分类号：　　密　　级：公开
学　号：20232008003　　单位代码：10759

石河子大学

硕士学位论文

基于优化共识算法的证件照数据存储和共享模型研究

学位申请人　常银恒
指导教师　李志刚 教授

申请学位门类级别　工学硕士
学科、专业名称　网络空间安全
研究方向　信息内容安全
所在学院　信息科学与技术学院

中国·新疆·石河子
2026 年 5 月

分类号：　　密　　级：公开

学　号：20232008003　　单位代码：10759

石河子大学

硕 士 学 位 论 文

基于优化共识算法的证件照数据存储和共享模型研究

学 位 申 请 人	常银恒
指 导 教 师	李志刚 教授
申请学位门类级别	工学硕士
学 科 、专 业 名 称	网络空间安全
研 究 方 向	信息内容安全
所 在 学 院	信息科学与技术学院

中国·新疆·石河子

2026 年 5 月

Research on Identity Photo Data Storage and Sharing Model Based on Optimized Consensus Algorithm

A Dissertation Submitted to

Shihezi University

In Partial Fulfillment of the Requirements

for the Degree of

Master of Engineering

By

Chang Yin-heng

(Cyberspace Security)

Dissertation Supervisor: Prof. Li Zhi-gang

May,2026

石河子大学学位论文独创性声明及使用授权声明

学位论文独创性声明

本人所呈交的学位论文是在我导师的指导下进行的研究工作及取得的研究成果。据我所知，除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确的说明并表示谢意。

研究生签名：常银恒　　时间：2026 年　5 月　19　日

使用授权声明

本人完全了解石河子大学有关保留、使用学位论文的规定，学校有权保留学位论文并向国家主管部门或指定机构送交论文的电子版和纸质版。有权将学位论文在学校图书馆保存并允许被查阅。有权自行或许可他人将学位论文编入有关数据库提供检索服务。有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

研究生签名：常银恒　　时间：2026 年 5 月 19 日

导师签名：　　时间：2026 年 5 月 19 日

摘要

随着信息技术发展与数字政府建设的推进，线上政务办理、考试申请、身份认证等服务逐渐普及，在提高政务效率和居民办事效率的同时，出现了各部门间的数据流通不畅和不敢分享数据到不同部门的现象，存在数据孤岛和部门间不信任的问题。本研究聚焦各部门之间“数据孤岛”的痛点，依托区块链不可篡改、去中心化、可溯源的技术特性，实现跨部门、跨系统的证件照数据安全共享。本文以证件照数据存储和共享为出发点，做以下研究：

（1）针对电子政务场景对共识机制安全性、运行效率及抗恶意节点能力的核心要求，提出一种基于信誉值的双层优化的实用拜占庭容错算法（Dual-Layer Reputation-based Practical Byzantine Fault Tolerance，DLR_PBFT）。节点分层策略通过细化分工，提高共识效率；信誉值机制客观评估节点行为，过滤恶意节点，降低其干扰。实验结果显示，在故障节点数量从 0 增至 11 时，DLR_PBFT 吞吐量仅下降 21.97%，时延波动幅度远小于对照组算法，在拜占庭恶意节点环境下能保持高效运行。

（2）基于 DLR_PBFT 的优化思路，在 HotStuff 算法的基础上，提出基于分组解耦和信誉值机制的 HotStuff 共识算法（HotStuff Consensus Algorithm Based on Group Decoupling and Reputation Value Mechanism，GD_RHotStuff）。该算法将节点分为共识组和验证组，对共识过程进行解耦分工；同时基于信誉值机制建立异常节点检测，实现恶意节点动态剔除，提升算法安全性与扩展性。实验数据表明，在拜占庭场景下，该算法平均吞吐量仅下降 31.16%，远低于原生 HotStuff 的 81.20%，在吞吐量、时延、鲁棒性和自愈能力上都得到提升，适配电子政务对高性能、高安全的需求。

（3）根据证件照数据存储和共享的需求和规范，提出中心链和工作链的双链结构，构建证件照数据存储和共享模型。结合电子政务证件照数据流的情况，设计多链架构，明确链条组成、数据结构与链间锚定规则。在 FISCO BCOS 平台进行模拟测试，结果显示，该模型相较对照组吞吐量最高提升 30%，平均交易时延最大降低 18%，在并发处理、响应速度上优势显著，可满足政务场景下证件照数据跨部门共享的高并发、高可靠需求。

综上，本研究提出 DLR_PBFT 与 GD_RHotStuff 两种优化共识算法，并结合电子政务证件照数据应用场景，搭建了契合政务环境下证件照数据跨部门共享的高效、稳定、安全的多链结构存储和共享模型。

关键词：电子政务；PBFT 共识算法；门限签名；HotStuff 算法；多链结构

Abstract

With the advancement of information technology and the development of digital government initiatives, services such as online government services, examination applications, and identity authentication have become increasingly widespread. While these developments enhance government and citizen service efficiency, they have also led to challenges including inefficient data flow between departments and reluctance to share data across agencies, resulting in data silos and interdepartmental distrust. This study addresses the pain point of "data silos" among departments by leveraging blockchain's immutable, decentralized, and traceable technical characteristics to enable secure sharing of ID photo data across departments and systems. Starting from the storage and sharing of ID photo data, this paper conducts the following research:

(1) To meet the core requirements of e-government scenarios for consensus mechanism security, operational efficiency and anti-malicious node capability, a Dual-Layer Reputation-based Practical Byzantine Fault Tolerance (DLR_PBFT) algorithm is proposed. The node hierarchical strategy improves consensus efficiency through refined division of labor; the reputation mechanism objectively evaluates node behaviors, filters malicious nodes and reduces their interference. Experimental results show that when the number of faulty nodes increases from 0 to 11, DLR_PBFT's throughput only decreases by 21.97%, and the delay fluctuation is much smaller than that of the control algorithm, which can run efficiently in the Byzantine malicious node environment.

(2) Based on the optimization idea of DLR_PBFT and the HotStuff algorithm, a HotStuff Consensus Algorithm Based on Group Decoupling and Reputation Value Mechanism (GD_RHotStuff) is proposed. This algorithm divides nodes into consensus groups and verification groups to decouple the consensus process; it also establishes abnormal node detection based on the reputation mechanism to dynamically eliminate malicious nodes and improve algorithm security and scalability. Experimental data show that in the Byzantine scenario, the average throughput of this algorithm only decreases by 31.16%, much lower than 81.20% of the original HotStuff. It has improved throughput, delay, robustness and self-healing ability, meeting the high-performance and high-security needs of e-government.

(3) According to the requirements and specifications of ID photo data storage and sharing, a dual-chain structure of central chain and work chain is proposed, and an ID photo data storage and sharing model is built. Combined with the data flow of e-government ID photos, a multi-chain architecture is designed, specifying chain composition, data structure and inter-chain anchoring rules. Simulation tests on the FISCO BCOS platform show that compared with the control group, the model's throughput can be increased by up to 30%, and the average transaction delay can be reduced by up to 18%. It has obvious advantages in concurrent processing and response speed, meeting the high concurrency and high reliability needs of cross-departmental ID photo data sharing in government scenarios.

In summary, this study proposes two optimized consensus algorithms, DLR_PBFT and GD_RHotStuff, and builds a multi-chain storage and sharing model that meets the efficient, stable and secure needs of cross-departmental ID photo data sharing in the government environment, combined with the application scenario of e-government ID photo data.

Key words: e-government; PBFT consensus algorithm; threshold signature; HotStuff algorithm; multi-chain architecture

目 录

第 1 章 绪论

1.1 研究背景和意义

随着国家数字政府和电子政务的发展，居民网上办理手续、报名考试、身份信息认证已经成为日常生活中的一部分。但是，随着政务服务的信息化不断发展，出现了大量急需解决的问题，这使得政府部门间安全可靠的数据共享成为研究热点[1]。其中，各个部门之间的“数据孤岛”问题使居民网上办事流程非常繁琐，办理不同的业务需要在不同的政府部门专门的政务应用上传同类型数据，导致不同平台反复上传同类数据的问题，最终的办事效果与线下办理相差无几。这与政务信息化、便捷性的理念背道而驰。例如，申请驾驶证时，需要提交个人电子版证件照和实体证件照照片；申请社保卡时也需要提交证件照，此类提交证件照办理业务的场景很多。如何打破“数据孤岛”，以及建设以公民为中心，在政府、公民、社会和市场思维协同的数字政府管理体制的构建上[2]，实现政务服务可信互通及业务链之间的可信协作，是目前电子政务发展中亟待解决的问题。

区块链技术作为一种安全可信的去中心化、块链式存储的分布式共享账本构建技术，为建立安全、高效、透明的数字政府提供强有力的技术工具[3]。根据数字政府在电子政务方面的规定，要求保障政务数据的安全性、隐私性和提升政务效率放在同样重要的地位。近年来，区块链技术在电子政务中应用不断涌现，根据已有的研究表明[4]，在提升电子政务的安全可靠的同时，可以解决不同部门之间的数据归属和权责问题。于此同时，国外研究人员在数字政府建设方面，提出了很多与区块链相关的基础研究[5]，将区块链技术作为构建政府信息共享系统的底层逻辑，能够提升政府整体的运行效率[6]，进一步提升了公民办事的便利性。为了解决电子政务部门之间的可信互通及不同部门之间的数据存储与共享问题，借助区块链相关技术，解决了区块链在应用于政务服务场景下存在部分的问题。然而区块链处理不同部门间的数据同步问题上，依赖的其共识算法的性能，提升共识算法的效率能够有效提升政务处理的效率。根据现有的研究，区块链在大规模节点的情况下，共识算法的效率较低，并且在超过共识算法容错的节点数量时，共识会陷入死循环。同时面对跨部门数据互通的现实需求时，区块链的单链结构无法满足。在证件照数据存储与共享方面，区块链依托自身数据不可篡改、去中心化、日志规则的优势，能够以联盟链的形式在政府不同部门间建立互信的数据存储与共享模型，解决目前各个部门之间存在的“数据孤岛”的问题，实现证件照数据一次上传，跨部门、多部门联合认证和使用，解决证件照数据需要多次上传和部门之间数据隔离的问题。

1.2 国内外研究现状

1.2.1 基于区块链的政务数据存储与共享研究现状

政务数据作为国家核心战略资源，其安全存储与高效共享是数字政府建设的核心议题。传统政务数据多采用中心化存储结构，存在“数据孤岛”、易篡改、共享数据权责不清、隐私泄露风险高等痛点。区块链技术凭借分布式存储、不可篡改、可追溯、智能合约自动执行、共识算法同步数据等特性，为破解政务数据存储与共享困局提供了全新技术路径，近年来成为了国内学术界与政务信息化领域的研究热点。

在电子政务数据存储与共享领域，区块链作为解决方案，发挥了重要作用。很多学者根据总结了当前的政务数据共享存在的问题[7]，例如、数据共享模式问题突出、共享的制度化和规则化程度低、安全性能缺陷、数据孤岛效应[8]等。

在政务数据共享可信性研究方面，KASSEN[9]分析了区块链对电子政务的影响，在区块链网络中，多方监管和验证可以有效避免腐败出现，总结了区块链的去中心化特性对解决传统电子政务服务缺乏互信的问题。Chen 等[10]提出了一种称为 GovChain 的 CP-ABE 与区块链融合的方案，构建了可信的身份认证环境，结合星际存储 IPFS,对电子政务数据存储提供了案例。在政务数据存储与共享模型研究方面，王亮等[11]根据当前政府数据信息共享的运行机制和核心因素，构建了基于区块链技术的政府信息资源共享与交换系统。余益民等[12]提出了基于区块链的政务信息资源共享模型，通过智能合约保障各政务机构间信息交换的合规性与准确性，该模型具备数据一致性与可溯源机制。温圣军等[13]提出一种迁移的省级政务数据共享模型方案，能够最带限度的减少对原有的信息系统的改造，为基于区块链的政务系统落地提供了参考方案。

在政务数据存储结构方面，诸多学者在算法和区块链数据存储结构上做了很多研究。Liu 等[14]提出了基于区块链的政务数据存储结构，实现了权限自主管理、逻辑统一、分布式物理架构，提出了符合实际的政务存储逻辑。王茜等[15]在保留现有政务多部门分布式存储和分头管理模式的同时实现海量政务材料高效共享，并全面提升设计的性能、安全性和去中心化能力，提出了一种基于链上链下数据协同的高可用共享方案。对单链进行拓展，提升其链上链下的数据协同能力，根据该方案设计的应用在安全、性能、去中心化各方面实施了多个卓有成效的方法，并在访问性能上做出了重点提升，尤其适用于高并发类的数据协同共享应用。王浩亮[16]等在分析传统电子证照库的基础上，运用区块链技术设计了一种链上数据存储、链下用证交易管理的交易系统，能够满足参与主体的需求并防止信息泄露。

国内外学者在政务数据的可信性、数据存储与共享模型和数据存储结构上做出了很多研究，为电子政务中证件照数据存储与共享提供了丰富的理论与技术基础。

1.2.2 PBFT 共识算法研究现状

共识算法作为提升区块链系统的技术核心，在维持分布式网络中的节点一致性中发挥重要作用。目前的共识算法根据其适配区块链类型，可分为三类，PoW(proof of work)算法[17]和 PoS(proof of stake)算法[18]用于公有链，私有区块链则使用授权股份认证共识算法 DPoS（delegated proof of stake）算法[19]，对于 PBFT[21]共识算法和 Raft[20]算法，则应用于联盟链[22]中。根据数字政府建设的要求，国家大力推行联盟链在电子政务、数字经济等领域的应用。PBFT 共识作为联盟链应用最多的共识算法也成为了研究的热点，在其基础上的算法改进的方案和新的算法层出不穷。但是，改进方案的提出多针对 PBFT 共识算法存在通信复杂度高[23]和视图切换[24]等问题。

PBFT 共识算法的提出，为数据分布式存储同步提供了一种解决方案，同时也解决了拜占庭将军问题，其高效性为区块链的节点数据同步提供了理论基础。在点对点网络中，节点之间的通信存在网络延迟，PBFT 算法能够保持分布式网络的高容错性，但随着节点数量的增加，通信开销也爆发式增加，共识效率会非常低。因此众多学者通过对 PBFT 的改进以使其适用于大规模节点的区块链系统。本节将从信誉值机制、流程简化、节点分层与分组、节点动态调整等方面论述国内外学者对 PBFT 的改进方案。

在信誉值机制和节点划分方面，黄世成等[25]提出基于信誉评价的动态双主节点共识算法，引入信誉评价机制对节点行为进行实时评估，结合时间感知因子动态调整节点信誉值，同时采用可验证秘密分享技术，将传统 PBFT 算法的 5 轮通信轮次降至 3 轮，有效降低了通信开销，提升了共识效率。翟社平等[26]提出 RC-PBFT 算法，基于信誉值对节点进行分组，仅选取高信誉节点参与核心共识过程，缩小了共识参与集，在保证安全性的前提下，显著降低了通信复杂度与共识时延。王婷等[27]融合节点竞价与信誉机制，设计了新型主节点遴选方案，既通过信誉机制筛选可信节点，又通过竞价机制平衡节点参与积极性，提升了共识系统的稳定性与灵活性。马海峰等[31]设计了基于多节点评估模型的改进 PBFT 多层共识算法，将系统分为核心层与边缘层，核心层节点承担主共识任务，边缘层节点负责数据验证与同步，通过多节点评估模型筛选核心层节点，提升了核心共识的安全性与效率，同时降低了边缘层节点的通信负担，实现了系统扩展性的提升。刘陕南等[32]提出基于分组和信用分级的改进拜占庭容错（CBFT）算法，首先根据节点信用等级对节点进行分组，再在各组内执行局部共识，最后通过组间同步实现全局共识，有效减少了全网交互频次，提升了系统在大规模节点场景下的吞吐量。

在信誉值与节点动态调整结合方面，李俊吉等[28]基于节点历史行为构建信誉评价模型，根据信誉值动态调整节点的共识权重，实现恶意节点的有效隔离，同时优化视图切换机制，减少视图切换过程中的开销。陈苏明等[29]提出基于节点分组信誉模型的改进 PBFT 算法，将节点按信誉等级分组，不同分组承担不同的共识职责，既提升了共识效

率，又增强了系统对恶意节点的容错能力。李凤岐等[30]提出了 CD-PBFT（credit score and dynamic double layer practical Byzantinefault tolerance）高效共识算法，采用分层结构和信誉值机制，双层架构实现交易验证和读写操作并行，信誉值机制移除故障节点，实现算法相较于 PBFT 实现了性能上的提升。袁昊天等[36]构建了基于改进 Raft 与 PBFT 的双层共识算法 DL_RBFT，上层采用 Raft 算法负责主节点选举与日志同步，下层采用 PBFT 算法保障共识的强一致性，既利用了 Raft 算法选主高效、开销低的优势，又发挥了 PBFT 算法强容错、高可靠的特点，适配高可用、高并发的分布式场景。潘彦炀等[35]将贝叶斯理论引入 PBFT 共识算法，提出 BC-PBFT 共识算法，凭借贝叶斯的推理能力，对节点的行为进行预测性评估，动态调整节点的容错权重，实现对恶意节点的精准识别与隔离，同时优化共识流程，提升了算法的安全性与自适应能力。

在节点聚类方面，杨雨浓等[33]基于 k-means 聚类算法，将节点按网络特性与行为特征进行动态分组，提出了 k-PBFT（k-means-practical Byzantine fault tolerance），实现多组织协同共识，适配跨域联盟链场景，解决了跨组织共识中的通信延迟与信任问题。石亦燃等[34]提出基于通信延迟聚类和节点信誉的 PBFT 共识算法，首先通过聚类算法将节点按通信延迟划分为不同集群，优先选取低延迟、高信誉的节点参与共识过程，减少通信延迟；同时优化共识阶段，合并冗余交互步骤，进一步降低通信开销，提升共识效率。

在通信流程简化和优化视图切换机制上。Golan-Gueta 等[37]通过主节点收集节点发送的消息，并采用门限签名技术简化通信流程，提出了 SBFT（Scalable Byzantine Fault Tolerance）算法。Yin 等[56]在 SBFT 的基础上进行改进，提出了 HotStuff 算法，借鉴流水线机制提升了共识的效率。HotStuff 作为第一个具有线性通信复杂度的 BFT 协议，其已被 Diem 平台和大量应用程序中得到应用。但 HotStuff 在主节点选举机制方面、签名验证方面、通信阶段方面仍存在问题。在这些问题的基础上，众多学者提出了一些新的共识算法，已经被验证过的拜占庭协议[38]、IT-HS[39]、Sync-HotStuff[40]、smashing[41]和 NWH[42]。这些共识算法在性能上都表现非常好，同时解决了 HotStuff 面临的部分问题。

对 HotStuff 的改进主要聚焦于其签名方法，Boldyreva[43]和 Shoup[44]提出的签名方法比 HotStuff 原本的签名方法更高效。Giridharan[45]使用一种新颖的聚合签名方案构建了一个两阶段的 HotStuff 协议，但引入了一个额外的假设，也增加了公钥的复杂度和加密的开销。Neiheiser 等[46]在其文章中验证了以上说法。在测试环境为理想环境和加密开销巨大，并且节点数量较多的情况下，采用适配的签名技术，能够有效的降低共识时间。

对 HoutStuff 通信过程的改进。HotStuff 作为三阶段的共识算法，其性能提升在两阶段时是最优的。Fast-HotStuff[50]、Jolteon[48]和 Bee-Gees[49]具有两阶段的正常情况操作，但在视图更改协议中具有二次通信开销。Abspeol 等[47]在依赖零只是证明的情况下，将 HotStuff 减少为具有线性成本的两阶段协议。Levrat 和 Rambaud[52]提出了一种具有响应

性视图变化的两阶段 BFT，使用一种称为非绝对多数证明(PnS)的新阈值原语，实现了线性通信复杂度，但其视图更换的复杂度为 O（n^2）。

HotStuff-2[51]、Moonshot[53]采用积极相应的策略简化共识通信的轮次，但是在网络环境差的情况下，其性能表现不佳。Marlin[54]在没采用乐观路径的基础上，使用更为复杂的数据结构，实现了无条件的二次通信，但验证过程复杂。Pike[55]在 Marlin 的基础上，提出三种视图切换模式，来避免视图切换的巨大开销，实现了数据结构简化和两阶段通信，算法性能得到了很大的提升。

Xu 等[57]通过优化 Commit 阶段流程和节点组划分，提出了区块链共识算法 SGPBFT，通过降低通信复杂度，进一步提高共识效率。公鹏飞等[60]提出了共识算法 MLH，MLH 通过引入多主节点并行出块机制，通过结合门限签名与聚合签名降低了分区内的通信复杂度，使 MLH 算法在连续视图切换的情况下仍保持线性通信复杂度不变。CHENG 等[59]结合多管道和计划批次机制，提出了 Mp-HotStuff（Multi-pipeline HotStuff,Mp-HotStuff）共识算法，显著提升了吞吐量，但管道并行机制对节点间状态同步精度提出了更高要求。李启南等[58]在 Fast-HotStuff 算法的基础上，通过改进了节点异常出现的领导者切换流程，使新一轮的领导者能够继续之前共识未达成的区块，虽然，一定程度上降低了共识的时延，但是增加了区块链分叉的风险。

综上所述，总结了共识算法存在的局限性。首先，多数改进算法基于静态节点假设，未充分考虑节点动态加入、退出的场景，难以适配动态变化的分布式环境，节点动态调整过程中的共识一致性与安全性难以保障。第二，信誉模型的设计仍存在缺陷，多数研究中信誉评价指标较为单一，缺乏对节点恶意行为的全面考量，且信誉值的更新机制不够灵活，抗攻击能力较弱，难以应对节点共谋、恶意刷分等复杂攻击。第三，复杂场景下的适配能力不足，现有改进算法多针对单一场景优化，在跨链共识、高并发、低时延等复杂场景下的性能表现不佳，且缺乏有效的形式化验证与安全性证明，难以保证算法在实际应用中的可靠性。对于 HotStuff 系列改进共识算法而言，依旧存在多处性能与设计短板，制约了算法在大规模分布式场景下的应用。核心问题集中在主节点选举机制模糊，缺乏标准化、透明化的选举规则，容易出现节点争抢掌权、恶意节点操控选举等问题，难以选出高可信、高可用的主节点，进而影响共识稳定性。其次，算法依赖门限签名与聚合签名，签名生成和验证流程繁琐，导致计算开销较大，会占用大量节点算力资源。除此之外，算法通信阶段依旧较多，消息交互流程复杂，在节点数量不断增多的场景下，网络传输压力剧增，签名聚合耗时变长，消息延迟显著上升，整体共识效率会大幅下滑，吞吐量与时延指标急剧恶化，无法适配大规模节点集群，也难以满足高并发业务场景的运行需求。

1.2.3 区块链存储方案研究现状

区块链存储的可扩展性是制约区块链技术广泛应用的关键瓶颈。目前的解决方案主要分为链上和链外两类：链上方案通过优化区块链内部架构与数据管理流程直接应对可扩展性挑战，核心在于重新设计系统的一个或多个基础功能，具体技术包括分片、修剪、压缩、重复数据删除及基于大数据的方案等；链外方案则借助外部系统与机制减轻链上存储负担，通过在外部环境处理数据存储并与主链保持安全可验证的连接实现，典型案例有状态通道、汇总、侧通道、分布式存储系统、云存储及分层存储。本文将重点介绍链上的分片方案、链外的侧链和 IPFS 方案。

在链上区块存储的分片方案方面，Wang 等[61]提出一种基于深度 Q 网络（DQN）的优化分片体系结构，可动态调整分片与一致性结构，不仅最大限度降低冗余，还提高区块链节点的空间利用率。与现有联盟区块链系统相比，该方法存储空间节省高达 78%，吞吐量提升 33%。Guo[62]等提出基于块访问频率和大小的分片存储模型（BAFS），核心是根据块的访问频率与大小分类管理，为不同类型块实施定制化存储方案，确保存储资源的最优配置与利用，满足区块链系统日益增长的需求。BAFS 的创新点在于动态适应性：通过持续监视每个块在特定时间间隔内的访问次数及存储大小，系统可灵活调整存储策略。Jia 等[63]提出基于区块链分片技术的优化数据存储模型，利用支持向量机的极限学习机（ELM）作为分类器提升分类效率。ELM 的集成使系统更高效地处理和分类数据，确保存储分配最优。模型的关键组成部分是节点内热块评估方法：作者设计全面评估框架，允许节点识别并分类本地存储最相关的热块，评估基于块热度、客观特征、节点关联特征、历史热度、隐藏热度及存储需求五个关键指标，从而确保节点优先在本地存储最关键、最频繁访问的块，优化存储效率与访问性能。

侧链是与主区块链并行运行的独立区块链，通过双向挂钩与主链连接，实现资产在两条链间的安全转移。Singh 等[64]将存储密集型操作分流至侧链，可减轻主区块链的存储负担并提升可扩展性。Yadav 等[65]提出基于侧链的解决方案，利用区块链技术提升土地登记数据的存储与检索性能。该框架将数据分配存储于主链与侧链，主链存储可公开访问的元数据，侧链存储非事务性数据（如图像、合同、PDF 及其他相关文档）。这种分离大幅降低主链存储消耗，使土地记录搜索更快速高效。该框架还结合摘要文件与星际文件系统 IPFS，文件仅对交易授权方开放，保障隐私与安全。实验结果表明，该方法缩短了搜索时间，减少了主链存储需求，是区块链管理土地注册数据的可扩展高效方案。Li 等[66]提出面向智能社区的新型侧链结构与优化双向 PEG 协议，私有侧链处理本地注册与认证，本地主链实现与其他智能系统的信息共享。优化的双向 PEG 协议通过动态评估设备可信性（基于身份验证方法、历史记录、本地结果等标准），防止认证数据共享中的无用信息注入攻击。

路宇轩等[67]基于侧链思路提出多链共识方法 MC-RHotStuff，将节点划分为待准入节点、备选节点与共识节点，每条工作链配备共识节点与备选节点，并引入协作链机制。

实验证明，该方法较现有系统的交易吞吐量与延迟综合提升约 15%。

蔡维德[68]教授团队根据侧链思想提出的 ABC/TBC 双链结构。该方案的 ABC 链属于私有链，记录机构内部信息，TBC 链属于公链，记录 ABC 链之间的交易信息。该双链结构能够有效实现不同机构的数据共享。

星际文件系统（IPFS）[69]通过提供去中心化的对等文件存储解决方案来应对区块链存储挑战。IPFS 并非直接在区块链上存储大文件，而是通过分布式网络离数据通过链存储，并借助加密哈希（CID）与区块链链接。这种方式既能降低链上存储成本、避免数据膨胀，又能确保数据的完整性、不变性与可访问性[70]。

Medina 等[71]提出了一种可扩展且经济高效的区块链系统，通过将离链存储的数据聚合、压缩技术与 IPFS 相结合，有效提升存储容量并解决区块链网络事务吞吐量低的问题。该方案同时增强了数据持久性，确保离链数据具备更高可用性。类似地，Kaur 等人[72]建议将 IPFS 作为离链存储方案，以降低区块链节点的存储成本。与在链上存储完整交易细节不同，该方案仅在区块链上记录数据的加密哈希，大幅减少了存储需求。另一种创新方法是为多视图系统设计的区块链碎片存储概念[73]，该方法通过图像拼接技术减少 IPFS 的存储开销及区块链上存储的哈希数量，还采用改进的 Shamir 秘密共享方案将交易数据分割为多个份额并生成 n 个数据块，进一步减轻单个节点的存储负担。这些方案通过优化数据存储、提升可扩展性与降低成本，共同应对区块链存储挑战。

综上所述，众多学者在区块链的存储结构扩展上做了许多的研究，但针对特定的方面的链式结构缺研究很少，因此本文将在借鉴的基础上构建证件照数据存储的结构模型。

1.3 研究内容

本文首先概述了电子政务场景的证件照数据存储和共享模型的研究背景与重要意义，分析了其在提升政务办事效率和打破“数据孤岛”的关键作用，提出了当前证件照数据存储与共享面临的问题，特别是数据共享安全和存储效率方面的挑战。其次探讨了区块链在数据存储与共享领域的优势，分析了限制模型效率的因素，即区块链的核心，共识算法和链式结构。在联盟链场景下，根据联盟链对更高效共识算法的需求，对 PBFT 共识算法进行优化研究，结合具体场景，提出 DLR_PBFT 共识算法和 GD_RHotStuff 共识算法。分析证件照数据存储与共享流程，设计高效的存储与共享 MBC/WBC 多链，并搭建基于优化共识算法的证件照数据存储和共享模型。本文的主要内容包括：

（1）基于 PBFT 共识算法优化研究。为了满足搭建高效率的证件照数据存储和共享模型，作为模型的核心共识算法，需要满足高安全、高效率及抗恶意节点的能力。融合 BLS 门限签名、节点分层策略与信誉值机制，提出 DLR_PBFT。设计对比实验，验证 DLR_PBFT 在共识时延、吞吐量和容错能力的表现情况。