算等资源共同提供基础设施云服务,并提供网络主权下多节点的身份认证和管理。在区块链应用场景间形成链间通信网络，建立底层构架的交互协议。
- 数据层。基于贵阳块数据平台，建立主权区块链上的分布式加密数据库,并与块数据共享和开放平台实现对接，推进链上和链下相融合的大数据分析。
- 共识层。基于主权区块链的和谐包容的共识算法和规则体系，整合区块链的各类共识机制算法，包括工作量证明机制

（PoW，Proof of Work）、权益证明机制（PoS，Proof of Stake）股份授权证明机制（DPoS，Delegated Proof of Stake）、拜占庭容错算法机制等。共识机制算法是区块链的核心技术，是区块链系统中各个节点达成一致的策略和方法，应根据系统类型和应用场景的不同灵活选取。

- 激励层。将价值度量衡、钱包、账户等集成到主权区块链技术体系中来，建立经济和社会价值激励的发行机制和分配机制等，推进激励行为的可管理。在主权区块链中，必须激励遵守规则参与记账的节点，并惩罚不遵守规则的节点，才能让整个系统朝着良性循环的方向发展。

- 合约层。集成各类脚本、算法和智能合约，建立可监管、可审计的合约形式化规范，是主权区块链可编程特性的基础，

- 应用层。封装主权区块链的各种应用场景和案例，包括政用、民用和商用多场景交织的应用模式。

设立基于主权区块链的政府数据共享开放网络模型，根据数据载体、数据受体、数据拥有者三方的敏感程度，构建政府各职能部门的联盟链、政府面向民众的公有链和公安政法等涉密体系的私有链，形成政府数据共享开放的区块链“绳网”结构，打造可信的政府数据共享开放平台，保障政府各职能部门之间的数据共享开放安全，解决大数据关联风险。一是建立身份公信力系统，对数据的共享、开放、获取与使用的主体及其行为进行权威记录

和公信力评价。二是建立联盟业务公信力支撑系统，并与身份公信力系统组成大数据应用安全机制。三是形成数据共享开放的应用成果监管平台，构建由数据的使用者、数据价值输出、数据价值分配共同带动的基础产业转型态势系统。

7. 联盟现有典型应用

7.1. 仓储/供应链/物流领域应用

仓储区块链应用方面，联盟单位重点围绕仓单监管、货权转移进行仓储区块链应用平台的研发，具体围绕钢卷业务开展区块链应用场景设计和实施，建立钢卷在仓储环节中的区块链存储模型，同时保障物资在出库、入库、货权转移等方面的业务逻辑的可信、不可抵赖，形成钢卷仓储业务的区块链典型示范性系统，并计划在后期围绕仓储链，打通生产链、物流链、金融链，实现传统行业 DT 转型，发展和支持新的业务需求。

7.2. 医疗领域的应用

区块链技术重点围绕医疗数据记录和身份管理，将所有医疗平台的重要数据连接到一起，保证了数据的有效性和安全性。基于区块链技术的医疗减少换诊医疗错误，并保护病人隐私。对于医疗行业而言，这使得医院、保险公司等能够实时连接并且即时无缝分享信息。

7.3. 数据交易领域的应用

联盟单位国信优易正在搭建一个完善的基于区块链的数据交易平台，它包含了五大功能：数据增值转换通道：分类、定价、计费、交易规则、结算；多方用户开发：源方、需求方、加工服务商、应用服务商、中介服务商;数据交付开放：API、数据包、在线；流程化运营：需求受理、定制管理、数据登记、数据交割；权益保护：合规检查、确权、追溯、取证；平台把数据产品放到链上，变成数字资产，且具有唯一性，不可篡改、不可复制，不能被双花，在交易环节进行流通转移，在价值转移的同时完成清算、对账和记账，产品供应链参与企业可以在链上，自由地进行信息传输与价值增量交易。

8. 蓝皮书修订过程

修订时间	进展及相关内容
2017-2-5 至 2017-2-22	完成了主权区块链项目实施方案的顶层设计部分
2017-2-22 至 2017-3-1	完成了《技术蓝皮书》的总体框架，明确了基于主权区块链业务需求部分
2017-3-1 至 2017-3-8	完成了主权区块链商业模式整体设计部分
2017-3-8 至 2017-3-15	搭建主权区块链分布式网络环境，完成基本的记账功能
2017-3-15 至 2017-4-24	完成了主权区块链系统记账节点管理指标要求部分，满足政府数据的部门主权管控需求
2017-3-24 至 2017-4-10	完成了账户管理部分指标，将身份信息加密后置

	于链上保护用户隐私等部分
2017-4-10 至 2017-4-20	完成了数据共享、测试数据上架、数据价值、使用流程等部分
2017-4-20 至 2017-5-2	完成了电子合同指标部分，明确电子合同可生产智能合约，技术上保护数据双方的权益等问题
2017-5-2 至 2017-5-12	完成了主权区块链对接方式部分，包括在测试环境中进行内测、用例测试、压力测试等工作内容
2017-5-12 至 2017-5-25	完成本技术蓝皮书发布稿