ICS
CCS 点击此处添加 CCS 号

DB4401

广　州　市　地　方　标　准

DB 4401/T ××××—××××

政务区块链跨链数据格式规范

Cross chain data format specification for government blockchain

（征求意见稿）

××××－××－××发布　　××××－××－××实施

广州市市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广州市政务服务和数据管理局提出并组织实施。

本文件由广州市政务服务和数据管理局归口。

本文件起草单位：广州市区块链产业协会、xxx、xxx。

本文件主要起草人：xxxx。

本文件为首次发布。

政务区块链跨链数据格式规范

1 范围

本文件规定了政务区块链跨链数据格式规范，具体规定了以下内容：

a）政务区块链的跨链数据结构；

b）政务区块链的跨链数据分类及其相互关系；

c）政务区块链的跨链数据元的数据格式要求。

本文件适用于：

a）为计划使用政务区块链跨链系统的组织提供数据格式参考；

b）指导政务区块链跨链服务组织提供跨链数据结构；

c）为政务区块链跨链系统建设过程的中间件服务组织提供数据格式参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 30850.4-2017 电子政务标准化指南 第4部分：信息共享

GB/T 39044-2020 政务服务平台接入规范

GB/T 39047-2020 政务服务平台基本功能规范

GB/T 43572-2023 区块链和分布式记账技术 术语

GB/T 42752-2023 区块链和分布式记账技术 参考架构

T/CESA 6002—2017 《区块链 数据格式规范》

T/CESA 1128—2020 《区块链电子签章 参考架构》

T/SIA 007—2018 《区块链平台基础技术要求》

W3C UDDIv2《数据结构规范》

3 术语和定义

下列术语和定义适用于本文件。

3.1 跨链

通过一定的技术措施实现相对独立的不同区块链系统之间数据和资产的链接互通。

3.2 跨链事务管理

基于区块链来管理一笔交易在多个不同链之间的执行状态，以确保数据处理的一致性。

3.3 跨链身份管理

基于区块链为上层应用提供可信身份服务。

3.4 应用链

允许Scala的开发和基于分布的分散的应用程序使用一个易于使用的，功能齐全的生态系统。

4 跨链数据分类

政务区块链的跨链数据分为以下两类：

a）跨链身份数据：指描述政务区块链事务的发起者、接收者等相关方的数据。

b）跨链事务数据：指描述政务区块链系统上承载的具体业务过程的数据。

5 跨链数据元属性

政务区块链的跨链数据元通过数据标识符、中文名称、英文名称、数据类型、数据长度、数据说明、数据备注7个属性来描述。具体属性说明见表1。

表 1 政务区块链的跨链数据元属性表

属性名称	属性说明
数据标识符	各跨链数据元的唯一标识，编号是以阶层式分类。
中文名称	跨链数据元的中文名称，在一定语境下名称应保持唯一。
英文名称	跨链数据元的英文名称，在一定语境下名称应保持唯一。
数据类型	描述跨链数据元的特征和基本要素，主要包括：字符串类型、整数类型、数组类型。
数据长度	描述该跨链数据元的长度，用定长或不定长表示，并给出了推荐字节长度。
数据说明	详细描述该跨链数据元的内容和表达的含义。

6 跨链身份数据格式规范

6.1 跨链身份数据分类

跨链身份数据主要包括以下五种类型数据元：

a）账户公钥；

b）账户私钥

c）账户资产；

d）数字证书；

e）账户所属机构。

6.2 账户公钥

账户公钥的数据格式要求见表2。

表2 账户公钥数据格式

属性	内容
中文名称	账户公钥
英文名称	Account Public Key

数据类型	字符串
数据长度	定长，推荐64字节
数据说明	根据PKI体系为用户生成的密钥对里，可公开的部分。
数据备注	必选

6.3 账户私钥

账户私钥的数据格式要求见表3。

表3 账户私钥数据格式

属性	内容
中文名称	账户私钥
英文名称	Account Private Key
数据类型	字符串
数据长度	定长，推荐32字节
数据说明	根据PKI体系为用户生成的密钥对里，不公开的部分。
数据备注	必选

6.4 账户资产

账户资产的数据格式要求见表4。

表4 账户资产数据格式

属性	内容
中文名称	账户资产
英文名称	Account Asset
数据类型	数组
数据长度	不定长
数据说明	账户拥有的资产说明，包括资产名称，资产列表，余额等。
数据备注	可选

6.5 数字证书

数字证书的数据格式要求见表5。

表5 数字证书数据格式

属性	内容
中文名称	数字证书
英文名称	Digital Certificate
数据类型	数组
数据长度	不定长
数据说明	数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。
数据备注	可选

6.6 账户所属机构

账户所属机构的数据格式要求见表6。

表6 数字证书数据格式

属性	内容
中文名称	账户所属机构
英文名称	Institution
数据类型	数组
数据长度	不定长
数据说明	机构为加入到政务区块链网络的成员，账户可以在组织关系上归属于某个机构。
数据备注	可选

7 跨链事务数据格式

7.1 跨链事务数据分类

跨链事务数据主要包括以下四种类型数据元：

a）事务标识；

b）事务类型；

c）签名者；

d）事务时间戳。

7.2 事务标识

事务标识的数据格式要求见表7。

表7 事务标识数据格式

属性	内容
中文名称	事务标识
英文名称	Transaction ID
数据类型	字符串
数据长度	定长
数据说明	事务处理中，可保证事务数据的唯一标识，通常为哈希值。
数据备注	必选

7.3 事务类型

事务类型的数据格式要求见表8。

表8 事务类型数据格式

属性	内容
中文名称	事务类型
英文名称	Transaction Type
数据类型	字符串或整数
数据长度	定长
数据说明	进行事务操作时，定义事务操作的事件类型，可以有一或多种类型。

数据备注	可选

7.4 签名者

签名者的数据格式要求见表9。

表9 签名者数据格式

属性	内容
中文名称	签名者
英文名称	Signers
数据类型	字符串
数据长度	定长
数据说明	进行事务操作时，对事务进行签名的签名者的集合。
数据备注	可选

7.5 事务时间戳

事务时间戳的数据格式要求见表10。

表10 事务时间戳数据格式

属性	内容
中文名称	事务时间戳
英文名称	Transaction Timestamp
数据类型	整数
数据长度	32字节
数据说明	正整数，从1970年起的时间计数，精度为毫秒，正序增加。
数据备注	可选

8 政务区块链跨链技术要求

8.1 通用要求

8.1.1 安全可靠

政务区块链的跨链系统应实现不同智能合约之间的数据隔离；应保障不同智能合约的业务数据彼此独立，不应直接访问其他合约的数据；应经过外部权威机构的测试和认证。

8.1.2 快捷便利

政务区块链的跨链系统应具备完善的说明文档，如API接口、数据协同的流程和协议等。

8.1.3 可扩展性

政务区块链的跨链系统的文本类型数据，应符合GB/T 18030《信息技术 中文编码字符集》要求；日期和时间类型数据，应符合GB/T 7408—2005《数据元和交换格式 信息交换 日期和实践表示法》要求。

8.1.4 互操作性

政务区块链的跨链系统应支持外部应用或其他区块链产品便捷实现区块链互访功能。

8.1.5 可审计性

政务区块链的跨链系统应支持生成单独的持久化日志，区分于产品其他日志信息，记录调用的关键信息，如调用结果、时间戳等，能够满足审计要求。

8.2 跨链系统架构

政务区块链跨链系统架构应采用分层的结构，即满足层级化的管理方式，也具备更高的扩展性。

政务区块链跨链系统主要涵盖应用层与治理层，见图 1。

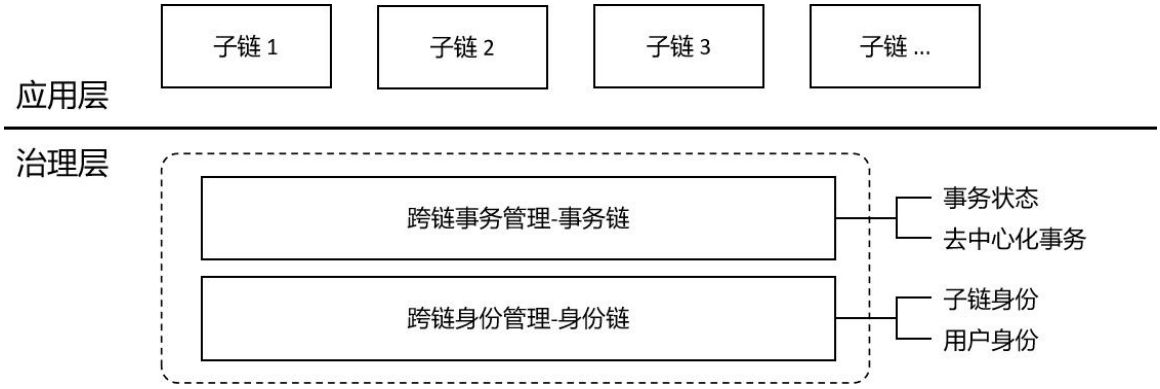

图 1 政务区块链跨链系统架构

政务区块链跨链系统的应用层，应支持构建大量平行的应用子链，支持应用子链构建有不同的业务、不同的区块链平台。其中，子链聚焦于区块链应用，并提供相关的 API。

政务区块链跨链系统的治理层，应具备应用层子链的跨链协作与数据流通的支撑能力，其功能涵盖跨链事务管理与跨链身份管理两部分。

8.3 跨链关键过程

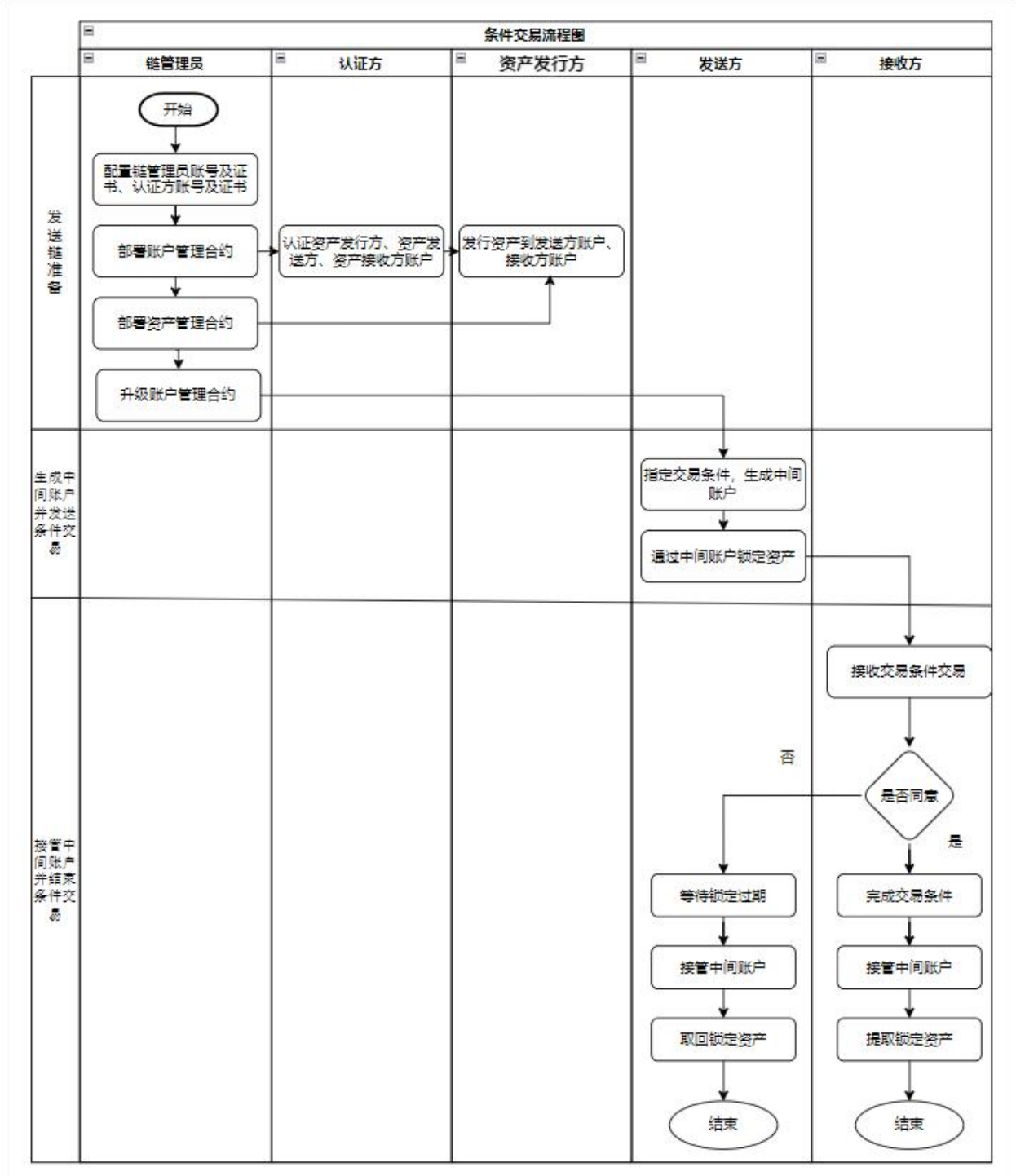

图 2 政务区块链跨链关键过程

应采用一种无需改造目标链的跨链事务处理机制，通过条件交易实现原子性事务，确保操作要么全部成功，要么全部失败。机制通过建立中间账户和增加新合约方法，避免跨合约调用风险，保障合约安全。主要流程包括三个阶段：发送链准备、生成中间账户并发送条件交易、接管中间账户并结束条件交易。

1.发送链准备阶段

配置链管理员、认证方账户及证书。
部署账户管理合约，提供账户认证、证书绑定方法，仅认证方可调用。
部署资产管理合约，提供资产发行和转移方法，仅授权账户可调用。
认证方通过签名交易认证并注册资产发行方、发送方、接收方账户，并绑定证书。
资产发行方通过签名交易发行资产到发送方和接收方账户。
管理员升级账户管理合约，增加中间账户建立、证书绑定方法。

2.生成中间账户并发送条件交易
发送方通过签名交易调用合约方法生成中间账户。
发送方将资产转移至中间账户，中间账户未绑定证书，资产处于锁定状态。
发送方可重复向中间账户锁定多笔资产。

3.接管中间账户并结束条件交易
接收方根据出块数据和支付条件决定是否满足条件。
若满足条件，接收方通过签名交易绑定中间账户证书，将资产转出，完成支付。
若不满足条件，接收方未采取行动或过期时间到，发送方通过签名交易将中间账户证书绑定到发送方，资产回滚。

8.4 跨链数据验证

政务区块链通过跨链技术对接多条主流联盟链，依据跨链路由定义，确定目标链合法性验证规则，进一步调用跨链适配器，实现对跨链数据的合法性验证。

跨链网关负责对跨链数据进行验证，待验证的数据包括区块数据、交易数据。跨链网关依据跨链路由定义，确定目标链的类型及对应的合法性验证规则，进一步调用跨链适配器，实现对跨链数据的合法性验证。

a）当条件支付交易在来源链出块，目标链验证用于互换的资产是否被锁定。——即目标链通过跨链网关，验证发起跨链互操作的来源链上的锁定操作是否有效，也即验证调用该锁定操作的签名交易是否有效。跨链网关依据跨链路由配置，确定来源链类型，进一步调用对应类型的适配器，依据来源链合法性验证规则返回验证结果。

b）如果目标链上目标账户同意互换，并执行了预期条件，来源链验证该交易是否已经在目标链出块。——即来源链通过跨链网关，验证执行互换操作的目标链上的操作是否有效，即验证调用用于互换的操作的目标链签名交易是否有效。跨链网关依据跨链路由配置，确定目标链类型，进一步调用对应类型的适配器，依据目标链合法性验证规则返回验证结果。