Source Blockchain
根 源 链

根源链·技术白皮书

基于数据信息追溯及确权的泛物联网应用公有链基础设施

版本 v1.0.21

修订日期 2018.6.22

根源链团队

目录

通用术语表

术语/缩略语	英文释义	中文释义
SC	Source Chain	根源链
BOS	Blockchain Operating System	区块链操作系统
SCI	Source Chain Infrastructure	根源链基础设施
PoW	Proof of Work	工作量证明
PBC	Public Block Chain	公有链
LLS	Large Legacy System	大型设施系统
PDL	Protocol Description Language	协议描述语言
IDL	Interface Description Language	接口描述语言
Off-Chain	Out of Block Chain	链下，区块链之外
On-Chain	On the Block Chain	链上，区块链之上
WD	Wallet Driver	钱包驱动器
GW API	Gate Way Application Programming Interface	网关应用程序接口
SDK	Software Development Kit	软件开发包
ASL	Application Service Layer	应用服务层
BSL	Baseline Service Layer	基础服务层
HDL	Hardware Driver Layer	硬件驱动层

SCA	Side Chain Adapter	侧链适配器
2WPP	2 Way Peg Protocol	双向锚定协议
MI	Management Interface	管理接口
AI	Account Interface	账户接口
Hash	Hash	散列，哈希
GPU	Graphics Processing Unit	图形处理单元
OpenCL	Open Computing Language	开放式计算语言
CUDA	Compute Unified Device Architecture	统一计算设施架构
FPGA	Field Programmable Gate Array	现场可编程逻辑门阵列
SCT	Smart Contract Template	智能合约模板
CP	Cryptographic Protocol	加密协议
DCP	Distributed Consensus Protocol	分布式共识协议
MMPP	Miner and Miner Pool Protocol	矿工矿池协议
SCPL	Side Chain Protocol Layer	侧链协议层
SCIL	Side Chain Implementation Layer	侧链实现层
PL	Protocol Layer	协议层
BCL	Block Chain Layer	区块链层
BLL	Business Logic Layer	业务层
CL	Cryptographic Layer	加密层

Compiler	Compiler	编译器
Interpreter	Interpreter	解释器
Key	Key	密钥
Account	Account	账户
Config	Configuration	配置
Monitor	Monitor	监控
DashBoard	DashBoard	仪表盘
SDKPL	SDK Protocol Layer	SDK 协议层
SDKIL	SDK Implementation Layer	SDK 实现层
ASIC	Application Specific Integrated Circuit	专用集成电路
CPU	Central Processing Unit	中央处理单元
ABI	Application Binary Interface	应用二进制接口
Arch	Architecture	架构
x86	x86	x86 硬件架构
MIPS	Microprocessor without Interlocked Pipeline Stages	MIPS 硬件架构
ARM	Acorn RISC Machine	ARM 硬件架构
DES	Data Encryption Standard	数据加密标准
3DES	Triple DES	3 密钥 3 次加密

AES	Advanced Encryption Standard	高级加密标准
RSA	Rivest-Shamir-Adleman	RSA 加密方法
DSA	Digital Signature Algorithm	数字签名算法
ECC	Elliptic Curves Cryptography	椭圆曲线加密学
MD5	Message Digest algorithm 5	单项散列算法 5
SHA	Secure Hash Algorithm	安全哈希算法
scrypt	scrypt	典型：莱特币
scrypt-c	scrypt-cacha	典型：ya 币
ETHASH	Ethereum hash	典型：以太坊
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法 典型：瑞波币
X11	XCurrency 11	典型：达世币
SHA-256	SHA 256	典型：比特币
lyraz2	lyraz2	典型：零币
ECDH	Elliptic Curve Diffie–Hellman key Exchange	椭圆曲线 D-H 密钥交换
SM1	Secret Management 1	国密 1
SM2	Secret Management 2	国密 2
SM3	Secret Management 3	国密 3

SM4	Secret Management 4	国密 4
HMAC	Hash-based Message Authentication Mode	哈希运算消息认证码
AES-CRT	AES Counter	AES 计算器模式
AES-ECB	AES Electronic Codebook Book	AES 电码本模式
AES-CBC	AES Cipher Block Chaining	AES 分组链模式
AES-CFB	AES Cipher FeedBack	AES 密码反馈模式
AES-OFB	AES Output FeedBack	AES 输出反馈模式
DDOS	Distributed Denial of Service	分布式服务拒绝攻击
Stratum	Stratum	Stratum 矿池协议
DAO	Distributed Autonomous Organization	分布式自治组织
DApp	Distributed Application	分布式应用
SCLSR	Source Chain Link State Routing protocol	根源链链路状态路由协议
SCFD	Source Chain Forward Daemon	根源链转发守护进程
SCFace	Source Chain Face	根源链分布式转发接口
IT	Information Table	根源链分布式转发信息存储表
WST	Waiting Sender Table	根源链分布式转发等待发送列表

FIT	Forward Information Table	根源链分布式转发信息询路表
PGP	Pretty Good Privacy	PGP 加密协议
RSK	Root Stock	RSK 合约侧链实现
MAST	Merklized Abstract Syntax Tree	梅克尔抽象语法分析树
CP	Counter Party	对手方合约方法
LN	Lighting Network	闪电网络合约方法
SPV	Simplified Payment Verification	简单支付验证
RSMC	Revocable Sequence Maturity Contract	到期可撤销合约
HTLC	Hashed Timelock Contract	哈希时间锁定合约
SCNC KMS	Source Chain NC Key Management System	根源链分布式密钥管理系统

1 根源链

根源链是一个基于数据信息追溯及确权的泛物联网应用公有链基础设施。

根源链全称为根源链 BOS（Source Chain Blockchain Operating System），一般简称为根源链。根源链使用区块链技术来实现对社会经济协作与泛金融活动过程产生的信息和数据进行溯源、登记确权以及实现数据交易，是一个社群性公有链，具有安全可靠、稳定性高、可拓展性强的技术特点。

2 概述

2.1 背景

随着信息化时代的发展，各类社会活动均会产生大量的信息和数据，如金融服务、大宗交易、商品贸易、日常消费、产品质量与供应链管理、社交互动、电子政务、游戏活动以及物联网/互联网安全等,这些信息数据往往经过了各种各样的“包装”变成了一种可以交易的资产被社会广泛地接受.数据变成资产后,具备了流动性,金融属性就变得很强, 围绕数据进行交易成为了催生信息产业升级的元力, 也成为了滋生信息的暗网交易、个人隐私数据泄漏、基于大数据杀熟营销、行业溯源造假等一些灰色的产业生态.

另外，由于行业竞争力加剧,社会信用机能不足、企业保护商业隐私等原因使得业务发展过程产生的数据和信息无法联通、不能共享与交换,成为了制约大数据产业应用的障碍。如何明确数据信息主体、客体的权责边界;如何形成良好的数据开发和使用氛围，处理好安全和发展的关系。成为了根源链建设公有链的初衷及未来践行的方向。

2.2 应用生态

根源链坚持聚焦在产业应用主航道,将为不同领域的客户提供通用的分布式数据接入组件, 并逐步与产业应用生态伙伴研发诸如产品溯源、数据确权、分布式电商网络、轻量应用挂载平台等落地应用。

根源链社区在建设应用生态时，主张开放、合作、共赢, 与产业伙伴合作创新、扩大产业价值。在大数据确权交易、食品药品溯源与流通、企业供应链管理、文化资产版权管理、电子政务、智慧城市建设、文娱游戏开发、广告营销、供应链金融、商业积分、快销品 B2B 销售等领域，会逐步形成完善的行业解决方案,并将根据技术与应用特点，不断扩展应用范围，持续进行底层技术与生态的升级。

3 技术要点

根源链 BOS 属于典型的公有链基础设施范畴。参考 wikipedia 给出的描述，公有链定义如下：

Public blockchains：

A public blockchain has absolutely no access restrictions. Anyone with an internet connection can send transactions to it as well as become a validator (i.e., participate in the execution of a consensus protocol). Usually, such networks offer economic incentives for those who secure them and utilize some type of a Proof of Stake or Proof of Work algorithm.

Some of the largest, most known public blockchains are Bitcoin and Ethereum.

因此，作为公有链，其技术要点可简单归纳为：

(1) 不限制参与者，更不限制时空位置

(2) 权益证明算法，例如 POW

(3) 经济激励

根源链 BOS 作为基础设施符合人类社会在数字空间的基础，其特性简单归结为：

(1) 新型分布式计算范式

(2) 匿名不可篡改

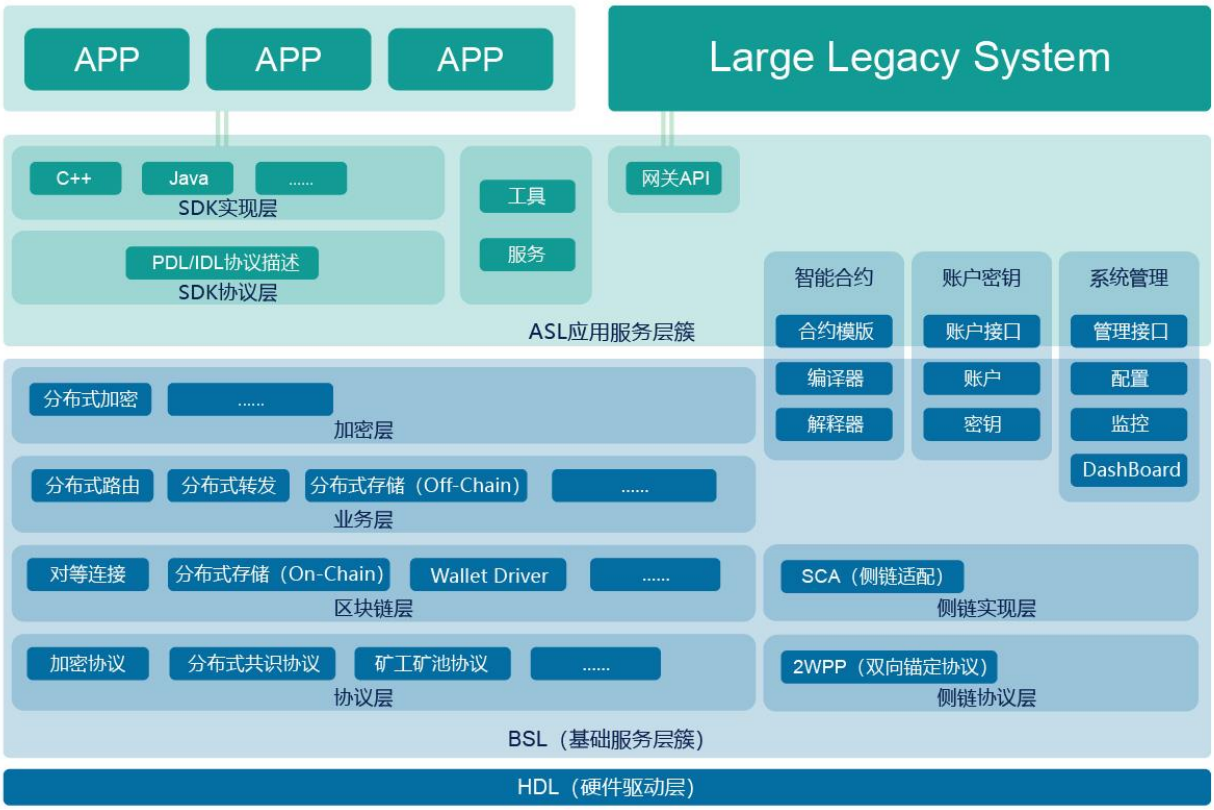
(3) 组件可插拔设计

(4) 新型溯源规范

(5) 激励策略池

而根源链则基于通用型区块链基础设施，结合物联网及应用化需求进行了必要的技术优化与扩充。以下对根源链的系统架构及其各部分技术要点进行简要解释。

3.1 系统架构



3.2 硬件驱动层 HDL

区块链计算机硬件驱动是硬件加速引擎激活的前提，定制化的区块链计算机具有深度挖掘软硬件的性能潜力，大幅提高区块链系统性能，表现为：

(1) Hash 计算

(2) 硬件计算：GPU 编程(openCL、CUDA)、FPGA 编程(Field - Programmable Gate Array)、ASIC 编程(Application Specific Integrated Circuit)

(3) CPU 计算：X86 体系、MIPS 体系、ARM 体系

(4) 加解密计算：使用专用加解密板卡提高加解密性能

3.3 协议层

协议层是根源链 BOS 的核心，不仅具备抽象可插拔的能力，而且灵活、低耦、易扩展。

3.3.1 加密协议

内容包括：

(1) 签名验证算法（RSA,ECDSA,SM2）

(2) 数字信封算法（RSA,ECDH,SM2，NULL）

(3) 哈希、MAC 算法（SHA256，HMAC,SM3）

(4) 对称加密算法（AES-CBC,AES-ECB,SM4，NULL）

其中括号内为目前支持的算法，包括美标和国密两种标准，更多的算法还在继续扩展中。

3.3.2 分布式共识协议

为了易于扩展分布式共识算法，根源链 BOS 提出了分布式共识协议，从而便于任何共识算法的接入。换言之，分布式共识协议促使任何共识、一致性算法作为插件接入到根源链 BOS 中。

3.3.3 矿工矿池协议

目前矿工支持包括：Mining software，BFGMiner，CGMiner，libblkmaker

目前矿池支持包括：ckpool，Eloipool，Stratum-Mining

3.4 区块链层

区块链层承载的是根源链公链的核心，包括对等连接、分布式存储(On-Chain)、钱包驱动(Wallet Driver)。

3.4.1 对等连接

根源链 BOS 的对等连接主要体现在去中心化的底层所使用的网络拓扑，实际为 P2P 的网络，正常时 P2P 网络是很难被 DDOS 攻击的，网络中的所有节点都是相同角色，并不存在某个有着特殊含义的中心化节点，所以攻击者找不到特定的攻击目标来实现 DDOS 攻击。

从防护安全的角度出发，对等连接和 DDOS 攻击是根源链 BOS 重点考虑的。

(1) 攻击只会影响到单个节点。

单个节点很可能会因为 DDOS 攻击而导致服务不可用，单个节点的下线对整个网络而言，影响可以不计。只要该节点恢复，马上就会自动连接到 P2P 网络，并且从网络中同步因为 DDOS 攻击而没有同步的区块数据，相应的服务能很快恢复。

(2) 攻击只能针对于网络通讯底层

如果攻击者采用区块链网络协议对节点进行 DDOS 攻击，寄希望于通过协议使得 DDOS 的影响能自动洪泛于 P2P 网络，但这种是不可行的。

- Case A: 如果攻击者构造异常的数据包，那么在该数据包到达的第一个节点，节点就会对数据包进行校验处理，校验不通过将直接丢弃报文，使得攻击的效果仅限于网络中的第一个节点。
- Case B: 如果攻击者伪造为 P2P 网络中的一个节点，向 P2P 网络发送异常的数据包，和 A 类似，该报文在和伪造节点相连的一个或多个节点被抛弃，而且此时相邻节点在验证出错误报文后，会对报文的来源节点启用惩罚机制，当达到惩罚的阀

值之后，自动关闭和该节点的连接。这样很快的时间内，伪造节点就会被从 P2P 网络中剔除，整个 P2P 网络不会有任何影响。

(3) 正常攻击报文的成本因素

如果攻击者构造正常的交易数据包和区块数据，交易中不管是查询类型还是创建类型，都需要耗费相应价值的数字货币，这种攻击的费用代价相当高，而费用会自动转移到被攻击的钱包，最后的效果是攻击者没有达到攻击的效果，被攻击的一方反而赚的盆满钵满。

3.4.2 中继激励

角色定义：

要素名	含义
Client	客户端，属于使用匿名服务的用户，细分为资源的提供方（Provider Client），资源的消费方（Consumer Client）
Relay	中继端，属于提供匿名中继的服务侧，细分为 Entry，Middle，Exit 三类。 Entry 的含义是靠近 Provider Client 的中继 Middle 的含义是具备邻居的中继 Exit 的含义是靠近 Consumer Client 的中继
Assignment Server	分配服务器，属于提供建立 Consensus Group，以及间接建立 circuit 的服务主体

Consensus Group	共识组，属于分配服务器提供 SCPATH 能力的实例，1）只要连接到分配服务器的客户端和中继，都能够提供它们的公钥到共识组 2）执行这些公钥的验证 3）输出一个 circuit，并将该 circuit 给到 circuit 中定义了的客户端们。 任何共识组的生成都是临时的。
circuit	环路/线路，包含了客户端和若干中继的数据结构。分配服务器需要依赖这个 circuit 作为输入，输出最终的路径搜索结果（Path Lookup）。 任何 circuit 的生成都是临时的。

安全性评价：

要点名	含义
Anonymity	匿名性
Group Formation	（共识）组的编排方法
Circuit Diversity	环路/线路的多样性
Persistent Guards	持久防护性

匿名中继激励要点：

1）只有在 circuit 上的客户端和中继才被允许挖矿。

2）挖到的币具有特殊的分配规则：基于 circuit 上所有的客户端和中继，按照各自吞吐率分配所获币。

匿名中继激励过程：

1）每个 Client 和每个 Relay 生成自己的临时密钥 R，并计算该密钥的 Hash

2）客户端发送一个元组（coin#，Rc）作为数据包，发送到这条 circuit，而且严格限制数据包数量必须达到 m

3）在这条 circuit 中，每个中继都向元组发送自己的密钥的 Hash 值，分别表示为 Re，Rm，Rx，并且每个中继都将该元组发送到下一个中继

4）在这条 circuit 中，Exit Relay 生成一个币提交数据包 B=(coin#，Rc，Re，Rm，Rx)

5）在这条 circuit 中，Exit Relay 使用自己的临时公钥去签这个 B 数据包，表示为 Sxb。并且发送元组（B，Sxb，Rx）到 Middle Relay。

6）在这条 circuit 中，每个参与者都区使用自己的公钥签数据包 B，表示为 Sib，并将这个数据注入到元组中，最后再将这个元组转发到当前参与者的前驱参与者。

7）在这条 circuit 中，客户端生成 PoB，表示为 P=(B，Sxb，Smb，Seb，Scb，Rx，Rm，Re，Rc)，这说明任何参与者都可以验证 Client，Entry，Middle，Exit 四个参与者的公钥。

8）在这条 circuit 中，客户端进行 Hash(CSi，B，Rx，Re，Rm，Rc)的值的低位区数值是否等于 0，表示 BSTK 已经被挖到。

并验证 BSTK 的有效性。

9）最终，在这条 circuit 中，客户端依旧使用根源链的方式，以 BSTK 支付这条 circuit 上的每个中继。

3.4.3 分布式存储（On-C）

分布式存储(On-Chain，链上)有别于分布式存储(Off-Chain，链下)，因为链上数据是稀有的，所以链上数据具备特殊性。根源链 BOS 针对链上数据进行了独特的设计，主要依赖的技术包括 OP_RETURN 和 MultiSig。

根源链 BOS 使用 OP_RETURN 作为链上数据的选择主要是出于两点需要。第一是 BSTK 销毁，第二是 PoE 存在证明。根源链 BOS 扩展了 PoE 的能力，使其具备了会计属性(记账、查账、对账、审账、分账和销账)。

根源链 BOS 使用 MultiSig 作为链上存储是源于 P2SH 的衍生产物，对 n-of-m 型的多签名地址，因为只需要提供 n 个有效签名就可以花费该交易，但剩下的 m 减 n 个签名的内容还是分配了存储空间，根源链 BOS 巧妙地设计并重新利用这些剩余的存储空间，这种方法的好处是该交易依然可以继续被花费。

3.4.4 钱包驱动

根源链 BOS 重新构建了钱包使其具备驱动能力，建立密钥与账户的映射关系。钱包驱动的好处在于面向数据所有权方面提供了密钥、账户所需要的接口，而面向用户层面使用所有权时并不关心驱动是如何调度的。

我们知道权益是通过数字密钥、地址和数字签名来确立的。密钥的独立特性使得密钥数据库也具备独立特性，钱包的本质就是密钥数据库(KeyStore)。根源链 BOS 通过重建密钥数据库，使得上层模块调度请求时，钱包驱动能够灵活地去读写账户密钥模块。

3.5 业务层

业务层是根源链 BOS 的功能核心，不仅引入了许多先进技术，而且自主实现了多领域、多场景、易定制的诸多模块。主要包括分布式路由、分布式转发、分布式存储(Off-Chain)，以及业务层接入的核心术语单元。

(1) Blocklabel，作为根源链 BOS 区块网络命名规则（SCBN，根源链区块网络）的一部分，用于标识根源链 BOS 全局、唯一的一般数据或资源；它的形式表示为 URI，以/为分隔符，分隔符之间是元素；例如，/sourcechain/bstk/what/do/you/want/to/do；这种形式不仅简单易理解，而且容易扩展，最关键的是它作为根源链 BOS 核心协议词之一；此外，命名所带来的优势是传统 P2P 网络无法比拟的；

(2) Market，用于表示市场的参与者角色；其中，参与者可以是纯粹的生产者或者消费者，亦可以是产销共同体；

(3) Contract，用于验证交易的数据类型，由合约代码组成，合约代码包含数据、行为、输入和输出；具体定义参考合约模板章节；

(4) Price，用于 Blocklabel 对应数据的定价，在 Market 的参与下，促进信息披露与价值流通；Price 的引入与分布式存储(Off-Chain)有关，用于标识 BlockLabel 指向的资源的定价；

使用命名技术和区块网络的目的是友好的分布式实现、安全易扩展及数据标识等，从而形成一个具备区块链属性的 Label-NDN 分布式存储网络。

分布式实现不同于 P2P 并不意味者两者之间的优劣。业务层引入命名化的分布式计算是为了有效驱动分布式存储(Off-Chain)的读写与数据传输，而面向应用层面是透明的。

安全易扩展是区块网络的重要特性之一，原因在于基于 IP 网络安全需要对终端和连接同时信任。IP 网络接受任何人发送的任何内容，不管数据包的内容，只要发送者看似合法，这种情况导致恶意信息发送到接收者，这是 IP 网站容易被攻击的根源；通过签名

加密了关于数据请求者的信息，除非点对点链路直接连接到发出请求的主机，否则路由器将只知道有人请求某些数据，但不知道是谁发起请求，具备一定的匿名性(Anonymous)。

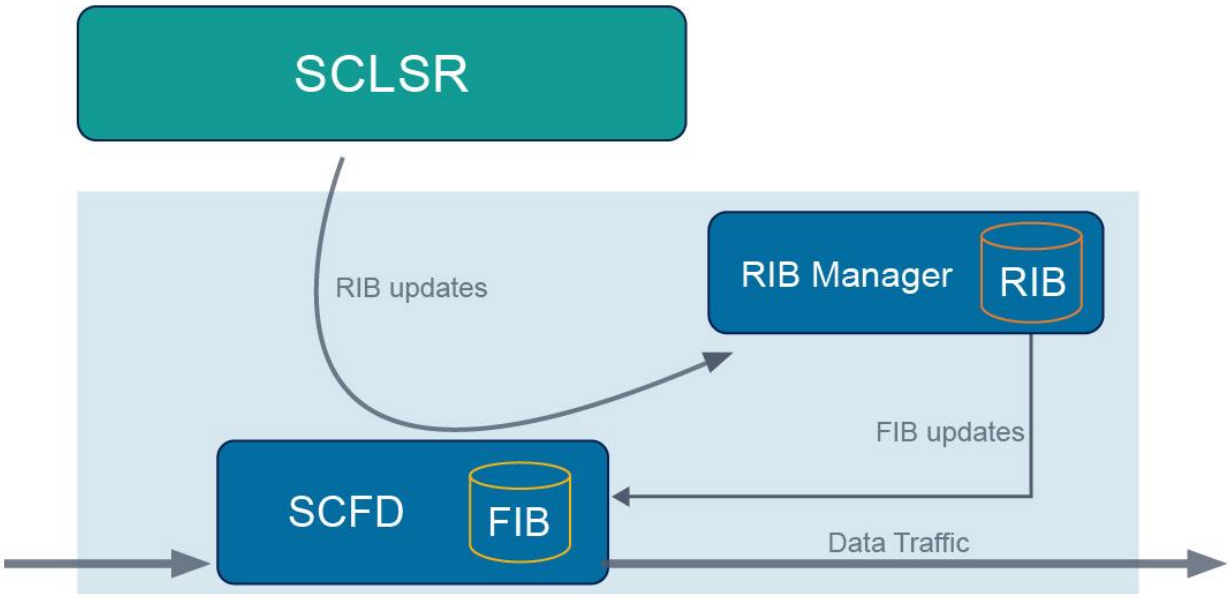
数据标识是基于区块网络命名规则层次化演进而来，不仅符合区块网络要求的命名规则，而且易于用户层的易读易理解。此外，信息的命名化还有利于应用层的领域编程。

3.5.1 分布式路由

根源链 BOS 的分布式路由是基于命名概念建立的。基于数据资产的安全性要求，通过部分继承命名链路状态路由协议，实现根源链 BOS 自主研发的分布式路由组件 SCLSR。此外分布式转发组件依赖于路由组件。

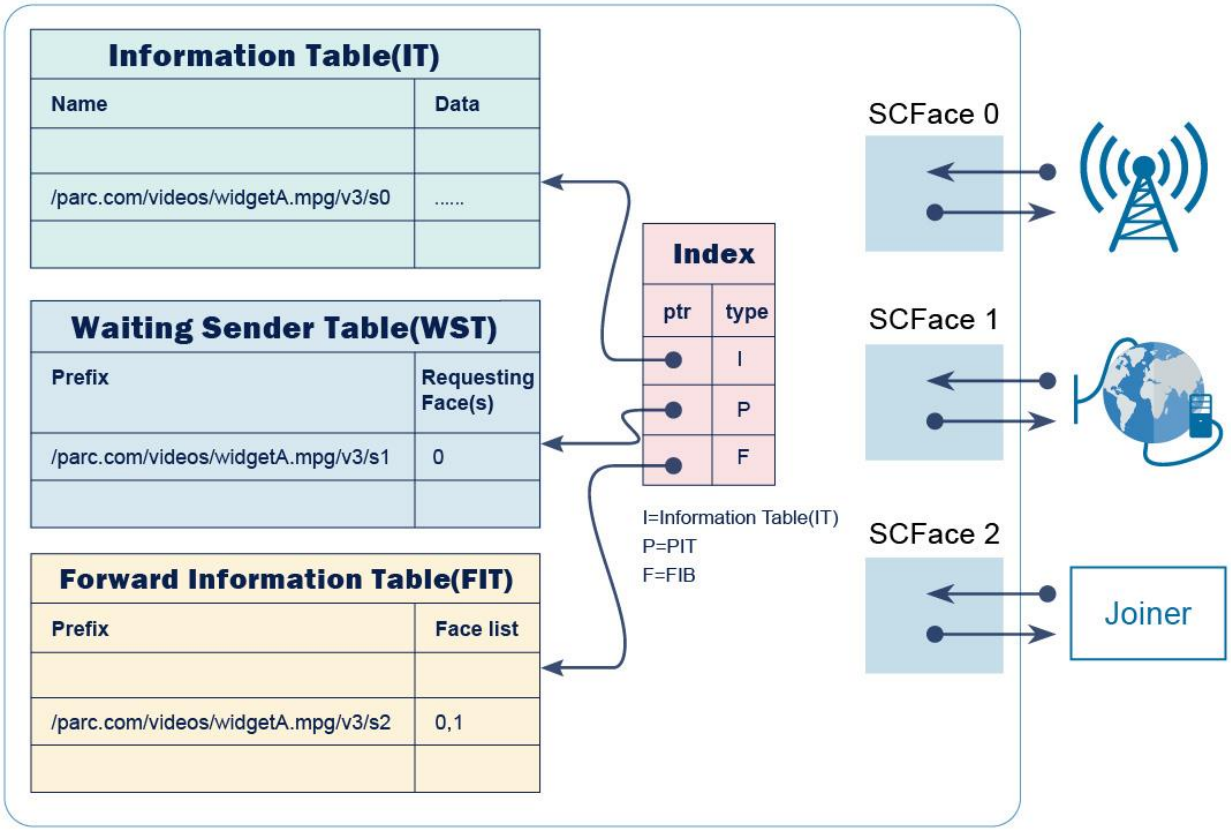
SCLSR 的主要设计目标是提供路由协议来填充区块网络的 FIT 表。SCLSR 使用链路状态或双曲线路由计算路由表，并为单个授权域中的每个可到达命名前缀生成多个 SCFace。

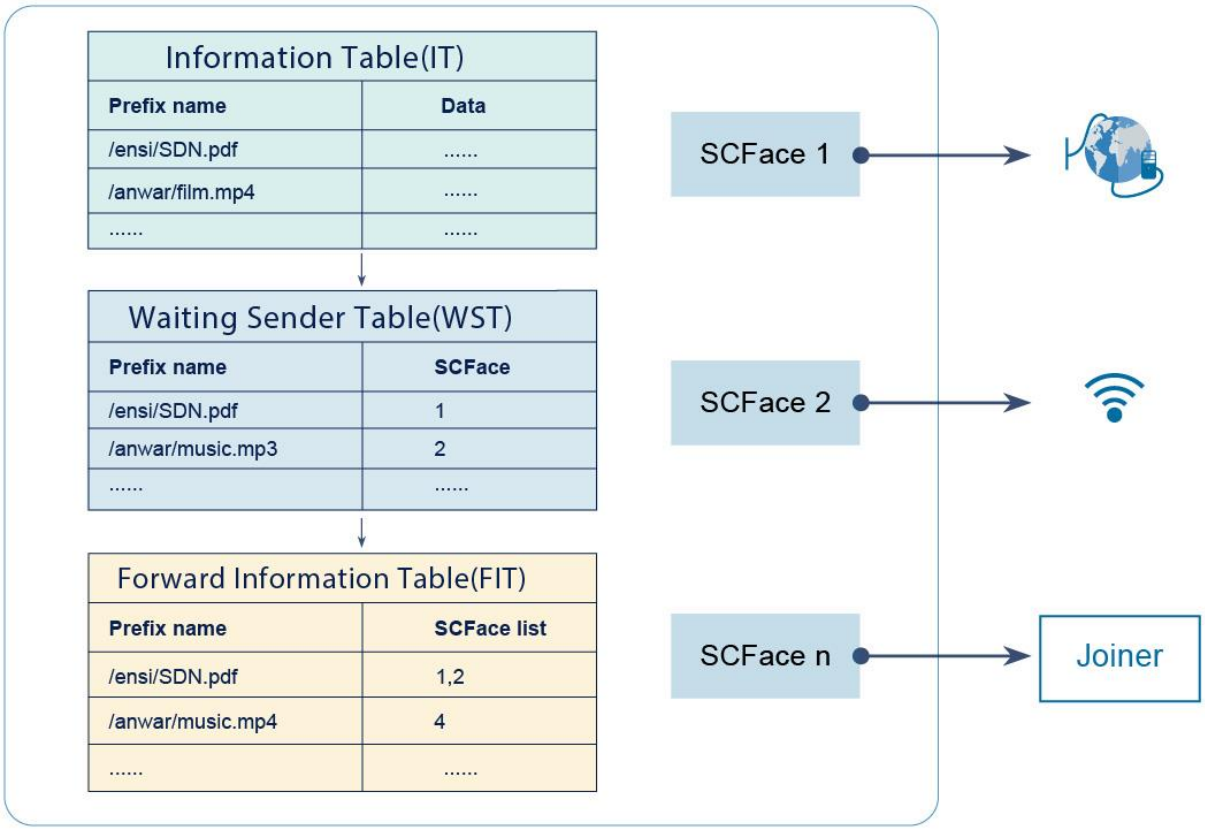
下图表示 SCLSR 构建 FIT 转发表的过程以及 SCLSR 与 SCFD 的关系：



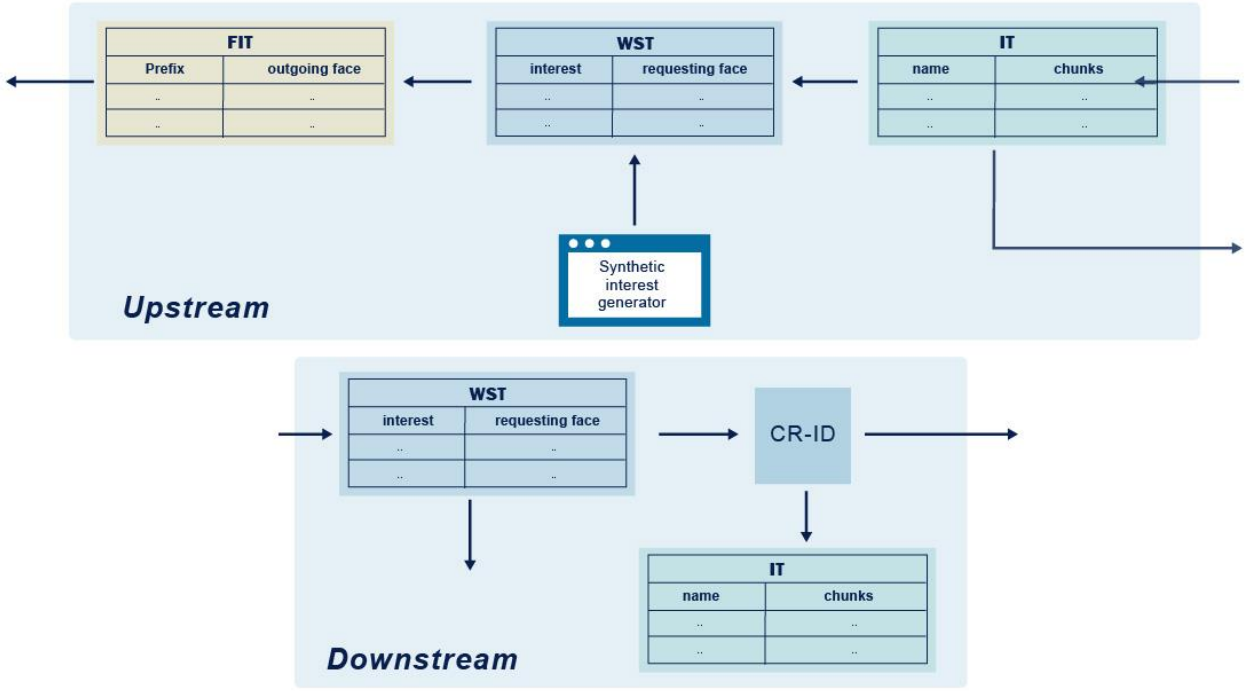
3.5.2 分布式转发

根源链 BOS 的分布式转发同样基于命名概念创建与工作。其中，FIT 表的构建依赖于 SCLSR，根源链 BOS 自主研发的分布式转发组件 SCFD 作为命名数据网络的核心实例，其内部构成如下图。





下图则说明了基于 SCFD 的上层数据发出(Upstream)，上层数据的接收(Downstream)逻辑。



3.5.3 分布式存储（Off-C)

根源链 BOS 分布式存储(Off-Chain)的底层存储基于 CEPH、BigChainDB，并引入了 BLFS（Block Label File System）技术机制。

在面向内容方面，CEPH 是用于存储内容可寻址文件的一种高可靠标准。内容可寻址存储是一种基于其内容而不是其位置来检索的信息存储机制。

根源链 BOS 重构了 CEPH 接入层的实现并结合分布式转发的命名规则，实现了基于内容的分布式存储(Off-Chain)服务实例。使用 CEPH 存储的所有文件名称都是从其内容的散列中生成的，并意味着同一个文件在每台计算机上都具有相同的名称，并且更改文件内容会导致文件名称的更改。当从服务器下载一个文件夹时,可以根据服务器提供的内容重新计算文件名称来验证文件是否为所请求的文件。CEPH 的 P2P 网络层,允许计算机根据其唯一的名称发现和共享文件。

面向检索，由于业务数据的规模庞大，数据存在查询检索的需要，根源链 BOS 链下存储服务实例又引入了 BigChainDB 作为业务数据的存储引擎。BigChainDB 具有去中心化控制、防篡改和创建传输数字资产等区块链技术的优点。防篡改通过几种机制实现:分片复制、不允许更新或修改、定期备份数据库、所有交易签名加密、区块和投票。任何有资产创建权的实体都可以创建一个资产，一个资产只有当新所有者满足加密条件时才可以被新所有者接收。这意味着黑客或者恶意管理员不能任意更改数据，而且没有单点错误风险。

另一方面，在面向内容时，根源链 BOS 基于区块链属性与特点引入了 BLFS 机制，当前公链基础设施在支持实际应用时，一大核心问题是数据存储如何解决。由于区块链是采用分布式存储方式，每个节点同步其他节点数据，即使经过优化，也面临着大量数据的存储问题。在结合了 BlockLabel 技术后，根源链引入了 BLFS 机制，形成了一种高效、高可靠的区块链形态分布式存储结构。BLFS 弥补了现有区块链系统在文件存储方面的短板，它为所有的区块链准备好了数据存储结构，可以链接到不同的区块链项目。用户可以使用 BLFS 来处理大量数据，然后把对应的加密哈希存储到区块链中并打上时间戳，这样就无需将数据本身放在链上，不但可以节省其他区块链的网络带宽，还可以对其数据进行有效保护，于是，BLFS 就成为了根源链这一公链基础设施中存储功能的实现方式。总之，链上(On-Chain)的 PoE 属性和链下(Off-Chain)的命名和内容规则共同组成了根源链 BOS 分布式存储。

3.6 加密层

根源链 BOS 的加密层主要包含三部分，第一是加密协议的实现，第二是硬件加密板卡的封装，第三是依赖加密协议实现和硬件加密之上的分布式加密服务组件。

3.6.1 分布式加密设计

基于分布式存储的需要，根源链 BOS 分布式加密组件引入了 KMS 密钥管理服务以及 Barbican。由于分布式存储是基于 CEPH 和 BigChainDB，所以必须依赖 KMS 和 Barbican 组件。数据资产的存储要求体现在安全方面在分布式机密组件中进行了重构和封装，并将这些接口暴露给 ASL 层。换言之，这些内容面向用户层面是透明的。

基于应用服务层 ASL 的需要，根源链 BOS 分布式加密组件提供了 SDK 与网关加密依赖。主要包括如下。为了保证数据资产的安全，P2P 节点之间的通信支持使用加密通道。现代信息安全技术所依赖的加密机制主要分为两种，一种是对称加密方式；一种非对称加密方式。两者在性能和应用场景上相互有区别。为了保证网络的安全性并且兼顾系统运行的性能，面向数据通讯采取对称加密机制；对称密钥的协商和传输采取非对称加密机制。

为了系统安全性及后续系统扩充方面考虑，根源链并未规定具体的加解密算法，而是参考 SSL 机制，实现了一套加密算法和加密密钥的 P2P 协商模块，用于 P2P 节点之间的通信协商。

3.6.2 对称加密机制

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，对称加密算法使用起来简单快捷，密钥较短，且破译困难，除了数据加密标准（DES），另一个对称密钥加密系统是国际数据加密算法（IDEA），它比 DES 的加密性好，而且对计算机功能要求也没有那么高。IDEA 加密标准由 PGP（Pretty Good Privacy）系统使用。为了更好的解释分布式加密的对称加密部分，如下几个问题值的注意。

- 要求提供一条安全的渠道使通讯双方在首次通讯时协商一个共同的密钥。直接的面对面协商可能是不现实而且难于实施的，所以双方可能需要借助于邮件和电话等其它相对不够安全的手段来进行协商；

- 密钥的数目难于管理。因为对于每一个合作者都需要使用不同的密钥，很难适应开放社会中大量的信息交流；
- 对称加密算法一般不能提供信息完整性的鉴别。它无法验证发送者和接受者的身份；
- 对称密钥的管理和分发工作是一件具有潜在危险的和烦琐的过程。对称加密是基于共同保守秘密来实现的，采用对称加密技术的贸易双方必须保证采用的是相同的密钥，保证彼此密钥的交换是安全可靠的，同时还要设定防止密钥泄密和更改密钥的程序。

常用的对称加密算法有 DES、3DES、Blowfish、IDEA、RC4、RC5、RC6 和 AES。

3.6.3 非对称加密机制

与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。甲方只能用其专用密钥解密由其公用密钥加密后的任何信息。

非对称加密算法的保密性比较好，它消除了最终用户交换密钥的需要，但加密和解密花费时间长、速度慢，它不适合于对文件加密而只适用于对少量数据进行加密。

非对称加密的典型应用是数字签名。常见的非对称加密算法有：RSA、ECC、Diffie-Hellman、El Gamal、DSA（数字签名用）。根源链的区块链层使用的非对称加密实现是基于 DSA 的 ECDSA 算法。

3.6.4 加密协商模块

加密协商模块完成 P2P 节点两两之间的加密套件协商。需要协商的加密套件内容包含签名验证算法（RSA,ECDSA,SM2），数字信封算法（RSA,ECDH,SM2，NULL），哈希、MAC 算法（SHA256，HMAC,SM3），对称加密算法（AES-CBC,AES-ECB,SM4，NULL）

其中括号内为目前支持的算法，包括美标和国密两种标准，更多的算法还在继续扩展中。其中 NULL 代表不加密或者不用数字信封。

这部分是协议层加密协议的实现，而且也是应用层 SDK 和网关 API 加密部分的基础服务组件。

3.6.5 密钥及证书管理

证书中存储着用户的公钥。公钥用来对签名的验证，也可以用来做数字信封。公钥证书管理证书的验证，证书中公钥的管理和使用。

- 私钥管理，非对称加密中私钥的管理包括私钥的生成、使用、删除以及导入、导出。
- 数字信封，对称密钥从发送方给接受方需要用到数字信封。数字信封确保加密密钥不被第三方窃取。
- 对称加密密钥管理，加密的双方密钥的生成、使用、删除。可以根据加密协商模块协商出来的对称加密算法，生成不同算法的密钥。

3.6.6 压缩传输支持

为了提高整个系统的吞吐量，传输的时延以及网络可靠性将很大程度上影响整个系统的稳定性。因此我们引入了压缩机制，采取压缩算法能大幅度降低节点之间数据资产和区块传输的数据量大小。

节点之间的数据压缩算法和加密协商一致，在加密协商时节点协商自身的压缩能力（7z，zip，NULL）。

3.7 侧链

侧链的出现是为了解决不同类型区块链实例和不同类型数字货币实例的对接问题。根源链 BOS 将侧链技术规划为协议部分和实现部分，其中协议部分主要是指 2WPP 双向锚定协议的自主化定义，不仅包含了业界侧链的规范约定，而且包含了根源链 BOS 的内部多链侧链的协议规范内容。

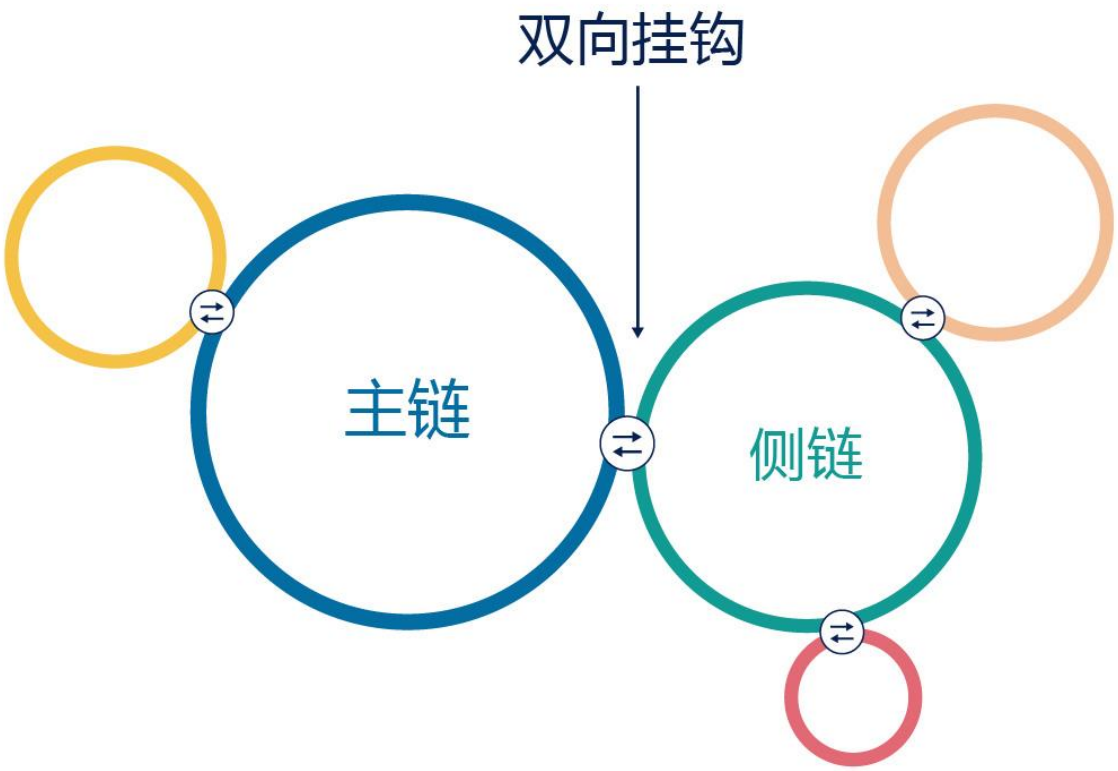
3.7.1 侧链协议层与 2WPP 双向锚定协议

在协议层，首先约定主链实例（Parent chain instance），然后约定其他类型区块链实例作为侧链，二者通过双向锚定（2WPP），可实现主链到侧链，侧链到主链进行流通的需要。

侧链可以是一个独立的区块链，有自己按需定制的账本、共识机制、交易类型、脚本和合约的支持等。侧链不能发行 Token，但可以通过支持与主链 Token 挂钩来引入和流通一定数量的 Token。当主链 Token 在侧链流通时，主链上对应的 Token 会被锁定，直到这些 Token 从侧链回到主链。可以看到，侧链机制可将一些定制化或高频的交易放到主链之外进行，实现了区块链的扩展。

侧链的核心原理在于能够冻结一条链上的资产，然后在另一条链上产生，可以通过多种方式来实现。

根源链 BOS 的 2WPP 协议的设计难点在于如何让资产在主链和侧链之间安全流转。简言之，接受资产的链必须确保发送资产的链上的 Token 被可靠锁定。



3.7.2 侧链实现层

2WPP 协议要求采用双向锚定机制实现主链向侧链转移和返回。主链和侧链需要对对方的特定交易做 SPV 验证，因此实现 SPV 验证是侧链实现层的主要内容。

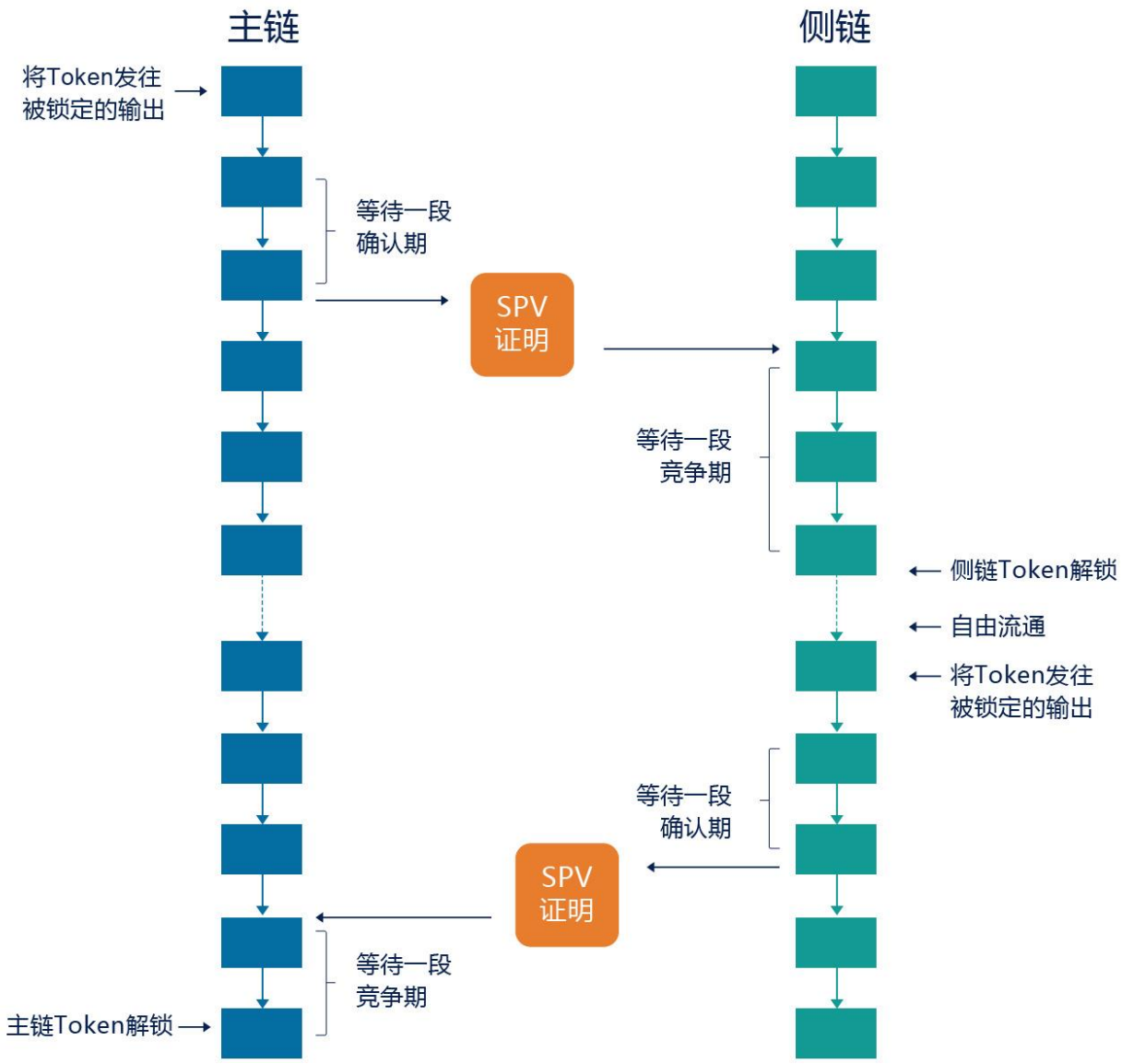
简单支付验证（Simplified Payment Verification，SPV）能够以较小的代价判断某个交易是否已经被验证过（存在于区块链中），以及得到了多少算力保护（定位包含该交易的区块在区块链中的位置）。对方链(主链或者侧链)只需要下载所有区块的区块头（Block Header），并进行简单的定位和计算工作就可以给出验证结论。

2WPP 协议中，用 SPV 来证明一个交易确实已经在区块链中发生过，称为 SPV 证明（SPV Proof）。一份 SPV 证明的文本结构包括两部分内容：一组区块头的列表，表示工作量证明；一个特定输出（output）确实存在于某个区块中的密码学证明。

3.7.3 SCA 侧链适配器

根源链 BOS 的 SCA 侧链适配器的完整实现过程如下

- 事件发生端要向侧链转移 Token 时，首先在主链创建交易，待转移的 Token 被发往一个特殊的输出。这些 Token 在主链上被锁定。
- 等待一段确认期，使得上述交易获得足够的工作量确认。
- 事件发生端在侧链创建交易提取 Token，需要在这笔交易的输入指明上述主链被锁定的输出，并提供足够的 SPV 证明。
- 等待一段竞争期，防止双重花费攻击。
- Token 在侧链上自由流通。
- 当事件发生端想让 Token 返回主链时，采取类似的反向操作。
- 首先在侧链创建交易，待返回的 Token 被发往一个特殊的输出。
- 先等待一段确认期后，在主链用足够的对侧链输出的 SPV 证明来解锁最早被锁定的输出。
- 竞争期过后，主链 Token 恢复流通。



3.8 智能合约

根源链 BOS 的合约层技术实现符合可插拔要求，面向合约技术而言，当前支持 RSK、MAST、LN、CounterParty 等主流合约技术，并基于其上来实现根源链自有的 SC-LN 等技术。

Rootstock（RSK）是基于侧链技术实现，其目标是通过实现智能合约、即时支付和更高的可扩展性等问题，为主链赋能，实现主链的智能合约功能，为主链生态系统增加价值和实用性。关于侧链技术已经阐释不再赘述。

引入 RSK 作为根源链 BOS 的合约层技术实现之一，是基于：

(1) 主链无智能合约功能或者脚本系统功能较为简单

(2) 主链确权速度慢

(3) 对等网络速度慢

(4) 网络拥堵

(5) 交易手续费高

具体实现为：

(1) 引入智能合约的图灵完备性的虚拟机（RVM）

(2) 门限签名方案实现的安全联合工作量证明挖矿机制

(3) 嵌入延迟低的中继骨干网络支撑点对点通讯

(4) 2WPP

MAST 方案由三部分构成，分别是支付给脚本 hash(P2SH)，抽象语法树 AST 和 Merkle 树。MAST 的典型实现是基于脚本系统，AST 给出了脚本语法的分解规则。根源链 BOS 基于 MAST 扩充了脚本系统的语法分析树，提高了语法分析的效率。

根源链 BOS 目前正在尝试引入 XCP 的实现，用于促使智能合约的多样性。因为 XCP 具备“燃烧”的概念，它符合根源链 BSTK 销毁机制的需要。

根源链 BOS 引入了闪电网络 LN 的基础技术并加以改进，用以形成 SC-LN。 这是因为 LN 不仅具备分布式系统的特征，而且具备良好的独立性，易于插拔。基于 SC-LN，无需信任对方以及第三方即可实现实时海量的交易网络。LN 是基于微支付通道演进而

来，创造性的设计出了两种类型的交易合约：序列到期可撤销合约 RSMC（Revocable Sequence Maturity Contract，哈希时间锁定合约 HTLC（Hashed Timelock Contract）。基于以上合约技术的稳定与高效，RSMC 和 HTLC 合约技术也同样作为根源链 BOS 合约层的实现技术基础来使用。

3.8.1 合约模板

合约模板处于应用服务层，面向 SDK 和网关 API 进行了封装层面的选择设计。首先允许使用方选择合约类型，其次提供合约模板接口。

3.8.2 编译器

当前合约层具备基于 RSK、MAST 协议实现的编译器 SCRSK compiler、SCMAST compiler。

3.8.3 解释器

当前合约层具备基于 RSK、MAST 协议实现的 VM 包括 SCRVM、SCMVM。

3.9 账户密钥

账户密钥层主要包含两部分，第一是已经封装的分布式存储依赖的账户密钥组件 KMS 和 Barbican 暴露的接口，第二是根源链 BOS 分布式账户密钥管理系统。

根源链 BOS 分布式账户密钥管理系统是基于 NuCypher 实现，SCNC KMS(分布式去中心化的密钥管理服务)可以帮助 DApp 开发者对其分布式代理进行重新加密作为服务的区块链上的数据进行安全保护。关于 DApp 开发的 SDK 和网关 API 已经将这一部分重新封装。

根源链 BOS 账户密钥层的系统 SCNC KMS 具备账户和密钥管理两部分，允许用户把密文从一个公钥转换到另外一个公钥中，使用其再加密钥，用户不需要了解任何的基础信息。其核心的基础设施就是能够使开发者得以储存、共享和管理公共区块链上的私人数据。

3.9.1 账户接口

使用者通过用户服务层系统管理的 DashBoard 或者使用应用服务层命令行工具，轻松创建、导入和轮换密钥，以及定义使用策略和审计使用情况。

3.9.2 账户密钥

SCNC KMS 为您提供加密密钥和账户的控制。SCNC KMS 当前提供的能力包括如下。

- 主密钥（无论是导入的还是由 KMS 自行创建的）都以加密格式存储在高持久性的存储中，以帮助确保在需要时可对其进行检索。
- 每年自动轮换一次在 KMS 中创建的主密钥，而无需重新加密已使用主密钥加密过的数据。
- 无需记录旧版主密钥，因为 KMS 会保持其可用，以解密以前加密的数据。
- 创建新的主密钥，并对谁有权访问这些密钥以及它们可用于哪些服务随时加以控制。
- 从自己的密钥管理基础设施导入密钥并在 KMS 中使用。

3.10 系统管理

系统管理主要包括管理接口、配置、监控、分析仪表。其中管理接口是负责调度配置接入，便于运维人员进行操作；通过管理接口调度监控服务，便于系统管理员实时查看平

台的运行情况；通过管理接口调度分析仪表服务，方便使用者查看并允许操作响应模块，例如账户密钥。

3.10.1 管理接口

管理接口的实现基于 Cockpit。

3.10.2 配置

配置模块分为两部分，一部分是 GUI，另一部分是 CLI。

3.10.3 监控

监控模块的实现基于 Prometheus。

3.10.4 分析仪表

分析仪表的实现基于 Grafana。

3.11 SDK

SDK 协议层的实现基于 IDL 规范，由于面向开发者和面向基础服务层两部分，所以根源链 BOS 在考虑实现 SDK 时，不仅要符合低耦合、易扩展、兼容等要求，还要具备向后兼容便于升级更新。

3.11.1 协议层描述语言 SCIDL/PDL

SDK 协议层实现使用 SCIDL/PDL，定义了接口和精简分布式对象的过程。作为一种类似 Java 的规范语言，SCIDL/PDL 用于分离对象的接口与其实现，且剥离了编程语言和

硬件的依赖性。SCIDL/PDL 使用 IDL/PDL 定义接口的客户端，而应用端的开发者并不知道接口背后的实现细节。SCIDL/PDL 基于此可提供一套通用的数据类型，并以这些数据类型来定义更为复杂的数据类型。

3.11.2 SDK 实现设计

由于 SDK 的特殊性，根源链 BOS 在 SDK 实现层一开始对于 SDK 的一些通用的整体的元素的设计做了充分和反复的考量。因为 SDK（尤其平台 SDK,使用的应用成百上千）一个及其细微的调整都会影响很多开发者的版本周期。因此前期的设计显得尤为重要。

当前根源链 BOS 实现 SDK 主要支持 C++、Java、Go、Python，由于不同语言的差异性，叙述较为复杂，所以这里仅描述我们在实现时的原则。

- 接口名称、参数名称要足够清晰
- 一个接口只做一件事
- 接口参数要尽可能少
- 接口参数要一定要校验、需要转义或者转换的一定要尽可能早的处理
- 通用的名称要统一
- 同步和异步接口
- 多线程
- 第三方平台
- 配置

3.12 工具与服务

根源链 BOS 在应用服务层提供的工具包括协议层查看器、分布式路由工具集、分布式转发工具集、分布式存储工具集、分布式加密工具集、合约交互命令行工具(包括编译器)、账户密钥工具集、系统管理接口调度器(命令行方式)、侧链适配器工具集、区块链层工具集(包括交易、钱包驱动)

根源链 BOS 在应用服务层提供的服务包括区块链层后台服务、分布式路由服务、分布式转发服务、分布式存储服务簇、分布式加密服务、合约解释器服务、分布式账户密钥服务、系统管理服务簇、侧链协议服务、网管 API 后台服务

3.13 网关 API

URL 使用 RESTful 风格，通讯数据使用 Json 与 ProtoBuf 风格。

4 应用场景

4.1 泛物联网 IoT

4.1.1 实物溯源

基于根源链提供的记账和分布式数据存储基础设施，结合物联网线下数据采集和核心功能，为溯源、电商、数据确权等业务场景应用，提供线上线下完整的基础支撑平台，其中重要的业务内容及产品系统如下：

- IoT 设备分类及标示

  涉及到的 IoT 设备包括气象站，墒情系统，RFID 芯片，智能控制系统，GPS，图像识别；手持智能终端等；

  针对这些设备根据业务及应用的场景，进行分类并进行标示，并建立对应设备采集到的数据序列和集合，相关信息的标示和处理是基于根源链的 BSTK，关键性信息经技术处理后存储到根源链分布式网络。

- IoT 设备的采购及其与业务对象的绑定

  相关的设备结合区块链技术进行相关的分类处理后，供相关的商户采购，这些采购的 IoT 设备预期生产场所、加工包装、仓储物流等相关设施及资产进行管理或绑定，实现对应业务环节业务数据的信息化处理和数据上链。其中，IoT 设备的采购、业务对象绑定、资产及数据确权等在时间和空间维度上数据的处理，使用 BSTK 进行标示或计量，根据业务需要部分数据技术处理后会存储到根源链分布式网络体统。

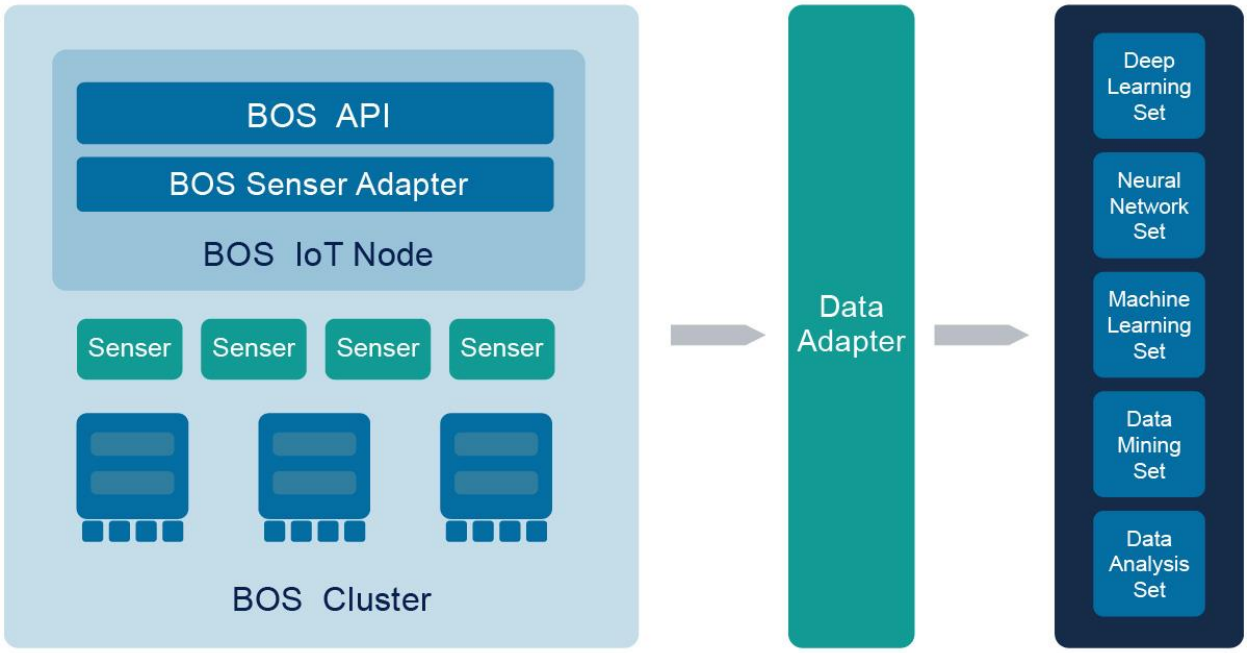
- IoT 设备数据采集及处理

  被 IoT 设备监控的对象（生产资料，产品等）在生产环节、加工包装环节、仓储物流等环节的在时间上的延展，和做空间上的变化，其中和各业务环节相关及用户关心的

数据，依次被线下 IoT 设备采集并不断通过各软件节点处理，相关的数据在根源链分布式网络系统不断累积。

4.1.2 车联网

基于根源链的信息确权向汽车提供数字身份，根源链就可以利用 GPS 追踪汽车获取的输出数据，在区块链上给它的位置添加时间戳，进而利用区块链相关的功能属性。消费者、应用开发者和制造商就可以合理利用与分享汽车联网获得的数据。



在根源链的车联网-无人驾驶相关应用中，按照行业和行业边界的构想，可以在链上定义无人驾驶的静态和行为数据结构，并基于数据构建合约来代替合同，从而确保后继的平台训练数据的完备、准确、安全性。此时结合 Token 激励体系，对无人驾驶的各个环节参与者积极性，都可以进行有效的激励。

4.1.3 无人机

无人机是典型面向技术的 IoT，更确切的说是面向人工智能(AI)，包括机器学习(ML)、深度学习(DL)以及神经网络(NN)，它们都有一个核心共通点：数据。结合区块链的无人机技术，无疑是规范化，可控制化的，并且符合管理需求。例如，无人机与自然人身份的溯源，可以避免非现场犯罪的可能。

对此类或者类似的应用，根源链提供一套完整的 IoT 智能合约，智能合约模块属于 BOS D-Right 模块，提供桩与代理接入模型，配对 BOS 节点通过代理获取合同的具体细则，以及合同的控制 API。

4.2 公证

传统的公证行业在数据的存储和使用方面主要以中心化方式实现，不仅维护成本高，而且不利于公证业务的市场拓展，主要表现在用户端的存证、取证、公证等业务环节。

根源链解决了公证行业的存证取证在传统大数据平台、分布式平台中的数据不可靠、易篡改、不可信、权益第三方等问题；通过 BOS 节点设备提供的一整套方案组合，不仅满足了数据存储的需要，而且结合了最新最全的区块链技术作为支撑

根源链解决了公证行业的取证所签署的电子存证指纹的中心化、存证孤岛问题；通过使用区块链存证 ID 作为指纹数据，不仅确保存证数据的去中心，而且确权数据随着时间的推移越来越牢固。

4.3 分布式电商

基于区块链技术的分布式电商作为一种全新的在线信息分发共享和交易系统，既为区块链分布式网络上的各个节点提供点对点的信息发布、产品检索、交易及确权等平台支

持，也为基于传统在线交易系统提供溯源产品、商品防伪、信息保全、交易记账、数据确权等服务。分布式电商核心组成部分如下：

- **在线交易系统**

  在线交易系统作为整个分布电商软件的载体，会发布 PC、IOS、Android、H5 及小程序等版本。

- **商品检索系统**

  分布式电商系统商品的信息来自溯源系统，并通过溯源系统接口获得商品的厂家、生产

  制作包装、物流等溯源 信息；

- **交易及记账系统**

  分布式电商的交易及记账基于区块链产品系统，目前版本使用根源链系统，今后计划推出基于比特币及以太坊的版本；

- **用户账户体系**

  在分布式电商体系内商品交易计价单位的源点及用户资产数量计算，是基于根源链的 BSTK，源点按比例与 BSTK 映射；

根源链计划发布一个轻量化 DEMO 应用：买卖大集。买卖大集作为分布式电商的一种形式，其在前端商品信息推送、营销活动等功能方面采用传统电商的处理方式，前端是一个 H5 网站，后端商品、交易及结算、账户体系则是基于根源链系统。

4.4 信息数据溯源确权服务

根源链溯源系统使用 IoT 物联网设备进行数据采集和监控，并通过根源链系统实现数据存储，实现产品信息的可追溯，不可篡改，为各种业务应用场景提供基于分布式区块链网络的数据存储和时空数据溯源的功能。

4.4.1 溯源系统的基础

- **IoT 物联网硬件设备**

  数据采集和跟踪监控设备：气象站，土壤墒情系统，RFID 芯片，GPS 设备，图像及识别设备，声纹及识别设备，加速度等传感器

  前端数据处理及智能前端机：区块链计算机，智能控制系统，手持智能终端

- **区块链分布式记账系统**，早期版本使用根源链实例

4.4.2 溯源系统对外提供的服务

- **商品溯源**

  对商品的生产环节、包装鉴定环节、物流环节、交易和消费环节进行相关的信息的追溯。

- **数据确权**

  基于 IoT 物联网设备及区块链分布式网络系统，追溯和记录各个业务环节的关键信息，并对相关的实物商品及相关的数据进行权责确认，并形成确定数字标签进行对所有权进行数字化。

4.4.3 溯源系统对外服务的提供方式

- API 接口

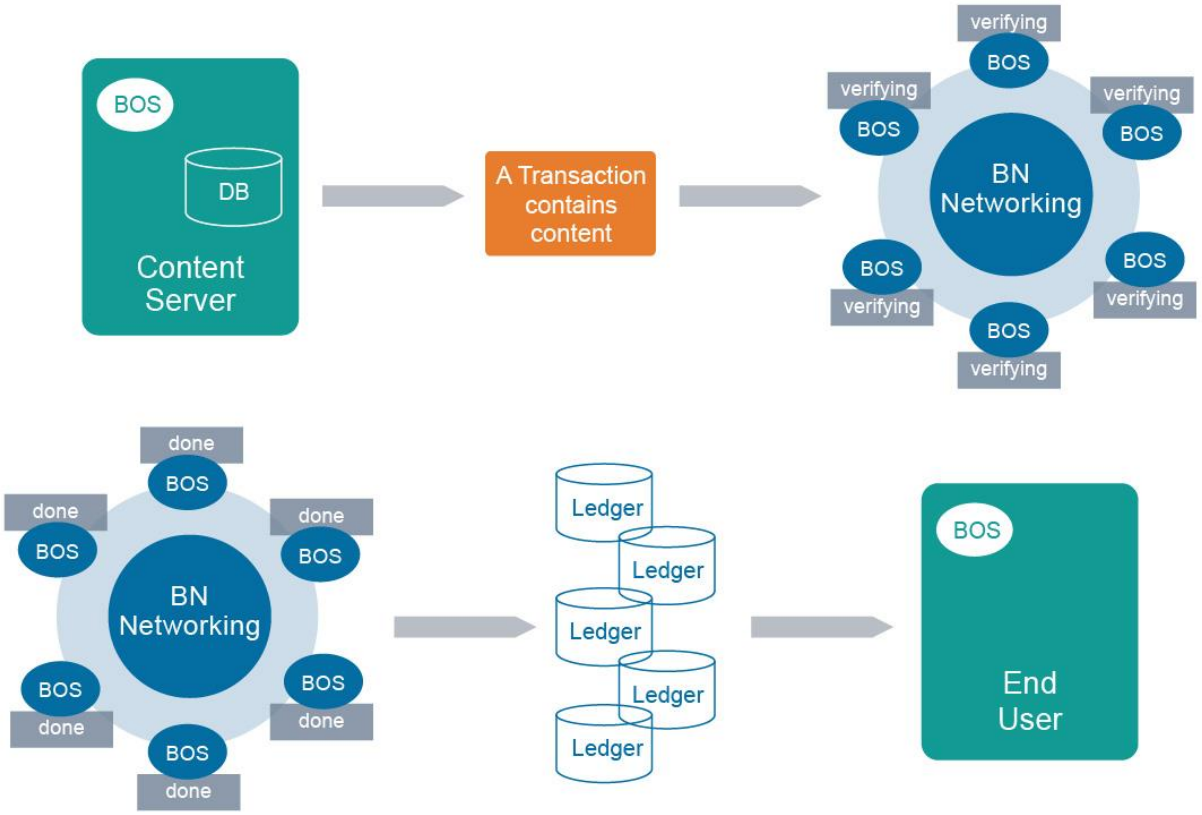
- SDK（Android 及 IOS 版本）
- H5 网页

4.5 多媒体内容服务

多媒体分发也称为内容交付。根源链的多媒体内容服务基于各类基础资源与 BLFS 等存储相关的技术特性，且支撑所有数据的加密安全、共识、转发以及存储。

作为一种多媒体内容的数字分发形式，其所描述的多媒体主要包括音频，图像和视频。与传统处理方式相比，例如专用富媒体应用服务器、基于 CDN(内容分发网)的云端 DaaS，甚至分布式流媒体服务，这些方案没有一个解决侧重于交付内容的安全性和完整性等问题。

业务层面的区块链媒体服务过程：



- 服务端接收到资源请求以后发送出资源，并且包含一笔 Transaction；
- 接下来通过业务层 网络每个 BOS 端的共识验证；
- 通过所有 BOS 端共识之后，将这笔 Transaction 记账并汇总于总账本；
- 最终，用户端接收到安全和完整的媒体数据。

4.5.1 实时版权保护算法

根源链可以实现对多媒体的版权保护，并计划基于 API，针对此种需求进一步提供一种分布式实时水印系统，当服务节点接收到来自用户的请求时，通过实时水印处理之后向用户发送期望数据。

4.5.2 根源链多媒体平台

- 根源链引入了相位算法，并结合块嵌套和自嵌入水印的概念；
- 根源链提供了可信赖的机制，以及分布式内容框架；
- 智能合同促使了媒体信息承接双方的行为约定；
- 在根源链强有力的支撑下，基于小波的自嵌入水印算法解决了内容不完整、安全检测不均衡、篡改、失效销毁等问题，实现了一种独具创新的多媒体平台。

4.6 其他应用场景

4.6.1 DApp

分布式应用程序或“DApps”是大家较为熟悉的区块链应用概念，而根源链基于结合物联网的公链基础设施特性，可以支持，尤其是支持和物联网相关紧密的各类 DApp。

通过根源链提供的各类基础与合约 API，DApp 可以更容易的将后端部署在区块链上，并依靠根源链提供的计算、网络、存储、加密能力来向后端提供完整的运行环境。

目前，DApp 主要以积分类型的轻量化应用为主。

4.6.2 DCC 分布式云计算

与 DApp 类似，由于根源链可以提供计算、网络、加密、存储等基础资源并通过 API 等多种方式来调用，并且能够形成规格化调用，同时又能通过 Token 机制来协调更多的 Off-Chain 同步/异步资源，因此适合作为分布式云计算基础设施使用，例如解决并行计算。

此外，根源链具备资源的分布式调度特性，大量的碎片化资源对于去中心化的网络来说最为理想，不仅可以帮助解决基础资源服务提供商的服务滞后问题，而且可以有选择性地实施数据的同步和过滤。

4.6.3 政务

作为公链，根源链的透明度和不可篡改有助于保持政务信息和执行监督的透明与公正，以及政府形象的维护。

基于区块链技术提供政务应用或政务公开记录并不是根源链的首创，但根源链在政务方面的应用，相比其他私有链、联盟链，所提供的能力与应用更为多样、全面。

具体表现为：

- 合约机制可以用于一些需要公开和强制执行的事务；
- 信息上链记录可以用于公告；
- BLFS 存储在法院存证、交通证据存证方面提供远高于其他区块链解决方案的存取能力和读写速度，同时提供足够高强度的防篡改；

- 基于根源链的计算能力和可调度加密能力，可以作为政务网的安全应用网关等等。

4.6.4 大数据与人工智能

海量获取任何类型的大数据来源对任何想要进行机器学习的人来说都是一项挑战。基于根源链的 Token 激励机制，可以对提供数据与计算等基础资源能力的对象进行激励，而让需要数据进行机器学习的使用者参与进来并使用 Token 交换。在参与者的生态圈中，提供者的数据转化为 token 再转化为等价交换物，使用者输入等价交换物获得 token 再转化为需要的数据。相比传统的数据采集模型，根源链无疑提出了一种新的范式，不仅有利于该范式下的参与者，而且促进了平台数据获取的永续性，进一步加强了根源链生态建设的活力。

根源链改变人工智能的途径：

- 人工智能技术的发展依赖于大量来源的数据可用性，根源链作为公链，天然具备公开、透明的数据提供者角色
- 人工智能的发展取决于数据的获取方式永续性，根源链作为永续的数据源，是机器学习进行数据训练的福音，彻底解决了数据匮乏的问题
- 人工智能的发展取决于数据的流动性，根源链作为公链的分散性意味着人工智能的发展不再束手束脚
- 人工智能的发展取决于数据的可信性，根源链比封闭的人工智能有更高的透明度利于审计，而且新型的密码学实现促使数据更加安全可靠
- 人工智能的发展取决于数据的安全性，根源链的算力共识机制保证了基础设施固若金汤，确保数据安全、可靠

5 经济原型

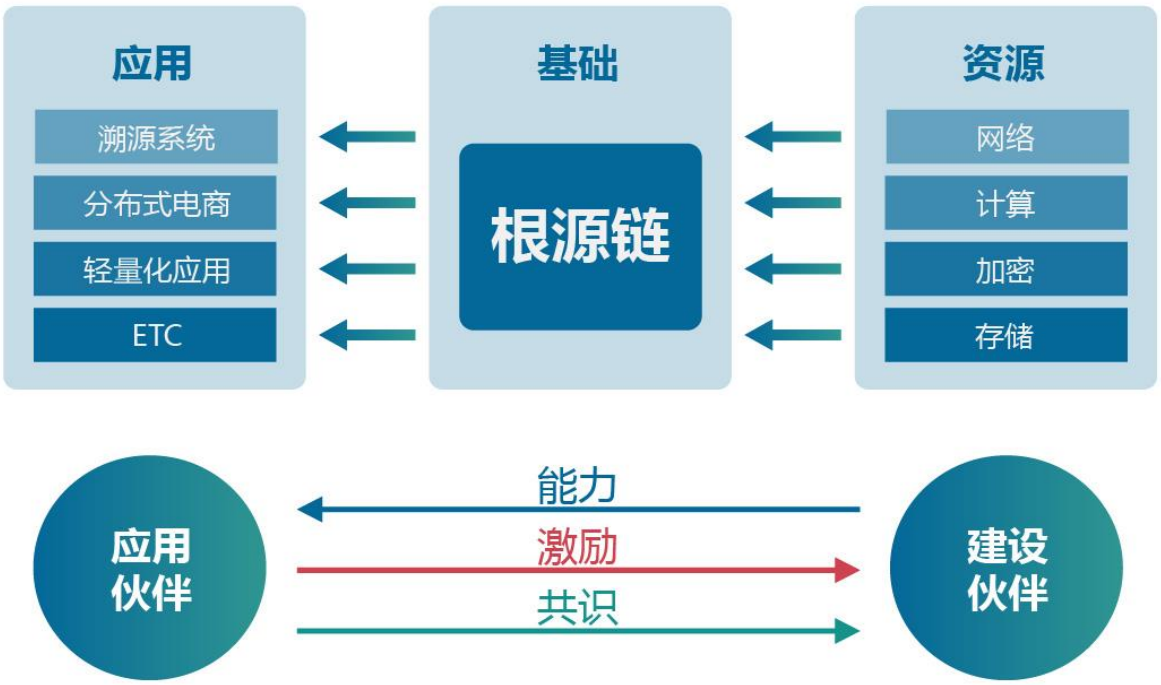
5.1 经济体系

根源链网络基于参与根源链生态体系建设的各方所提供的资源与能力，通过抽象与运算，记账生成根源链经济体系通证 BSTK（BlockChain Source Token），其正式名称为根源链通卡，简称为根源卡，BSTK。

BSTK 总量上限为 210 亿个，约 147 年生成完毕。实际流通的 BSTK 数量受根源卡驱动行为机制限制，总是小于甚至远小于当前已生成的 BSTK；基于同样原因，BSTK 的实际总量亦小于总量上限。

5.1.1 通用经济体系

根源卡 BSTK 不是单纯的代币或者数字加密货币。根源卡是根源链网络中用于各类资源贡献与奖励的结算工具，亦是根源链的数据溯源与确权的基本载体，同时具备经济价值与使用价值。在经济体系中，根源卡 BSTK 是根源链生态中不可或缺的组成部分。



（1）生态体系

根源卡是根源链所使用的唯一通行的加密数字令牌，它在各类参与根源链生态的不同角色用户之间建立经济关联，通过基于根源卡为结算工具的交易行为，使能力与激励的计算形成公平共识，简化交易环节，促进经济协作发展；通过使用基于根源卡驱动的各类链上应用，实现 Off-Chain to On Chain 关联，实现区块链化的应用生态，共同建设可信的技术与经济体系。

（2）建设伙伴

为了构建完整的生态体系，根源链需要对参与根源链生态建设，并提供基础资源的建设伙伴提供公平奖励。建设伙伴付出和使用自己的资产、设备、资金、资源，通过各类通用或定制型的软硬件及物联网设施，向根源链提供网络、计算、加密、存储等基础性资源，甚至基于区块链计算机和算力服务进行优化，提供一次加工型资源，而根源链则基于相应的共识机制向建设伙伴给予根源卡奖励。建设伙伴及最终用户均可以将获得的根源卡用于各类使用根源卡驱动的应用中，或用于兑换根源链上各类应用伙伴提供的增值服务。

（3）应用伙伴

通过建设伙伴提供的各类实体或数字化的资源，及其通过根源链 BOS 转化后形成的支持能力，根源链逐步形成强大的生态体系；并基于这部分基础资源，为应用伙伴提供可靠的公有链基础设施能力支持，为整个商业经济带来活力。 应用伙伴基于根源链这一基础设施，搭建各种商业应用，实现链上与实体经济的双重获益。应用伙伴使用根源卡获得相应的资源，以及使用基于根源卡驱动的业务流，低成本的建设自己的商业应用，同时将具体的服务提供给最终用户，获得根源卡或法币资金收益。

5.1.2 链上经济体系和根源卡驱动行为机制

在根源链生态体系中，根源卡 BSTK 不仅是通用经济体系中的结算工具，亦在和区块链紧密结合的环节中，承担技术-经济的双重交互身份。

（1）记账挖矿行为

使用定制的区块链计算机、算力服务等定制型的资源提供设施，用户可以快速成为根源链建设伙伴，向根源链网络提供网络、计算、加密、存储等基础资源，这一过程接近于传统的数字货币挖矿；用户将通过获得新生成的根源卡 BSTK 的形式，获得基础的记账挖矿奖励。

（2）根源链使用行为

应用调用根源链 API，进行数据查询、统计、分析、计算，以及在特定合约机制下运行 DAPP，交易转移 BSTK 等，这些过程相当于将 BSTK 作为 GAS 使用，会消耗一定数量的根源卡，并由对应的资源提供方在记账挖矿过程中，基于共识计算获得。

（3）根源卡驱动行为

大多数基于根源链的应用，其基本的数据信息传递载体需要使用相应数量的根源卡 BSTK。这一过程中，所使用的根源卡将以类似锁定的状态限制在应用交互环境内，并在遵循上文的消耗方法的前提下，根据应用自身特性，存在根源卡销毁机制。

例如，在某一食品溯源应用中， 基于应用伙伴企业 A 的商业考虑，使用一定数量（e.x：1000 万个 BSTK）的根源卡进行产品溯源。则在企业 A 的食品溯源应用持续运行过程中，该 1000 万 BSTK 会被 Label 染色等机制锁定在本应用内，无法流通至二级市场，也不能和未作 Label 处理的 BSTK 混用；同时，根据企业 A 的产品特性，这一部分 BSTK 在应用运行结束后，会有一定比例被永久销毁。

不仅在商业应用中，这一行为机制同样广泛适用于基于根源链生态的各类应用环境与应用级别。例如，在基于根源链的 LN 交易环境中，若节点服务作为固定服务设施长期存在，则其根据交易上限锁定的对应数量的 BSTK（e.x：500 万个 BSTK）同样无法进行流通和交易，但不存在销毁机制。由于这一机制的存在，使用根源卡驱动行为的应用越多，根源卡的实际可流通数量越少，总量上限也会因此减少。

5.2 通证分配

5.2.1 通证比例

根源卡 BSTK 总量为 210 亿。基于根源卡 BSTK 并非一次产生，大部分是由记账挖矿生产而来，因此以下通证分配比例均 BSTK 总量的比例计算，实际流通数量远小于该总量。部分分配比例存在锁定，见通证方案一节所述。

由于根源卡驱动行为机制的存在，根源卡 BSTK 不存在固定的流通比例。任意时刻实际流通量可按如下方式进行计算：

当前流通量=当前记账挖矿生产总量-当前动态锁定量+解锁流通量

根源卡 BSTK 的总分配比例为：

记账挖矿生产：70%

-动态锁定：52%

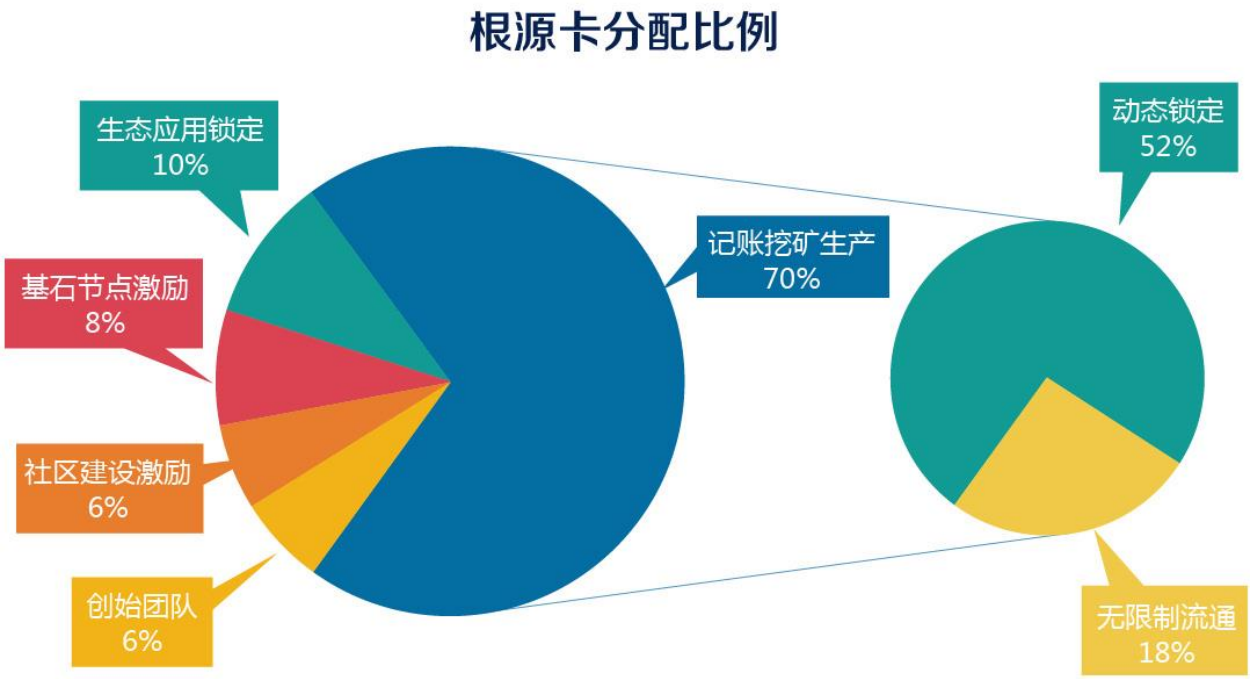
-无限制流通：18%

生态应用锁定：10%

基石节点激励：8%

社区建设激励：6%

创始团队：6%



5.2.2 通证方案

（1）记账挖矿生产

通过向根源链提供相应资源，从而记账挖矿生产是根源卡 BSTK 的直接获取方法。挖矿记账生产的根源卡占总量的 70%，即 147 亿个，平均每年产生约 1 亿个，147 年左右产生完毕。实际产生速度受根源链网络规模与应用规模影响，约在 140-210 年之间。任何向根源链生态提供相应资源的用户，均可以成为建设伙伴，通过此种方式获得 BSTK。

在这一方式获取的 BSTK 中，会锁定最多占当前已通过记账挖矿生产数量的 75%（最多占根源卡总量的 52%）的根源卡，通过根源卡驱动行为机制，动态锁定于根源链应用生态中，无法进行不受限制的流通和交易。为了保证根源卡的通用经济体系正常运作，根源链将保证最低有占当前已通过记账挖矿生产数量的 25%（根源卡全部生产完毕时，最少占总量的 18%）的根源卡属于无限制流通的根源卡。由于记账挖矿生产的特性和以上条件，根源卡初始无限制流通的数量为 0，随着记账挖矿行为，逐年提升。

（2）生态应用锁定

根源链是为应用服务的基础设施公链，为促进应用生态发展，永久锁定总量的 10%，即 21 亿个，用于根源卡驱动行为的应用使用。和动态锁定的部分不同，该部分锁定的根源卡永不进入无限制流通，仅在各生态应用内部的相关交互环境中使用，作为信息数据传递和记录的凭证。

由于生态应用对根源卡的实际需求大于 21 亿个，因此实际环境中，挖矿记账中的动态锁定部分会动态补充应用的需求。实际应用中，被锁定而无法流通的根源卡所占的实际比例最大是 62%，即 130.2 亿个。该数量会随着挖矿记账产生根源卡而动态变化。

（3）基石节点激励

为了根源链基础资源能力快速达到相应技术所要求的基准，根源链提供占根源卡总量的 8%，即 16.8 亿个，用于基石节点激励。在根源链的不同发展阶段，使用各类基于根源链网络技术优化要求的网络、计算、加密、存储、物联网等综合资源设施，持续参与和推进根源链网络快速发展的用户，会根据其资源类型和节点贡献，获得额外的基石节点激

励。该部分存在锁定，自奖励确认后第 30 日起，分 N 日（最长 360 日）发放，每日发放 1/N，直至发放完毕。获得奖励的用户中途不符合奖励标准的，后续奖励停止发放。

（4）社区建设激励

根源链需要社区的力量以快速发展和完善。根源链提供占根源卡总量的 6%，即 12.6 亿个，用于社区建设激励，包括但不限于支持和孵化各种基于根源链的 DAPP 及应用生态，额外奖励早期记账节点和重大贡献，作为社区合作，项目合作经费，推进生态样板应用发展，增强根源卡流通性与价值管理等使用。该部分存在锁定。对于个人或团队所获得的奖励性质的根源卡，自奖励确认后第 6 个月起，每 6 个月释放 20%，直至释放完毕。

（5）创始团队

根源链将提供占根源卡总量的 6%，即 12.6 亿个，用于奖励创始团队前期对于根源链项目的探索和开发，激励其长期维护与发展根源链。该部分存在锁定。自主网上线后第 6 个月，第一年解禁该部分 40%，第二年解禁 20%，第三年解禁 20%，第四年解禁剩余部分。

6 结语

区块链技术将开启全新的经济协作生态。本白皮书主要对根源链当前阶段的整体技术框架以及所涉及的相关基础技术进行了简明的解释，然而随着技术的进步与应用领域的拓展，根源链也将持续不断的更新与进化，相应的，根源链的白皮书也会紧随项目的发展而不定时的进行持续更新。根源链作为一个基于数据信息追溯及确权的泛物联网应用公有链，将不断追求技术上的进步与突破，成为高可用型公链基础设施。根源链团队也欢迎新老伙伴一如既往的支持根源链与根源链社群，共同参与根源链项目建设，参与区块链行业，分享区块链带来的价值。