doi：10.11835/j.issn.1000-582X.2020.289

基于区块链的电力营销数据存储机制

王凌宇[1]，傅　宏[1]，杨　云[2]，刘　俊[3]
（1. 国网重庆市电力公司客户服务中心，重庆 400000；2. 国网重庆市电力公司，重庆 400014；
3. 重庆邮电大学 软件工程学院，重庆 400065）

摘要：随着电力的发展电力营销数据持续增长，传统的集中式数据存储模式已经不能满足电力业务数据存储的安全性和高效性需求。针对上述问题，提出了一种基于区块链的多级加密电力营销数据存储架构，该存储架构以区块链技术作为底层技术支撑，结合分布式存储提供稳定性高、安全可靠的电力数据存储方案。同时在区块链的基础上提出多级加密机制，该机制支持电力数据上链及电力数据传输等流程的逐级加密及验证，使得电力数据存储的安全性得到进一步的保证。通过创建分布式存储设施，对提出的存储机制与集中式存储机制进行对比实验，分析实验结果发现提出的存储机制在电力数据存储方面相比于传统的存储机制在系统延迟、响应时间和吞吐量上都更具有优势，表明了该存储机制合理可行，具有良好的应用前景。

关键词：区块链；分布式存储；电力大数据；数据完整性证明
中图分类号：TP309.2　　**文献标志码**：A　　**文章编号**：1000-582X(2021)08-156-09

Storage mechanism of electricity marketing data based on blockchain

WANG Lingyu[1]，*FU Hong*[1]，*YANG Yun*[2]，*LIU Jun*[3]
（1. Customer Service Center，State Grid Chongqing Electric Power Company，Chongqing 400000，P. R. China；2. State Grid Chongqing Electric Power Company，Chongqing 400014，P. R. China；3. School of Software Engineering，Chongqing University of Posts and Telecommunications，Chongqing 400065，P. R. China）

Abstract：With the development of electricity supply，electricity marketing data continue to grow. Traditional centralized data storage modes have been unable to meet the security and efficiency requirements of power business data storage. To address the issues，this paper proposes a multi-level encrypted electricity marketing data storage architecture based on blockchain. The storage architecture uses the blockchain as the underlying technical support and combines with distributed storage to provide highly stable，secure and reliable power data storage scheme. At the same time，a multi-level encryption

收稿日期：2020-01-15　　**网络出版日期**：2020-03-18
基金项目：重庆市高校优秀成果转化资助项目（KJZH17116）；重庆市创新创业示范团队培育计划（CSTC2017kjrc-cxcytd0063）；重庆市技术创新与应用示范重大主题专项（CSTC2018JSZX-CYZTZX0185）；重庆市基础科学与前沿技术研究项目（CSTC2017jcyjAX0270）。
Supported by the Chongqing University Outstanding Achievement Transformation Funding Project（KJZH17116），Chongqing Innovation and Entrepreneurship Demonstration Team Cultivation Plan（CSTC2017kjrc-cxcytd0063），the Chongqing Technology Innovation and Application Demonstration Major Theme Project（CSTC2018JSZX-CYZTZX0185），and the Chongqing Basic Science and Frontier Technology Research Project（CSTC2017jcyjAX0270）.
作者简介：王凌宇（1993－），男，助理工程师，主要研究方向为网络与信息安全，（E-mail）1625159399@qq.com。

mechanism is proposed on the basis of the blockchain. This mechanism supports step-by-step encryption and verification of power data on-chain and power data transmission processes, which further guarantees the security of power data storage. The proposed storage mechanism is compared with the centralized storage mechanism by creating a distributed storage facility. The experimental results show that the proposed storage mechanism has more advantages in terms of system latency, response time, and throughput than traditional storage mechanisms, indicating that the proposed storage mechanism is reasonable and feasible and has good application prospects.

Keywords: blockchain; distributed storage; power big data; data integrity certification;

由于电力系统其本身结构复杂、设备众多，且随着中国工业用电与居民用电需求越来越高从而产生海量的电力数据[1]，如何高效且安全地对 TB(trillionbyte)甚至 PB(petabyte)级别的电力交互数据进行存储成为当前电力企业发展的一个重要问题。

目前电力公司数据管理平台多采用关系型数据库(如 Oracle、MySQL 等)，针对关系型数据库对海量数据的读写性能比较差[2-3]，宋亚奇等[4]提出了基于 Hadoop 和 HBase 的电力设备采样数据的云存储方案，实现了海量数据存储和快速查询。但是在云存储环境中，当非法用户取得对电子记录的控制权时，云存储的数据容易复制和篡改。同时云存储服务器可能会故意删除电子记录以节省成本，从而对电子记录的所有者造成不可挽回的损害。

针对云存储存在数据丢失、信息安全受限等问题，颜拥等[5]提出将区块链应用到电力行业场景之中，以区块链技术作为电力电子合同安全存储的底层支撑，实现电力行业网中电子合同数据的完整性保存。

普通用户在日常用电的过程中会产生用电数据信息，主要包括用户名称、用户地址、电价电费、用户电量、用户联系信息及受电装置等。这些信息涉及用户的个人隐私，在向企业提供营销数据信息的同时需要对其安全性进行分析。笔者以区块链技术为核心，提出一种基于区块链技术的多级加密电力数据存储机制，相比于传统的电力数据存储方案，该存储机制利用区块链技术解决电力的存储安全问题，同时结合分布式存储技术，解决数据不断增长集中式存储硬件设备容量有限的问题，该存储机制满足分布式数据库的高并发性、高可用性，经过实验证明该存储方案能够满足电力营销数据的安全存储性能的要求和服务可靠性的要求。

1　相关背景知识

区块链是一种分布式数据结构，可以在网络成员之间进行复制和共享。它被引入比特币[6]来解决双重花费问题[7]。区块链是一种基于分布式计算和数据存储的新兴技术，受密码学数字签名和分布式共享机制的组合保护。即使存在网络攻击和通信中断的情况下，区块链系统中的各个节点依旧可以达成区块链网络状态的一致性协议。在区块链系统中有公有链、联盟链和私有链 3 种类型[8]，对比关系如表 1 所示。

表 1　各区块链系统类型对比

Table 1　Comparison of various blockchain system types

比较内容	公有链	联盟链	私有链
网络结构	完全去中心化	部分去中心化	中心化
节点规模	全网节点	部分节点	私有节点
数据读取	任意读取	受限读取	受限读取
共识机制	PoW，PoS 等	PBFT，RAFT	Paxos，RAFT
激励机制	代币激励	无代币激励	无代币激励

区块链技术的核心优势在于其去中心化中达成信息的共识。通常可以将区块链看作一个日志，它的记录被处理成时间戳保存为区块，每个块由其密码散列标识。其中每个块都引用它之前的块的哈希值。这将在块之间建立一个链接，从而创建一个块链或区块链，如图1所示。

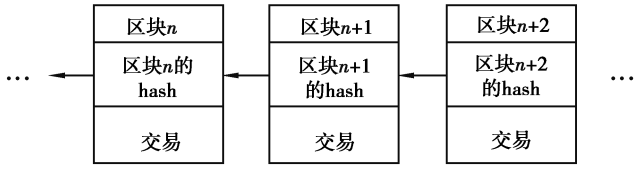


图1 区块的链式结构

Fig. 1 Blockchain structure

在区块链网络中的任何一个节点都可以访问这条链连接的区块列表存储的数据[9]。这些节点形成一个对等网络(peer to peer, P2P)，区块链的交互流程如下：

1)节点之间交互。节点通过私钥/公钥与区块链进行交互[10]。其中私钥来进行自己的交易，并且可以通过公钥在网络上寻址。区块链中使用非对称加密技术将信息认证，数据完整性和不可否认性带入到区块链网络。

2)交易验证。区块链网络中的对等节点对交易进行验证，确保这个进入区块链中的交易有效，然后再进一步转发，进行全网的同步，无效的交易会被丢弃。

3)挖矿。挖矿是指在约定的时间间隔内，由网络使用上述流程收集和验证的事务，且将各事务进行排序并打包成一个时间戳成为候选块的过程。

4)事务验证。当节点验证的交易包含事务的有效性，即当前的散列引用其链上的前一个区块的散列值时，他们会将区块添加到其链中，否则丢弃该候选的区块。

区块链应用程序为各种场景提供了应用程序接口(API)。用户通过这些API与他们直接交互，而不必担心底层的技术细节。通常在区块链应用中把它作为一个附加的数据库，由对等网络节点维护[11]。在区块链系统中，任何节点都可以签署和发布事务，如果它们被验证通过则加入到新的区块中。区块链系统中的节点将随时检查其分散网络中的其他节点，每个节点都可以加入协商过程，将新的区块扩展到区块链中。区块链中数据具有防篡改特性，在新区块生成过程中需要其他节点的验证，因此在全局账本中记录的所有有效的区块和交易实际上都是不可变的。此外，整个全局账本在区块链节点之间按照协商一致的机制进行同步[12]，使区块链上存储的数据真实性和准确性有了更大的保障。

2 区块链系统的数据存储技术

区块链中的每个区块包含区块头和区块体两个部分[13]。区块头主要用于构成区块的链式结构，主要有前一个区块哈希值(prev hash)、时间戳(timestamp)、随机数(nonce)和交易的根哈希(root hash)组成，其中目标区块的哈希值由前一个区块的哈希值和随机数生成，根哈希用于验证交易的真实性使得交易不可伪造[13]。区块中的区块体部分主要存储交易数据，交易数据的结构由区块链系统支持的功能所决定。

2.1 区块链的主要数据结构

区块链是基于交易的系统[8]，在区块链系统中存在大量的交易数据，这些交易数据存储结构为Merkle树。Merkle树的数据结构可以是二叉树也可以是n叉树，在比特币中使用的是二叉树结构[14]，如图2所示。Merkle树需要大量数据，将其压缩为一个简单的字符串，可以证明Merkle树所保存数据的真实性，而无须透露原始数据[15]。Merkle树采用自底向上方式构建，在区块链中叶节点为基础交易数据，每个中间节点是它的子节点的哈希，根节点是根哈希。在Merkle树结构中如果根据某种标准正确命名，则用户可以识别内容，而无须解压缩并打开包含的文件。不同的区块链系统在数据存储结构上有所不同，主要在根哈希结构、根哈希数量和存储编码等方面，典型的区块链存储结构对比如表2所示。

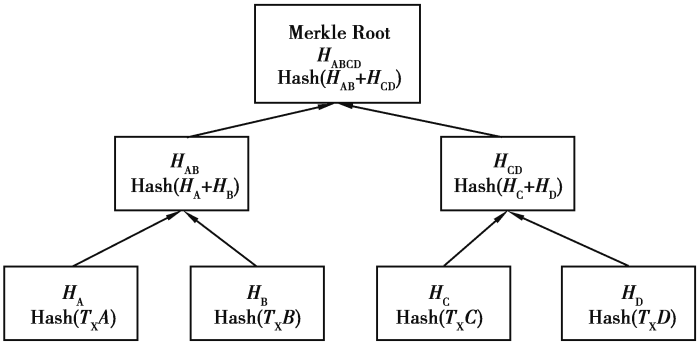


图 2　Merkle 树

Fig. 2　Merkle tree

表 2　典型区块链存储结构对比

Table 2　Comparison of typical blockchain storage structures

比较内容	以太坊	比特币	超级账本
根哈希结构	Merkle Patircia 树	Merkle 树	Merkle 树
根哈希数量	3	1	1
数据存储编码	RLP 编码	Base58Check 编码	Json 编码

2.2　区块链的数据存储方式

当前主流的区块链系统对区块头采用数据文件方式进行存储，对区块体及元数据主要使用 Key-Value 的形式进行数据存储。区块链系统的数据库主要基于 Key-Value 的 LevelDB 数据库，以此为代表的主要为以太坊和比特币，而超级账本 Fabric 的数据可以在转换成 Json 格式后选择存储在 LevelDB 或 CouchDB 之中。其他基于区块链的存储系统，如 Storj、Filecoin、BigchainDB 等系统也均采用了 LevelDB 或 MongoDB 等基于键值模型的数据库系统存储元数据信息[16]。

区块链系统中，不仅要存储区块头和区块体的数据，还需要根据功能设计管理状态数据、索引数据和元信息等数据，因此在数据组织方式上也具有较大的差异，主要的区块链系统存储组织对比如表 3 所示。

表 3　典型区块链系统存储对比

Table 3　Comparison of typical blockchain system storage structures

比较内容	以太坊	比特币	超级账本
数据存储系统	LevelDB	LevelDB	LevelDB、CouchDB
数据库数量	3	2	4
数据库存储内容	账户状态 收据信息 区块头和交易	UTXO 数据 区块的元数据	状态数据库 索引数据库 历史数据库 账本数据库
数据索引	Bloom Filter	Bloom Filter	Key-Value
区块链数量	单链	单链	多链

3 基于区块链的多级加密电力数据存储机制

3.1 基于区块链的电力营销数据存储架构

将区块链应用到电力行业电力营销数据存储的场景之中，提出基于区块链技术的电力营销数据存储模型，该模型具有2个数据库，其中1个为分布式存储数据库和联盟区块链，分布式存储数据库为区块链提供存储服务，区块链为分布式存储数据库提供系统安全支撑，存储架构如图3所示。

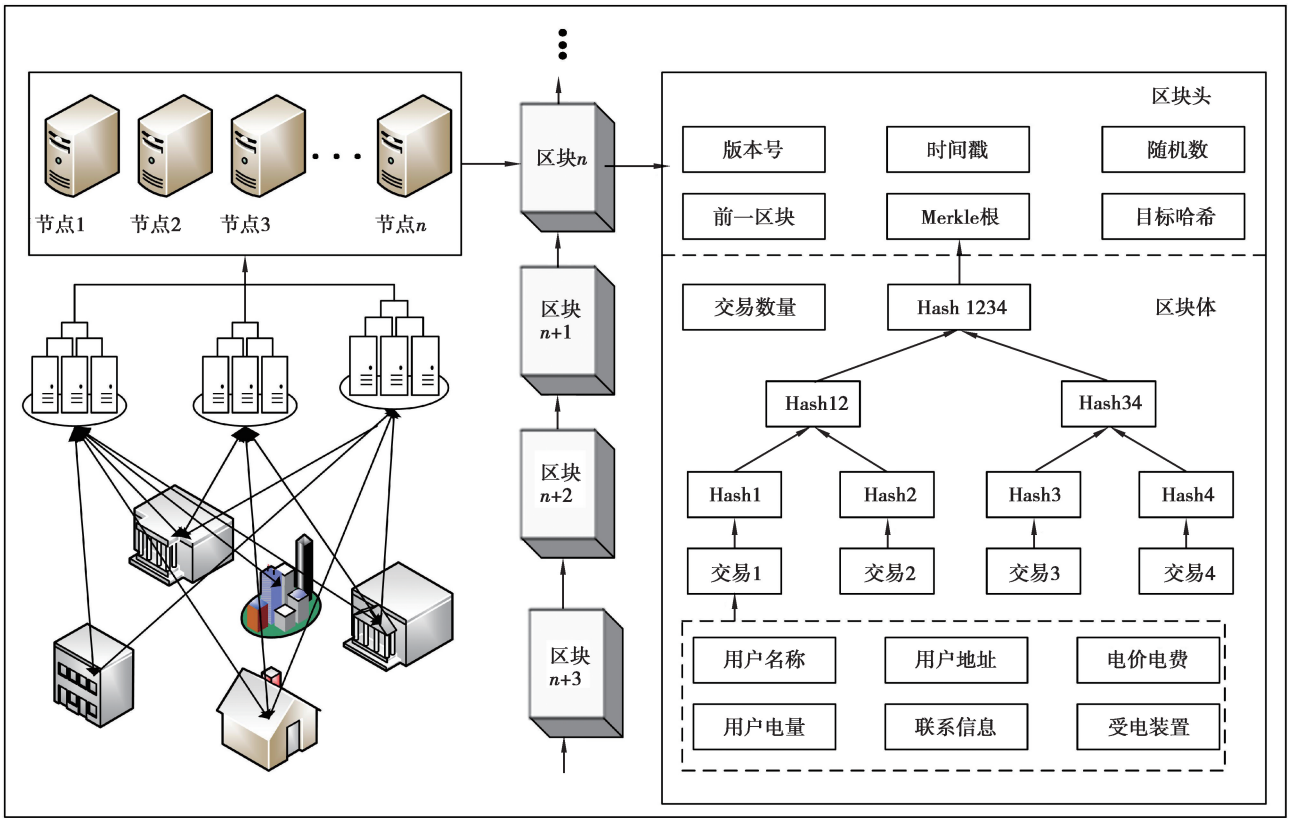


图3 基于区块链的电力营销数据的分布式存储架构

Fig. 3 Distributed storage architecture of power marketing data based on blockchain

基于区块链的多级加密电力数据存储主要包括电力营销数据的分布式存储服务和电力营销数据的多级加密服务两部分。其中基于区块链的电力数据分布式存储主要包括以下流程，首先智能电网设备或用户向本存储系统发出存储资源节点的请求，然后由本系统中的分布式存储节点提供存储服务，在存储服务完成后需要在区块链上登记存储记录，最后由智能电网设备或用户评价存储服务。

第1步，智能电网设备或用户向基于区块链的多级加密电力数据存储系统发送存储请求，需要在分布式存储节点中选择某个在线的存储节点作为存储服务的对象。在基于区块链的电力营销数据存储系统中设定一旦终端发送请求，在60 s内不能再选择其他存储节点发送存储请求，且收到存储节点的确认后，直接传送存储数据。

第2步，当在线存储节点收到存储请求时需要为请求节点提供存储服务，且按请求节点请求时间的先后顺序回复节点。当智能电网设备或者用户收到存储节点的确认消息后，即向存储节点传输电力数据。

第3步，存储记录信息上链，在存储节点完成响应请求的存储服务之后，存储节点将存储记录信息传输到区块链上。最后由智能电网设备或用户评价此次存储服务，评价信息作为存储节点的信用分，可根据该信用分评判该存储节点的存储性能。

3.2 电力营销数据的保密机制

在基于区块链的电力营销数据存储机制中提出一种基于数据分割的多级加密机制以保护电力营销数据

的安全性和隐私性。使用多级加密机制与分布式存储相结合可以很好地解决数据分割的使用场景，可有效提高系统效率，该多级加密机制支持电力数据上链、电力数据传输、智能合约调用等流程的逐级加密及验证，多级加密机制流程如图 4 所示。

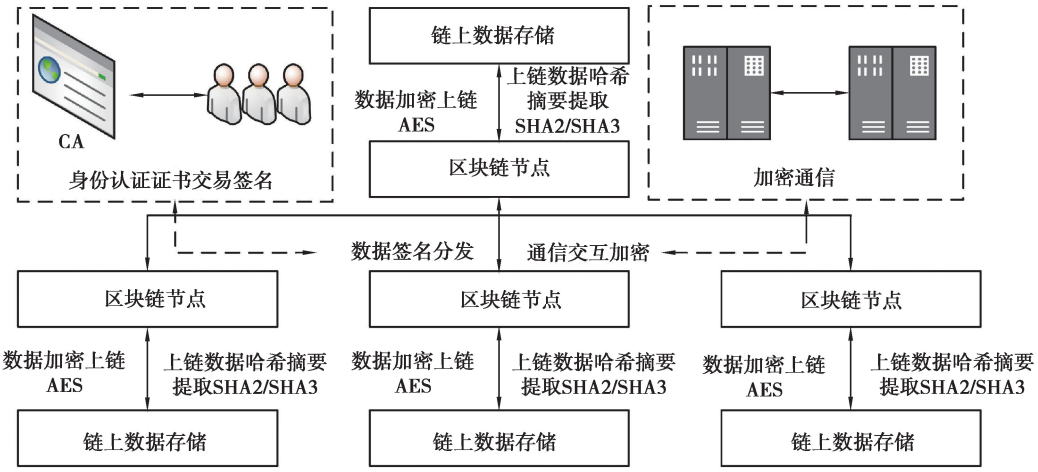


图 4　多级加密机制

Fig. 4　Multi-level encryption mechanism

在本文中所提出的多级加密机制主要由以下组成：身份认证模块、数据加密上链模块、上链数据哈希提取模块、加密通信模块。在身份认证模块中使用 RSA 算法生成公私钥，公钥可对用户电力营销数据加密，用作数据隐私保护，私钥用作智能电网设备或用户签名。为了提高系统效率同时减少密钥管理难度采用密钥长度为 128 bit RSA 加密算法，具体算法流程如图 5 所示。

RSA 加密算法

密钥生成：

选择两个质数 p 和 q

计算 p 和 q 的乘积 $n=p\times q$

计算 n 的欧拉函数 $\varphi(n)=(p-1)(q-1)$

随机选择一个整数 e，满足 $1<e<\varphi(n)$，且 e 与 $\varphi(n)$ 互为质数

计算 e 对于 $\varphi(n)$ 的模反元素 d

将 n 和 e 封装成公钥，n 和 d 封装成私钥

加密

利用公钥 (n,e) 对明文 M 进行加密：

$$c = M^e \bmod n$$

解密

利用私钥 (n,d) 对密文进行解密：

$$M = C^d \bmod n$$

图 5　RSA 加密算法流程

Fig. 5　RSA encryption algorithm flow

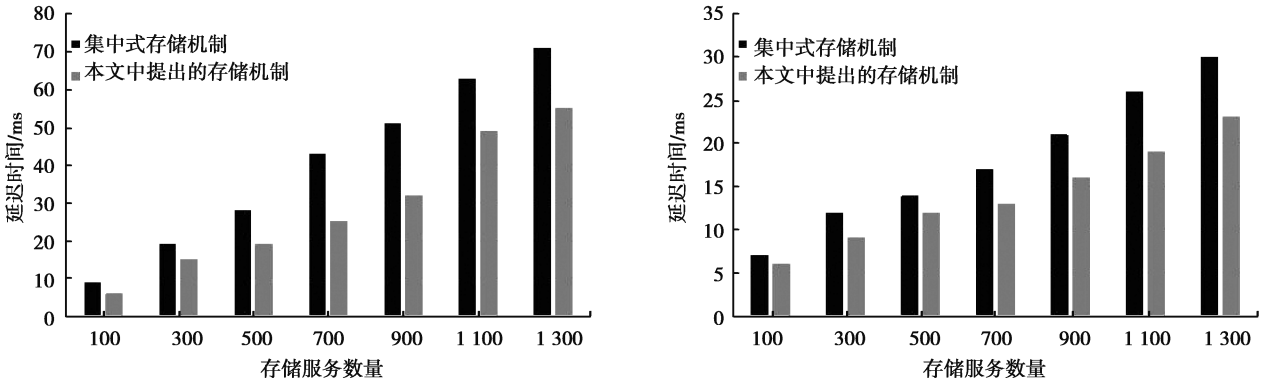
数据加密模块采用密钥长度为 192 bit 的非对称加密算法 AES 完成数据加密，从而实现电力营销数据的安全存储机制。AES 加密密钥由智能电力设备或用户口令通过 Hash 方式生成。在数据解密时，必须获取密文对应的密钥来对密文进行解密。上链数据哈希提取模块主要采用当前主流的 Hash 函数 SHA-2/SHA-3，哈希算法将任意长度的二进制值映射为固定长度的二进制值，Hash 函数已经广泛应用对当前生活的各个领域。在通信过程中使用 TLS 协议栈防止恶意用户非法截取通信数据。

3.3　实验仿真

这里将详细讨论传统的集中式存储机制与所提出基于区块链的存储机制之间的性能对比，给出基于区块链的电力营销数据存储架构的评估结果。主要使用延迟、吞吐量和系统响应时间作为性能指标来具体评

估所提出的存储方案。首先使用4台主机搭建基于区块链的多级加密电力数据分布式存储系统,其中每台主机的配置均为32 GB RAM和Intel i5处理器。同时,智能电力设备由笔记本电脑模拟提供,笔记本电脑是使用区块链技术以分布式架构的方式链接而成的实验节点,笔记本电脑配置为16 GB RAM和Intel i7处理器。

使用传统集中式存储机制与提出的基于区块链的多级加密分布式存储机制延迟情况对比如图6所示,图6(a)为延迟与接入设备数量之间的关系,图6(b)为延迟与存储服务数量之间的关系。由图可知,当随着连接的设备数量与存储服务数量增加时,存储的延迟会增加,但是所提出的基于区块链的多级加密分布式存储机制延迟情况均要优于传统的集中式存储。



(a)设备数量增加时延迟时间对比 (b)存储服务数量增长时延迟时间对比

图6 两种存储机制的延迟对比

Fig. 6 Delay comparison of two storage mechanisms

存储系统的吞吐量为单位时间内存储信息的量,是衡量存储系统的性能标准之一,将传统的集中式存储机制与基于区块链的存储机制进行对比,使用电力营销数据作为存储服务,结果如图7所示。与传统的存储机制相比,所提出的存储方案具有较高的吞吐量,实现了存储效率的改进。图8为文件大小与系统响应时间的对比,结果表明,在小文件存储过程中响应速率相差不大,但是在大文件存储时所提出的存储方案具有更快的响应速度,满足电力大数据的存储效率需求。

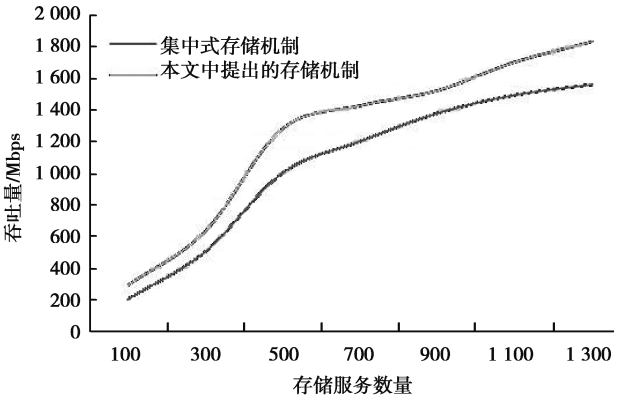


图7 系统吞吐量变化对比

Fig. 7 Comparison of system throughput changes

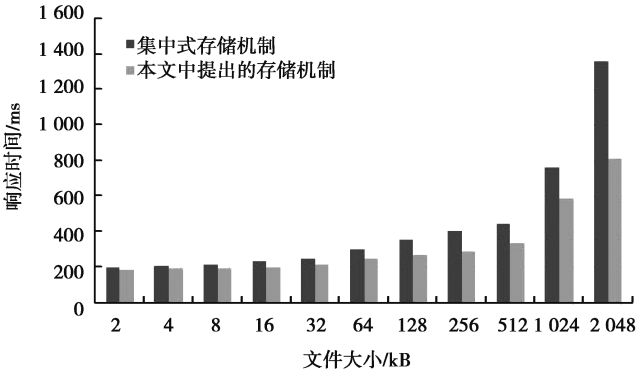


图8 响应时间与文件大小关系对比

Fig. 8 Comparison of response time and file size

4 数据安全性分析

目前针对数据的安全防护技术有加密和脱敏2种方法,数据加密是通过使用加密算法对原始数据进行加密,以密文的形式进行数据存储,适用于数据安全存储,而数据脱敏是通过使用脱敏算法对原始数据信息

进行变形，适用于数据安全保护。通过使用 AES 与 RSA 加密算法对原始的电力营销数据进行加密，使数据以密文的形式进行传输与存储，更有效地对电力营销数据进行保护。

实验表明所提出的基于区块链的多级加密电力营销数据存储机制能够提供存储稳定性高、更安全、可靠的存储性能，但是在该系统中由于采用分布式数据库存储电力营销数据，需要考虑数据完整性。数据完整性是指存储提供方严格按照用户的要求存储数据，存储的文件不能丢失，使用时用户的文件没有被伪造或篡改的情况发生[17]。这里通过采用抽样的策略对存储在分布式数据库中的数据文件进行完整性分析。通常数据完整性证明有 Setup 和 Challenge 两个阶段，具体流程如下。

Setup 阶段：

1）随机选取一个范德蒙矩阵 $\boldsymbol{A}$ 作为散布矩阵，经过一系列初等变化后，$\boldsymbol{A}=[I/P]$，生成挑战密钥 k_{chal} 和置换密钥 K_{PRP}。

2）生成编码文件

$$\boldsymbol{G}=\boldsymbol{F}\cdot\boldsymbol{A}=\{G^1,\cdots,G^m,G^{m+1},\cdots,G^n\},\tag{1}$$

式中：$\boldsymbol{G}^m=(g_1^m,g_2^m,L,g_i^m)^{\mathrm{T}}$，$g$ 为 $\boldsymbol{G}$ 的生成元；$\boldsymbol{F}$ 为随机函数；$\{G^{m+1},\cdots,G^n\}$为冗余信息。

3）生成验证元数据：为每个服务器 $j\in[1,2,\cdots,n]$，预选生成 t 个验证元数据，每个标签 i 由式(2)计算得来：

$$v_i^j=\sum_{q=1}^{r}\alpha_i^q\times G^j[f_{ki}(q)],1\leqslant i\leqslant t,\tag{2}$$

式中 $\alpha_i=f_{k\text{chal}}(i)$，$k_{\text{prp}}^i\leftarrow K_{\text{PRP}}$。

4）屏蔽冗余信息$\{G^{m+1},\cdots,G^n\}$：$g_1^j\leftarrow g_i^j+f_{kj}(s_{ij})$，$1\leqslant i\leqslant t$。

5）将 G 存入分布式服务器，本地保存和认证元数据$\{v_i^j\}1\leqslant j\leqslant n$，$1\leqslant i\leqslant t$ 和 P。

Challenge 阶段：

1）验证者重新生成 $\alpha_i=f_{k\text{chal}}(i)$，$k_{\text{prp}}^i\leftarrow K_{\text{PRP}}$，并将其发送给分布式服务器；

2）服务器计算响应集合：$\{R_i^j=\sum_{q=1}^{r}\alpha_i^q\times G^j[f_{k_{\text{prp}}^i}(q)],1\leqslant j\leqslant n\}$，并将其返回给验证者；

3）接收到响应集合后，去除冗余信息的屏蔽值

$$R^j\leftarrow R^j-\sum_{q=1}^{r}f_{kj}(s_{I_q,j})\cdot a_i^q,I_q=f_{k_{prp}^i}(q)。\tag{3}$$

根据本地存储的和 P，判断式(4)是否成立：

$$(R_i^1,\cdots,R_i^m)\cdot P=(R_i^{m+1},\cdots,R_i^n),\tag{4}$$

如果等式成立则文件是完整未损坏的。

4）不成立，继续比较

$$R_i^j=v_i^j,$$

如果仍不相等表明服务器 j 上的文件已损坏。

5　结　语

针对传统的集中式数据存储模式无法满足电力业务数据存储所要求的安全性、低延迟和扩展性问题，提出了一种基于区块链的多级加密电力数据存储架构。该存储机制具有存储稳定性高、安全可靠、数据可追溯、可审计及可扩展等诸多优势，同时提出的多级加密机制支持电力数据上链、电力数据传输等流程的逐级加密及验证，使得电力数据存储与数据访问的安全性得到进一步的保证。通过实验证明，相比于传统的集中式电力数据存储机制，所提出的电力数据存储机制延迟更低，吞吐量更高和响应时间更低能够满足电力营销数据存储的稳定性和安全性要求。

参考文献：

[1] 范冬梅. 电力用户用电信息采集系统数据分析与处理技术[J]. 工程技术：全文版，2016(8)：199.
Fan D M. Data analysis and processing technology of power consumer information collection system[J]. Engineering Technology: Full Text Edition, 2016(8): 199. (in Chinese)

[2] 楚文师，李进. 电力系统信息管理自动化的研究[J]. 工程技术：文摘版，2016(4)：163.
Chu W S, Li J. Research on automation of power system information management[J]. Engineering Technology: Abstracts Edition, 2016(4): 163. (in Chinese)

[3] 李常国. 基于云平台的电力行业数据处理[D]. 北京：北京邮电大学，2017.
Li C G. Electric power data processing based on the cloud computing platform[D]. Beijing: Beijing University of Posts and Telecommunications, 2017. (in Chinese)

[4] 宋亚奇，刘树仁，朱永利，等. 电力设备状态高速采样数据的云存储技术研究[J]. 电力自动化设备，2013，33(10)：150-156.
Song Y Q, Liu S R, Zhu Y L, et al. Cloud storage of power equipment state data sampled with high speed[J]. Electric Power Automation Equipment, 2013, 33(10): 150-156. (in Chinese)

[5] 颜拥，周自强，涂莹，等. 基于区块链的电力数据保全应用研究[J]. 浙江电力，2019，38(7)：63-69.
Yan Y, Zhou Z Q, Tu Y, et al. Research on application of electric power data preservation based on blockchain[J]. Zhejiang Electric Power, 2019, 38(7): 63-69. (in Chinese)

[6] Urquhart A. The inefficiency of Bitcoin[J]. Economics Letters, 2016, 148: 80-82.

[7] Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084-2123.

[8] Yang Z, Yang K, Lei L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 1495-1505.

[9] Bocek T, Rodrigues B B, Strasser T, et al. Blockchains everywhere - a use-case of blockchains in the pharma supply-chain[C]// 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), May 8-12, 2017, Lisbon, Portugal. IEEE, 2017: 772-777.

[10] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[M]// Advances in cryptology - ASIACRYPT 2003. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 452-473.

[11] Zheng Z B, Xie S A, Dai H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]// 2017 IEEE International Congress on Big Data (BigData Congress), June 25-30, 2017, Honolulu, HI, USA. IEEE, 2017: 557-564.

[12] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481-494.
Yuan Y, Wang F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494. (in Chinese)

[13] Wright C S. Bitcoin: a peer-to-peer electronic cash system[J]. SSRN Electronic Journal, 2008: 1-9.

[14] Andoni M, Robu V, Flynn D, et al. Blockchain technology in the energy sector: a systematic review of challenges and opportunities[J]. Renewable and Sustainable Energy Reviews, 2019, 100: 143-174.

[15] 邵奇峰，金澈清，张召，等. 区块链技术：架构及进展[J]. 计算机学报，2018，41(5)：969-988.
Shao Q F, Jin C Q, Zhang Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988. (in Chinese)

[16] 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[J]. 计算机科学，2018，45(12)：12-18.
Wang Q G, He P, Nie T Z, et al. Survey of data storage and query techniques in blockchain systems[J]. Computer Science, 2018, 45(12): 12-18. (in Chinese)

[17] 冯朝胜，秦志光，袁丁. 云数据安全存储技术[J]. 计算机学报，2015，38(1)：150-163.
Feng C S, Qin Z G, Yuan D. Techniques of secure storage for cloud data[J]. Chinese Journal of Computers, 2015, 38(1): 150-163. (in Chinese)

（编辑 张 苹）