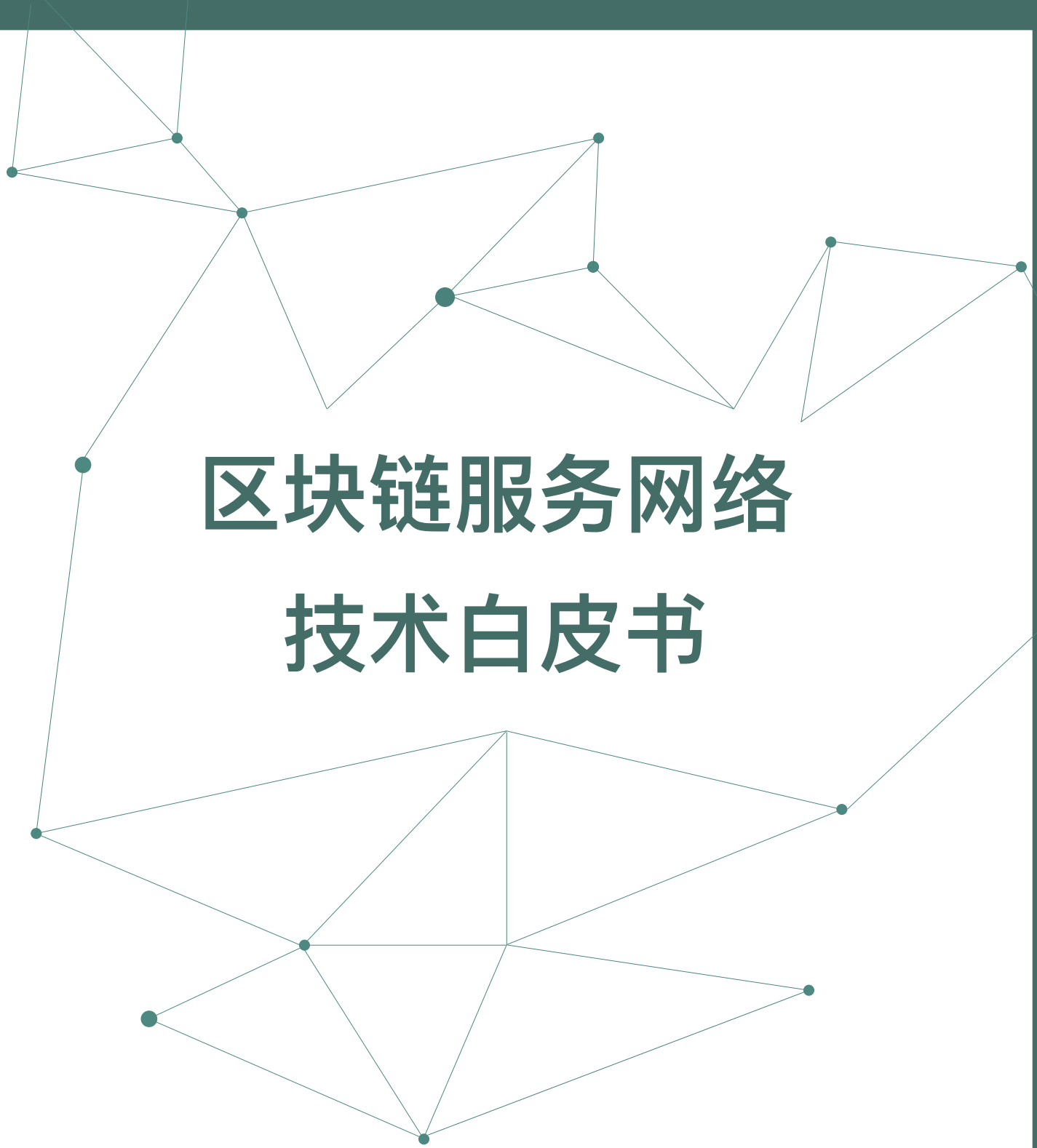

区块链服务网络
技术白皮书

区块链服务网络发展联盟
二〇二〇年四月

目录 CONTEXT

白皮书撰写参与单位

序号	单位名称
1	国家信息中心信息化和产业发展部
2	中国移动通信集团设计院有限公司
3	中国银联电子支付研究院
4	北京红枣科技有限公司

注：本白皮书最后更新时间为 2020 年 4 月 25 日，版本号 1.0.0。

第一章 目 的

本白皮书主要用来解释区块链服务网络（以下简称为“服务网络”或“BSN”）的核心技术特点，对已在《区块链服务网络基础白皮书》中涉及的内容将不再重复。

从设计到建设的整个过程中，服务网络的核心理念始终是建立一个对标互联网的区块链公共基础环境，并提供整合了云资源、底层框架、运行环境、密钥管理、开发 SDK 和网关 API 的一站式区块链部署和运行服务。开发者可以以极低的成本在服务网络上便捷地部署和运行区块链和分布式账本应用（以下简称为“应用链”），并且不论底层是否异构，服务网络上所有的应用链均可以进行数据交互，带来类似互联网上快速搭建网站并高效互联互通的优质体验。

本白皮书将会根据服务网络的技术迭代进行持续更新。目前版本主要对服务网络的公共城市节点、数据安全以及 BSN 赋能平台三个方面进行介绍。

第二章 公共城市节点

公共城市节点（以下简称为“城市节点”、“Public City Node”或“PCN”）是组成服务网络的基本组织单元。该名称中的节点很容易与区块链中的节点混淆。因此特别强调，公共城市节点并不是一个区块链节点，而服务网络本身也并不是一条链。公共城市节点实际上是一个资源池，用于将其所部署的云服务和数据中心内的一部分计算力（CPU）、存储和流量资源接入到服务网络内。在这个资源池内建有完整的区块链运行环境，包括多个区块链底层框架、记账节点、CA 管理、权限链、城市节点网关和城市节点管理系统等。开发者可以通过任何一个 BSN 门户部署自己的应用链，具体过程为：选择区块链底层技术框架编写并上传智能合约，选择部署应用链的一个或多个公共城市节点，选择每个城市节点内部署的记账节点数，点击发布。应用链的智能合约通过安全检查后，将由服务网路的运维中心自动部署到开发者已选定的公共城市节点内的记账节点并开始运行。开发者的链下业务系统通过连接任何一个部署了应用链的城市节点的网关，实现与相关应用链的数据交互。公共城市节点主要包含以下功能模块：

1. 多底层框架

服务网络的核心理念之一是支持尽量多的区块链底层框架。目前区块链技术还处在早期阶段，我们希望能够通过服务网络为所有底层框架建立一个良性发展和公平竞争的环境，促进底层框架方持续推动区块链底层技术发展，不断提升服务品质。在每个城市节点内，所有已经适配到服务网络的框架均会作为基础系统进行安装。同时，多个框架并不是简单地堆砌在一起，而是根据《区块链服务网络底层框架适配标

准》，在密钥算法、CA 管理、接入 SDK 和智能合约管理等方面实现了统一。使得开发者可以使用一个私钥发布和管理多个底层异构的应用链并实现应用链之间的互联互通。在这一过程中，每个底层框架将保留具有各自特点的智能合约和共识机制。

2. 记账节点

针对已适配的底层框架，每个城市节点均部署了一组对应的记账节点，通过各框架自身所带的通道、群组或子链机制，让每个记账节点可以服务多个应用链，在确保每个应用链的交易处理、智能合约和账本数据与其他应用链完全隔离的同时，所有应用链共享系统资源。同时，可实现开发者按照低至 10TPS（Transactions Per Second）在服务网络上按需购买资源，在服务网络部署应用链的最低成本仅为传统区块链云服务成本的几十分之一。

3. 权限链

权限链作为系统底层管理链部署在所有城市节点内。权限链内存储了用户的应用接入密钥(公钥)和应用的权限配置。当用户链下业务系统接入城市节点网关时，网关会对用户的身份进行校验，仅允许用户访问拥有授权的应用链，并按照应用链的权限配置调用相应的智能合约方法。

4.CA 管理

每个公共城市节点均部署了服务网络统一的CA管理系统，用于该城市节点内所有应用链用户交易密钥的全生命周期管理，包括：生成、发放、更新和吊销等。用户交易密钥用于用户接入应用链时对数据的加密和签名。用户交易密钥和应用接入密钥的生成和管理方式详见第三章数据安全。

5. 城市节点网关

城市节点网关是服务网络以外的业务系统与服务网络内

部署的应用链发生数据交互的唯一入口。每个城市节点都有网关，用户可以选择任何一个应用链部署的城市节点接入，但建议根据就近原则进行选择。城市节点网关除了对用户身份进行验证外，还具有交易鉴权、交易路由、限流控制、负载均衡、网关 API 和 SDK 等功能。

6. 城市节点管理

城市节点管理系统是负责城市节点与服务网络运维中心进行连接的功能模块。运维中心从各个 BSN 门户接到指令后，通过节点管理系统在每个城市节点进行管理应用链、部署智能合约、配置记账节点、管理密钥证书、设置应用权限和获取运行信息等操作。

服务网络本身并不是一个链，不会出现公有链面临的运行效率问题。在服务网络部署的每个应用链的交易性能取决于部署的记账节点数量、使用的底层框架类型、选择的城市节点数量以及这些城市节点之间的公网距离。例如：在同一城市节点部署 3 个记账节点的应用链，其运行效率将明显高于在 20 个城市节点部署 30 个记账节点的应用链。服务网络是一个区块链公网化的体系，节点之间的互联网传输速度是决定应用链效率的重要因素。另外，我们建议单个应用链在服务网络上部署的记账节点数不要超过 40 个。

目前开发者可以在任何 BSN 门户内自行发布不超过 500TPS 的应用链。如果需要更高 TPS，需要联系服务网路的运维人员进行定制化部署。对绝大多数联盟链和分布式账本应用来说，500TPS 足以满足业务需求。

当一个公共城市节点内的资源使用量达到饱和时，服务网络运维中心将停止在其上部署新的应用链。云服务商可以根据业务需求及时提高配置，为城市节点增加新的资源。理论上，一个城市节点内的资源池可以无限扩大。

第三章 数据安全

区块链和分布式账本是基于密钥证书体系的技术，本身的安全性就比较高。在服务网络的底层设计中，数据安全和用户隐私保护的优先级是最高的。开发者在使用服务网络的过程中，几乎每个环节都有数据安全的支撑机制。服务网络提供一套比较复杂的密钥管理和权限设置功能，开发者可以根据自己应用链的具体需求进行自由组合，形成适合自己的数据安全体系。以下是服务网络提供的安全机制的具体内容:

1. 服务网络在开发者手册内反复提醒开发者：在将链下系统的数据上传至应用链前，最好能够对数据进行加密。如果开发者使用服务网络 SDK，我们在 SDK 内提供了若干种加密机制和建议，供开发者选择使用。

2. 开发者在任何 BSN 门户内发布一个应用链时，有两种应用接入密钥模式可供选择: 密钥托管模式或上传公钥模式。密钥托管模式是用户委托服务网络生成密钥，由用户在 BSN 门户内下载后使用。上传公钥模式是由应用链用户在本地生成密钥，再将公钥通过 BSN 门户上传，然后使用私钥进行交易签名连接城市节点网关，完成应用的接入鉴权。密钥托管模式比较方便，但上传公钥模式更自主化，具体使用哪种模式完全由开发者自行选择设定。

3. 对已经发布的应用链，开发者在设置用户交易密钥时，可以为整个应用链设置一个统一的密钥，供所有接入用户使用，也可以为每个用户设置单独的用户交易密钥。密钥设置的模式也分为密钥托管模式和上传公钥模式。与应用接入密

钥不同的是，城市节点网关提供了用户交易密钥的管理接口，不需要开发者和用户在 BSN 门户内另行设置。

4. 开发者在发布应用链的智能合约时，可以将智能合约内的方法自由组合成各类角色，每个角色拥有调用一个或多个方法的权限，例如：有些角色可以写入数据，有些角色只能查询数据。当用户加入应用链时，可以被分配一个或多个角色。这些角色和对应的权限信息存在于权限链内。当用户的业务系统通过网关接入该应用链时，只能执行所分配角色允许执行的功能和数据权限。

5. 开发者可以在智能合约的编写上进一步控制交易和数据处理。即使两个用户拥有同一个角色的权限，也可以在智能合约代码层面定义这两个用户可以查询和执行不同的数据交易操作。

以上五种机制在应用链数据安全方面形成服务网络的完整体系，既保证了数据的绝对安全，又让开发者有足够的空间根据业务需求设计自己应用链的安全机制。特别是使用上传公钥模式时，安全等级可达到比特币钱包的级别，除了开发者和授权用户外，没有任何人可以接触到应用链上的业务数据。

第四章　BSN 赋能平台

服务网络的具体运维管理是由运维中心平台（以下简称为“运维中心”）统一负责。如需在服务网络上发布和管理应用链，所有的 BSN 门户和其他前端服务均需要在自己的系统内安装 BSN 赋能平台，通过赋能平台与运维中心通信，并由运维中心执行各 BSN 门户发送过来的相关指令。赋能平台主要包括服务网络对外提供的所有核心管理接口。下面是所有接口的简单分类和功能说明：

接口类型	接口数量	功能说明
城市节点管理	4	用于获取区块链公共城市节点信息、城市节点上资源价格信息等
服务框架管理	2	用于获取底层框架信息，包括各框架关联的可售资源等
服务管理	8	用于实现应用链的发布、升级、启停、卸载、资源配置的升级等操作
服务参与管理	10	用于实现应用链的参与、用户权限和证书密钥的管理
节点运行信息管理	3	用于获取节点运行情况信息，包括相关应用链的运行情况、区块信息等
流量信息	1	用于获取相关应用链的流量使用情况信息

服务网络的官方门户（www.bsnbase.com）也是完全基于 BSN 赋能平台搭建的。除了能够建设 BSN 门户外，赋能平台还能够为众多网站、APP 和 SaaS 服务提供嵌入式区块链应用和数据服务。以文档协作管理网站为例：通过赋能平台，可以在其网站内为用户提供在服务网络上一键生成应用链，并选择哪些共享协作的文件数据自动上链保存的服务。

服务网络非常重视开发者和应用链用户的个人隐私，因此，在服务网络和运维中心内完全不保存任何用户的隐私数据。门户内使用的赋能平台没有个人隐私数据的接口，所有开发者和应用用户的个人信息均由每个 BSN 门户自行管理。在服务网络的运维中心内，只能追溯某个应用链是通过哪个门户发布的以及这个应用链有多少用户，但无法获得应用链开发者和应用链用户的具体信息。

第五章 联系我们

服务网络需要持续地研发和优化，这是一项浩大和繁杂的工程。我们欢迎有经验和有资源的科技公司能够加入服务网络，共同将服务网络打造成真正意义上的区块链互联网。

有兴趣的公司请联系：support@bsnbase.com。