

基于 Fabric 的电网采购交易数据平台^①



李冉冉, 周少丹

(南方电网物资有限公司, 广州 510655)
通信作者: 周少丹, E-mail: 2512488566@qq.com

摘要: 我国电网采购交易平台具有交易金额巨大、供应商数量众多、流程管控要求严格的特点. 本文提出的电网采购交易数据平台, 基于 Hyperledger Fabric 技术, 结合数据库层面的数据哈希计算、数据指纹提取、权限访问控制、数据快速读取等方法, 实现了覆盖采购交易数据全生命周期的多级数据防护与数据防篡改, 可以有效管控由于采购交易平台各主体间的信息不对称可能导致的信任危机. 最后, 通过对该策略原型系统的防护性能进行试验分析, 验证了该原型系统的可行性.

关键词: 采购交易; Hyperledger Fabric; 数据防护; 数据防篡改

引用格式: 李冉冉, 周少丹. 基于 Fabric 的电网采购交易数据平台. 计算机系统应用, 2022, 31(8): 99-107. <http://www.c-s-a.org.cn/1003-3254/8689.html>

Data Platform of Power Grid Procurement Transaction Based on Fabric

LI Ran-Ran, ZHOU Shao-Dan

(China Southern Power Grid Materials Co. Ltd., Guangzhou 510655, China)

Abstract: China's transaction platform for grid procurement features a huge transaction amount, a large number of suppliers, and strict process control requirements. The transaction data platform for grid procurement proposed in this study is based on Hyperledger Fabric technology and methods at the database level, such as hash calculation of data, data fingerprint extraction, access control, and fast data reading. It can achieve multi-level data protection and data tamper-proofing through the entire life cycle of procurement transaction data and can effectively control the trust crisis that may be caused by the asymmetry of information among subjects of the procurement transaction platform. Finally, the feasibility of the prototype system for the proposed strategy is verified by the experimental analysis of the protection performance of the system.

Key words: purchase transactions; Hyperledger Fabric; data protection; data tamper proof

近年来, 随着电子商务和管理信息化的迅猛发展, 基于纸质标书传统招投标活动弊端日益凸显. 采用传统纸质标书投标, 不仅成本高昂、效率低下, 还存在诸如人为因素多、过程透明度低、标书存档利用困难、不符合低碳环保要求等缺点. 为此, 电子化招投标应运而生, 成为招标采购中的主流模式.

为了贯彻国家关于电子化招投标的精神, 南方电网物资有限公司于 2019 年完成南方电网电子采购交

易平台建设工作. 该平台支持各类招标及非招标采购方式, 实现发投标、开评标、费用支付、归档等全过程线上办理, 且已获得电子招标投标系统交易平台最高等级“三星”认证. 截至 2021 年 9 月, 业务项目的采购金额已突破 100 亿元. 与传统招投标相比, 电子化招投标技术的应用, 在招投标效率、数据准确性、节省人力物力、提高采购过程公正性等方面带来了巨大进步. 但是, 招投标过程涉及环节多、信息量大且信息敏

^① 基金项目: 南网物资公司区块链技术在供应链领域的研究应用项目 (ZBKJXM20200544)

收稿时间: 2021-11-12; 修改时间: 2021-12-13, 2022-01-05, 2022-01-24; 采用时间: 2022-01-28; csa 在线出版时间: 2022-06-16

感, 仍然存在一些必须解决的问题。

随着区块链技术的发展, 其有望于解决电子化招投标过程中存在的问题, 并且将区块链应用于电子招投标也成为了当前电子招投标研究的热点。文献 [1] 将智能合约应用于政府招标, 构建一个公平、透明且可审计的政府招标平台。文献 [2] 提出一种应用在以太坊区块链上进行简洁可验证的密封投标拍卖的智能合约协议。文献 [3] 引入了基于区块链的电子投标系统, 在不需要可信第三方的情况下, 由智能合约处理所有投标交易, 确保投标过程的完整性。文献 [4] 提出了“大数据+区块链技术”在电子招投标平台的应用方案, 保证招投标活动的“公平、公正、公开”。文献 [5] 提出了一种基于区块链的可信电子投标系统 (BCES), 以解决投标数据文件分发、验证和回溯过程中的操作合规性、多方协调和网络安全问题。文献 [6] 考虑到拍卖的隐私性和安全约束, 提出了基于区块链的公开竞价拍卖系统框架, 增强了拍卖人和投标人之间的安全性。文献 [7] 提出了基于以太坊区块链的解决方案, 以确保数据完整性和透明度并消除中间人。

上述文献研究了将区块链技术应用于电子化招投标中。然而, 当前在面向电力行业的电子化招投标应用较少, 区块链技术未能赋能电力物资供应链电子化招投标, 导致在电力行业中电子化招投标过程中数据的真实性及合法性仍被质疑, 影响并阻碍了南方电网电子采购交易平台建设工作的进一步展开。因此在电子招采过程中, 如何将区块链技术应用于电网企业的电子化招投标过程, 并且保证数据的防篡改, 将具有非常重要现实意义。

1 问题与挑战

南方电网电子化招投标和传统的纸质化现场招投标相比, 采购交易形式发生了较大的变化, 减少了传统的人力、物力投入, 但存在以下两个问题:

(1) 数据真实性问题

与传统招投标相比, 电子化招投标技术的应用, 在招投标效率、数据准确性、节省人力物力、提高采购过程公正性等方面带来了巨大进步。但是, 招投标过程涉及环节多, 信息量大且信息敏感, 仍然存在一些必须解决的问题。如: 交易数据的真实性与完整性容易让人质疑, 监管部门难以对交易数据进行有效的核验, 平台主体间的信任危机以及针对招投标公平性的质疑时有

出现, 因数据共享不畅导致的招标投标组织工作负担重、效率低, 以及数据验证不好追溯等问题。

(2) 中心化数据存储易篡改问题

目前的采购及电子招投标信息都采用集中式存储方式, 由系统管理员进行数据管理, 包括数据录入、数据查询、数据添加、数据删除、数据更新等各种操作。由于系统管理员拥有数据处理的所有权限, 其可以未经授权私自篡改数据; 也可以在领导授意下篡改数据, 从而无法保证招投标信息的真实性, 影响采购和招投标的公平公正, 也给廉政建设带来隐患。此外, 集中式的数据存储还容易受到内/外部攻击^[8]; 有很多企业采用数据异地冗余备份技术^[9,10], 但这显然大幅度增加了数据存储和数据维护的成本。

区块链技术具有分布式共享、防篡改、数据可追溯等特点, 可以有效解决数据被篡改的问题。区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新账本数据、利用密码学方式保证数据传输和访问安全、利用智能合约来编程和操作数据的一种全新的分布式计算范式^[11], 具有分布式共享、非篡改、数据可追溯的特点, 可以解决数据可信和单点故障、遭受攻击等问题, 因此在电力行业得到了丰富的应用^[12-16]。

本文将结合数据分片、数据指纹、数据指纹数据库、智能合约等技术, 设计与实现基于 Fabric 的电网采购交易数据平台, 平台面向电力物资供应链领域, 实现了采购交易数据不可篡改、数据随时可验证、数据访问控制等功能, 从而保证在电子招标采购过程中数据的完整性、真实性, 同时减少人工参与, 从而减少人为篡改数据的风险。

2 电网采购交易数据平台

本节介绍平台的具体细节, 第 2.1 节对原型系统的总体架构进行描述, 并且对技术选型以及整个采购交易业务流程进行说明, 第 2.2 节、第 2.3 节及第 2.4 节对重要模块进行说明, 其描述的模块分别为数据访问控制权限模块、数据访问控制权限模块以及数据取证及验证模块。

2.1 系统总体架构

基于 Fabric 的电网采购交易数据平台分为底层区块链、数据存储层、系统层以及门户层, 如图 1 所示。底层区块链模块主要负责采购交易的信息及全流程行为, 数据一旦上链, 无法篡改。监管机构对智能合约进

行签名认证,参与方通过智能合约提交中间结果,验证方通过智能合约验证中间结果.数据存储层用于多云互联管理系统存储,包含关系型数据库、非关系型数据库、分布式文件系统、对象存储等.系统层用于平

台业务实现,包含数据管理、上链管理、合约管理、用户管理、权限管理等模块.门户层用于给各类不同用户提供一致的操作体验,包含数据可视化门户、服务门户、管理门户、运营门户模块.

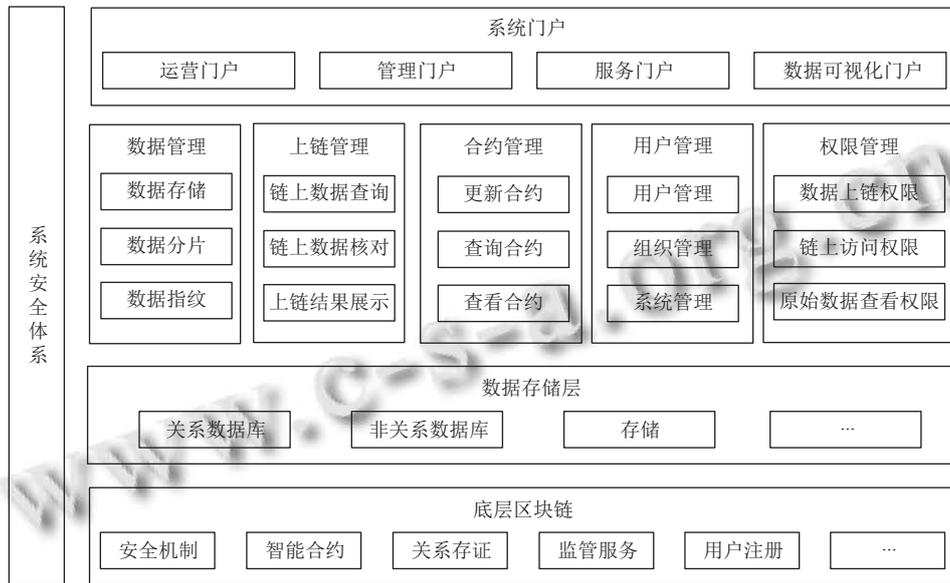


图1 系统架构

系统的技术选型包括界面展现技术、服务器开发技术以及架构技术,其中界面展现技术包括HTML、JavaScript和CSS,服务器开发技术语言为Java和PHP,架构技术为微服务架构.开发平台为微服务平台.接口包括RESTful API,接口遵循Spring Cloud框架约定的规范.

图2为基于区块链的采购交易数据上链业务流程图,其流程描述如下:先由需求人员提出需求,分包人员进行项目分包,然后经由项目承办人员完成采购方案的制定,之后项目经办人员完成以下流程:编写采购文件,发布采购公告,进行项目发售,项目发售中包含供应商购标、制作标书、投标、澄清等流程,然后进行开标,评标配置,评标;之后项目承办人员完成定标,由项目经办人员进行结果公示和结果公告,在公告结束后进行结果通知,最后完成项目归档.

其中,在采购公告环节可以利用区块链技术进行关键信息上链操作,开标阶段可以将供应商信息,报价,项目信息(包括项目编号名称),标包的关键信息进行上链;在结果公示和结果公告环节中可将供应商名单上链存证.

而在交易过程中产生的电子数据—交易电子数据,需要我们对它进行存储并且防篡改.交易电子数据具有易创建、易存储、易传输和高利用率等特点,是可靠、有证明力度的电子数据证据.数据存证首先要对数据按类型进行很好的存储保存,并且还要对数据的可信性、完整性有很好的保障,并且还要方便对数据进行存储、共享、验证等操作.对于上链存证的电子化招投标项目中的关键信息、公示公告等内容,通过设置访问权限,对不同的身份主体划分权限.

2.2 数据指纹提取及上链

在区块链中,数据上链的流程如图3所示,主要包括上链前处理阶段和上链处理阶段.在上链前处理阶段,有业务数据处理和数字签名两个处理步骤.业务数据处理的业务数据可以是任意的内容,比如供应商信息,报价,项目信息(包括项目编号名称)或者对应数据的哈希值等,这些业务数据通过服务器处理;在上链处理阶段,有广播、打包、共识等处理步骤.

在业务数据处理阶段,使用类Merkle树算法对数据进行处理,提取业务数据的数据指纹,具体算法步骤如算法1所示.

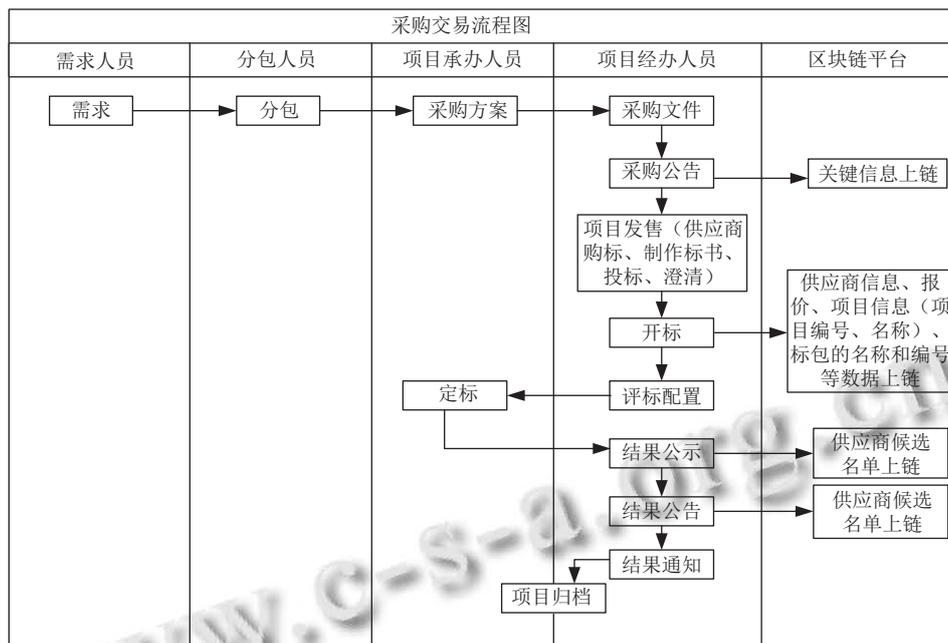


图2 基于区块链的采购交易数据上链业务流程

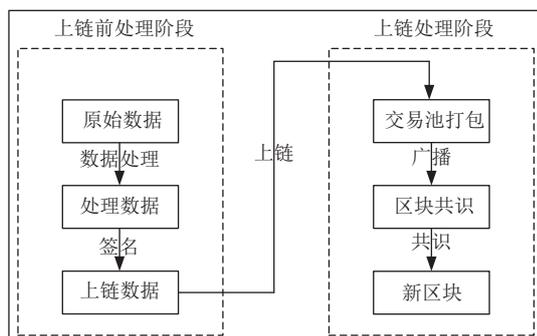


图3 数据上链流程图

算法 1. 类 Merkle 树算法

- 1) 从数据库中获取业务原始数据;
- 2) 将业务原始数据分块;
- 3) 采用 SHA256 作为哈希函数来计算数据块的哈希值;
- 4) 构建 Merkle 树, 提取数据指纹;
- 5) 数据指纹签名.

在算法 1 中, 数据块的分块大小首先由 SHA256 的原理确定, 同时采用 GPU 对数据块哈希值的计算进行加速, 所以分块的大小还基于 GPU 的性能. 通过构建 Merkle 树^[17] 的形式, 构建数据指纹树, 得到业务数据的数据指纹, 逻辑示意图如图 4 所示.

在完成数据的指纹提取之后, 对数据进行签名, 得到带有签名的数据指纹信息. 然后对带有签名的数据

指纹信息打包, 放进区块链交易池中, 排序节点对交易排序之后, 将带有签名的数据指纹信息构建默克尔哈希树, 并将所述默克尔哈希树的默克尔根作为所述采购交易数据文件的元数据储存到区块链的区块头中.

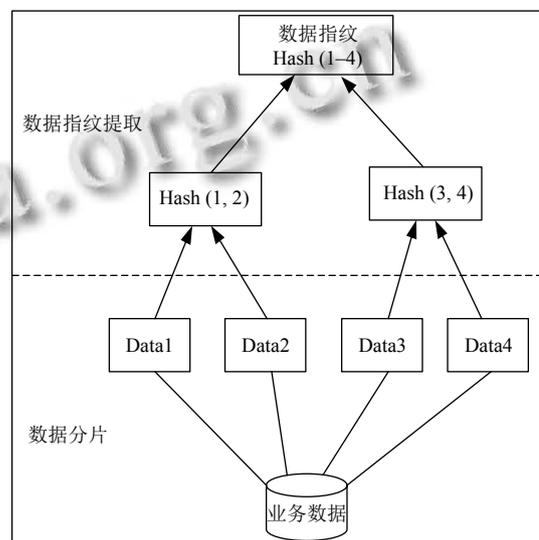


图4 数据处理逻辑示意图

与所有区块链结构相同, 区块链链上数据包括两部分结构, 即区块头和区块体中交易数据字段. 区块头数据主要由系统产生和维护, 用于区块链数据的保护, 区块头数据结构如表 1 所列. 用户数据主要存储在区

块体的交易记录中,交易记录以交易列表的形式存储在区块体中,表2中给出与查询相关字段的相关说明。

表1 区块头字段说明

字段	字段说明	大小 (B)
区块ID	区块编号,代表区块高度	4
区块哈希值	唯一标识当前区块	20
父区块哈希值	唯一标识前序区块	20
Merkle根	区块内交易的校验值	20

表2 交易事务列表中包含的主要字段

字段	字段英文表示	字段说明
交易ID	TransID	交易索引编号
交易哈希值	Transhash	该笔交易的数字签名
项目编号	ProjectID	该交易所属项目的项目编号
项目阶段属性	Stage_attribute	此交易文件产生的项目阶段
存储文件哈希值	Files_hash	文件的数据指纹
采购部门	Files_department	项目采购部门编号
时间戳	Timestamp	交易产生时间
文件标识	Files_ID	关联链下原始文件的唯一标识

2.3 数据访问控制权限

由于供应需求,不同的部门存在需要其他部门的供应商信息的情况,对于其他部门的访问,则需要设置访问权限。此外,对于上链存证的电子化招投标项目中的关键信息、公示公告等内容,通过设置访问权限,对不同的身份主体划分权限。根据用户不同角色,提取用户的如下信息:用户属性、所属部门,基于这些信息,设计如下的角色、部门及权限对应规则,如表3所示。

表3 用户访问权限表

用户角色	属性	部门	存证	取证
部门用户	DepartmentUser	department	N	Y (只能取证所属部门及公开的数据)
管理员	AdminUser	null	Y	Y
普通用户	GuestUser	null	N	Y (只能取证公开数据)

面向用户的权限访问控制将用户分为了3类:部门用户、管理员和普通用户。其中,只有管理员具有存证权限;3种用户都具有取证权限,只是取证的数据范围不同:管理员可以取证所有数据,部门用户只能取证所在部门的数据以及公开数据,普通用户只能取证公开数据(如电子招投标的公示信息)。

完成用户权限设计后,通过智能合约的链码逻辑来响应基于用户属性的访问控制。声明 GetAttributeValue() 函数来获取用户的属性值,声明 GetDepartmentInfo() 函数来获取用户所属的部门信息。访问控制链码伪代

码如算法2,显示了访问控制逻辑,根据不同的用户属性,允许执行不同的存证和取证操作。图5为用户访问获取链上数据流程图。

算法2. 访问控制链码伪代码

```

1. attr := GetAttributeValue()
2. departmentinfo := GetDepartmentInfo()
3. switch attr {
4. case "GuestUser":
5.     //执行取证操作,仅限于公开信息
6. case "AdminUser":
7.     //执行存证和取证操作
8. case "DepartmentUser":
9.     //执行取证操作,仅限于公开信息以及属于 departmentinfo 部门的信息;

```

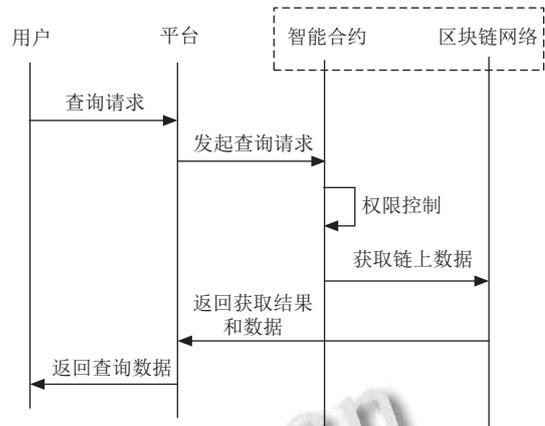


图5 用户访问获取链上数据流程图

2.4 数据取证及验证

数据取证是为调取链下文件对应的链上哈希值,利用哈希函数的抗碰撞性,将文件的链上数据指纹与链下文件生成的数据指纹进行对比,以验证数据在存储前后的一致性,确保数据在存储和处理过程中没有发生丢失或篡改。区块链是一种不断增长的数据库,当上链存证信息数量较大时,区块链数据库面临遍历查询效率偏低和查询功能有限的问题^[18]。本文基于外联数据库查询思想^[19],设计链上数据指纹索引库扩展链上数据查询功能,在链下建立关联各上链存证文件的数据指纹索引表,提高查询取证的效率。

数据取证与验证的流程和各数据库之间的交互如图6所示,数据取证之前需要在区块链数据库和外部数据指纹索引库之间同步关联数据,取证及验证具体步骤如下。

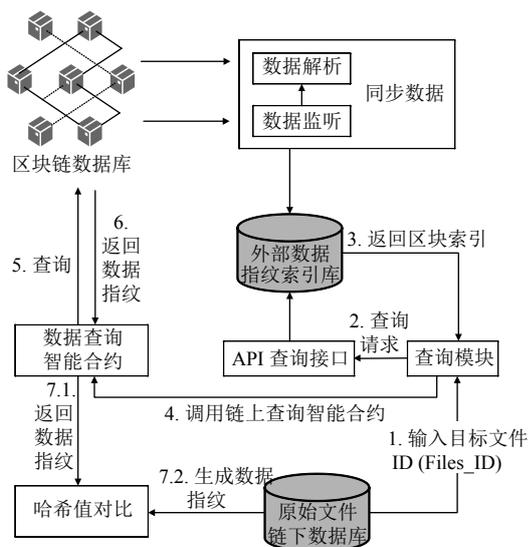


图6 数据取证及验证执行流程

(1) 数据关联: 外部数据指纹索引库通过 API 接口监听链上状态, 一旦区块链中存储一笔招标采购事务上链, 通过接口将区块数据同步导入到缓冲区, 缓冲区的数据利用数据解析模块将区块中和外部数据库的关联数据经处理导入数据指纹索引库, 关联数据包括区块 ID、交易 ID、项目编号、项目阶段属性和文件标识等。

(2) 数据取证: 调用数据指纹索引库 API 接口, 利用文件标识和项目编号作为数据库之间的关联值进行查询操作, 数据库通过 API 接口返回目标文件所在区块号和交易索引号. 查询操作调用链上数据获取智能合约, 以区块 ID 和交易 ID 作为合约触发条件的输入, 定位目标文件哈希值所在位置, 并返回目标文件的链上哈希值。

(3) 数据验证: 将链上数据哈希值与链下文件哈希值进行对比, 若一致, 则证明采购交易文件在链下存储过程中没有被篡改。

3 系统展示与分析

本节实验与分析首先对基于 Fabric 的电网采购交易数据平台中数据防篡改进行理论分析, 然后对系统进行关键性指标分析, 最后对系统的一些模块进行界

面展示。

3.1 数据安全性分析

对于数据防篡改的理论分析从数据库和区块链两个层面进行分析。

(1) 数据库层面

在数据处理的时候, 对业务数据进行分块, 将容量大的业务数据分成容量小的数据块数据, 并且将每个划分的数据块进行哈希运算, 采用类 Merkle 树的思想, 对数据块构建一个数据指纹树. 对业务数据的一小部分数据进行篡改, 都将得到一个不同的数据指纹。

(2) 区块链层面

将数据指纹上传到区块链系统中, 区块链作为一个分布式、多方参与的系统, 链上的数据均可查询, 通过访问权限设置, 实现不同主体对于数据的访问, 从链上获取的数据, 能够与链下的数据进行指纹比对, 进一步实现数据的防篡改。

3.2 关键性指标分析

针对上述系统的可用性, 本文利用 Hyperledger 提供的工具“Hyperledger Cliper”, 对关键性指标进行测试, 其关键指标为对存证和查询的时间, 如表 4 和表 5 所示. 系统部署在 3 台 2 核 4 GB 内存的主机中, 系统使用的版本为 Ubuntu 20.04.3 LTS, Fabric 版本为 1.4.1, Docker 版本为 20.10.8, Docker-compose 版本为 1.26.0, Golang 版本为 1.14.9 Linux/amd64. Fabric 部署在 docker 容器中, 首先下载及安装环境必需的软件和依赖, 包括 Go、docker、docker-compose 等; 其次搭建多节点环境, 环境中搭建了 4 个 ordered 节点及 10 个 peer 节点; 然后生成创世块, 并搭建组织通道; 最后, 在通道中部署、安装实例化链码. 系统共识采用常用的 PBFT 共识, 该共识通信复杂度低, 且实用性强, 系统部署的 4 个 ordered 节点也符合 PBFT 共识的边界条件 (为了应对 1 个恶意节点, PBFT 算法至少需要 4 个共识节点)。

由表 4 所示, 通过 Cliper 的测试可知, 上链事务成功率为 100%, 并且随着发送速率的增大, 吞吐量也在增大, 写 3 000 条记录的平均延时均在 0.1 s 以下。

表 4 上链存证测试结果表

测试	名称	成功	失败	发送速率 (TPS)	最大延迟 (s)	最小延迟 (s)	平均延迟 (s)	吞吐量 (TPS)
1	write	3 000	0	160.2	0.12	0.04	0.07	159.8
2	write	3 000	0	194.5	0.18	0.05	0.09	172.3
3	write	3 000	0	186.4	0.17	0.05	0.08	185.5

表5 数据查询验证平均时间

数据条目	传统交易哈希查询验证 (s)	数据指纹数据库查询验证 (s)
1 000	0.02	0.01
2 000	0.02	0.01
3 000	0.03	0.01
4 000	0.02	0.01

对于本论文设计的基于数据指纹哈希索引库的外部关联查询方法,包括两次查询操作.第1次查询操作为通过文件ID和项目编号在数据指纹索引库中执行,由于数据指纹哈希索引库采用关系型数据库的形式,因此对数据的查找可直接利用主键查询的方式,查找速度快,且数据量的增长并不会影响数据的查询速度.第2次查询操作为调用智能合约以区块号和交易索引号为查找条件进行链上查找,由于已经知道数据指纹所在的区块号和交易索引号,因此不同于传统区块链的遍历查找,传统区块链的数据查找方式,查询的时间消耗与数据量的增长呈正比,而本文的查找方法直接通过索引进行定位查询,在查询速度上有很大提升.

由于数据量较大,因此采用数据分片的方法,将数据进行分片,然后采用GPU并行计算的方法,将数据

并行计算哈希值,提取数据指纹,最后将数据指纹上链.系统采用基于CUDA的数据并行处理方法,相对于传统的CPU(OpenSSL)计算,业务数据量越高,并行计算的效果越好,如图7所示.

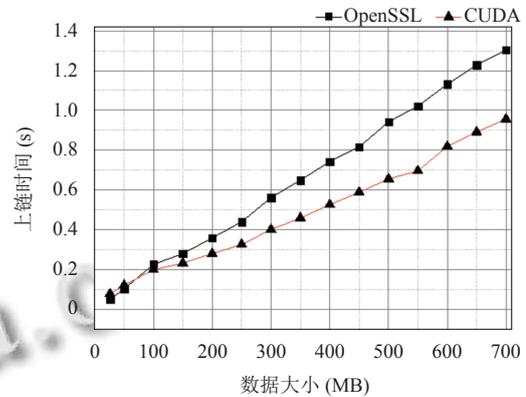


图7 基于 OpenSSL 和 CUDA 的上链时间对比图

3.3 系统展示

如图8所示,为业务数据指纹提取展示界面,通过对数据分块以及GPU计算,采用类Merkle树的形式,得到了业务数据的数据指纹.

序号	文件名称	更新时间	大小	数据指纹
1	南网科研院重要交叉跨越线路健康评估方法研究	2021-7-25 12:32:23	2.3MB	2a94e9cd96df43e6036c9e8da025fe34
2	2021年公司数字化水平提升项目	2021-6-2 18:33:21	6.7MB	33b3e4875b392a2d295f3ed0112904c3
3	2021年自动化保护专业防冰抗冰、35kV攻坚货物专项采购	2021-6-17 16:40:28	3.2MB	5d4d897a0699d6e1b32a6637e438cfe6
4	南方电网主干综合数据网经济技术支持	2021-7-5 13:18:29	5.8MB	8ff695f47df00d449f79bcee5649b111
5	输电线路耐张塔X射线无损检测项目	2021-8-29 16:30:11	3.8MB	40b1a7de043ab9c928ffa50298e9c417
6	跨省区电网交换功率可行性分析	2021-7-18 16:23:56	10.6MB	6f98b90dbf5f287fe2db920bcd121f37

图8 业务数据的数据指纹展示图

如图9所示,为用户访问权限控制,可以从图中看出没有权限的用户没办法查询更多的数据,会有一个弹窗显示没有权限访问.如图10所示,为业务数据的数据验证示意图,通过数据指纹数据库快速获取区块链中的区块链中的数据,然后与链下的数据进行哈希比对,可以知道数据是否被篡改,图中数据因为篡改,导致哈希值对比时出现问题,显示数据

被篡改.

4 总结

本文给出了基于Fabric的电网采购交易数据平台的设计与实现方案,通过指纹提取、数据访问控制、数据指纹库设计等手段确保了电子化招标采购过程的中数据的防篡改性和真实性验证.平台采用前后端分

离的模式,保证了系统的高内聚和低耦合,试运行表示能够解决招标采购中的采购交易数据篡改问题.在未

来的系统优化中,将加入合同签约等功能模块,进一步提高电力物资供应链中各环节的业务效率.



图9 权限访问控制展示图



图10 数据防篡改展示图

参考文献

- 1 Hardwick FS, Akram RN, Markantonakis K. Fair and transparent blockchain based tendering framework—A step towards open governance. Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). New York: IEEE, 2018. 1342–1347.
- 2 Galal HS, Youssef AM. Succinctly verifiable sealed-bid

- auction smart contract. Proceedings of the ESORICS 2018 International Workshops on Data Privacy Management, Cryptocurrencies and Blockchain Technology. Barcelona: Springer, 2018. 3–19.
- 3 Manimaran P, Dhanalakshmi R. Blockchain-based smart contract for E-bidding system. Proceedings of the 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT). Jaipur: IEEE, 2019. 55–59.
- 4 田钰平, 刘猛. “大数据+区块链技术”在电子招投标平台中

- 应用研究. 大众标准化, 2021, (11): 23–26. [doi: 10.3969/j.issn.1007-1350.2021.11.011]
- 5 Li XC. BCES: A Blockchain based credible E-bidding system. Proceedings of the 2020 IEEE 6th International Conference on Computer and Communications. Chengdu: IEEE, 2020. 2415–2421.
- 6 Sarfaraz A, Chakraborty RK, Essam DL. A tree structure-based improved blockchain framework for a secure online bidding system. Computers & Security, 2021, 102: 102147.
- 7 Omar IA, Hasan HR, Jayaraman R, *et al.* Implementing decentralized auctions using blockchain smart contracts. Technological Forecasting and Social Change, 2021, 168: 120786. [doi: 10.1016/j.techfore.2021.120786]
- 8 Tso R, Liu ZY, Hsiao JH. Distributed E-voting and E-bidding systems based on smart contract. Electronics, 2019, 8(4): 422. [doi: 10.3390/electronics8040422]
- 9 陈贵海, 吴帆, 李宏兴, 等. 基于 DHT 的 P2P 系统中高可用数据冗余机制. 计算机学报, 2008, 31(10): 1695–1704. [doi: 10.3321/j.issn:0254-4164.2008.10.004]
- 10 王帅, 常朝稳, 王禹同, 等. 面向多云盘的 N+i 模式的编码冗余存储机制. 小型微型计算机系统, 2016, 37(2): 236–240. [doi: 10.3969/j.issn.1000-1220.2016.02.009]
- 11 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494.
- 12 刘芯汝, 高辉, 张卫国, 等. 基于区块链技术的 P2P 电能交易平台与配电网协同仿真. 计算机系统应用, 2021, 30(4): 54–61. [doi: 10.15888/j.cnki.csa.007864]
- 13 郭欣沅, 董思晴, 黄文涛, 等. 区块链技术在电力行业物资合同管理中的应用. 计算机系统应用, 2019, 28(7): 65–71. [doi: 10.15888/j.cnki.csa.006968]
- 14 付杨, 王景中, 杨洵, 等. 基于区块链的视频版权存储架构. 计算机系统应用, 2020, 29(8): 58–66. [doi: 10.15888/j.cnki.csa.007485]
- 15 徐睿, 孟祥君, 马锋, 等. 基于防篡改技术的电子签约服务平台. 计算机系统应用, 2018, 27(4): 39–46. [doi: 10.15888/j.cnki.csa.006331]
- 16 曹迪迪, 陈伟. 基于智能合约的以太坊可信存证机制. 计算机应用, 2019, 39(4): 1073–1080. [doi: 10.11772/j.issn.1001-9081.2018092005]
- 17 黄根, 邹一波, 徐云. 区块链中 Merkle 树性能研究. 计算机系统应用, 2020, 29(9): 237–243. [doi: 10.15888/j.cnki.csa.007528]
- 18 余涛, 牛保宁, 樊星. FabricSQL: 区块链数据的关系查询. 计算机工程与设计, 2020, 41(10): 2988–2995.
- 19 王千阁, 何蒲, 聂铁铮, 等. 区块链系统的数据存储与查询技术综述. 计算机科学, 2018, 45(12): 12–18.

(校对责编: 孙君艳)