荣泽区块链底层技术平台（RBC）

白皮书 V2. 4. 2

江苏荣泽信息科技股份有限公司

目录

一、 产品概述

(一) 简介

荣泽区块链底层技术平台(RBC)是荣泽科技自主研发的一款高性能、高安全、可扩展的区块链基础性软件产品。2018 年顺利通过了工信部下属信通院功能、性能两项可信区块链评测， 2021 年产品通过公安一所的区块链安全评测。

(二) 名词解释

专有名词	解释说明
RBC	RBC（Rongzer Blockchain）荣泽区块链底层技术平台
ROracle	ROracle（Rongzer Oracle）荣泽预言机
P2P	P2P（Peer to Peer）对等网络
TLS	TLS（Transport Layer Security）传输层安全性协议
EVM	以太坊智能合约运行时的沙箱环境
HVM	轻量级 Java 智能合约运行时的沙箱环境
API	API（Application Programming Interface）应用程序编程接口
SDK	SDK（Software Development Kit）作为外部编程接口通过内部的 HTTP 服务器同底层平台进行交互
BFT	BFT（Byzantine Fault Tolerance）拜占庭容错共识算法
CFT	CFT（Crash Fault Tolerance)）非拜占庭容错共识算法
TEE	TEE（ Trusted Execution Environment）可信执行环境
DID	DID（Decentralized Identity）分布式数字身份标识符
IPFS	IPFS（InterPlanetary File System）星际文件系统
LICENSE	本文档指 RBC 的软件许可证

(三) 版本发布

1. 版本说明

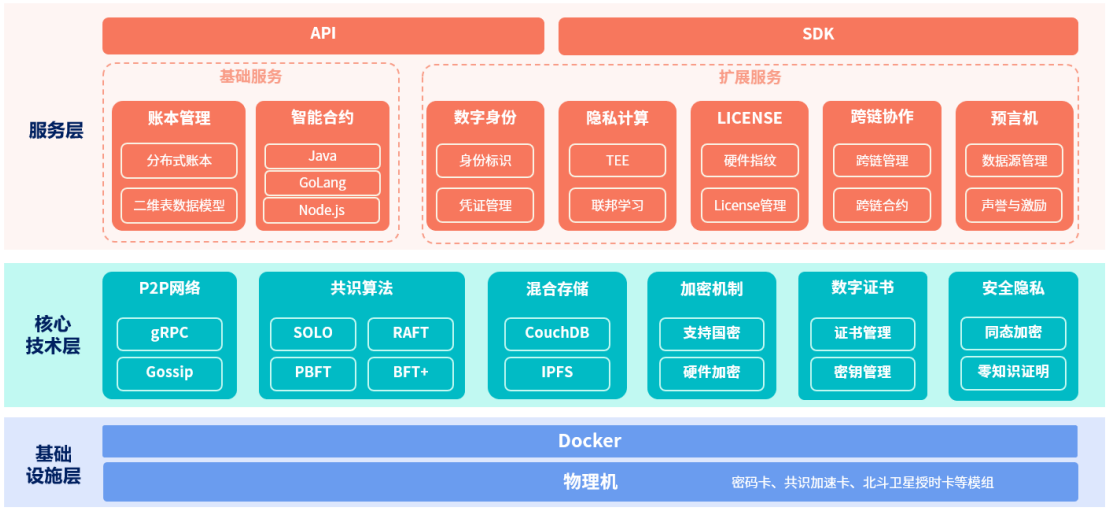
版本	修订日期	修改内容	作者
V2. 4. 2	2022 年 9 月 9 日	初稿	曾小冬
V2. 4. 2	2022 年 9 月 29 日	终稿	王君、朱俊领、曾小冬

2. 版本功能特性

基础特性	网络通信	P2P 作为节点之间点对点进行数据传输和共识的技术，是区块链系统的网络基础
	证书服务	符合 PKI 规范及支持证书的分层分级管理，提供实体证书、中间证书、根证书三种
	共识算法	支持根据不同业务场景的不同要求，提供有 Raft、PBFT 及 Solo 等共识算法
	账本管理	支持并提供分布式账本和结构化数据模型
	安全隐私	提供数据存储安全、数据访问安全、数据共享安全和合约执行安全以及数据隐私、合约隐私、网络隐私、跨链隐私和应用隐私保护
	加密算法	支持国际通用密码标准和国密标准 SM 两种密码体系
	智能合约	支持 Java、Go Lang、Node. js 等智能合约开发语言，并对运行容器进行了安全增强
扩展特性	云原生	支持云原生技术，充分利用云平台的弹性和分布式优势，实现快速部署、按需伸缩、不停机交付等优势，在不同层级部署区块链节点和对智能合约进行管理
	数字身份	提供符合 W3C 标准的分布式数字身份，为主体和抽象主体提供唯一标识以及可验证的数字凭证
	硬件加密	提供硬件密码卡进一步提高加/解密和验签性能
	隐私计算	提供数据在可用不可见的情况下实现数据价值共享，在数据共享过程中实现价值挖掘与隐私保护之间的平衡
	IPFS	提供接入 IPFS 系统数据存储服务，对区块链的冷/热数据进行分类，热数据存储在链中，冷数据存储在 IPFS 系统中
	LICENSE	提供 license 许可证管理服务，将权限绑定在一体机的硬件指纹上，只有授权的一体机可运行区块链软件
	跨链协作	提供不同区块链间的协作机制，为多链跨链协同提供统一、规范化的协议与服务
	预言机	提供区块链预言机服务，桥接链外数据，执行更复杂的业务逻辑，扩展更丰富的的业务场景

二、 RBC 产品介绍

（一） RBC 产品架构



上图：荣泽区块链底层技术平台(RBC)产品架构

（二） RBC 产品功能

1. 基础功能

（1）网络通信

P2P 作为节点之间点对点进行数据传输和共识的技术，是区块链系统的网络基础。RBC 提供的 P2P 网络，主要采用传输层与网络层解耦的方式，便于灵活应用于节点、传播、同步和流控间服务，提高区块链网络的适用性和灵活性。

① 节点类型

采用不同类型的节点进行分层协同运行管理。RBC 提供根据链上节点不同的类型角色对节点类型进行了划分，并将不同类型的节点做了协同优化管理，RBC 的节点分为验证节点、非验证节点。

- 验证节点：是区块链网络中参与共识验证的节点，RBC 赋予验证节点绝对的参与权，并且拥有全量的数据；
- 非验证节点：在区块链网络中不参与共识验证，仅参与账本记账，需要依附验证节点来保证与全网状态的最终一致性。同时 RBC 赋予非验证节点完善的状态恢复机制，可以很好的为上层提供读写分离服务。

② 传播策略

RBC 通过在事务执行（背书和提交）对等节点和事务排序节点之间划分工作负载来优化区块链网络性能、安全性和可扩展性。RBC 提供网络操作的解耦实现了一个安全、可靠和可扩展的数据传播协议-Gossip，确保数据的完整性和一致性。RBC 通过 Gossip 数据传播协议完成 3 个功能。

- 管理节点发现和 channel 的成员关系；
- 同 channel 上的所有 peer 扩散账本数据；
- 同 channel 上的所有 peer 间同步账本状态。

Gossip 数据传播协议通过推送数据和拉取数据两种数据传输方式，最终将数据传播到网络中的每一个节点。

③ 同步策略

RBC 提供节点之间使用数据同步保证账本数据和状态数据的即使更新，数据同步主要有 2 类：

- 主动广播，广播新打包的区块，排序节点把区块发送给主节点，它基于 Gossip 的推送数据；
- 主动请求，新加入的节点，向已存在的其他组织锚节点请求数据，锚节点给它响应，它基于 Gossip 的拉去数据。

④ 流控管理

RBC 根据业务需要对允许进入区块链系统的流量进行策略控制，当系统流量超过系统设置的上限，将对超过部分进行拒绝接收。目的是为了防止网络通信过程中因大量无用交易请求占用了节点处理时间，而耽误其他交易以加强系统在满足业务要求的前提下保证系统的安全性。

（2）证书服务

RBC 按照 PKI 规范提供证书服务，证书按照在证书链中的位置，可以被分为最终实体证书、中间证书、根证书三种。中间证书和根证书都可以签发证书，而最终实体证书不能继续签发证书。在证书链中，相邻的两个证书是签发和被签发的关系，因此可以相对地称二者为父证书和子证书。

① 证书类型

证书名称	证书说明
RootCA	根证书，用于 Ecert、SDKCert 的签发和验证，RBC 区块链网络中可能存在多个 RootCA，一个 RootCA 只能验证由自己颁发的证书的合法性
ECert	节点准入证书，用于证明该节点为验证节点，持有 Ecert 的节点才能参与共识
SDKCert	客户端准入证书，用于证明 SDK 的合法性，持有 SDKCert 的客户端才能访问区块链网络，向节点发送请求
TLSCA	安全传输层协议根证书，用于 TLSCert 的签发和验证
TLSCert	安全传输层协议证书，用于传输层网络通信，在传输网络传输过程中需要验证传输层安全协议证书的安全性，验证通过即可以进行正常网络通信，反之则无法进行网络通信

② 证书体系

RBC 提供的证书体系分为非分布式 CA 认证体系、分布式 CA 认证体系两种方式。

- 非分布式 CA：非分布式 CA，即中心化 CA，可以由外部安全性与权威性的可信机构提供，也可通过自建 CA 体系实现。自建 CA 体系遵循 PKI 系统，建立安全完整的运营管理体系，有唯一的 CA 进行证书的签发与管理。
- 分布式 CA：分布式 CA 是将证书管理权限由中心机构移到区块链各参与方，已参与的区块链节点经过共识达成一致后颁发准入证书给新加入的节点，在建立连接阶段完成证书认证，具有协同共建、多方治理等优点。

③ 证书验证

验证证书的有效性分为 3 个步骤：验证证书内容、验证证书签名、查询证书是否被吊销。

- 验证证书内容

  除了验证证书过期时间、签发结构和被签发主体身份等基本信息，还会验证和区块链有关的信息，包括：

  证书用途：证书中有相应字段规定证书用途，其中，ECert 配置在节点上用于节点身份的验证，SDK 证书 SDKCert 配置在 SDK 上用于 SDK 身份的验证。

证书所属节点 hostname：证书中的 hostname 字段用于绑定证书和节点，因此 node1 的证书拷贝到 node2 下是无法正常工作的。

- 验证证书签名

验证证书签名是一个验签的过程，RBC 会使用父证书的公钥验证该证书的签名是否有效。

- 查询证书是否被吊销

通过查询吊销列表完成。

④ 私钥管理

为应用适配层提供两类接口：非托管型接口和托管型接口；同时提供私钥保险箱，私钥的写入和读取在保险箱体系里以密文的方式传输和存储。

- 非托管型接口

适合有能力在应用端实现安全级别较高的私钥生成和使用的企业机构。例如，在金融领域，将私钥的生成与管理跟现有的 U 盾、电子签名等安全的客户端体系相结合。

- 托管型接口

适用于互联网化程度较高的应用场景。公私钥直接作为用户名和密码使用，对普通用户来说存储与记忆成本较高同时体验也差，因大多数用户已习惯传统用手机号、邮箱、昵称等作为用户名。在 RBC 提供的托管型接口里，通过安全的私钥生成与管理的体系，使应用层用户信息与区块链地址映射，让上层应用层用户和底层区块链平台都不触碰到用户的私钥情况下无感运用私钥。

- 私钥保险箱

私钥的写入和读取在保险箱体系里以密文的方式传输和存储。用户与密钥一一对应。密钥在客户端侧生成且客户端不用保存，每次需要使用私钥签名时，客户端能够通过盲签名流程得到加密过的私钥以及解密的密钥。

（3）共识算法

RBC 提供根据不同业务场景中对可靠性、性能、安全性、防作恶等不同要求的自适应共识机制，支持 PBFT、Raft、Solo 以及 CFT/BFT+等不同共识算法来满足不同业务场景需求。

① PBFT

PBFT 是 Practical Byzantine Fault Tolerance 的缩写，意为实用拜占庭容错算法，实现了在有限个节点的情况下的拜占庭问题，在确保容错性同时保证一定的性能，最大可容忍小于 1/3 个无效或者恶意节点。

角色划分：首先在 PBFT 共识机制中，节点共分为三种角色：

- 客户端节点，负责发送交易请求。
- 主节点，负责将交易打包成区块和区块共识，每轮共识过程中有且仅有一个主节点。
- 记账节点，负责区块共识，每轮共识过程中有多个记账节点，每个记账节点的处理过程类似。

其中，主节点和记账节点都属于共识节点。

算法流程：

- request 阶段：首先客户端向主节点发起交易请求。
- pre-prepare 阶段：主节点收到来自客户端的请求后，将信息打包，向全网广播请求信息。
- prepare 阶段：所有节点在收到主节点广播的信息后，把带有自己签名的投票消息广播给其他节点。
- commit 阶段：主节点在收到来自 2n+1 个诚实节点的反馈后，将消息打包反馈给客户端。

② RAFT

与 BFT 类共识算法相比，CFT 共识，尤其是 Raft 共识算法，从性能、可理解性和可实现性等方面来说具有一定优势。对于所有参与节点的身份都是已知的，每个节点有很高的可信度，故在某些可信度高的业务场景下可采用非容错拜占庭节点的 Raft 共识算法。

角色规划：首先在 Raft 共识机制中，节点共分为三种角色：

- 领导者（Leader）：接受客户端请求，并向从节点同步请求日志，当日志同步到大多数节点上后将提交日志，并广播给从节点。
- 从节点（Follower）：单向接收并持久化主节点同步的日志。
- 候选节点（Candidate）：主节点选举过程中的过渡角色，当从节点在规定的超时时间内没有收到主节点的任何消息，将转变为候选节点，并广播选举消息，且只有候选状态的节点才会接收选举投票的消息。候选节点有可能被选举为主节点，也有可能回退为从节点。

在同一时刻，集群中只有一个 Leader，负责生成日志数据（对应在区块链中即负责打包）并广播给 Follower 节点，为了保证共识的正确性和简单性，所有 Follower 节点只能单向接收从 Leader 发来的日志数据。

共识流程：Raft 算法共识流程分为主节点选举和日志同步两步。将时间分为一个个的任期（term），每一个 term 以 Leader 选举开始。在成功选举 Leader 之后，Leader 会在整个 term 内管理整个集群。如果 Leader 选举失败，该 term 就会因为没有 Leader 而结束。

③ SOLO

为了降低平台的试用门槛和特定场景的私有链搭建，平台提供了单节点 solo 共识算法。基于 solo 共识算法的单机版节点屏蔽了网络延迟等不可控因素，这使得开发人员可以专注于自己模块本身的开发和调试。

（4）账本管理

区块链本质上是一个分布式账本系统，账本的设计至关重要，RBC 在账本存储管理上提供分布式存储系统和结构化数据模型能力。

① 分布式存储系统

通过分布式存储系统存储账本数据，账本数据主要包含区块数据和状态数据。区块数据通过区块的形式进行串联，所有区块被从后向前有序地链接在一个链条里，每一个区块都指向其父区块，保证了用户交易的不可篡改以及可追溯性；状态数据采用数据模型维护区块链系统的状态，实质是一系列键值对（Key，Value），

每次执行一笔交易，修改一系列状态变量，从底层来看，就是更新了一批 KV 键值对。

② 结构化数据模型

采用结构化数据模型方便存储结构化数据和模糊查询。CouchDB 将数据存储为非关系性的 JSON 文档，这使得用户可以与现实世界相似的方式来存储数据，并支持二进制数据以满足所有数据存储需求。CouchDB 具有高可用性和容错引擎，在确保数据的安全性下，提供丰富查询能力。

（5）安全隐私

RBC 提供完备的安全保障与隐私保护机制，保障数据安全、身份隐私和数据隐私。

① 安全保障

从存储安全、访问安全、传输安全和环境安全方面，提供数据安全保障。

- 存储安全

基于区块链的分布式账本技术、共识机制及加密机制等技术基础，提供对结构化数据加密，保障数据的容错性、一致性及安全性；同时提供对非结构化数据存储在链下 IPFS 节点中，将 IPFS 节点返回的哈希值存放到链上，可形成“链上索引，链下存储”。

- 访问安全

提供黑白名单、身份认证和授权访问控制保障数据访问安全，身份认证采用基于区块链的分布式 PKI 体系，关联用户身份与证书公私钥，鉴定用户的真实身份；访问控制采用基于智能合约的角色权限模型，保证用户仅能合法访问享有权限内的数据。

- 传输安全

在黑白名单机制排除威胁地址的基础上，节点间基于 TLS 传输层安全性协议，通过 TLSCA 签发的证书进行安全通信，验证通过即可以进行正常网络通信，反之则无法进行网络通信。

- 环境安全

提供基于硬件隔离的安全执行环境（TEE），隔离安全世界来保护环境安全。非安全世界的进程禁止访问安全世界，以保障存储在安全世界的代码和数据不被非法访问或窃取，有效减少操作系统漏洞、外界的攻击和病毒的入侵。

② 隐私保护

RBC 中，提供身份隐私保护和数据隐私保护。在身份隐私保护方面指的是用户身份信息和区块链匿名地址间的关联数据；在数据隐私保护方面不仅指区块链系统中的交易信息，还包括拓展业务内涉及的业务数据。

- 身份隐私保护

在身份隐私的保护上，不仅提供分布式数字身份标识符（DID），根据不同的场景需披露的信息，使用不同的 DID 标识符，避免被进行关联性分析；还提供环签名和零知识证明等，保障区块链用户的身份隐私安全。

- 数据隐私保护

数据隐私指区块链上存储的数据的隐私，RBC 不仅提供多链多通道来实现不同业务交易数据的隔离，还提供交易数据哈希值上链、链下数据加密上链，即先在链下通过加密的方式将隐私数据加密后，再将密文上链存储。

（6）加密机制

RBC 采用可插拔的加密机制对业务完整生命周期进行不同策略的加密。具体采用散列算法（哈希）、非对称加密算法、硬件加密和密钥管理机制，支持国际通用密码标准和国密标准（SM）两种密码体系。

① 哈希算法

通过哈希算法生成体积可控、不可逆推的数字指纹，如交易摘要、合约地址、用户地址等，保证平台的数据安全，支持 SHA 系列（SHA2-256 等）、国密 SM3。

② 非对称加密

采用基于椭圆曲线算法的国际标准算法 ECDSA 等和国密算法 SM2 等实现非对称加密，应用主要包含数字签名、密钥协商和公钥加密。

③ 硬件加密

- 提供硬件加密卡，支持国产密码算法，SM2、SM3、SM4 算法
- 加密卡符合密码模块安全等级第三级要求，保证密钥管理和算法实现的高安全性；
- 加密卡，提供高性能高稳定的密码运算服务；支持多线程、多进程同时访问；支持异步访问机制，有效降低访问延迟；支持负载监控，便于弹性分配密码运算资源；支持多卡并行，支持密钥同步，互为备份，提高系统应用的可靠性；支持 Docker 等虚拟化环境调用，便于云环境部署；
- 硬件密码卡性能指标

类别	项目	密码卡
通用项目	接口	OPENSSL、JCE、SDF
密码算法	对称算法	SM4
	非对称算法	SM2
	摘要算法	SM3
密钥存储	SM4 密钥	以密钥密文存储在外部
	SM2 密钥对	以密钥密文存储在外部
密钥生成速度	SM2	20000 对/秒
	随机数	14Mbps
密码运算速度	SM2 签名	50000 次/秒
	SM2 验签名	15000 次/秒
	SM2 加密	14000 次/秒
	SM2 解密	17000 次/秒
	SM3 摘要运算	1Gbps
	SM4 加解密	5～20Gbps
可靠性指标	平均无故障时间 MTBF	≥30000 小时
物理参数	尺寸	168*79*22mm
	接口	PCI-E 3.0 X8
	最大功耗	20W

环境参数	工作环境温度	0℃～55℃
	工作环境相对湿度	10%～90%非凝结
	存储环境温度	-10℃～70℃
	存储环境相对湿度	5%～90%
	最低风速	400 LFM

④ 密钥管理

采用密钥托管和非托管方式对密钥管理。托管通过国家密码管理局认证的用户智能密码钥匙完成密钥管理功能，用于保管用户私钥和签名；非托管通过结合U盾、电子签名等私钥的生成与管理的客户端安全体系来保障。

（7）智能合约

智能合约，又称为链码（Chaincode），是运行于区块链上的应用程序。使用计算机语言描述合约条款、交易的条件、交易的业务逻辑等，通过调用链码实现交易的自动执行和对账本数据的操作，是应用程序与底层区块链交互的媒介。

RBC提供的链码服务如下：

- 支持两种链码，分别是系统链码和用户链码。系统链码用来实现系统层面的功能，包括系统的配置，用户链码的部署、升级，用户交易的签名和验证策略等；用户链码用于实现用户的应用功能，开发者编写链码应用程序并将其部署到网络上，通过与网络节点交互的客户端应用程序调用链码。
- 支持Java、GoLang、Node. js作为链码开发语言，让大多数开发人员能快速上手。
- 支持通过 Web IDE，提供开发者编写链码无需安装任何工具即可在线查看、比较、下载与升级链码。
- 支持对链码整个生命周期操作，包含打包、安装、实例化、升级、停止和启动。

- 提供链码运行于隔离的 Docker 容器中，在链码部署的时候会自动生成合约的 Docker 镜像，通过 gRPC 与背书节点连接，双方通过发送 ChaincodeMessage 来进行交互通信，以及操作账本中的数据。
- 提供链码与数据分离的。RBC 链码和底层账本是分开的，升级链码时并不需要迁移账本数据到新的链码当中，真正实现了逻辑与数据的分离。
- 支持链码的账本是与其他链码互相隔离，不能直接访问，只有链码在获取相应的许可后才能调用其他链码及其账本。

2. 扩展功能

（1）数字身份

数字身份是指将真实身份信息浓缩为数字代码，可通过网络、相关设备等查询和识别的公共密钥。数字身份覆盖的范围非常广，小到可以是个人身份，大到可以是公司主体，甚至物和资产也可以具有数字身份。数字身份的发展阶段大致经历了四个阶段：中心化身份、联盟身份、以用户为中心的身份和自主主权身份。

RBC 提供的数字身份是自主主权身份，相对于传统的基于 PKI（Public Key Infrastructure，公钥基础设施）的身份体系，基于区块链建立的 DID 数字身份系统，具有分布式认证、隐私保护、自主管理等特点，将用户身份的管控权还给用户，并打破跨平台间的信息屏障。

RBC 提供的数字身份目前以账户的形式提供服务，其服务包含如下：

- 提供用户“创建”自己的身份，通常是通过创建自己的惟一标识符(或多个标识符)，然后将身份信息附加到该标识符上（DID），利用区块链账本的不可篡改性，并结合密码学算法，将身份数据加密上链，用户通过掌握个人身份私钥进行身份信息的可信授权。
- 通过统一的分布式数字身份平台，提供连接凭证发行方和凭证应用方，为主体提供可验证的凭证管理，解决身份凭证在不同业务主体间流通的难题。

- 通过一系列可插拔的适配器，提供将凭证发行方的接口服务转换成可验证的凭证，凭证应用方提供统一、规范化的凭证验证服务。
- 提供分布式认证和可移植服务，用户不仅可以通过分布式的社会关系获得全面的身份认证，同时可以携带自己的身份，不局限于某一通道、应用或平台。
- 提供自主可控服务，用户可以完全拥有、控制和管理自己的身份，不依赖于应用方，对自我信息、组织信息、设备信息的管理和自我凭证创建与管理。

（2）隐私计算

隐私计算是在保护数据本身不会对外泄露的前提下实现对数据价值挖掘和开发利用的信息技术，是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。

区块链与隐私计算的有机结合，实现更广泛的数据协同。一方面使原始数据在无需出域与归集的情况下，可实现多节点间的可信协同计算和数据隐私保护；另方面能够解决大数据模式下存在的数据过度采集、数据隐私保护，以及数据储存单点泄露等问题。

RBC 通过结合隐私计算技术中的可信执行环境(TEE)、联邦学习(FL) 和安全多方计算(MPC)实现在无需共享原始数据的情况下，实现多节点间的协同计算和数据隐私保护。

① 可信执行环境

RBC 结合基于可信硬件的可信执行环境。提供了：一是基于硬件隔离的安全世界来保护敏感数据的安全计算；二是对用户的身份、密钥和证书等敏感信息加密和完整性保护。

② 联邦学习

RBC 结合基于人工智能的联邦学习。在不可变性和可跟踪性的区块链系统中，提供了协作构建强大的机器学习模型的能力，并使用隐私保护机制(防御蒸馏和对抗训练正则化)来保护数据的隐私。

③ 安全多方计算

RBC 结合基于密码学（同态加密、零知识证明等）的安全多方计算。提供了在密钥管理、身份认证、分布式存储、共识机制、计算压缩与扩容等环节中，以提升区块链系统的安全性的隐私性。

（3）IPFS

RBC 结合 IPFS 系统数据存储框架，提供对区块链的冷/热数据进行分类，热数据（世界状态）存储在链中，冷数据（交易日志）存储在 IPFS 系统中。具体将账本中的世界状态存放到区块链 Couch DB 数据库中，将账本中的交易日志数据打包存放到 IPFS 系统中，将 IPFS 返回的哈希值存放到区块链上，形成“链上索引，链下存储”的数据存储模型，不仅优化了链的性能，也节省了链存储空间和有效缓解链数据存储压力。提供功能如下：

- 支持 GB 级别图片、音频、视频等各类文件上链存储，通过哈希值上链存储，保证文件内容无法篡改，真实可信。
- 支持分层分片、节点白名单和用户白名单，自定义授权存储节点与用户权限，保障文件数据安全隐私。
- 支持上传数据前对数据加密获得密文，再将密文上传至 IPFS 系统，避免因为地址泄露等问题而泄露数据的内容信息，进一步保障数据存储中的保密性。
- 支持通过验证链码，获取存在区块链上的哈希值，通过该哈希值去 IPFS 系统中查询相对应的交易日志数据，然后取出想获取的数据。

（4）LICENSE

RBC 提供基于 license 许可证激活方式的许可证管理系统，它将权限绑定在节点机的硬件指纹上，只有经过授权的节点机可以运行区块链软件。

节点机首先检查、验证 license 许可证协议。如果无授权，需先取得授权；如果授权在时间内，将允许节点机运行区块链软件；如果许可证过期仅赋予节点

机查询权限。其中许可文件是 license 许可证授权管理的重点，结合 RBC 系统的特殊性，该许可证文件的提供功能如下：

- 生成的许可证文件信息，针对每一个许可证文件有一个唯一的 LICENSE_ID 来标识。
- 支持绑定的节点机的指纹信息包括 CPU 和主板的 ID 及 MAC 地址。
- 支持绑定节点机所属企业主体的名称和统一信用代码。
- 支持对所有信息进行加密，保证整个文件的完整性。

（5）跨链协作

RBC 提供不同区块链间的协作机制，为多链跨链协同提供统一、规范化的协议与服务。促进跨行业、跨机构和跨地域的不同区块链间信任传递和商业合作，解决产业互联中端边云规模化组网的困难，从而达成应用互联及产业协同。主要包括服务部署、服务监控、跨链授权、跨链访问账本、跨链执行合约、跨链事务等功能。

- 服务部署：支持自动化部署跨链服务；支持 docker 容器部署方式；支持部署时选择多台主机、选择插件、指定部署节点数量。
- 服务监控：支持跨链数据统计，包括跨链通道数量、跨链授权数量、跨链合约数量、跨链交易数量；支持监控跨链服务状态，包括所在主机的 CPU、内存、磁盘 IO、网络等信息的监控；支持实时监控与指定时间段监控。
- 跨链授权：支持授权管理，包括增加、查看、修改、删除、访问、推送等；
- 跨链访问账本：已授权的链，支持有权限的链访问该链的区块链账本数据，包括链区块头、链区块、链交易等。
- 跨链执行合约：支持授权执行智能合约的权限，具体通过的跨链合约执行已授权链上的智能合约。
- 跨链事务：支持事务管理，包括新建事务、查看、编辑、删除事务等；支持执行事务，包括已定义的跨链事务的各数据填写和已执行过的跨链事务的各记录查看。

（6）预言机

RBC 提供区块链预言机服务（ROracle），预言机作为区块链和外部世界的桥梁，打破了区块链系统的封闭性，能够主动将外部数据引入区块链中，执行更复杂的业务逻辑，支持更加丰富的的业务场景。

主要功能点：

- 支持丰富数据源，包括网站数据、传感器采集数据、随机数、跨链数据等实时、动态、可变的数据。
- 提供灵活自主服务模式，用户可使用积分自主选择某预言机节点获取数据，同时预言机节点可通过提供数据服务获得积分奖励。
- 为预言机节点提供声誉系统，将预言机节点的历史服务水平、安全配置等指标作为评级标准，保障为用户提供的数据更优质更安全。
- 提供更全面的数据模型，便于用户使用智能合约实现更多场景应用。
- 提供健全的安全保护机制，支持 TEE 硬件可信的预言机服务，保证数据处理过程中的真实可信，支持 HTTPS、TLS 等安全传输协议，保证数据传输过程中的安全性。

三、 RBC 产品优势

（一） 性能优势

1. 快速交易验证

通过对签名算法、账本结构、数据操作、序列化、共识机制、消息扩散等关键环节的优化，荣泽区块链底层技术平台(RBC)可以实现秒级的快速交易验证。

2. 海量数据存储

区块链复式记账的模式，在系统长时间运行下，历史数据不断累积；荣泽区块链底层技术平台(RBC)借鉴传统金融系统中冷热数据分离存储、分表存储的机制，实现海量数据的有效存储。

3. 高吞吐量

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。为保证数据的一致性，防止拜占庭将军问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，荣泽区块链底层技术平台(RBC)的处理性能已经能满足每秒千级的吞吐需求。

（二） 扩展性优势

1. 满足多业务的块链结构

荣泽区块链底层技术平台(RBC)的块链结构，能够满足不同业务领域的需求，提高系统的可扩展能力和维护效率。即可用于标记资产和资产转移，也可提供不可篡改的多维事件记录，还可以用于溯源以跟踪物品的流通过程。

2. 权限控制策略

提供数据信息写入与读取两类权限控制策略。数据信息写入权限，同一账户下设置多个使用用户，并针对不同的操作设置相应的权限，满足多方签名控制的使用场景；数据信息读取权限，用户可以授予和撤回单用户或用户组对数据的操作权限，用户组可以由用户灵活配置。数据包括用户账户信息，交易信息等，粒度可以细化到交易或账户的各属性字段。

（三） 安全优势

1. 安全私钥存取

为方便用户使用区块链产品服务，除了传统的客户端生成和保存的机制，荣泽区块链底层技术平台(RBC)提供网络托管存取和硬件私钥存取（U-key）两种方案。网络托管存取，即把用户名和密码通过特定算法映射成私钥并在服务端进行存储，服务器端存储的私钥均为加密数据，私钥仅能在用户端解密；提供硬件私钥为满足金融行业及物联网行业的使用需求。

2. 多重隐私保护方案

提供多重隐私保护功能。区块链底层提供同态加密等方式，用户所有数据均加密存储，仅用户本身可见。

（四） 运维方面

1. 全平台部署

荣泽区块链底层技术平台(RBC)的所有代码均可跨平台编译运行，平台相关代码均封装成基础库，业务逻辑可实现在云平台上快速部署。

2. 可视化运维

提供运维管理所需的可视化工具。区块链节点上部署的荣泽区块链管理服务平台（RBaaS）：支持业务（区块、交易、合约、共识等）、网络（组网、时延、吞吐量等）、系统层面（CPU、内存、磁盘等）的数据信息监控；同时提供完备的日志、告警与通知机制，便于商用系统的维护。

3. 低成本接入方式

荣泽区块链底层技术平台(RBC)不仅抽象出适用于多种业务场景的 API 接口，如：资产、溯源、存证等，供业务场景下用户快速接入，满足业务功能需求；同时又提供已封装了支持多种主流开发语言的 SDK 软件开发包。