安全高效，可信互联
——工行区块链创新平台 1.0 介绍

中国工商银行软件开发中心区块链与生物识别创新实验室　万涛　邱玉华

区块链作为一种新兴技术，正在推动信息互联网向价值互联网转化。2017 年第四季度，中国工商银行（以下简称“工行”）软件开发中心区块链与生物识别创新实验室（以下简称“实验室”）以“自主研发，兼容并蓄”为原则，研究出工行首个自主可控的区块链 1.0 平台，平台具有安全高效、可信互联的特点。它自诞生之日起就瞄准企业级产品化运营能力，具备快速构建上层应用业务的能力，能满足大规模用户数量的应用场景。工行区块链平台 1.0 的核心价值在于构建可信任的多中心体系，成为构建价值互联网的基础设施，本文主要从产品架构、技术特色与优势、应用前景等方面介绍工行区块链平台产品。

一、工行区块链平台产品架构

工行区块链平台可支持在应用平台云 PaaS 上部署，整个区块链平台在技术架构上划分为区块层、合约层、交易层 3 层结构，彼此相对独立（如图 1 所示）。

交易层：向应用层提供接入服务、CA 安全认证、消息服务、流量控制等集成支撑框架功能。

合约层：面向交易层提供基于 Docker 容器的智能合约动态管理，交易执行的可靠性控制机制以及交易请求的同异步转换机制。

区块层：提供区块链核心技术功能，集成国密算法、可插拔的共识算法管理。

基础设施层：提供区块链基础服务。

配套工具：各种产品支持工具，提供开发、测试、部署、运维的全生命周期配套工具。

工行区块链平台在外部对接方式上支持互联网直联、API 接口互联、通讯前置互联、跨链互联等多种接入方式，实现与合作方的数据传递。

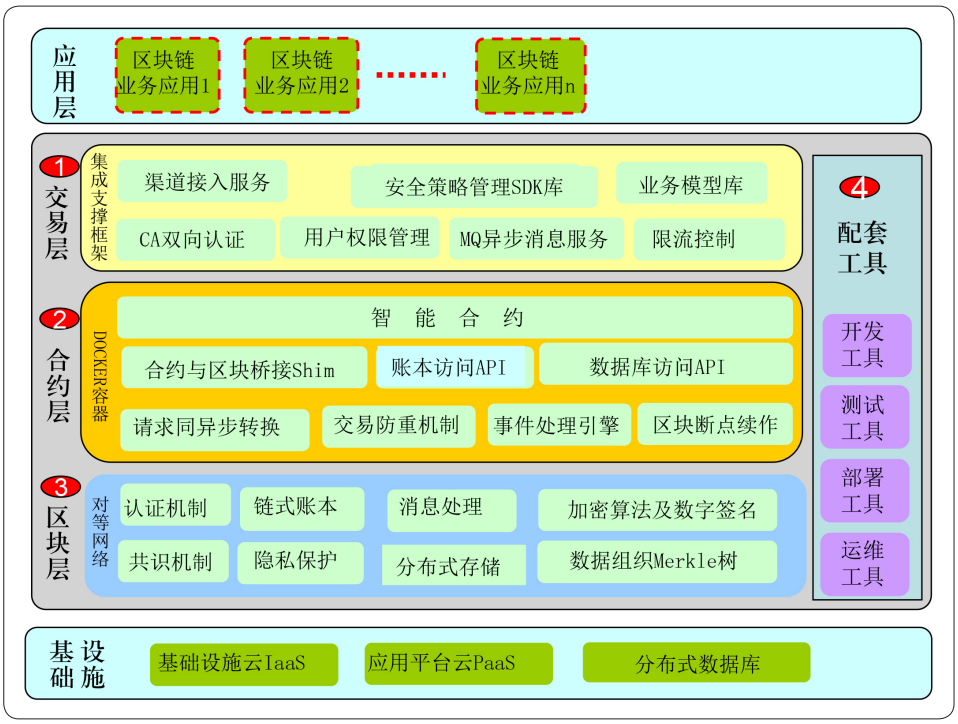

图 1　工行区块链平台 1.0 产品架构

二、工行区块链平台的技术特色和优势

1. 三级多维度的高安全体系

工行区块链平台打造企业级系统安全体系，提供可靠的企业级数据安全、用户隐私和交易匿名、权限控制及数据隔离机制。节点须以用户身份登录，经授权才可加入网络，所有交易信息须经数字签名才可记录在链上。工行区块链平台根据用户身份对链上数据进行加密，确保仅有经授权的节点才可访问链上数据，实现链上数据的访问隔离。平台采用报文防重检查降低交易重复提交概率，通过交易限流控制、柔性处理等措施进行流量管控。同时，开展日志监控审计确保交易的安全。三级多维度安全控制体系如图 2 所示。

接入安全：借鉴开放平台系统的安全控制机制，扩展实现了 REST 协议双向 CA 接入控制的安全控制功能，确保所有加入网络的节点须经过 SSL 的双向 CA 授权认证，且所有登录系统的用户需经过身份认证才可访问内部数据。

访问控制：设计基于区块链的用户访问控制机制，扩展实现了用户角色及权限控制功能，赋予不同的角色不同的操作权限，根据用户访问权限矩阵严格控制不同用户角色对系统的访问权限，保障数据访问的安全。

交易安全：工行区块链支持交易匿名证书 TCert 颁发，区块链上每一笔交易都使用匿名 TCert 来进行签名，区块链系统能验证交易的正确性及防篡改，同时保证了用户交易的隐私性及匿名性。采用报文防重检查机制控制交易的重复提交，通过交易的限流控制，柔性处理等措施进行流量管控，大幅提高了系统的安全性。

数据安全：为满足国家对金融机构安全控制的需要，工行区块链平台引入了国密非对称加密算法 SM2、对称国密算法 SM4 以及哈希函数 SM3 的支持，完成整个区块链技术平台在数据签名存储、传输及校验等环节对数据的安全控制，保证业务请求数据在传输及存储时防抵赖及防篡改功能。同时对于用户信息存储按照机构、角色、用户等划分具体的访问控制权限控制，实现用户加密数据在区块链内部的逻辑隔离，非授权用户无法访问存储在本地的加密后的数据，从而保障各个机构及用户角色之间的数据访问安全性。

监控系统：实验室研发了针对区块链特色的监控系统平台，将区块链的运行环境及内部运行情况纳入生产监控管理，实现区块链网络节点状态、区块高度、性能容量等监控预警。

2. 高性能的处理机制

双通道技术机制：工行区块链平台双通道技术机制将交易数据流及共识数据流进行分离，实现交易请求接入 / 返回、心跳检测、数据同步、视图切换等低频数据流和拜占庭共识数据流隔离，并使用不同的消息通道进行处理，大大提升了系统处理能力。

异步转同步处理机制：在业界通用的区块链处理机制中，对于前端提交的联机交易请求都需要进行联机转批量的处理，应用层需通过轮询的机制实现对异步处理结果的确认。工行区块链平台引入异步转同步处理机制，实现区块链中交易处理结果实时返回，相对于轮询机制对于交易处理结果的应答及时性可从秒级提高到毫秒级。

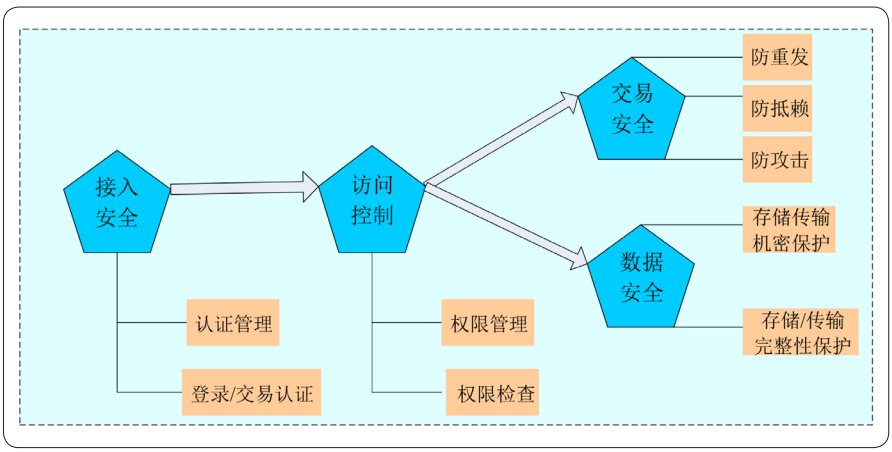

图 2 三级多维度安全控制体系

精简架构流程：优化交易请求处理流程，将 NVP 到 VP 节点之间的短连接调整为 API 接口调用方式，实现模板与模块之间的 API 调用，使得系统 TPS 进一步提升。

3. 高便捷的研发支撑技术

智能合约多语言支持：为降低开发人员编程语言学习成本以及各个应用接入区块链技术平台的门槛，促进便捷研发，区块链平台应用持续集成开发框架，提供多种编程语言智能合约支持，包括 JAVA、GO 以及工行区块链平台的接入 SDK、JAVA 的智能合约编程工具和单元测试工具，实现智能合约的自动化构建管道，上层应用可轻松接入区块链，并可跨平台地快速开发、部署以及持续集成测试。

全流程图形化支持：实验室通过优化 IDE，实现智能合约的开发、调试、联调、部署的一体化的图像集成开发环境，常用功能的拖拉拽式开发，大大节省智能合约编写的门槛。

持续集成支持：实验室通过重构和模拟底层接口类，完成测试用例的持久化和持续集成，实现智能合约的自动化构建管道。通过抽象和模拟底层工行区块链平台接口类，实现智能合约脱离 Docker 容器即可编译执行。

4. 易扩展的可插拔技术

跨链对接互访技术：目前通过体系外的业务应用层的 API 接口也可实现跨链数据访问，但存在数据容易篡改，事务完整性难以保证，区块生成后无法回滚等难题。实验室研究跨链技术，实现多个同 / 异构区块链的互联互通，共识管理及数据交换处理等功能。

云平台支持：把区块链平台纳入 PaaS 云平台管理，实现区块链节点间的集中监控，按需分配资源。

可插拔数据存储：通过构建数据访问层，支持多种可插拔数据存储架构，如关系型数据库、非关系型数据库 KV 云存储等多种海量存储方式。

三、工行区块链金融创新实践

工行积极探索区块链技术在公益扶贫、金融产品交易、见证服务等领域的应用创新，力争用最好的技术、持续提升的服务创建金融科技新生态。

金融产品交易平台以账户贵金属产品为切入点，支持不同机构加入联盟，共建金融产品交易二级市场，为注册客户提供金融产品买卖、转让及赠送等服务，支持客户与商家或个人直接完成产品买卖。支持联盟链方式引入合作伙伴，形成开放性的金融资产交易平台，拓宽客户的投融资渠道，打造金融资产交易平台生态圈。提高理财产品、贵金属、大额存单等资产的流动性，拓展中间业务收入来源。

工行脱贫攻坚基金区块链管理平台以区块链技术为基础，通过制定对接的接入标准和规范，对外提供标准的接入和金融业务服务，实现脱贫基金的资金划拨管理、投后管理等功能，确保资金划拨管理上链，使资金审批每个步骤都有迹可循，这让政府管理部门和银行机构自动加入监管之中，使得整个审批过程真正透明，消除腐败滋生的可能。该项目于 2017 年 5 月 16 日顺利投产，随着第一笔扶贫资金通过新的管理平台顺利拨付到位，标志着新的基金管理模式正式投入使用，新的管理模式在扶贫工作管理上取得较好的成效。

四、应用前景

商业模式决定了区块链技术能发挥的作用，区块链技术丰富了商业模式的选择。工行区块链平台 1.0 提供了高安全、高性能、高便捷、易扩展的区块链应用基础平台，通过此平台，各领域的合作伙伴可以快速搭建上层区块链应用，帮助企业将精力聚焦在业务本身和商业模式的运营上，形成一个“各尽其职、各取所需、共同成长”的商业生态，让用户、商户、机构在多样化的应用场景中受益。

后续，实验室将继续吸收业界其他区块链平台的优秀思想，把区块链与人工智能、大数据、生物识别等新兴技术融合，打造一个更加开放灵活、兼容并蓄、安全稳定、性能高效、部署便捷的企业级区块链平台。FCC