计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210300051

基于区块链的人事档案管理系统研究

王 辉 陈 博 刘玉祥
南京工业大学计算机科学与技术学院 南京 211816
(wanghui@njtech.edu.cn)

摘 要 根据我国人事档案管理的现状,提出了一种基于区块链的人事档案管理系统方案,从系统框架出发介绍改进的 PBFT 共识算法和系统方案设计。系统采用改进的 PBFT 共识算法,将档案数据安全有效地存储在人事档案区块链系统中,保证了档案数据的可追溯性和有效性;并利用智能合约和星际文件系统(IPFS)等技术实现人事档案的本地备份和转移共享,以防止不可信的第三方对档案数据的恶意破坏,保证了档案数据的安全性。实验数据表明,改进的 PBFT 共识算法与其他成熟的共识算法相比,在输出性能、共识速度以及安全性等方面具有明显的优势,提供了更高的安全性和吞吐量。实验分析表明,基于区块链的人事档案管理系统有望改变传统人事档案管理的弊端,以满足日益增长的人事档案数据保护与共享的需求。

关键词:区块链;共识算法;数字档案;IPFS;智能合约
中图法分类号 TP393

Research on Personnel File Management System Based on Blockchain

WANG Hui,CHEN Bo and LIU Yu-xiang
School of Computer Science and Technology,Nanjing University of Technology,Nanjing 211816,China

Abstract According to the current situation of personnel file management in China,this paper puts forward a scheme of personnel file management system based on blockchain,and introduces the improved PBFT consensus algorithm and system scheme design from the system framework. The system uses the improved PBFT consensus algorithm to store the file data safely and effectively in the personnel file blockchain system,which ensures the traceability and effectiveness of the file data and uses technologies such as intelligent contract and inter planetary file system (IPFS) to realize the local backup and transfer sharing of personnel files,so as to prevent the malicious damage of the file data by the untrusted third party and ensure the security of the system. Experimental data show that the improved PBFT consensus algorithm has obvious advantages in output performance,consensus speed and security compared with other mature consensus algorithms,provides higher security and throughput. Experimental analysis shows that the personnel file management system based on blockchain is expected to change the disadvantages of traditional personnel file management to meet the growing demand of personnel file data protection and sharing.

Keywords Blockchain,Consensus algorithm,Digital archives,Inter planetary file system,Smart contract

1 引言

由从事不同活动的个人、社会团体和国家机关直接制作的具有保留价值的历史记录称为档案,它存在的形式有文字、图表、音像等。自我国档案开放利用以来,全国各级综合档案馆开放档案约 1.3 亿卷(件),公开出版编研材料 6080 种,达 21 亿字[1]。其中,人事档案记录的是个人身份证明、学历证明、工作经历证明等。具有法律效用的人事档案是记录人生轨迹的重要依据,也是我国人事管理制度中一项必不可少的重要依据。

目前,我国的人事档案大多为纸质档案,易丢失、易造假、管理流程复杂、检索缓慢等问题十分普遍,一旦人事档案丢失或被破坏会影响当事人的人生命运。因此,构建数字档案馆并采取安全保护机制已成为一个刻不容缓的现实课题。数字档案馆是一套电子档案数据集成管理系统,其利用众多现代信息技术对档案数据进行采集、处理、存储和管理,满足了信息社会对档案资源管理和利用的新需求,同时也提供了公共档案信息服务。

近年来,国内外许多学者对数字档案、电子档案进行了研究,其中国外学者对数字档案馆研究较为丰富,他们对数字档案馆的研究主要集中于数字档案馆系统建设、专题数字档案馆建设、数字档案馆资源管理研究等方面[2]。国内很多学者也运用区块链、数据库、云计算技术等新技术,在数据保护与共享领域进行研究与实践,文献[3]运用云计算技术解决了目前大多数数字档案馆的“信息孤岛”模式,实现档案信息资源的海量存储、高效管理、多方共享,为开展数字档案馆多元多样化信息服务提供了平台。文献[4]提出了一种云环境下的数字档案馆海量电子档案处理原型系统和存储系统 Cloud-DA,其中包含 HUABASE 数据库和 THCFS 文件系统。HUABASE 的应用领域主要是诸如存储元数据和索引信息这样的结构化数据,而 THCFS 则适用于存储大量的档案文件。

通信作者:陈博(chen_bo97@163.com)

在上述研究基础上，结合目前国内传统人事档案管理档案中心化存储、安全性差、易篡改和丢失的现状，本文运用以太坊联盟链设计了一个数字人事档案管理系统。该方案所应用的是改进 PBFT 共识算法，可以把档案数据存储于人事档案区块链系统中，并保证其安全有效，同时应用智能合约和星际文件系统(IPFS)等技术能够实现人事档案数据的本地备份和转移共享。与普通电子档案管理系统相比，本文建立的以区块链技术为基础的人事档案管理系统解决了存储空间庞大、数据易被篡改、档案转移困难的弊端；与其他基于区块链的档案管理系统研究相比，本文方案运用星际文件系统(IPFS)存储人事档案备份数据，既保证了链下数据无法篡改，又防止网络拥塞而无法从区块链上获取档案数据。通过改进 PBFT 共识算法保障了档案系统的安全性和不可篡改，最后通过数字签名技术保证了用户档案的隐私，档案保存方或档案管理员需获得用户授权才能完成档案的更新与转移。

2 理论背景

2.1 区块链

区块链是一个去中心化的账本技术，它由一系列按时间顺序排列的区块组成，区块链中的每个数据块通常包括区块头和区块体[5]。区块头由父哈希值、Merkle 树、时间戳、计算难度和随机数等信息组成。区块体由详细的交易数据以及一个计数器所组成。仿照计算机网络的七层模型建立区块链系统模型，将区块链系统模型划分为数据层、网络层、共识层、合约层、服务层以及应用层，如表 1 所列。按照不同的应用范围，可以将区块链划分为私有链、联盟链和公有链。如今，大多数区块链项目基于公有链，公有链面向众多用户和市场网络节点访问开放。私有链和联盟链也有属于自己的应用领域。例如，一些垂直行业的公司，如银行业，正将私有链作为自己的数据交换平台。

表 1 区块链模型

Table 1 Blockchain model

层	主要技术或部件
数据层	数据块、链结构、时间戳、Merkle 树、密码学
网络层	P2P 网络、验证机制、广播协议
共识层	PoW，PoS，DPoS，PBFT，…
合约层	智能合约、脚本编码、激励机制
服务层	以太坊、超级账本、IBM Azure BaaS
应用层	加密货币、医疗保健、云服务…

2.2 区块链共识算法

共识机制是区块链系统的核心组成部分，常见的共识机制包括权益证明机制(PoS)、工作负载证明机制(PoW)以及实用的拜占庭容错机制(PBFT)[6-7]。在实际交易中，区块链共识协议消耗了大量的计算资源和能量，导致系统吞吐量低、系统延迟长，因此很多学者[8-10]优化了 POW，POS 和 PBFT 等常见的共识机制，来解决这种问题。

在设计和优化共识算法时，应该考虑 Fischer 等[11]在 1985 年发表的 FLP 定理。FLP 定理指出，遵循异步通信模型的分布式系统的特点是，只要存在一个失败的进程，则总体共识就无法达成；在同步通信模型的分布式系统中所使用的时钟频率是一致的，在有限的时间内出现错误并不影响总体共识的达成。当前大多数共识算法都是基于完全同步通信模型或弱同步通信模型，其中为消息传输设置了超时机制。假设区块链共识算法采用弱同步通信模型，则必须保证共识算法的一致性和活性。在保证一致性和活跃度的前提下，区块链的其他方面可以根据应用需求进行设计，比如提高吞吐量、增加可扩展性、降低资源成本等。本文研究方案是基于联盟链的档案区块链，需要满足低时延和高吞吐的特性，因此选择 PBFT 作为优化和改进的算法。

2.3 智能合约

智能合约这个概念是由 Szabo[12]提出的，它是区块链 2.0 共享账本的核心技术。通过将事务委派到其以太网地址，并根据为事务指定的输入执行该事务，可以触发智能合约。智能合约有效提升了区块链系统处理数据的能力，但同时又对其系统和用户的安全性提出了更高的要求。此外，智能合约具有管理智能资产、进行资产交易和处理数据的能力。基于 docker 容器的 Fabric 允许开发人员使用 Java 高级语言以及 GO 语言进行智能合约的开发，是目前主流的支持智能合约的区块链。

2.4 IPFS 技术

星际文件系统 IPFS(Inter Planetary File System)是一种共享存储文件的协议，它能够实现防篡改、去冗余地保存分布式共享文件以及内容可寻址。所有节点都在一个 P2P 分布式网络中，借助于内容寻址和点对点的超媒体分发协议，形成一个分布式文件系统[13]。当上传一份档案至 IPFS 网络时，会得到一个基于档案内容计算的哈希值，若档案内容被修改，随之其哈希值也将改变，所有节点之间通过共享 swarm-key 相互信任，因此可以保障档案的完整性和真实性。依照应用范围划分，可以将 IPFS 分为共有 IPFS 和私有 IPFS，私有 IPFS 是只允许某个组织内部或某个团体使用。本文也是拟搭建私有 IPFS 来备份存储人事档案。

3 系统描述

图 1 给出了系统的整体架构流程，系统由 6 个部分组成，即用户学生，经授权认证的学校、用人单位和人才市场，密钥中心，服务器，联盟链，IPFS 集群网络。

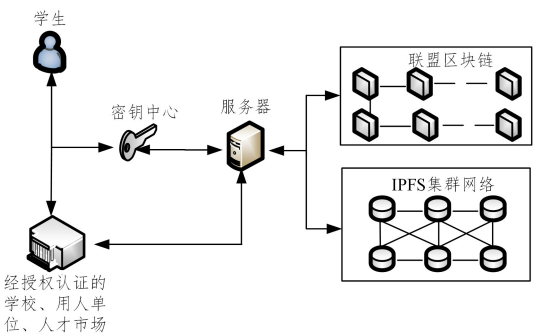


图 1 人事档案管理系统架构

Fig. 1 Structure of personnel file management system

在系统中，用户学生提供人事档案，其中包含学生的政治面貌材料、学历材料等。经授权认证的学校、用人单位和人才市场是人事档案暂时的管理者和保存方，密钥中心产生了每位学生的公钥和私钥，学生使用私钥对自己的人事档案进行签名，保障档案的隐私性和安全性，同时以便档案的读取、更改和转移，联盟区块链可以保障档案的安全与机密，实现无丢

失的转移，IPFS 集群网络则是存储备份电子人事档案文件。

档案数据的公共数据的公共信息例如档案的哈希值、存储地址和授权许可证明等被记录到块上，这些公共信息是可见的，但不能被篡改。授权许可的档案管理员利用用户的公钥加密人事档案，人事档案区块链系统利用哈希算法处理生成的档案数据。

表 2 为联盟区块链中区块结构内容，电子人事档案数据部分分为数据块和元数据块。使用每个学生独一无二的身份证号码作为每个区块的 ID，通过身份证号码可以方便有效地检索档案数据。

表 2　区块结构的内容

Table 2　Content of block structure

结构部分	字段	内容
区块头（Header）	ID	学生身份证号码
	DataHash	新区块哈希值
	PreviousHash	上一区块哈希值
数据（Data）	Timestamp	数据添加时间戳
	TinID	数据添加者 ID
	Text	电子人事档案内容
	SIGNATURES	数据添加者的签名信息
元数据（MetaData）	TIMES	区块数据添加次数
	BASE	学生基本信息

数据块内容包括每次档案数据添加的时间戳、添加者 ID 和其签名信息以及原先电子档案的内容，当添加档案内容时则是对区块中的数据块的 4 个部分进行添加。元数据块包括添加电子文件数据的次数和用户学生的基本信息，例如姓名、性别、籍贯信息、父母信息、家庭住址等。

3.1　改进的 PBFT 算法

本方案中共识算法的基础是三阶段共识，同时也满足在拥有 N 个共识节点的共识网络中可以容忍 f 个错误节点的存在，其中 $N=3f+1$。本方案中的共识算法主要针对联盟档案区块链改进设计，主要目的在于限制某些节点可以加入共识网络和每个节点的许可级别，针对传统的 PBFT 共识算法无法应对节点的动态变化的缺陷做出主要改进。这将大大节约新加入节点的资源，提高了数据传输效率，从而实现高吞吐、低时延。

改进的共识算法的共识流程如图 2 所示。

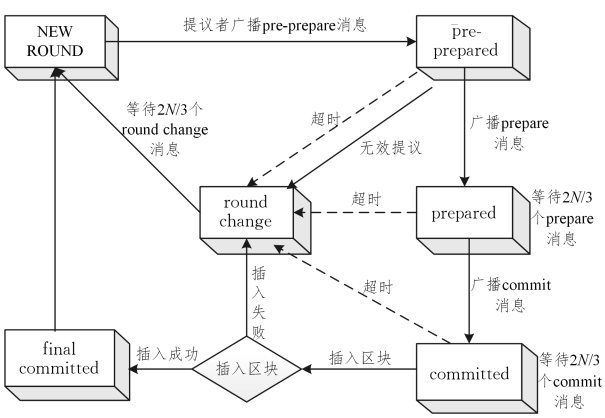


图 2　共识算法状态转换过程

Fig. 2　State transition process of consensus algorithm

共识协议从第 0 轮开始，验证者以循环的方式从他们中挑选一个提议者。然后，提议者将提出一个新的块建议，并与预先准备的消息一起广播。为了确保所有验证器节点都在同一个序列和同一轮中工作，当节点收到来自提议者的 pre-prepare 消息时，其他验证器节点验证传入的消息，进入 pre-prepare 状态并分别给其他节点广播 prepare 消息的状态。为了通知其他验证器节点接收新的块，准备把块插入到链中时，在每个节点从其他节点接收到 $2N/3$ 个 prepare 消息时，验证器节点切换到 prepared 状态并广播 commit 消息。最后，验证器节点接收到 $2N/3$ 个 commit 消息随之进入 committed 状态后，将块追加到链中。改进的 PBFT 算法是一种状态机复制算法。为了达成块一致，所有验证器节点分别维护一个状态机副本。

本文共识算法与传统的 PBFT 有如下几点显著的差异：

(1)PBFT 的验证器集合是静态的，而本文共识算法有一个动态的验证器集合，验证器可以添加到集合中，也可以从集合中移除；

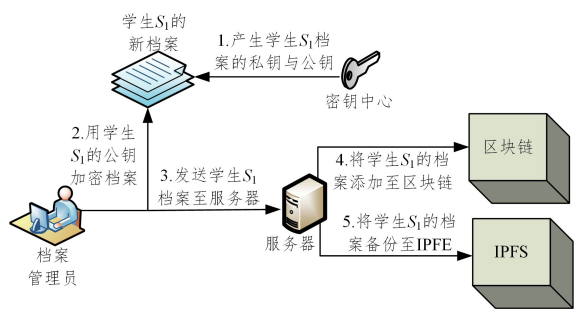
(2)本文共识算法没有客户端向网络提交请求，相反，所有验证者可以依次提出一个块请求；

(3)本文共识算法允许验证区块但不参与共识过程的标准节点和参与共识过程的验证器节点同时存在；

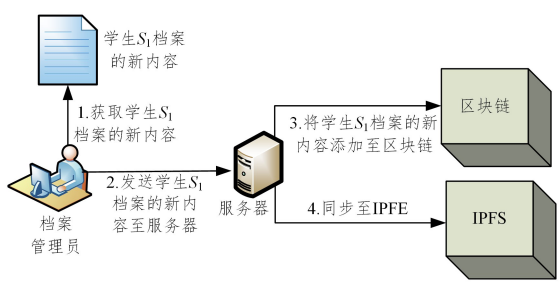
(4)本文共识算法指定了 PBFT 的 View-Change 消息的简化版本，但不包括 PBFT 协议中包含的 New-View 消息。

3.2　人事档案系统方案

新增与更新档案数据的流程如图 3 所示，首先密钥中心直接产生学生 S_1 的私钥与公钥，若本地联盟区块链中还未存在学生 S_1 的档案，则需要添加新增档案，授权的老师或工作人员即档案管理员用学生 S_1 的公钥加密档案材料，再由服务器添加至区块链与 IPFS 集群网络。



(a)添加新档案



(b)更新档案

图 3　添加新档案与更新档案

Fig. 3　Add new archives and update archives

档案管理员把档案发送到 IPFS 集群网络备份，发布档案的唯一地址是由每个用户的私钥签名得到的，当其他用户访问 IPFS 集群网络时，它能够验证签名以确保合法性。其中，每个学生的人事档案存储于联盟区块链每一个块中，区块详细的结构内容如表 2 所列。此外，档案管理员能够添加档

案的内容，如学生的基本信息、档案年度、档案保管期限、文件材料标题和类型等众多属性，同时可以为学生的档案区块添加、删除多个附属文件，并为每个文件增加或删除多种属性如名称、文件类型和备注等。管理员修改档案时则需要预先通过学生 S_1 的私钥解密档案，然后更新和重置人事档案的所有文件与字段。

当学生 S_1 毕业后选择继续升学或工作时需要转移其人事档案，档案的转移过程如图 4 所示，首先学生 S_1 需要向档案管理员提交转移档案申请，档案管理员通过系统服务器从区块链中取出加密过的学生 S_1 的人事档案，再由服务器将档案发送给档案转移方。转移档案的申请包含申请人、转移档案的原因、档案转移方具体地址、升学或工作证明。通过转移申请的人事档案使用用户的私钥加密后，通过系统服务器发送到智能合约，并调用 AACC 合约从数字签名中恢复学生公钥信息，与 DICC 合约中记录的学生公钥进行对比验证，若通过验证则在合约中添加档案信息，完成档案的转移与共享。

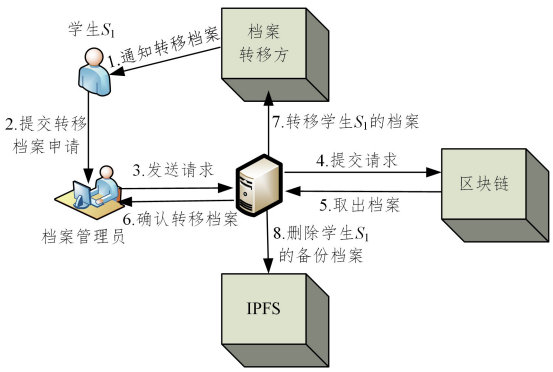


图 4 档案转移过程

Fig. 4 Archives transfer process

4 系统分析

4.1 人事档案区块链系统安全分析

人事档案区块链建立了一个让每个人在其中拥有自己完整个人档案数据的系统，在系统中用户、档案保存方和第三方机构之间存储和共享的档案数据是安全可靠的。人事档案区块链在理想的情况下，应具备以下特征：安全便捷的档案转移共享互操作性、用户档案所有权、存储安全性和防篡改性。

档案材料存储安全可靠是人事档案区块链的一个重要特征，可从公共信息、档案生成和档案转移接收 3 个方面分析其存储安全性。档案数据的公共信息例如档案的哈希值、存储地址和授权许可证明等被记录到块上，这些公共信息是可见的，但不能被篡改。授权许可的档案管理员利用用户的公钥加密人事档案，人事档案区块链系统利用哈希算法处理生成的档案数据。档案管理员还会把档案发送到 IPFS 集群网络备份，发布档案的唯一地址是由每个用户的私钥签名得到的，当其他用户访问 IPFS 集群网络时它能够验证签名以确保合法性。通过转移申请的人事档案使用用户的私钥加密后，通过系统服务器发送到智能合约，并调用 AACC 合约从数字签名中恢复学生公钥信息，与 DICC 合约中记录的学生公钥进行对比验证，若通过验证则在合约中添加档案信息，完成档案的转移与共享。这些机制保证了档案数据源的真实性、档案信息的安全性和档案转移传输的可靠性。

4.2 实验准备

本文对改进的共识算法进行测试时运行负载测试的工具是 golang 测试工具；同时，运用基于 docker 的容器技术，将区块链的共识节点的代码和运行配置都装载在 docker 虚拟容器中。为了获得更好的测试结果，由 helm 部署到 kubernetes 节点的每个验证器都使用足够的资源来运行。实验测试的环境如表 3 所列。

表 3 实验环境信息

Table 3 Experimental environment information

环境信息	配置名称
CPU	i5-6200U
内存	8GB
操作系统	Windows 10

4.3 吞吐量性能测试分析

吞吐量(Transaction per second)通常用于加密的数字货币，它被定义为每秒执行的交易量。每秒执行的交易数量越多，在同一平台上执行、验证和确认事务的速度就越快。例如，如果一个加密货币每分钟执行 18 个交易，那么它的吞吐量为0.3。最大吞吐量是区块链可以确认事务的最大速率。

本文对 PBFT 和改进的 PBFT 算法进行吞吐量的对比实验，将节点数固定为 4，在相同的交易量下比较两种共识算法的吞吐量，实验结果分别取在交易量为 1 000，1 500，2 000，2 500，3 000，3 500 和 4 000 下 40 次测试的平均值，结果如图 5 所示。

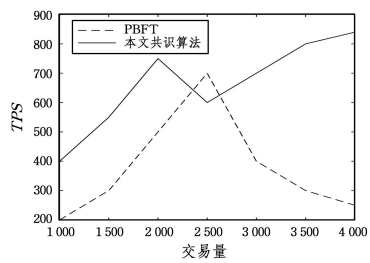


图 5 不同交易量下的 TPS 对比

Fig. 5 TPS comparison under different transaction volume

分析实验结果得知，本文改进的 PBFT 算法的吞吐量在总体上是高于 PBFT 算法的，PBFT 算法在产生 2 500 个交易量之前随着交易量的增多，吞吐量也逐渐增大，但交易量超过 2 500 个之后共识节点的处理能力下降，导致线程堵塞，吞吐量也随之降低。而本文改进的 PBFT 算法虽然在 2 000 个交易量时吞吐量有所减少，但在超过 2 500 个交易量后吞吐量又呈上升趋势，在产生 3 500 个交易量之后吞吐量也呈缓慢上升的趋势。

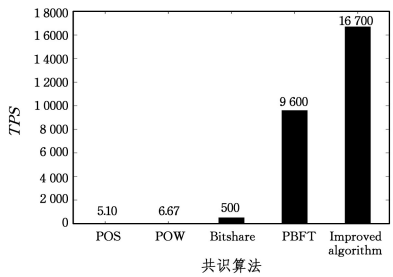


图 6 不同共识算法的吞吐量比较

Fig. 6 Throughput comparison of different consensus algorithms

本文又将改进的 PBFT 算法的吞吐量与 POS，POW，Bitshare 和 PBFT 对比，分别选取测试的吞吐量平均值，对比结果如图 6 所示。POW 和 POS 为了保证高安全性和容错性，只能牺牲大量的算力去挖掘和验证区块，导致单位时间内的吞吐量很低。本文改进 PBFT 的共识算法在单位时间内的吞吐量明显优于 POS，POW 和 Bitshare 算法，而且与 PBFT 相比也提升了将近一倍的吞吐量。

4.4　出块速度测试分析

在区块链系统中，将交易打包成区块，完成共识并记录在链上的过程即为出块，这个过程所消耗的时间为出块速度。算法的性能效率与算法应用在实际系统中的出块速度成正比。表 4 为 4 种较为成熟的共识算法以及本文改进的算法的出块速度，由表中数据可见，本文改进 PBFT 算法的出块速度明显优于其他 4 种共识算法。

表 4　不同共识算法出块速度比较

Table 4　Comparison of the block speed of different consensus algorithms

共识算法	出块时间
PBFT	3.6s(Ripple)[14]
POS	64s(Blackcoin)[15]
DPOS	3s(Bitshares)[16]
DBFT	15～20 s(NEO)[17]
本文共识算法	0.3 s

为了缓解 POW 算法资源消耗过高的问题，POS 算法的提出减少了达成共识的时间，但 POS 算法仍属于算力驱动的机制。DPOS 算法从一定程度上解决了 POW 算法资源浪费的问题，同时降低了共识时间，减小了参与共识过程的节点数量，但需要代币鼓励机制作为奖励，易于形成寡头。据 NEO 白皮书[17]所述，DBFT 每 15～20s 可生成一个区块，但该算法未经过大规模网络验证，系统的实际安全性未知。而本文改进的共识算法有效避免了算力资源消耗过大的问题，区块生成效率高，降低了共识时间，提高了共识效率的优势。

4.5　性能分析

为了更好地获取数据，假设实验每次交易量为 1，取节点数量分别为 4，7，10，25，分别测试并研究 PBFT、CFT、POA 和本文改进的共识算法的性能。依据实验测试的结果，可以得出本文算法的优劣，主要通过共识算法的输出性能、速度和可扩展性 3 个方面来综合体现。从图 7 可看出，本文算法在吞吐量和输出效率上具有一定的优势，同时输出性能是与其比较的 PBFT，CFT 和 POA 中最好的；在速度上本文算法也超越了 PBFT 和 CFT，具有较高的共识效率；在可扩展性方面虽然本文算法优于 PBFT 算法，但还是有提升优化的空间。

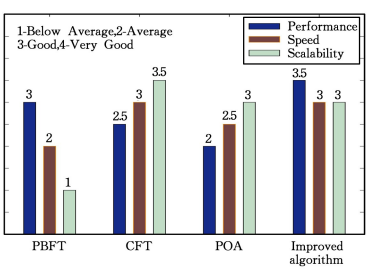


图 7　不同共识算法综合性能的对比

Fig. 7　Comprehensive performance comparison of different consensus algorithms

结束语　本文所构建的基于区块链的人事档案管理系统，为解决传统档案管理的弊端提供了有效的解决方案，它包含用户档案所有权、数据保护、存储安全性、防篡改和安全便捷的档案转移互操作性等特征，有效解决了传统档案管理的弊端。该系统采用数字签名技术实现了档案保存方对人事档案的安全管理；结合 IPFS 集群网络以及智能合约技术使档案数据的备份功能得以实现；为了保障档案数据的更新、转移与共享，运用了联盟区块链。本文还针对原始 PBFT 共识算法的不足提出了一种改进 PBFT 的状态机复制算法，该算法采用了三阶段共识，运用动态的验证器节点集合维护一个状态机副本，达成块一致。通过实验测试数据证明了本文改进共识算法的性能优势和安全性，且其具有高共识效率、高吞吐量的优点。本文改进的算法仍有不足之处，如整个算法的活性问题，出现这个问题的原因主要是节点可能会存在的传输延迟，诚实节点会锁在不同的区块上，导致没有足够的 1/3 的节点可以支持整个共识过程的进行。未来将进一步优化改进的共识算法出现的问题，使得该算法更好地融合人事档案管理系统。

参 考 文 献

[1] State Archives Administration. Issued by the State Archives Bureau Outline of the 13th five year plan for National Archives Development[EB/OL]. http://www.saac.gov.cn/news/2016-04/07/content_136280.htm.

[2] CHEN H，NAN M J. Construction of Digital Archives Based on Interactive Archives Information Service Mode-Take The United States，Britain，Canada And Australia as Examples[J]. Shanxi Archives，2019(5)：103-111.

[3] YOU S S. Research on Information Service of Fujian Digital Archives Based on Cloud Computing[D]. Fujian Agriculture and Forestry University，2016.

[4] ZHANG G，SI X X，HUI L F，et al. Massive electronic Records Processing for Digital Archives in Cloud[C]// International Conference on Pervasive Computing. 2012：814-829.

[5] PENG C W，DA H W，YU Z，et al. Blockchain Data-based Cloud Data Integrity Protection Mechanism[J]. Future Generation Computer Systems，2020，102：902-911.

[6] CAO B，ZHANG Z H，FENG D Q，et al. Performance Analysis and Comparison of PoW，PoS and DAG Based Blockchains[J]. Digital Communications and Networks，2020，6(4)：480-485.

[7] CASTRO M，LISKOV B. Practical Byzantine fault tolerance [C]// Operating Systems Design and Implementation. 1999：173-186.

[8] SHENG G，TIAN Y Y，JIAN J Z，et al. T-PBFT：An Eigen Trust-Based Practical Byzantine Fault Tolerance Consensus Algorithm[J]. China Communications，2019，16(12)：111-123.

[9] WANG K，PEI S R，CHEN C M，et al. Proof of X-repute Blockchain Consensus Protocol for IoT Systems[J]. Computers & Security，2020，95：101871.

[10] YU B，LIU J，NEPAL S，et al. Proof-of-QoS：QoS Based Blockchain Consensus Protocol[J]. Computers & Security，2019，87：1015801. 1-101580. 13.

[11] FISCHER M J，LYNCH N A，PATERSON N A. Impossibility of Distributed Consensus with One Faulty Process[J]. Journal of The ACM (JACM)，1985，32(2)：374-382.

[12] SZABO N. Smart contracts[OL]. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.
[13] WU X, HAN Y, ZHANG M, et al. Secure Personal Health Records Sharing Based on Blockchain and IPFS[C]// Trusted Computing and Information Security (CTCIS 2019). Communications in Computer and Information Science. Springer, Singapore, 2019.
[14] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. http://bitcoin.org/bitcoin.pdf, 2008-11-8.
[15] Ethereum White Paper. A Next-Generation Smart Contract and Decentralized Application Platform [EB/OL]. http://github.com/ethereum/wiki/wiki/White-Paper.
[16] Delegated Poof-of-Stake Consensus[EB/OL]. http://bitshares.org/technology/delegated-proof-of-stake-consensus/.
[17] NEO white paper [EB/OL]. http://docs.neo.org/zh-cn/whitepaper.html.

WANG Hui, born in 1962, Ph.D, professor. Her main research interests include optical communication and signal processing.

CHEN Bo, born in 1997, postgraduate. Her main research interests include blockchain and data security.

(上接第 704 页)

对于整体性能的提升占比不是很大。方案二通过计算模式的转变，主要进行了 K 维度的优化，故在 16×4 的分块下，采用方案二计算模式的性能提升不如 4×4 分块下的显著。

要实现高性能的程序例程，需要从各个方面进行细致优化，即便对于 16×4 的分块采用方案二的性能提升不如 4×4 分块下的显著，但 GEMM 函数选择 16×4 分块的整体性能仍是最高的。同时，从实验数据可以看出本文提出的方案二的计算模式有一定的性能优化提升，对于 M, N, K 3 个维度分块相同的方式，采用方案二的计算模式性能提升会更为显著。

根据以上 4 组实验的结果，可以看出无论是算法优化提出的计算模式转变还是结合平台进行的向量化优化、分块选择对比等都与理论预估一致。这表明本文提出的使用 SIMD 向量化进行核心代码优化的算法实现是行之有效的。

结束语 本文提出了一种使用 SIMD 向量化进行核心代码优化的算法实现，分别进行了数据排布、选择计算数据块、寄存器分配、使用向量化指令不对界载入和高低位不对界存储等指令，充分利用平台 Cache 行存储与向量化计算达到平台性能更优化。结合平台架构和资源提出的 GEMM 向量化最优分块为 16×4。实验结果表明，本文提出的 SIMD 向量化进行核心代码优化的算法实现能够在申威 1621 平台上获得较高的性能。同时，本文提出的 GEMM 算法计算模式变换，不仅仅适用于申威 1621 平台，对于其他平台，同样可使用该算法计算模式来获得一定的性能提升。下一步的工作是使用本文的方法优化整个 BLAS3 的函数，研究 BLAS3 的其他几个函数是否有能与平台密切结合的其他特性，以及结合多核多线程相应的优化技术进行多线程加速，在申威 1621 平台上对整个 BLAS3 库进行高性能实现。

参 考 文 献

[1] GOTO K, GEIJN R A. Anatomy of high-performance matrix multiplication[J]. ACM Transactions on Mathematical Software (TOMS), 2008, 34(3): 1-25.
[2] ZHANG X Y, WANG Q, ZHANG Y Q. Model-driven Level 3 BLAS Performance Optimization on Loongson 3A Processor [C]// 2012 IEEE 18th International Conference on Parallel and Distributed Systems. Singapore, 2012: 684-691.
[3] WANG E, ZHANG Q, SHEN B, et al. Intel math kernel library [M]. High-Performance Computing on the Intel © Xeon Phi-. Springer, Cham, 2014: 167-188.
[4] AMD. 2012. AMD Core Math Library[OL]. http://developer.amd.com/tools/cpu/acml/pages/default.aspx.
[5] cuBLAS. Basic Linear Algebra on NVIDIA GPUs [OL]. https://developer.nvidia.com/cublas.
[6] GOTO K, VAN DE GEIJN R. High-performance implementation of the level-3 BLAS[J]. ACM Transactions on Mathematical Software (TOMS), 2008, 35(1): 1-14.
[7] JIANG M Q, ZHANG Y Q, SONG G, et al. Research on High Performance Implementation Mechanism of GOTOBLAS General Matrix-matrix Multiplication[J]. Computer Engineering, 2008(7): 84-86, 103.
[8] LIU H, LIU F F, ZHANG P, et al. Optimization of BLAS Level 3 Functions on SW1600 [J]. Computer System Application, 2016, 25(12): 234-239.
[9] LIU Z, TIAN X. Vectorization of Matrix Multiplication for Multi-core Vector Processors[J]. Chinese Journal of Computers, 2018, 41(10): 2251-2264.
[10] VAN ZEE F G, SMITH T M. Implementing High-performance Complex Matrix Multiplication via the 3m and 4m Methods[J]. ACM Transactions on Mathematical Software, 2017, 44(1): 1-36.
[11] KIM K, COSTA T B, DEVECIM, et al. Designing vector-friendly compact BLAS and LAPACK kernels[C]// IEEE International Conference on High Performance Computing Data and Analytics. 2017.
[12] Chengdu Sunway Technology Corporation Limited. 2017. Sunway1621 processor structure manual [OL]. http://www.swcpu.cn/uploadfile/2018/0709/20180709030836489.pdf.

LI Shuang, born in 1992, postgraduate. Her main research interests include high performance computing and so on.

WANG Lei, born in 1977, master, professor, master's tutor. His main research interests include high performance computing and basic mathematics function library design and optimization research and development.