电力供应链场景下智能合约个性化升级方法*

李 达[1,2],王 栋[1,2],阮倩昀[3],柏德胜[1,4],许洪华[5],霍冬冬[3]

(1.国网电子商务有限公司(国网雄安金融科技集团有限公司),北京 100053;
2.国网区块链科技(北京)有限公司,北京 100053;3.中国科学院 信息工程研究所,北京 100093;
4.国家电网有限公司区块链技术实验室,北京 100053;5.国网江苏省电力有限公司,江苏 南京 210000)

摘 要:针对电力供应链场景下智能合约升级机制存在的不足,提出了智能合约个性化升级方法。该方法使具备验证待升级合约有效性资质的电力企业负责新合约及有关数据的上链验证,无资质企业无法验证。为了验证模型效果,设计了一个电力交易合约升级数据上链的业务逻辑。结合区块链网络,实现了用户通过应用程序与区块链进行交互以完成合约的个性化升级。最后分析了合约升级验证场景的功能性、响应速度和数据安全,结果表明该智能合约个性化升级方法有效降低了合约升级数据的失真风险,这种针对合约安全升级的增强方案也有助于加速链上链下数据的协同化。

关键词:电力供应链;联盟链;智能合约;合约升级

中图分类号:TP311 **文献标识码**:A **DOI**:10.19358/j.issn.2096-5133.2021.09.008

引用格式:李达,王栋,阮倩昀,等. 电力供应链场景下智能合约个性化升级方法[J].信息技术与网络安全,2021,40(9):44-53.

Personalized upgrade method for smart contracts in power supply chain scenarios

Li Da[1,2], Wang Dong[1,2], Ruan Qianyun[3], Bai Desheng[1,4], Xu Honghua[5], Huo Dongdong[3]

(1.State Grid E-Commerce Co., Ltd., (State Grid Xiongan Financial Technology Company), Beijing 100053, China;
2.State Grid Blockchain Technology(Beijing) Co., Ltd., Beijing 100053, China;
3.Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
4.State Grid Blockchain Technology Laboratory, Beijing 100053, China;
5.State Grid Jiangsu Electric Power Co., Ltd., Nanjing 210000, China)

Abstract: Aiming at the shortcomings of the smart contract upgrade mechanism in the power supply chain scenario, a personalized upgrade method of smart contract is proposed. This method enables the electric power companies with the qualification to verify the validity of the contract to be upgraded to be accountable to the verification of the new contract and up-chaining data, and the unqualified companies cannot verify it. For proving the availability of the model, we design a business logic that the data of the power transaction contract upgrade is put on the blockchain. Users can make interactions with the blockchain through applications to complete the personalized upgrade of the contract coupling with the blockchain. Finally, we analyze the functionality, upgradeability and cost of the contract upgrade verification scenario, and the results show that the smart contract personalized upgrade method effectively reduces the risk of distortion of the contract upgrade data. The enhanced solution for contract security upgrades also helps to accelerate the collaboration of on-chain and off-chain data.

Key words: supply chains in power systems; consortium blockchains; smart contracts; contract upgrading

0 引言

随着电力体制改革加快推进,电力行业逐渐从垂直一体化的内部供应链体系,转变为由多个相对独立环节构成的外部供应链体系。根据电产品的生产和流通过程,电产品的生产、输送、分配和销售等环节将构成一条完整的电力供应链。电力供应链

*基金项目:国家电网有限公司2020总部科技项目(5700-2020723-72A-0-0-00)

上的主体角色多样，包括了独立生产、分配、销售电力的企业和电力用户。电力企业通过实施供应链管理，有效降低了成本以保证收益，也使得供应链的总体流动效率和电力企业的管理水平得到了显著的提高。

当前，电力市场正在经历由以电网为核心、交易单一能源品种逐渐向多主体参与、能源交易品种多样化转变，由此带来分布式能源数量庞大且分散、主体间信息不对称、可信任度低等问题日益严峻。具备隐私保护性、不可篡改性、分布式容错性、可信任性等特性的区块链技术，是解决能源交易中间环节较多、主体间信息不对称、信任缺失、交易成本高、用户隐私难以保障等问题的重要技术手段。但随着电力供应链业务交易数据量日益增长，部分业务交易流程繁琐、实时性要求高，急需一种自动化处理复杂业务的应用模式。

“智能合约”由密码学家 Szabo 于 20 世纪 90 年代首次提出，他指出智能合约是一种可计算的交易协议，以计算机程序的方式来执行合约条款[1]。目前，业内对智能合约的定义还未统一，文献[2]定义智能合约的实质为一段脚本代码，该脚本代码具备可复用性、模块化编程和满足条件即可触发执行等特点。文献[3]强调了区块链对智能合约的可实现性有着巨大意义，每个合约声明的执行都记录为存储在区块链中的不变交易。

近年来，许多国内外专家学者在电力领域对区块链智能合约技术展开了研究，取得了较显著的成果。在合约实现数据上链方面，文献[4]提出了一种基于区块链的电力交易管理方法，该方法利用自动执行的智能合约维护和管理电力交易数据，根据合约内容自动化地转移资金，并存储由智能电表采集的实时电能信息以便后续分析和使用。文献[5]提出了一个弱中心化的能源互联网架构模型，该模型利用区块链技术实现了各类能源节点和售电企业节点的交互，通过验证并注册身份，从而保障了各节点之间的安全交易。基于区块链的分布式特性使得各节点在交易过程中做出较公平的决策，并利用智能合约实现了源-售双边交易信息的存储和管理。文献[6]提出了一种分布式微电网交易和能源的任务调度策略，并在此基础上提出了基于面向订单转移的动态智能合约的制定方法，实现了降低用户经济开销与提高数据中心经济收益的目标。文献[7]提出了基于区块链的电力交易和调度系统，该系统针对微电网中典型的业务处理逻辑，设计了面向电力购买、电力输送和电力结算等场景的智能合约，并有效实现了将微电网主体的关键数据记入区块链中。在合约的可升级性方面，文献[8]利用智能合约设计并提出了一个访问控制框架，该框架由三类定制化的合约组成，分别为面向用户的访问控制合约、判断合约和注册合约，将注册访问控制合约中的访问控制信息、判断合约中的不良行为信息以及智能合约中的信息，交由注册合约统一进行注册、更新和删除等管理。文献[9]提出了一种自动支持智能合约更新的方法，通过计算目标智能合约的代码语法和语义相似度，从而发现相似的智能合约，并从智能合约源代码中提取差异化的代码以支持目标智能合约的更新。文献[10]提出了一种基于区块链日志系统的智能合约自动更新的框架，该框架融合了区块链技术和机器学习方法，先将采用机器学习方法提取到的日志异常信息连续输入到智能合约中，再执行智能合约实现日志的异常检测，从而达到支持合约自动更新的目的。文献[11]提出了一种松耦合的智能合约链上升级模型，该模型通过定制的智能合约实现了各功能之间的顺利调用，也在保证合约的调用接口与数据结构不改变的同时，实现了合约的逻辑功能升级。文献[12]提出了一个基于区块链技术的线上公平合约交换协议，采用数字签名，在合约内容之后追加新内容并确认的方式，提供了公平合约的追加、更新和删除管理功能，以保证合约追加内容与过程的可靠性和不可抵赖性。在合约实现电力交易执行方面，文献[13]提出了一个基于区块链的虚拟电厂调度模型，该模型利用智能合约使得虚拟电厂中各主体之间的运行调度能够有序、安全且自动地发生。文献[14]从绿色低碳和经济效益角度出发，提出了一种弱中心化的电力市场交易出清模型，该模型利用智能合约技术使得电力交易中竞价和结算的过程安全和自动执行成为可能。文献[15]提出了一种弱中心化的电力交易清结算智能合约，该智能合约不仅将清算业务结构化，也提高了电费清算的效率，并通过不可销毁、篡改且透明的交易记录使得电费清算过程具备较高的可审计性和真实性。文献[16]提出了一种基于区块链的分布式电力交易方法，采用定制的智能合约实现了交易信息投标、P2P 交易、安全校核

和交易清算过程。文献[17]提出了一种弱中心化的面向电力供应链的主体利益分配模型，该模型利用智能合约自动匹配并结算利益，以实现电力供应链上各个企业的利益最优和整个供应链的利益最优。文献[18]设计了基于区块链的安全电力交易模型，通过在无线网络中引入区块链的智能合约进行数据的传输和决策，解决了集中电力交易中安全性低和可信任性低的问题，并设计了基于智能合约的可再生能源激励机制，以实现根据激励算法自动、公平地向可再生能源生产商支付报酬，有效鼓励了生产者提高电能质量、扩大生产能力。

当前，针对在电力供应链的智能合约技术研究还停留在保证链上所有用户数据的可信互联，还未深入到电力供应链场景下智能合约的管理，缺乏在电力供应链场景下对用户访问数据的权限做出细粒度控制。例如，在多用户的合约升级场景下，将会造成以下问题：受限于电力企业各自的职能，区块链上参与电力供应的某一个企业无法对所有待升级的智能合约的合法、合规性做出背书保证。

为解决上述提出的问题，本文设计并提出了一种智能合约个性化升级方法，该方法通过编写个性化的智能合约，使得具备验证待升级合约有效性资质的电力企业能够验证新合约及实现有关数据的上链，并确保不具备验证资质的企业无法进行合约的升级验证。对于验证通过的合约，其合约哈希值将被存至区块链链上，并与合约版本号码匹配，以用来索引新的合约。该方法采用智能合约结合背书策略的方式，进一步保证了智能合约升级的安全性和可靠性，并将该模型应用于电力交易合约的升级验证。本文实现了一个基于 Fabric 的合约升级验证方案，可降低电力企业合约升级验证数据上链的失真风险，推动链上链下合约升级数据协同发展。

1 相关背景

1.1 Hyperledger Fabric

Hyperledger 项目是 Linux 基金会支持的企业级开源分布式账本实现，Hyperledger Fabric 是第一个加入 Hyperledger 的项目，其目标是构建企业级的区块链基础核心平台，支持权限管理和数据安全，以下简称 Fabric。Fabric 最初是 0.6 版本，后来在 2017 年发布了版本 v1.0[19]。在 2020 年 1 月，IBM 正式发布了 Fabric v2.0，较之前的版本增添了一些新的特性和功能，新版本引入了智能合约的新链码应用模式、私有数据的优化增强、新的外部链码启动器、新的状态数据库缓存和新的基于 Alpine Linux 的 Docker 镜像[20]。Fabric 项目面向的是联盟链的场景，通常在许可区块链中的众多组织将组成一个联盟，每个单独的组织都构成一个信任域，组织内的实体彼此信任[21]。联盟在整体上定义了共同的规则、政策以及共享的业务逻辑。

本文基于 Fabric v2.0 进行研究讨论，下面给出 Fabric 的交易流程。

Fabric 中的一笔成功交易从客户端提交交易给背书节点开始，到确认节点将状态改变更新到区块中结束。具体的交易流程如图 1 所示。

Fabric 的交易流程由背书阶段、排序阶段和验证阶段组成[22]，根据图 1 将对整个交易流程进行如下概述。

(1)背书阶段

在背书阶段，首先由客户端发送交易提案的请求给背书节点。背书节点收到提案请求后，验证消

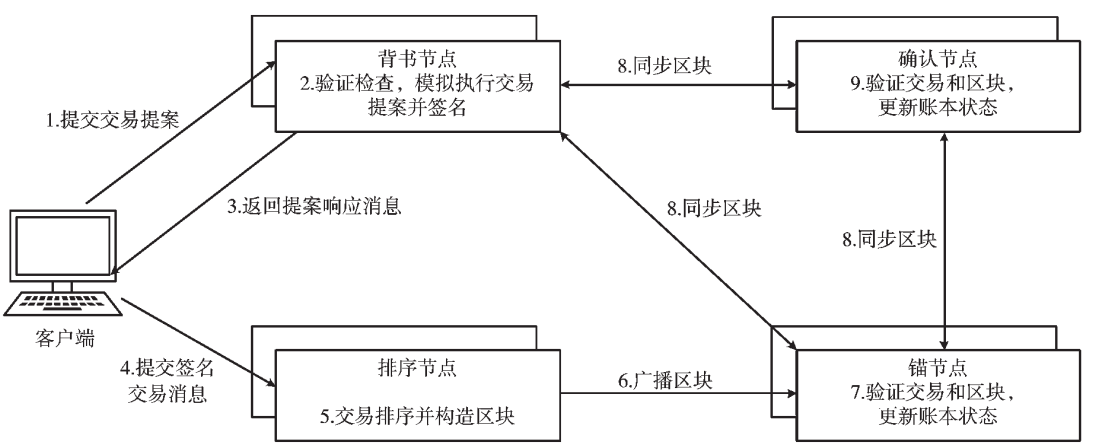

图 1 Fabric 的交易流程

息格式与签名合法性，以及检查签名提案消息的唯一性和是否满足通道权限策略。验证检查结束后，背书节点模拟执行交易提案，并对结果进行背书签名，之后将签名结果、模拟执行结果读写集、链码执行响应消息等封装为提案响应消息发送给客户端。收到提案的响应回复消息后，客户端将判断该消息结果是否合法。若该交易是“查询交易”，检查通过后，客户端将以提案响应消息结果作为下一步业务逻辑判断的依据。若该交易是“写交易”，下一步将进入排序阶段。

(2)排序阶段

客户端收到的提案响应消息包括链码执行响应消息和模拟执行结果读写集。在排序阶段，客户端需确保收到的所有提案响应消息都是按位相等的，否则返回错误，然后将提案消息、提案响应消息、背书信息列表等构造成签名交易消息，提交给排序节点。排序节点先对交易进行排序并构造成区块，然后以广播的方式发送给各组织的锚节点。

(3)验证阶段

在验证阶段，锚节点收到区块后，先验证交易和区块是否有效，验证通过之后将执行区块中的有效交易，并根据交易执行的结果对账本状态进行更新。之后将区块同步给组织内的其他节点，其他节点也需验证交易和区块，最后组织内所有节点的账本都会得到更新。

正是上述所描述的三个阶段组成了 Fabric 的共识机制，实现了 Fabric 内大部分节点对多个事件发生的顺序、某个键对应的值、谁是主节点等某个提案信息达成了一致。

1.2 典型电力供应链模式概述

按照电力供应链的上下游关系，典型的电力供应链大致可以分为发电、输电、配电、售电、用电等环节。其中，发电环节是指发电企业生产电能；输电环节是指电网企业把电能由发电企业输送到配售电企业；配电环节是指配电企业根据用户用电电压级别和用电需求与用户直接相连并向用户分配电能；售电环节是指售电企业向最终用户提供电能并完成电力交易；用电环节则是指终端用户消费电能。电力供应链的上下游主体关系简化图如图 2 所示。

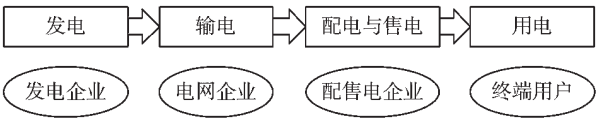

图 2 电力供应链的上下游主体关系

2 智能合约个性化升级模型和应用的设计

2.1 基于智能合约的个性化升级模型

在电力结算交易环境中，由于不同角色的主体之间的交互越来越频繁，为适应多用户场景下的合约升级需求、增强访问控制的安全性，提出了如图 3 所示的基于智能合约的个性化升级模型，模型利用智能合约实现了对用户访问控制和待升级合约信息的管理。

假设发电企业 Org1、电网企业 Org2、配售电企业 Org3 都采用基于智能合约的个性化升级模型，并且各个企业在链下拥有不完全相同的电力交易数据库。Org1－peer、Org2－peer、Org3－peer 代表企业用户，也是实际的 Fabric 网络节点，其中只有 Org1－peer 才有权限访问 Org1 的 IT 服务商，Org2－peer 和 Org3－peer 同理。当发电企业的用户 Org1－peer 发出只能让电网企业的用户 Org2－peer 验证带有“A”标签的待升级合约验证请求时，由设计的智能合约实现对用户的访问授权和合约信息的验证，规范性验证合约会判断当前运行合约的节点的身份，然后到安全对接的 IT 服务商查询合约信息的完整性、可靠性、真实性。

此外，当联盟链网络的背书策略采用满足任意成员签名的背书策略时，若没有智能合约对用户的访问控制，会导致每个 peer 节点都能执行并验证智能合约，即在同一个通道内的任意 peer 节点都能修改账本，这使得数据存在一定的泄露风险。因此，在智能合约内制定面向用户身份的访问控制策略，有利于增强隐私数据的安全性。该策略指的是在任意成员签名的背书策略情况下，同一个通道内的 peer 节点有同等修改账本的权利；在不同角色主体之间交互的情况下，智能合约能够实现不同角色主体的职能，以满足各个主体的多种需求。如果该用户具备验证待升级合约的有效性资质，且待升级合约数据的验证结果符合访问控制策略，则将合约的哈希值和版本号记入区块连；否则，则拒绝该请求。

2.2 基于 Fabric 的电力交易合约升级应用

本文将应用场景范围定位在有直接电力交易往来的发电企业、电网企业和配售电企业中，其中的电网企业位于交易供应链的中游。基于此应用场景，实现了一个基于 Fabric 的电力交易合约升级应

用。该应用的工作流程图如图 4 所示。在应用程序运行的过程中，整个工作流程由企业的普通用户和应用程序的交互、应用程序和 Fabric 网络的交互、智能合约和 IT 服务商的交互三部分组成。

图 4 所示为企业的普通用户经过身份认证之后进行电力交易合约升级的过程。首先，普通用户在电力交易应用中执行电力交易合约升级的命令；接着，应用将这交易发送到 Fabric 网络。在 Fabric 网络内执行交易的过程中，智能合约对运行合约的节点进行身份验证，再将待升级合约的哈希值和版本号与存储在 IT 服务商中的数据进行比对，随后得到比对后的结果；然后，当这一交易在 Fabric 网络内执行完成后，Fabric 网络将交易执行结果返回给电力交易应用；最终，电力交易应用返回执行命令结果给用户。

3 电力供应链交易合约设计与实现

3.1 联盟链网络

通过编写组织结构与身份证书、通道、组织的锚节点等配置文件，设计联盟链网络的结构。在本应用程序中，联盟链的结构示意图如图 5 所示。在

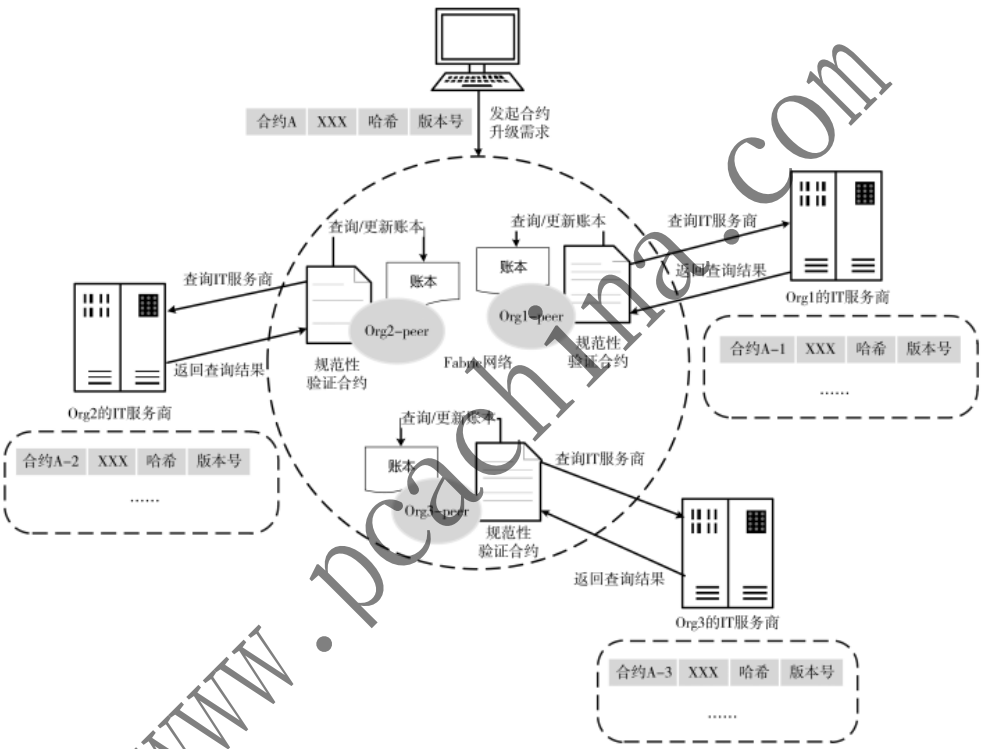

图 3 基于智能合约的个性化升级模型示意图

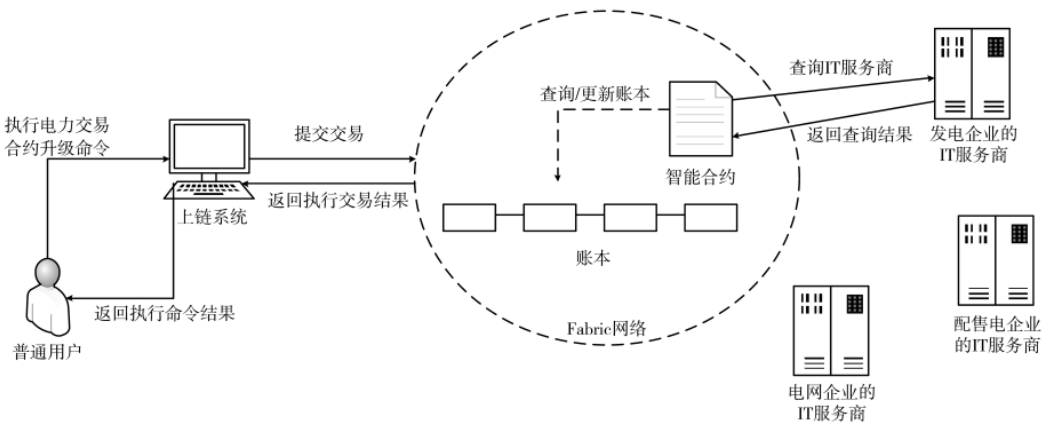

图 4 工作流程图

联盟链中，发电企业、电网企业和配售电企业分别用组织 Org1、组织 Org2 和组织 Org3 表示，并且为每个组织配置两个 Peer 节点，其中 Org1 中的 Peer0 节点、Org2 中的 Peer0 节点和 Org3 中的 Peer0 节点作为锚节点，且每个组织分别拥有自己的 CA 机构，记为 ca-org1、ca-org2 和 ca-org3，用于颁发相应组织的证书。联盟链网络提供了基于 etcdraft 共识的排序服务，并为联盟创建了一条名为“SCMchannel”的应用通道，Org1、Org2 和 Org3 中的 Peer 节点加入应用通道之后，可以安装与交易数据上链相关的“example”智能合约。Peer 节点物理上存放账本 ledger 的副本，而账本 ledger 逻辑上存放在“SCMchannel”应用通道上。

本应用程序采用基于容器的方式来快速部署网络，事先需要编写节点相应的配置文件，然后使用 docker-compose 工具将配置文件作为参数，启动提供网络服务的各个节点。其中，docker-compose 是一个 Python 程序，可以快速管理由多个 Docker 容器组成的服务。

3.2 智能合约

3.2.1 背书节点身份的获取

在 Fabric 中，实体的身份验证可以由成员服务提供者(Membership Service Provider，MSP)实现。成员服务提供者这一机制不仅能确认实体的数据签名，也能验证签名者的身份。Fabric 中的组织代表一组拥有相同信任的根证书的成员。通常，同一个企业组织属于同一个 MSP，同一个组织的成员节点在网络中可以被认为是同一个身份，代表组织进行签名。换句话说，统一组织内的成员节点有着相同的MSP信息。

在启动 Fabric 网络中所有的 Peer 节点之前，首先会检查节点启动所需的配置的完备性。在 Peer 节点的配置文件中，指定了 Peer 节点的环境变量配置，其中与所属组织 MSP 有关的环境变量是“CORE_PEER_LOCALMSPID”，该环境变量表示 Peer 节点所属组织的 MSP 的 ID 值，可以记为 mspid。例如，若该组织名为“Org1”，mspid 则为“Org1MSP”；若该组织名为“Org2”，mspid 则为“Org2MSP”。

当 Fabric 将 Go 语言作为编程语言时，在链码容器的 shim 层，通过使用“os”包下的 Getenv()方法，获取执行合约的背书节点的“CORE_PEER_LOCALMSPID”环境变量的值，然后再将该值传给智能合约。由此，智能合约获得了当前背书节点的身份，为实现个性化的访问控制授权做好准备。

3.2.2 智能合约与 IT 服务商的对接

为了实现待升级合约数据的校验，在智能合约

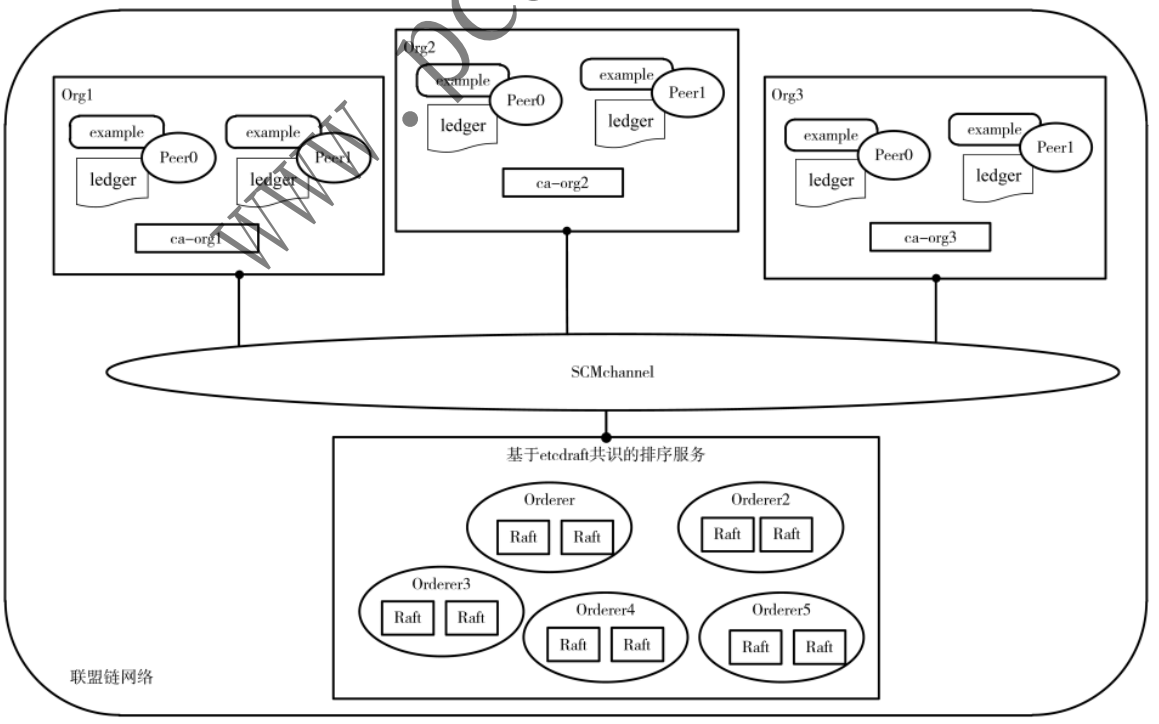

图 5 联盟链网络结构

内实现验证合约数据的业务逻辑的过程中，需向IT服务商请求查询数据库中该数据是否存在。通常，HTTP协议定义了客户端与服务器交互的不同方法。在上链数据的校验这一情景下，选择用于获取或查询资源信息的HTTP GET方法。

Golang语言编写的GET请求中的URL地址依次由服务器IP、端口号、信息系统的项目名称、项目内自定义的路径、GET请求附带的键值对组成。

GET请求回复消息为“true”或“false”，使用该值可以校验待升级合约数据的真实性、可靠性和完整性。

3.3 IT服务商

IT服务商的设计主要分为系统的分层结构设计、数据校验功能模块设计三个部分。

3.3.1 系统的分层结构设计

IT服务商采用了Spring MVC框架进行架构设计，系统内部在结构上可分为Controller层、DAO层和Impl层，具体实现的时序图如图6所示。

链码层通过HTTP协议向IT服务商内部的Controller层发送请求，收到请求的Controller层将调用DAO层的接口，以将业务交付给DAO层；DAO层为业务逻辑的设计了具体的类，该层业务逻辑的实现需调用Impl层接口完成；Impl层封装了对数据库的交互动作。当Impl层和数据库完成交互后，底层的MySQL数据库返回的访问结果将依次经过Impl层、DAO层、Controller层进行结果的分析和封装，最终的请求结果将返回给链码。

3.3.2 数据校验功能模块设计

与智能合约对接的IT服务商最重要的功能是校验交易数据的真实性、完整性和可靠性，因此在Controller层设计checkAccount()方法，接收智能合约请求、校验数据、返回请求结果，该过程的流程图如图7所示。

3.4 基于Node.js SDK的应用

在完成联盟链网络设计之后，Fabric提供了Node.js、Python、Java、Go等多种语言实现SDK应用程序的开发。本文选择功能较成熟和完善的Node.js语言进行开发，实现用户通过应用程序与联盟链进行交互并完成交易。基于Node.js SDK的应用程序的设计主要分为启动网络和关闭网络的脚本设计、应用程序和网络交互设计两部分。

3.4.1 启动网络和关闭网络的脚本设计

启动网络的脚本设计目标是：依据配置文件建立网络，启动链码容器，并将智能合约安装在节点上。启动网络具体的步骤如下：

(1)设置网络搭建的启动时间、智能合约的编程语言、智能合约的位置等环境变量；

(2)清除掉当前还在运行或活跃的容器等，以确保搭建Fabric网络前的环境是干净的；

(3)生成组织结构与身份证书；

(4)成系统通道的创世区块文件genesis.block；

(5)生成应用通道交易配置文件channel.tx；

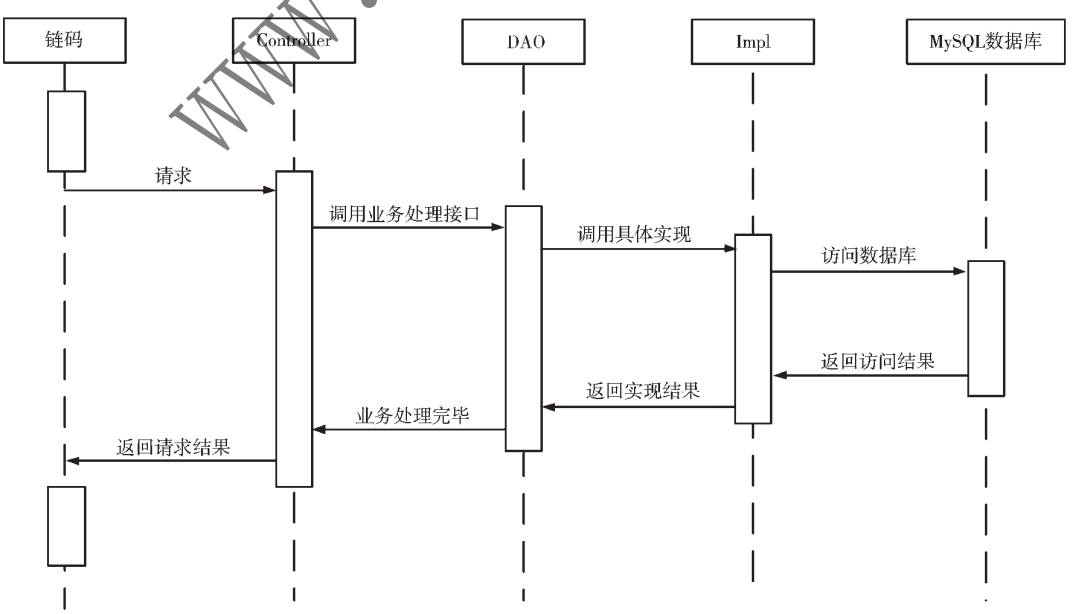

图6 IT服务商的分层结构

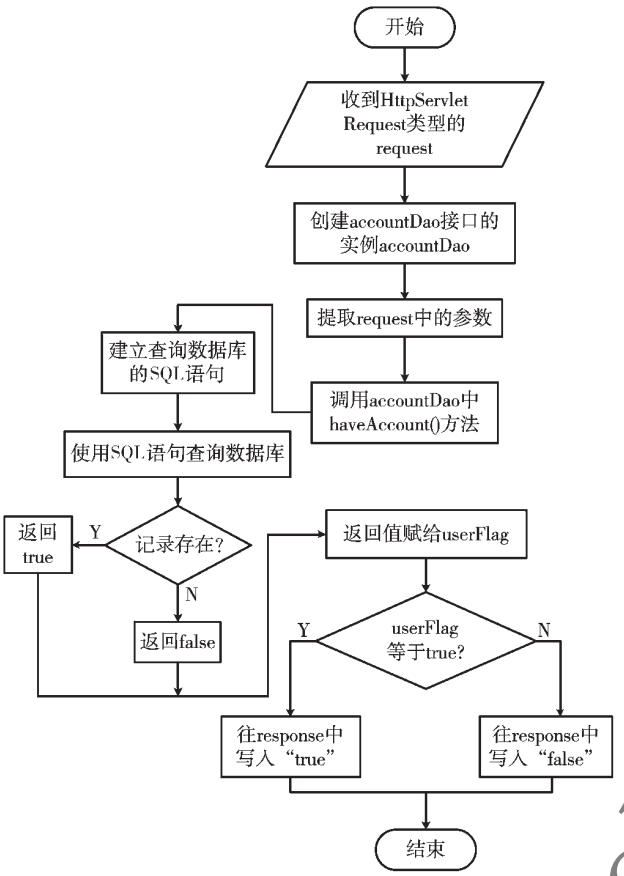

图 7 数据校验方法的流程图

(6)生成锚节点更新配置文件 Org1MSPanchors.tx、Org2MSPanchors.tx 和 Org3MSPanchors.tx,并采用基于容器的方式来快速部署网络;

(7)创建使 Peer 节点加入的“SCMchannel”通道;

(8)将 peer0.org1、peer0.org2 和 peer0.org3 更新为锚节点;

(9)org1、org2、org3 组织中的节点进行链码的打包、链码的安装以及安装的验证,并需要 org1、org2、org3 组织分别同意链码定义;

(10)在满足了链码定义的策略后,提交智能合约;

(11)输出启动网络所用的时间、应用与 Fabric 网络进行交互的命令。

关闭网络的脚本设计目标是:暂停并移除网络中的容器节点、删除网络启动过程生成的配置文件、删除账本备份和清除镜像文件,以实现清理网络环境的目的。

3.4.2 应用程序和网络交互设计

由于只有被 CA 机构认可的身份才能够在 Fabric 上进行交易,因此用户在首次使用该应用程序时,需先登记管理员用户,接着注册、登记普通用户,最后查询或更新账本。

管理员用户和普通用户的登记流程如图 8 所示。首先,“enrollAdmin.js”实现了向 ca-org1 认证机构注册 ID 为“admin”、密文为“adminpw”的管理员,管理员将收到证书、签名私钥、mspId 值和证书类型信息。接着,“registerUser.js”是实现了管理员在 ca-org1 机构注册一个普通用户,ca-org1 机构将返回密文。最后,密文用于普通用户在 ca-org1 机构的登记,登记完成后,普通用户将收到证书、签名私钥、mspId 值和证书类型信息,这些信息将被用于后续的交易数据上链操作。

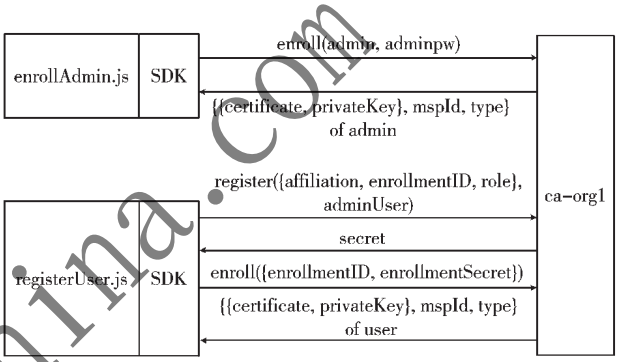

图 8 登记管理员用户和普通用户

接下来将设计交易数据上链相关的功能。为了减轻应用程序的负担,Fabric v2.0 在原本的 SDK 基础上加了一层网关 Gateway,用于将认证过的普通用户连接到某个组织的 Peer 节点。因此,基于 Node.js 实现 SDK 的特点,实现应用程序功能的基本过程如下:

(1)加载网络连接对象相关的配置;

(2)创建管理身份的流式文件,记为钱包;

(3)获得普通用户的身份,并检查用户是否登记过,若还未登记过,功能函数将在此处结束,返回空值;

(4)若用户已经登记过,接下来创建一个网关;

(5)利用网关,根据通道名称“SCMchannel”,获得部署在 Fabric 网络中的通道对象;

(6)根据打包后的智能合约名称,获得合约对象;

(7)若要实现查询交易方或账本数据的功能,调用智能合约对象的 evaluateTransaction()方法,相关参数作为传入值;若要实现注册交易方、交易数据上链等更新账本的功能,调用智能合约对象的 submitTransaction()方法,相关参数作为传入值。用户可以通过修改 evaluateTransaction()方法和 submitTransaction()方法传入的参数,实现不同功能。

4 仿真实验及分析

4.1 仿真实验环境测试

4.1.1 环境配置

为了对本文所述方案进行验证，实验环境配置如下：具体来说，每个 Fabric 节点被部署在相同配置的服务器上，它们使用相同类型的 vCPU(e3-1220 V5@3.00 GHz)，内存大小为 8 GB。所有服务器都在同一个局域网中，交换机的速率为 1.0 Gb/s。此外，当前 Fabric 网络内部的节点共识将基于raft 共识算法，使用五个排序节点来提供排序服务。

本文中将设定每一个部门节点(即 org)都对应一个 peer，并将针对不同数量的 peer 节点测试了两个典型背书策略："任意 peer 节点"、"全部 peer 节点"和个性化背书策略—"指定 peer 节点"三种。在验证过程中，每类实验重复 5 轮，取平均值作为最终结果。策略的含义如下："任意 peer 节点"表示客户端将交易提议发送给任意候选 peer 节点进行背书，在 Fabric 中对这种背书方式进行了一些优化，即具备一定的负载均衡属性；"全部 peer 节点"表示客户端将交易提议发送给全部候选 peer 节点进行背书；最后，"指定 peer 节点"是客户端只指定一个候选 peer 节点作为目标背书节点，即本文工作。

4.1.2 工作负载和评测程序

本文使用的智能合约是 powerDataOnChain，旨在模拟电力客户对智能合约升级的常见操作，包括管理员用户的注册、普通用户的注册、交易者的注册、待升级合约数据的上链、交易者信息的查询、已上链的待升级合约数据的查询、交易者账户的注销等。对于实验工作负载，本文为 powerDataOnChain 合约准备了 20 000 个假交易者账户。由于硬件资源有限，客户端只能以 500 次/秒的速度发送交易。

4.2 实验结果及评估

4.2.1 平均每秒交易数

Fabric 网络的吞吐量通常用平均每秒交易数(TPS)来表示，peer 节点数量的变化对 TPS 影响的结果如图 9 所示。随着 peer 节点数量的增加，三种策略的 TPS 均有所降低且趋于稳定。"任意 peer 节点"策略下的 TPS 值均高于其他两种策略。这是因为当 Fabric 网络的背书策略采用满足任意成员签名的背书策略且用户对数据的访问权限受限时，最好的情况是所选择的背书节点正好具备对数据的访问权限，从而可以进行背书，因此该情况下工作流程的平均每秒交易数最高，进而响应速度最快。

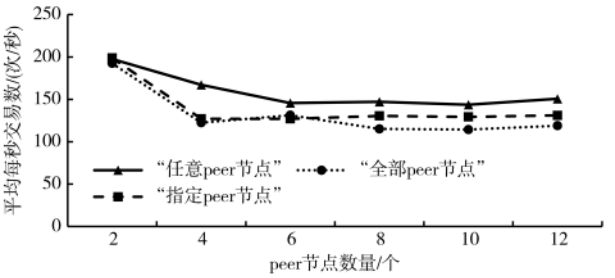

图 9 Fabric 网络的平均吞吐量

当 peer 节点数量大于 6 时，"指定 peer 节点"策略的 TPS 持续略高于"全部 peer 节点"策略。当 peer 节点的数量足够大时，"全部 peer 节点"策略需要选择遍历过所有节点才找到可以真正背书的节点，因此该情况下工作流程的平均每秒交易数最小，进而导致响应速度最慢。由于智能合约个性化升级方法在智能合约内制定面向用户身份的访问控制策略，因此，"指定 peer 节点"策略的工作流程的平均每秒交易数介于其他两种策略之间，从而响应速度也处于中间水平。

4.2.2 数据安全

在传统的智能合约升级中，区块链网络设置背书策略之后，所有满足背书策略的节点将共享相同的合约的升级验证数据，这难以满足电力供应链场景下多方机构对本方数据隐私保密的个性化需求。智能合约个性化升级方法则是基于机构对本方数据隐私保密的需求而设计的，该方法使得只有加入联盟链网络的实体才可以查看联盟链上的所有信息，通过智能合约验证后的实体才可实现合约的升级，这有利于保证合约数据的安全性，进而确保网络底层的数据安全。

5 结论

本文基于联盟链平台，构建了基于智能合约的个性化升级模型，使得具有验证上链数据有效性资质的电力企业负责验证上链数据。同时将该模型应用在电力供应链的场景中，设计实现了基于 Fabric 的电力交易合约更新应用。本文将区块链的智能合约融入到面向用户的访问控制和待升级合约数据的验证中，有效增强了对待升级智能合约的合法、合规性做出的背书保证，推动了链上链下合约升级数据的协同发展，进而提高了智能合约升级的安全性和可靠性。

参考文献

[1] WANG S, OUYANG L, YUAN Y, et al. Blockchain-enabled smart contracts: architecture, applications, and future trends[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 49(11): 2266-2277.

[2] 方轶, 丛林虎, 杨珍波. 基于区块链的数字化智能合约研究[J]. 计算机系统应用, 2019, 28(9): 225-231.

[3] ZHENG Z, XIE S, DAI H N, et al. An overview on smart contracts: challenges, advances and platforms[J]. Future Generation Computer Systems, 2020, 105: 475-491.

[4] 郜雪, 孙宏斌, 郭庆来. 能源互联网中基于区块链的电力交易和阻塞管理方法[J]. 电网技术, 2016, 40(12): 3630-3638.

[5] 龚钢军, 张桐, 魏沛芳, 等. 基于区块链的能源互联网智能交易与协同调度体系研究[J]. 中国电机工程学报, 2019, 39(5): 1278-1290.

[6] 李云波, 张子立, 张晋宾, 等. 基于区块链的分布式微电网交易与能源调度研究[J]. 华电技术, 2020, 42(8): 24-31.

[7] 朱兴雄, 陈绍真, 何清素. 基于区块链的微电网系统[J]. 电子技术与软件工程, 2018(1): 157-159.

[8] ZHANG Y, KASAHARA S, SHEN Y, et al. Smart contract-based access control for the internet of things[J]. IEEE Internet of Things Journal, 2018, 6(2): 1594-1605.

[9] HUANG Y, KONG Q, JIA N, et al. Recommending differentiated code to support smart contract update[C]// 2019 IEEE/ACM 27th International Conference on Program Comprehension (ICPC). IEEE, 2019: 260-270.

[10] SHAO W, WANG Z, WANG X, et al. LSC: online auto-update smart contracts for fortifying blockchain-based log systems[J]. Information Sciences, 2020, 512: 506-517.

[11] 刘云霞, 胡大裟, 蒋玉明. 面向智能合约链上升级的松耦合模型研究[J]. 计算机应用研究, 2021, 38(5): 1309-1313.

[12] 于雷, 赵晓芳, 孙毅, 等. 基于区块链技术的公平合约交换协议的实现[J]. 软件学报, 2020, 31(12): 3867-3879.

[13] 余维, 胡跃, 杨晓宇, 等. 基于能源区块链网络的虚拟电厂运行与调度模型[J]. 中国电机工程学报, 2017, 37(13): 3729-3736.

[14] 王辉, 廖昆, 陈波波, 等. 低碳形势下基于区块链技术的含微电网电力市场交易出清模型[J]. 现代电力, 2019, 36(1): 14-21.

[15] 鲁静, 宋斌, 向万红, 等. 基于区块链的电力市场交易结算智能合约[J]. 计算机系统应用, 2017, 26(12): 43-50.

[16] 杨选忠, 张浙波, 赵申轶, 等. 基于区块链的含安全约束分布式电力交易方法[J]. 中国电力, 2019, 52(10): 31-39.

[17] 侯文捷, 武鸿鹏, 高峰亭, 等. 基于区块链智能合约的电力供应链利益分配研究[J]. 信阳师范学院学报(自然科学版), 2020, 33(1): 144-148.

[18] Liu Z, Wang D, Wang J, et al. A blockchain-enabled secure power trading mechanism for smart grid employing wireless networks[J]. IEEE Access, 2020, 8: 177745-177756.

[19] NASIR Q, QASSE I A, ABU TALIB M, et al. Performance analysis of hyperledger fabric platforms[J]. Security and Communication Networks, 2018, 2018.

[20] Hyperledger Fabric v2.0.0[EB/OL]. [2021-05-10]. https://hyperledger-fabric.readthedocs.io/en/release-2.0/whatsnew.html.

[21] ANDROULAKI E, DE CARO A, NEUGSCHWANDTNER M, et al. Endorsement in Hyperledger Fabric[C]// 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019: 510-519.

[22] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operatingsystem for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference, 2018: 1-15.

(收稿日期: 2021-07-24)

作者简介:

李达(1991-), 男, 硕士, 工程师, 主要研究方向: 区块链、电力系统自动化。

王栋((1985-), 男, 通信作者, 硕士, 高级工程师, 主要研究方向: 区块链、信息安全。E-mail: hit-gql@hotmail.com。

阮倩昀(1997-), 女, 硕士研究生, 主要研究方向: 区块链安全。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所