·区块链技术专题·　　文章编号：1000-3428(2019)11-0009-07　　文献标志码：A　　中图分类号：TP309.2

基于区块链的电力数据容灾备份方案

劳卫伦[1]，王柏勇[1]，张　锐[2]，王加贝[2]

（1. 广州供电局有限公司，广州 510620；2. 中国科学院信息工程研究所 信息安全国家重点实验室，北京 100093）

摘　要： 对于种类众多、数量庞大并且安全性要求较高的电力数据，数据容灾备份应具有可扩展性和隐私保护性。为此，基于区块链不可篡改、去中心化和可追溯的特点，将其与 AONT 和门限秘密分享等密码学技术相结合，提出一种新的电力数据容灾备份方案，并在开源区块链平台以太坊上进行原型系统实现。分析与实验结果表明，该方案能够保证备份数据的一致性、不可篡改性和机密性，并且可扩展性强，可在减少基础设施建设开销的同时规避单点失效的风险。

关键词： 区块链；电力数据；容灾备份；数据安全保护；门限秘密分享；AONT 技术

开放科学(资源服务)标志码(OSID)：

中文引用格式： 劳卫伦，王柏勇，张锐，等. 基于区块链的电力数据容灾备份方案[J]. 计算机工程，2019，45(11)：9-15.

英文引用格式： LAO Weilun，WANG Baiyong，ZHANG Rui，et al. Disaster tolerance and backup scheme of power data based on blockchain[J]. Computer Engineering，2019，45(11)：9-15.

Disaster Tolerance and Backup Scheme of Power Data Based on Blockchain

LAO Weilun[1]，WANG Baiyong[1]，ZHANG Rui[2]，WANG Jiabei[2]

（1. Guangzhou Power Supply Bureau Co.，Ltd.，Guangzhou 510620，China；
2. State Key Laboratory of Information Security，Institute of Information Engineering，Chinese Academy of Sciences，Beijing 100093，China）

【Abstract】 Due to the large volume，various types and high security requirements of power data，its disaster tolerance and backup scheme should provide scalability and privacy protection. Blockchain is tamper-resistant，decentralized and traceable，which caters to such requirements. Therefore，this paper proposes a new blockchain-based disaster recovery and backup scheme of power data，integrating AONT，threshold secret sharing and other cryptographic technologies. The prototype system is implemented on an open-source blockchain platform，Ethereum. Experimental and Analysis results show that the scheme can ensure the consistency，tamper resistance and confidentiality of backup data. It is highly scalable，reducing the construction cost of infrastructure as well as the risk of single point of failure.

【Key words】 blockchain；power data；disaster tolerance and backup；data security protection；threshold secret sharing；All or Nothing Transform(AONT) technology

DOI： 10.19678/j.issn.1000-3428.0053925

0　概述

在信息技术迅速发展的大背景下，能源产业尤其是电力产业与信息技术的结合越来越紧密，随着电网信息化建设的不断发展，信息系统已经成为开展电网业务的关键组成部分。

电力产业是国家支柱型产业，其供电水平及安全状况直接关系到企业的发展和人民的日常生活。电力业务繁多复杂，其数据种类众多、数据量庞大，并且对数据的安全性要求较高。在各个业务环节的开展过程中，系统需要不断地与历史数据进行交互，同时产生大量的新数据并将其存储起来以便再次使用。这些数据的可靠存储是保证系统稳定运行的基础。

然而在系统实际运转过程中，任何断电、系统故障和人为不当操作等都有可能造成关键数据的丢

基金项目： 国家自然科学基金(61772520，61802392)。

作者简介： 劳卫伦(1979—)，男，高级工程师、博士，主研方向为区块链技术、大数据分析、信息安全；王柏勇，博士；张　锐，研究员；王加贝，博士研究生。

收稿日期： 2019-02-16　　**修回日期：** 2019-05-07　　**E-mail：** wangjiabei@iie.ac.cn

失,进而导致业务停滞,甚至给企业带来难以预计的经济损失,同时给人们的生活造成诸多不便,各种自然灾害(如火宅、水灾、地震等)和人为灾难(如误操作、病毒等)也可能造成重要数据丢失进而影响系统的正常运行。

为保证电力产业信息系统在遭遇灾害时仍然能够正常运行并迅速恢复业务连续性,本文结合区块链和密码学相关技术,提出一种新的电力数据容灾备份方案,以提升系统效率和可靠性。

1 相关研究

数据容灾技术通过创建多个数据备份,在系统遭遇灾难时提供可快速读取、恢复现有系统的数据对象。数据容灾备份应保障系统中业务数据的一致性、可靠性和完整性。进一步地,对于数据种类众多、数据量庞大且具有高安全性要求的电力数据,数据容灾备份应具有可扩展性并且包含数据隐私保护机制。

1.1 传统数据容灾备份技术

传统数据容灾备份技术通常依赖于中心化的技术,即分别设立主数据中心和备份数据中心,如图 1 所示。主数据中心存储业务数据,并将其中数据实时或分批次复制到本地备份系统和备份数据中心。备份数据中心通常在异地建立和维护[1-2],通过地理上的分散性或增加冗余备份数量,分散数据损坏风险,提升数据及相关业务对灾害的抵御能力。当主数据中心数据出现故障时,根据实情从本地备份系统或备份数据中心恢复数据,或者将数据网络切换至备份数据中心,从而最大限度地减少损失,保证系统的正常运行。

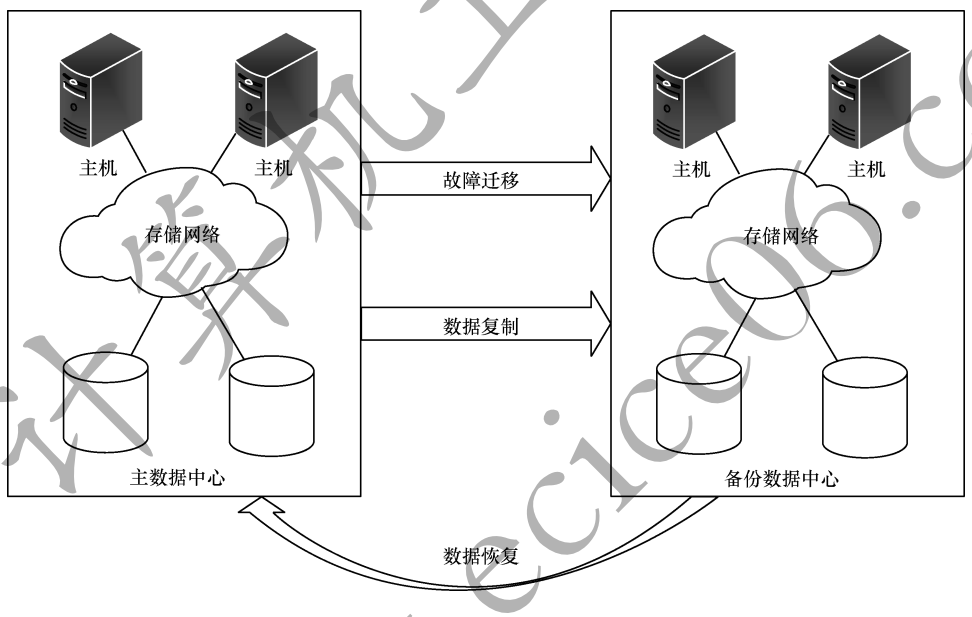

图 1 传统数据容灾备份框架

传统数据容灾备份技术依赖网络进行实时备份和数据恢复,存储区域网络(Storage Area Network,SAN)[3]、基于 IP 网络的存储区域网络(IP-SAN)[4]等网络存储技术的提出和升级是传统数据容灾备份技术得以发展的有力技术支撑,涌现了包括 EMC 公司的远程容灾备份软件 SRDF、IBM 公司自主设计的 GDPS(Geograpgically Dispersed Parallel Sysplex)等在内的一系列灾备技术。然而传统数据容灾备份技术存在以下不足:

1)主要依赖于备份数据中心,一旦备份数据中心出现故障,数据将无法有效恢复。

2)为保证与主数据中心的地理隔离,备份数据中心建设时需要企业投入大量的硬件资源,当数据规模不断扩大时将大幅增加企业的数据灾备成本。

3)增加数据冗余备份数量的方式可能会造成大量资源浪费。

4)无法有效验证数据的一致性和完整性,备份方式缺乏灵活性。

1.2 基于云存储的数据容灾备份技术

云计算的出现给企业提供了方便易用的存储和计算服务,能有效节省企业运营成本,整合资源,在一定程度上避免重复计算和存储,并能实现跨平台服务,具有灵活性。随着云计算在各行各业的深度应用和发展,越来越多的企业和政府使用基于云存储的数据容灾备份解决方案,有效降低了数据容灾系统的建设、维护难度及成本。基于云存储的数据容灾备份框架如图 2 所示。

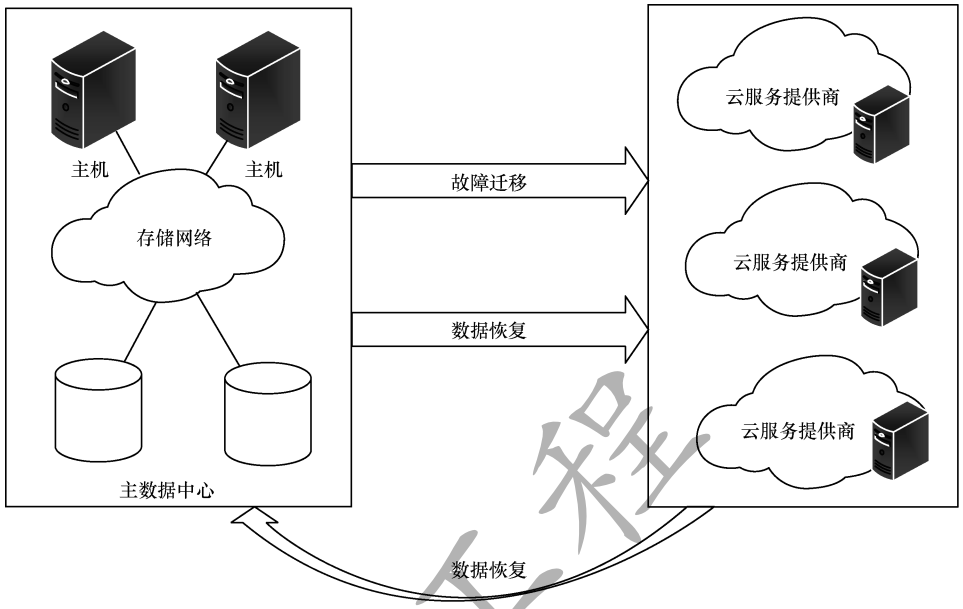

图 2　基于云存储的数据容灾备份框架

文献[5]提出了容灾即服务的概念,尝试使用云计算技术为个人或企业提供数据容灾备份服务,并实际对比测试了 RUBiS 系统在自建数据灾备数据中心和使用云存储服务 2 种模式下的容灾成本。通过对比发现,使用云存储服务实现数据容灾备份的方式在降低成本上具有显著优势。此外,云存储弹性扩展的特点使得这一技术能更好地应对数据规模的扩大。文献[6]提出一种基于管道同步的云备份方法,与传统数据容灾备份技术相比,该方法能保证备份数据的一致性,同时减少数据同步时的响应时间。此后,为进一步提升基于云存储数据容灾备份的可用性和效率,研究者针对不同应用场景开展了一系列研究,例如:文献[7]建立了基于教育云平台 Ren[8]的点对点企业数据备份模型;文献[9]针对物联网系统云存储中多用户访问的场景提出一种文件备份方法,以达到最小化用户访问开销的目的。

虽然基于云存储的数据容灾备份技术在降低容灾成本和提升数据一致性、系统扩展灵活性等方面具有优势,但这种利用云存储提供第三方数据灾备的技术,仍存在以下风险和不足:

1)通常情况下不能保证云服务提供商完全可靠,若企业或政府将关键数据备份至云服务器中,云服务器可能会对数据进行篡改或窥探,使数据隐私性受到严重威胁,不能保证数据的一致性。

2)依赖一个中心化的第三方,一旦云平台出现故障或彻底崩溃,将损失大量数据,威胁到企业数据的安全性和存储的可靠性。如亚马逊提供的简单存储服务,于 2009 年 2 月和 7 月发生过 2 次中断,使完全依赖于该存储服务的系统陷入瘫痪,而此类现象在主流的云服务提供商微软、Google、Rackspace 等也有出现,给云服务提供商以及相关用户都带来了巨大的损失。为降低单点失效的风险,有研究者提出使用多个云平台协同存储的模式(富云模式)备份数据,实现数据容灾,但这样的方式涉及平台众多,难于管理,如何解决跨平台之间数据统一和高效调度的问题,以及保证数据可靠性和完整性都具有极大的挑战。

1.3　基于区块链的数据容灾备份技术

区块链技术以其不可篡改、去中心化、可追溯等特点为数据容灾备份的设计拓展了新思路。区块链本身具有多点冗余备份的功能,基于区块链的分布式文件系统 IPFS(Inter Planetary File System)[10]就结合纠错码来提供数据冗余备份服务。国内区块链技术服务商众享比特也提出了 ChainSQL 技术,同时针对异地多活容灾和数据多点备份的场景分别推出了众享多活数据库中间件(AlAisc)和众享数据库灾备中间件(AlBisc)2 个产品。然而,对基于区块链的数据容灾备份技术,现有的相关研究仍处于探索阶段,也没有综合考虑企业的实际需求。因此,针对电力产业的场景定制契合电力数据特点的新型数据容灾备份技术具有重要意义。

2　相关研究

2.1　区块链

区块链技术起源于比特币[11],从数据角度看,区块链[12-13]本质上是一种分布式数据库。通过共识

机制,区块链网络中的节点共同维护一个按时间先后记录、不可篡改的账本。区块链经发展现已成为一种融合分布式数据存储、点对点传输、共识机制、加密算法等多种计算机技术的新型应用模式。

在区块链系统中,一段时间内产生的所有(交易)数据会被打包成一个区块,所有的区块会按照时间顺序依次排列,形成区块链。系统中的所有参与者(即节点)均拥有相同的区块链备份,并且任何节点都无法对其进行修改。在每一个区块被写入区块链之前,系统中的所有节点都需要共同运行共识算法[14-16],并根据共识结果决定该区块的写入权限属于哪个代表节点。此外,其他节点还需要对代表节点提交的新区块进行有效性及正确性验证。当且仅当超过一定比例的节点都认证通过之后,该区块才可真正被添加到区块链上,从而实现多实体间的信息共享和一致决策,确保交易信息的不可篡改和可追溯。

一般的区块链具有如图 3 所示的结构,为高效校验整个数据的完整性,区块链使用 Merkle 树[17],从而实现使用部分哈希值就能校验整个数据的完整性。本文方案将每一个备份的数据块视为一笔交易记录在区块链中,以保证备份数据的完整性。

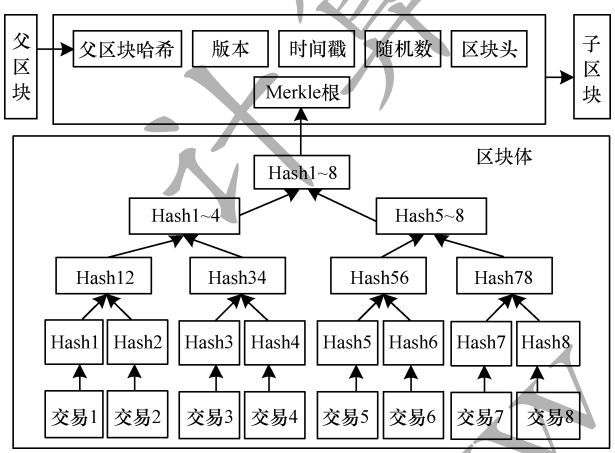

图 3 区块链的一般结构

2.2 AONT 技术

AONT(All or Nothing Transform)作为一种加密模式,通常与对称加密算法结合以实现强不可区分的数据加密机制。假设一种对称加密算法将明文序列 $f_1,f_2,\cdots,f_s$ 转换为密文序列 $c_1,c_2,\cdots,c_t$,强不可区分性要求在解密所有密文消息之前必须确定任何一个明文消息在计算上都是不可行的。

本文借鉴基于包转换的 ANOT 方案[18],其中包括如下算法:

算法 1 包转换算法

输入 固定公开密钥 K^*,原始消息序列 $f_1,f_2,\cdots,f_i,\cdots,f_s$

输出 伪消息序列 $\overline{f_1},\overline{f_2},\cdots,\overline{f_i},\cdots,\overline{f_{s'}}$

随机选择一个密钥 K^r

For $i\in[1,s]$ do

$\overline{f_i}=f_i\oplus Enc_{K^r}(i)$

$h_i=Enc_{K^*}(\overline{f_i}\oplus i)$

End For

令 $s'=s+1$

$\overline{f_{s'}}=K^r\oplus h_1\oplus h_2\oplus\cdots\oplus h_s$

算法 2 逆包转换算法

输入 固定公开密钥 K^*,伪消息序列 $\overline{f_1},\overline{f_2},\cdots,\overline{f_i},\cdots,\overline{f_{s'}}$

输出 原始消息序列 $f_1,f_2,\cdots,f_i,\cdots,f_s$

For $i\in[1,s]$ do

$h_i=Enc_{K^*}(\overline{f_i}\oplus i)$

End For

$K^r=\overline{f_{s'}}\oplus h_1\oplus h_2\oplus\cdots\oplus h_s$

For $i\in[1,s]$ do

$f_i=\overline{f_i}\oplus Enc_{K^r}(i)$

End For

上述算法中 *Enc* 表示对称加密算法。在本文方案中,最后一个伪随机消息 $\overline{f_{s'}}$ 包含了随机密钥和之前所有伪随机消息序列,若缺少任何一个伪消息块,则要确认任何一个原始消息都是不可行的。

2.3 门限秘密分享

门限秘密分享指将一个秘密划分为多份交由多个用户保管,只有获得达到一定阈值的秘密分量才能恢复原始秘密。本文使用门限秘密分享方案,一方面分散了节点的权利,可保证备份数据机密性,另一方面使得方案能够保证冗余备份的可靠性,并有效节省节点的存储开销。

本文使用传统的(q,n)门限秘密分享方案,即秘密在 n 个用户之间分享,任意 q 个用户持有的秘密分量可以恢复原始秘密。具体方法如下:将原始秘密分成 C_n^{q-1} 份,每个用户持有 C_{n-1}^{q-1} 份秘密分量,然后利用组合数学的方法为每个用户分配秘密。例如在(3,5)门限方案中,将原始秘密拆分为 $C_5^2=10$ 份,每个用户持有 $C_4^2=6$ 个秘密分量,设用户序列为 $U_1,U_2,\cdots,U_5$,拆分后的秘密编号为 $f_0,f_1,\cdots,f_9$,则可构造如表 1 所示的分配表,为用户每一个5 选3 组合分配一个秘密分量。

表 1 (3,5)门限方案秘密分配表

用户	秘密分量
U_1	f_0,f_1,f_2,f_3,f_4,f_5
U_2	f_0,f_1,f_2,f_6,f_7,f_8
U_3	f_0,f_3,f_4,f_6,f_7,f_9
U_4	f_1,f_3,f_5,f_6,f_8,f_9
U_5	f_2,f_4,f_5,f_7,f_8,f_9

3　系统模型

在本文方案中,通过对电力企业的业务数据进行一系列处理,将其备份存储至区块链中。当电力企业本地存储的业务数据因自然或人为灾难被损坏时,可通过区块链中的数据备份实现快速校验和数据恢复。一个基于区块链技术的电力数据容灾备份系统包括原始数据拥有者(企业)、可信数据处理机构以及区块链网络,其中区块链网络中包括多个参与共识的节点服务器,系统模型如图 4 所示。

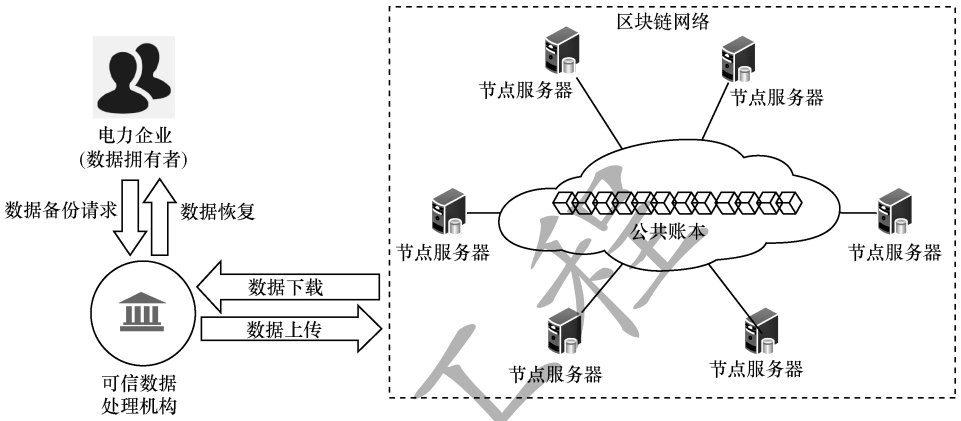

图 4　基于区块链的电力数据容灾备份模型

假设区块链网络中有 n 个存储能力相同的存储节点,并且至多有 t 个节点可能出现故障,有 m 个待备份的原始数据 $F^1,F^2,\cdots,F^j,\cdots,F^m$,根据最优的划分方法,将每个待备份的原始数据 F^j 分为 s 个不同的数据块 $F_1^j,F_2^j,\cdots,F_l^j,\cdots,F_s^j$。第 i 个节点的数据存储形式如表 2 所示,其中 $F_{\text{node-}i}^j$ 表示节点 i 存储的第 j 个原始数据的数据块集合。

表 2　第 i 个节点的数据存储形式

安全哈希函数	数据块集合
$\text{Hash}(F^1)$	$F_{\text{node-}i}^1$
$\text{Hash}(F^2)$	$F_{\text{node-}i}^2$
⋮	⋮
$\text{Hash}(F^j)$	$F_{\text{node-}i}^j$
⋮	⋮
$\text{Hash}(F^m)$	$F_{\text{node-}i}^m$

本文建立基于区块链技术的电力数据容灾备份模型,以保证即使区块链网络中至多有 t 个节点出现故障,剩余节点都可以恢复一份完整的数据备份,实现最优化的节点数据存储,并且保证数据的一致性、机密性和不可篡改性。

4　电力数据容灾备份方案

4.1　设计思想

对于电力企业产生的业务数据,可信数据处理机构首先对数据进行预处理,包括去除噪声或错误数据、类型转换等(本文不关注原始业务数据的预处理)。然后对原始数据进行分块,并利用 AONT 将原始数据块序列转换为强不可区分的伪消息数据块序列。可选地,对于隐私数据,系统可对伪消息数据块进行加密。在此基础上,基于门限秘密共享方法将数据块分配到各个区块链节点中备份存储。为进一步提升查询和备份恢复的效率,区块链中的每一个节点维护一个表格(如表 1 所示),并使用文献[19]提出的布谷鸟哈希算法解决哈希冲突问题,从而以较少的计算开销换取较大的空间。当电力企业需要下载某个备份数据时,向可信数据处理机构提交申请,机构下载任意 $n-t$ 个节点中该备份数据哈希对应的数据块集合,经过解密和 ANOT 逆转换,最终合并成完整的数据返回给电力企业。

4.2　具体算法

基于系统模型假设,本文方案分为数据上传和数据下载 2 个阶段。

4.2.1　数据上传

假设需要上传备份的一个原始数据为 F^j,区块链网络中有 n 个存储能力相同的存储节点,且至多有 t 个节点可能出现故障,则可信数据处理机构首先将 F^j 分为 $s-1=\mathrm{C}_n^{t-1}-1$ 份数据块,即 $F_1^j,F_2^j,\cdots,F_l^j,\cdots,F_{s-1}^j$,然后利用包转换 ANOT 算法将该序列转换为强不可区分序列 $\overline{F_1^j},\overline{F_2^j},\cdots,\overline{F_l^j},\cdots,\overline{F_s^j}$,根据电力数据的隐私保护需求,可选择对伪消息数据块进行加密,得到 $\overline{C_1^j},\overline{C_2^j},\cdots,\overline{C_l^j},\cdots,\overline{C_s^j}$。在此基础上,使用 2.3 节的门限秘密分享方案,将数据块 $\overline{C_1^j},\overline{C_2^j},\cdots,\overline{C_l^j},\cdots,\overline{C_s^j}$ 分享存储至区块链中的各个节点,每个用户持有该数据的 C_{n-1}^{t-1} 份秘密分量。

本文方案通过安全哈希函数重新构造包转换 ANOT 算法,以提高算法效率。假设 PRF 为伪随机函数,数据上传算法描述如下:

算法 3 数据上传算法

输入 待上传备份的原始数据 F^j,包含 n 个存储节点的集合 $Node=\{\text{node-1},\text{node-2},\cdots,\text{node-}n\}$,至多允许出现故障的节点数 t

输出 秘密分配表 $Table_{F^j}$

1. 将 F^j 分为 $s-1=C_{n-1}^{t-1}$ 份数据块,即 $F_1^j,F_2^j,\cdots,F_l^j,\cdots,F_{s-1}^j$
2. 选择一个随机密钥 K^r
3. For $i\in[1,s-1]$ do
4. $\overline{F_i^j}=F_i^j\oplus f_{K^r}(i)$
5. $h_i=\text{Hash}(\overline{F_i^j})$
6. End For
7. $\overline{F_s^j}=K^r\oplus h_1\oplus h_2\oplus\cdots\oplus h_{s-1}$
8. 随机选择一个对称加密密钥 K
9. For $i\in[1,s]$ do
10. $\overline{C_i^j}=\text{Enc}_K(\overline{F_i^j})$
11. End For
12. 令 $\overline{C^j}=\{\overline{C_1^j},\overline{C_2^j},\cdots,\overline{C_l^j},\cdots,\overline{C_s^j}\}$
13. 根据 2.3 节中的门限秘密分享方案,构造 $\overline{C^j}$ 的秘密分配表 Table_{F^j}
14. 返回密钥 K、Table_{F^j}

在上述算法中,密钥 K 被保存到可信数据处理机构,可信数据机构根据 $Table_{Fj}$ 分配给节点相应的秘密分量。每个节点在本地维护一个如表 2 所示的表,由于电力数据量庞大的特点,为解决哈希冲突,可使用布谷鸟哈希算法。进一步地,为提高搜索效率,可使用完美哈希算法。

4.2.2 数据下载

当电力企业需要下载数据时,向可信数据处理机构提交申请,可从区块链中任意 $n-t$ 个节点中下载该备份数据哈希对应的数据块集合 $F_{\text{node-}i}^j$,经过解密和 ANOT 逆转换,还原原始备份数据。数据下载算法描述如下:

算法 4 数据下载算法

输入 待下载的数据哈希 $\text{Hash}(F^j)$,任意 $n-t$ 个节点集合 $node^*\text{-}i(i\in[1,n-t])$

输出 原始数据 F^j

1. 从这 n-t 个节点的表格中,下载对应的数据块 $F_{\text{node}^*\text{-}i}^j(i\in[1,\text{n-t}])$,合并得到 $\overline{C_1^j},\overline{C_2^j},\cdots,\overline{C_l^j},\cdots,\overline{C_s^j}$
2. For $i\in[1,s]$ do
3. $\overline{F_i^j}=\text{Dec}_K(\overline{C_i^j})$
4. End For
5. For $i\in[1,s-1]$ do
6. $h_i=\text{Hash}(\overline{F_i^j})$
7. End For
8. 计算 $K^r=\overline{F_s^j}\oplus h_1\oplus h_2\oplus\cdots\oplus h_{s-1}$
9. For $i\in[1,s-1]$ do
10. $F_i^j=\overline{F_i^j}\oplus f_{K^r}(i)$
11. End For
12. 返回原始数据 $F^j=\{F_1^j,F_2^j,\cdots,F_l^j,\cdots,F_{s-1}^j\}$

5 原型系统实现

本文方案具有以下特点:1)即使区块链网络中至多有 t 个节点出现故障,剩余节点都可以恢复一份完整的数据备份,保证了数据备份的可靠性;2)通过使用 AONT 方案结合对称加密算法生成相应的密文数据,保证了电力数据的机密性;3)门限秘密分享方案的使用,能在实现可靠数据备份的同时,有效节省节点存储空间;4)将数据分散备份至区块链中的节点进行存储,利用区块链本身的性质保证了备份数据的一致性、不可篡改性和完整性。

为进一步验证本文方案的效率,依照图 4 所示的系统模型,本文在开源区块链平台以太坊上实现原型系统,主要包括数据上链、数据下载 2 个算法的实现。实验环境为 Ubuntu 16.04 操作系统 gcc 5.4.0 编译器 Intel(R) Core(TM) i7-4790 CPU@3.60 GHz。在算法的实例化选择上,伪随机函数 PRF 选择 HMAC-SHA256,Hash 函数选择 cshake128,对称加密函数选择 AES,假设区块链网络中存储节点数为 12,原始数据大小为 10 MB。如图 4所示,整个备份过程中的通信开销主要包括可信数据处理机构和区块链网络之间的数据传输,以及区块链网络内部账本与节点服务器之间的数据传输,这两部分均与最大出现故障的节点数 t 有关,同时 t 也影响了数据上传与数据下载算法的运行时间,因此,本文对 t 与通信开销和数据下载算法运行时间的关系进行分析。当区块链网络中最多出现 1 个 ~ 10 个故障节点时,算法运行 1 000 次数据上传和数据下载的平均运行时间如图 5 和图 6 所示。

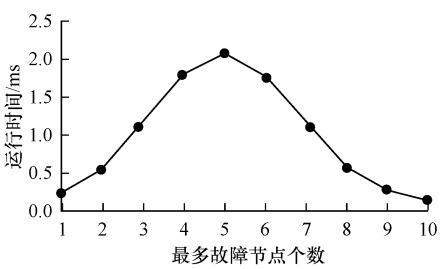

图 5 数据上传运行时间

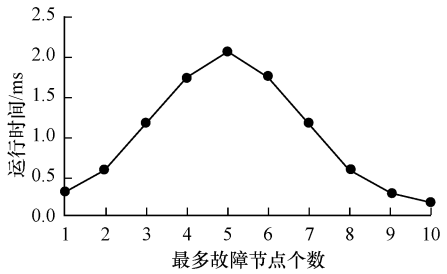

图 6　数据下载运行时间

数据上传和数据下载算法的运行时间与原始数据被分成的块数相关,当$t=(n-1)/2$ 时算法最耗时,实验结果与此相符。对 t 与通信开销的关系分析如下:假设原始数据的长度为 M,任意 $n-t$ 个用户持有的秘密分量可以恢复原始秘密,将原始秘密分成 C_n^{n-t+1} 份,每个用户持有 C_{n-1}^{n-t+1} 份秘密分量,因此,可信数据处理机构和区块链网络之间的数据传输量为 $n\cdot C_{n-1}^{n-t+1}\cdot\frac{M}{C_n^{n-t+1}}$,可化简为 $M(t+1)$,即当允许最多出现故障的节点数越大时,通信开销越大。企业可以根据实际情况调整合适的参数,从而优化备份效率,迅速恢复原始数据。

6　结束语

本文结合区块链和密码学技术,设计一个电力数据容灾备份方案,以保证备份数据的一致性、不可篡改性和机密性。相较于传统的容灾备份技术和基于云存储的容灾备份技术,本文方案能够减少基础设施建设的开销,规避单点失效的风险,增强可扩展性。下一步拟将该方案应用于实际的电力系统,并结合具体业务需求加以优化。

参考文献

[1] 顾启超,刘晓洁,李涛,等. 一种多点容灾系统的设计与实现[J]. 计算机应用研究,2008,25(8):2427-2429.

[2] 陈鹏,杨频,赵奎,等. 远程容灾系统的设计与实现[J]. 计算机工程与设计,2011,32(10):3247-3250.

[3] HOTS S, METER R V, FINN G. Internet protocols for network attached peripherals[C]//Proceedings of the 6th IEEE/NASA Conference on Mass Storage Systems and Technologies. Washington D. C., USA: IEEE Press, 1998:1-15.

[4] WATSON R W. High performance storage system scalability: architecture, implementation and experience[C]//Proceedings of IEEE Conference on Mass Storage Systems and Technologies. Washington D. C., USA: IEEE Press, 2005:145-159.

[5] WOOD T, CECCHETT E, RAMAKRISHNAN K K. Disaster recovery as a cloud service: economic benefits and deployment challenges[C]//Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing. Boston, USA: USENIX, 2010:8-15.

[6] WOOD T, LAGAR-CAVILLA H A, RAMAKRISHNAN K K. PipeCloud: using causality to overcome speed-of-light delays in cloud-based disaster recovery[C]// Proceedings of the 2nd ACM Symposium on Cloud Computing. New York, USA: ACM Press, 2011.

[7] VRABLE M, SAVAGE S, VOELKER G M. Cumulus: filesystem backup to the cloud[J]. ACM Transactions on Storage, 2009, 5(4):1-28.

[8] KHAN J I, TAHBOUB O Y. Peer-to-peer enterprise data backup over a Ren cloud[C]//Proceedings of International Conference on Information Technology: New Generations. New York, USA: ACM Press, 2011:959-964.

[9] HE Dian, LIANG Ying, HANG Zhi, et al. Replicate distribution method of minimum cost in cloud storage for Internet of things[C]//Proceedings of International Conference on Network Computing and Information Security. Guilin, China: [s. n.], 2011:89-92.

[10] BENET J. IPFS-content addressed, versioned, P2P file system[EB/OL]. [2018-12-26]. https://arxiv.org/pdf/1407.3561.pdf.

[11] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2018-12-26]. https://bitcoincash.org/bitcoin.pdf.

[12] 邵奇峰,张召,朱燕超,等. 企业级区块链技术综述[J/OL]. 软件学报:1-22[2019-08-20]. https://doi.org/10.13328/j.cnki.jos.005775.

[13] 张亮,刘百祥,张如意,等. 区块链技术综述[J]. 计算机工程,2019,45(5):1-12.

[14] KRAFT D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(2):397-413.

[15] WATANABE H, FUJIMURA S, NAKADAIRA A, et al. Blockchain contract: a complete consensus using blockchain[C]//Proceedings of the 4th Global Conference on Consumer Electronics. Washington D. C., USA: IEEE Press, 2016: 577-578.

[16] ZHENG Zibin, XIE Shaoan, DAI Hongning, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//Proceedings of IEEE International Congress on Big Data. Washington D. C., USA: IEEE Press, 2017.

[17] MERKLE R C. A digital signature based on a conventional encryption function[C]//Proceedings of CRYPTO'87. Berlin, Germany: Springer, 1987:369-378.

[18] RIVEST R L. All-or-nothing encryption and the package transform[C]//Proceedings of 1997 Fast Software Encryption Workshop. Haifa, Israel: [s. n.], 1997:210-218.

[19] PAGH R, RODLER F F. Cuckoo hashing[C]// Proceedings of European Symposium on Algorithms. Aarhus, Denmark: [s. n.], 2001:121-133.

编辑　金胡考