智能系统学报
CAAI TRANSACTIONS ON INTELLIGENT SYSTEMS

一种基于区块链技术的公安执法电子证据系统的设计与实现

王琪, 张嘉政, 刘文奇

引用本文:
王琪,张嘉政,刘文奇. 一种基于区块链技术的公安执法电子证据系统的设计与实现[J]. 智能系统学报, 2022, 17(6): 1182–1193.
WANG Qi,ZHANG Jiazheng,LIU Wenqi. Design and implementation of a public security law enforcement electronic evidence system based on blockchain technology[J]. *CAAI Transactions on Intelligent Systems*, 2022, 17(6): 1182–1193.

在线阅读 View online: https://dx.doi.org/10.11992/tis.202112034

DOI: 10.11992/tis.202112034
网络出版地址: https://kns.cnki.net/kcms/detail/23.1538.TP.20221014.1708.002.html

一种基于区块链技术的公安执法电子证据系统的设计与实现

王琪[1], 张嘉政[2], 刘文奇[1]

(1. 昆明理工大学 数据科学研究中心, 云南 昆明 650500; 2. 昆明理工大学 云南省计算机技术应用重点实验室, 云南 昆明 650504)

摘 要: 针对公安执法环境的复杂性和电子证据取证及证据固定的困难, 根据公安执法场景中电子证据的功能需求, 创建了一类基于区块链技术的公安执法电子证据模型的原型系统。该系统具备分布式、不可篡改、可溯源和安全性高等特点, 较好地解决了公安执法电子证据在取证和诉讼中证据的易变性、逻辑混乱和时间不一致等核心问题。该系统将执法过程中涉及举证的数据上链, 通过改进实用拜占庭将军容错(practical byzantine fault tolerance, PBFT)共识算法来监测试图篡改执法数据的行为, 利用层级监管特性启动备用共识节点以提高整体效率, 基于星际文件系统 (interplanetary file system, IPFS) 对超大文件上链进行数据存储, 有利于公安系统在处理大型数据信息时做到及时、安全与高效。最后通过公安局办案大厅执法场景的测试与分析, 验证了该系统的可行性。该系统的应用可赋能公安执法电子证据举证效力的提升和司法领域反腐倡廉, 并为案件侦破的串并案智能化提供可靠的数据基础。

关键词: 区块链; 电子证据; 分布式存储; PBFT 共识算法; 数据库; 异构共识; 数据差分; 公安执法
中图分类号: TP391 **文献标志码:** A **文章编号:** 1673−4785(2022)06−1182−12

中文引用格式: 王琪, 张嘉政, 刘文奇. 一种基于区块链技术的公安执法电子证据系统的设计与实现 [J]. 智能系统学报, 2022, 17(6): 1182–1193.
英文引用格式: WANG Qi, ZHANG Jiazheng, LIU Wenqi. Design and implementation of a public security law enforcement electronic evidence system based on blockchain technology[J]. CAAI transactions on intelligent systems, 2022, 17(6): 1182–1193.

Design and implementation of a public security law enforcement electronic evidence system based on blockchain technology

WANG Qi[1], ZHANG Jiazheng[2], LIU Wenqi[1]

(1. Center of Data Science, Kunming University of Science and Technology, Kunming 650500, China; 2. Yunnan Provincial Key Laboratory of Computer Technology Application, Kunming University of Science and Technology, Kunming 650504, China)

Abstract: We developed a prototype system for law enforcement electronic evidence data based on blockchain technology, focusing on the complexity of the law enforcement environment, the difficulties of electronic evidence collection and evidence fixation, and the functional requirements of electronic evidence in the scene of public security law enforcement. The system is distributed, non-tamperable, and traceable with a high level of security. It addresses the fundamental issues of variability, logic confusion, and time inconsistency in law enforcement electronic evidence collection and litigation for police. The system uploads the data involved in the law enforcement process to the chain, monitors the behavior of those attempting to tamper with the law enforcement data by improving the practical byzantine fault tolerance consensus algorithm, and uses the hierarchical supervision feature to activate the standby consensus node to improve overall efficiency. Based on the interplanetary file system, large files are uploaded to the chain and stored, which allows the public security system to process large-scale data in a timely, safe, and efficient manner. The feasibility of our system is validated by the test and analysis of the law enforcement scene in the case-handling hall of the public security bureau. The use of this system has the potential to improve the performance of law enforcement and anti-corruption efforts in the judicial field and provide a credible data foundation for the intelligentization of serial and parallel case detection.

Keywords: blockchain; electronic evidence; distributed storage; PBFT consensus algorithm; database; heterogeneous consensus; data difference; police law enforcement

电子证据是随着电子科技不断发展出现的一种全新的证据形式, 它属于传统证据的范畴[1]。电子证据解决了纸质证据中可能会出现的信息丢失、难获取等问题, 但也更容易被删除、篡改和转移。因此, 传统电子证据的完整性、客观性

收稿日期: 2021−12−15. **网络出版日期:** 2022−10−17.
基金项目: 国家自然科学基金项目(11971211,61573173).
通信作者: 刘文奇. E-mail: liuwenq2215@sina.com.

及认定标准还不足, 降低了传统电子证据的可信性, 电子证据举证效力低已成为当前电子证据系统的痛点[2-3]。公安执法业务中电子证据的获取和固定是司法过程中案件调查取证的重要环节, 其技术措施是电子证据举证效力的重要保证。长期以来, 由于公安执法过程复杂, 执法环境多变, 带来电子证据的取证和证据固定等诸多困难。在多变的公安执法环境中, 通信和取证设备性能不稳定, 容易导致在取证系统中某些节点出现宕机现象, 从而影响取证和证据固定。

区块链由是分布式存储、点对点交易、采用密码学和共识算法等技术的一种新型分布式数字账本。其特点是去中心化、极难篡改、安全可靠、可追溯性、公开透明等, 这些特点可用于解决网络上节点间信息不对称问题, 从而实现多个主体间的协作与彼此信任。例如, 在金融领域, 自从比特币开启了去中心化的 P2P 时代[4], 区块链成为了数字加密货币体系的核心支撑技术。就计算机技术而言, 区块链技术包含分布式存储[5]、点对点网络[6]、密码学[7]、智能合约[8]、拜占庭容错[9] 等一系列复杂技术。2013 年末, 以太坊[10] 作为区块链 2.0 时代, 将每次与区块链的交互作为交易信息写入区块链中, 为比特币脚本语言中扩展性不足等问题提供了较好的解决方法。如今, 随着区块链 3.0 时代的到来, 将区块链技术扩展到了社会各领域的应用中, 推动了产业变革。中央政治局第十八次集体学习时提出要将区块链作为核心技术自主创新的重要突破口, 加快推动区块链技术和产业的创新发展, 由此可见, 中国政府也将从国家战略层面全面推动区块链技术的发展和应用。

本文主要致力于将区块链技术与电子证据结合应用于公安执法。针对现有执法取证技术的不足, 结合区块链分布式存储结构的特点, 设计基于区块链的公安执法电子证据的数据模型, 通过改进的 PBFT 共识算法, 解决复杂执法环境下宕机问题和大规模文件传输困难, 并对真实的执法记录进行实证检测, 验证了电子证据取证的可靠性。通过区块链技术的不可篡改特性能够避免在公安执法过程中可能出现的警务人员滥用职权等问题, 去中心化特性又可消除现有公安数据库的中心化存储方式和加密方式的各种弊端, 从而降低电子证据采信带来的司法风险[11]。在数字化的时代, 通过公安执法电子证据区块链系统的使用, 使公安执法过程更加透明, 电子证据的可信度和办案效率得到提高, 有利于提升公安执法的公信力, 为公安行业反腐倡廉提供新的技术措施, 从而推动我国公安事业的技术进步。

1　公安执法电子证据区块链系统

1.1　区块链

区块链是由存放数据的区块根据时间先后顺序以及密码学方法串联起来的分布式结构列表, 它以对等网络(peer-to-peer network, P2P)作为其通信载体, 以时间戳、共识算法、哈希值、智能合约等来保证数据的安全与一致性。区块链作为一种典型的去中心化分布式数据库账本, 解决了在不可信环境中数据管理的可信问题[12]。其采用去中心化的数据管理模式, 让数据安全更有保障, 让各节点在互不了解、互不信任的情况下实现点对点交易, 从而为中心化机构数据存储普遍存在的高内存、高风险等问题提供了新的解决方案[13-15]。

区块链的共享性使得每一个参与方都可以下载完整的账本, 相比较传统的记账方式而言, 降低了多副本维护数据的成本, 同时提高了访问效率, 这样可以更好地规避公安执法中存在的不合理现状, 如公安人员的执法不严、滥用职权、伪造证据等问题。一个完整的区块链包括区块头和区块体两部分, 如图 1 所示。它以区块为单位, 通过时间戳技术明确执法数据生成的先后顺序, 并证实存放进区块中的数据在某一个特定时间点上是真实存在的; 采用链式结构对数据进行存储和校验, 让每个区块上的信息依顺序相连接, 采用 Merkle 树保证数据的不可篡改, 后一区块总是通过 pre-Hash 来保存前一个区块的 Hash 值, 所以任何一方想篡改执法案例或数据几乎是不可能的, 同时大大减少了信息在区块上的存储量。由此, 区块链技术在数据的安全性、可用性和真实性方面都能得到极大的保证[16]。

数据的安全性是以密码学算法给予保障的一种分布式数据库账本, 该账本具有非篡改、防伪造等特性, 通过把区块链特性运用到公安事业中, 对警察角色明晰化、公安机关职能转变和执法规范化建设等都提出了新的要求[17], 更好地完善公安执法体系的同时还会使之更加安全、方便、有效、快捷。

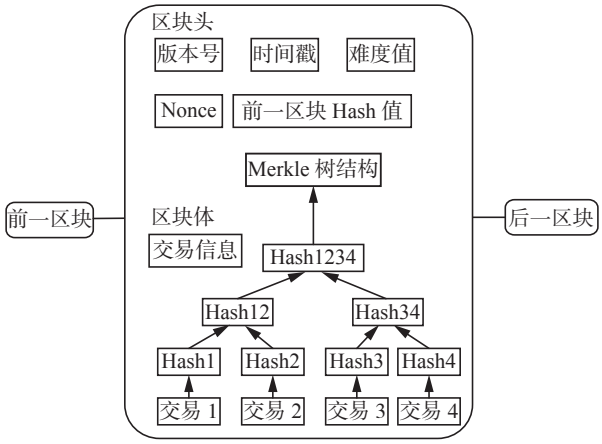

图 1　区块链结构

Fig. 1　Blockchain structure

1.2　“电子证据+区块链”影响因素分析

把区块链技术和电子证据相结合，将互联网中收集到的电子证据以及所产生的日志记录等通过哈希算法得出唯一的哈希值后传至链中，进行数据的封装固定及保存。通过比较区块中唯一的哈希值，便可知道证据是否经过篡改，在审查时确保了证据的可靠性、完整性和真实性，不再只以公证机构的纸质证明作为背书[18-20]，把有效信息全部写进区块链里进行公证，做到信息的全透明化。这样一来，当事人对案件的真实性认可提高，找公证处再次认证的概率降低，大幅度缩短了证据验证的时间，合法和关联性也更强，提高了司法效率，所以说，区块链技术与电子证据相结合是当前阶段电子证据变革的重要趋势之一。

从未来发展的情况来看，公安在执法活动中可以将电子证据转化为判案依据的标准，但就目前来说，尚缺乏科学的保管，导致有些电子证据被损坏且无法进行倒查。两种技术的结合正好可以弥补当前电子证据在真实性和安全性方面上的缺陷。此外，利用区块链中的智能合约还能够对电子证据进行法律的监管，降低公证处人员存在非法操作的风险。

综合来看，加入区块链技术，会从不同层面上展现出二者结合后的优势及影响力。虽然目前我国对区块链技术的发展还处于逐步探索阶段，但是“区块链+电子证据”技术的应用对整个司法体系带来的影响是可观的。

1.3　公安执法电子证据区块链系统

公安执法电子证据不仅包括在处警过程中的数据采集系统获得的警用执法记录仪、相关执法系统中获取的电子数据等，还包括警员在执法过程中取得的人证、物证等相关执法数据[21]。公安执法电子证据区块链采用 P2P 网络来组织和散布系统中所有要参与验证的数据节点[22]，从而实现系统的去中心化。

为了保证系统内数据的法律效力，上链的代码必须要在法律上进行有效验证，同时系统内区块链上的每个节点都保存着自己的本地数据。基于此，本文构建了基于公安执法电子证据区块链系统的服务子系统，其结构如图 2 所示。

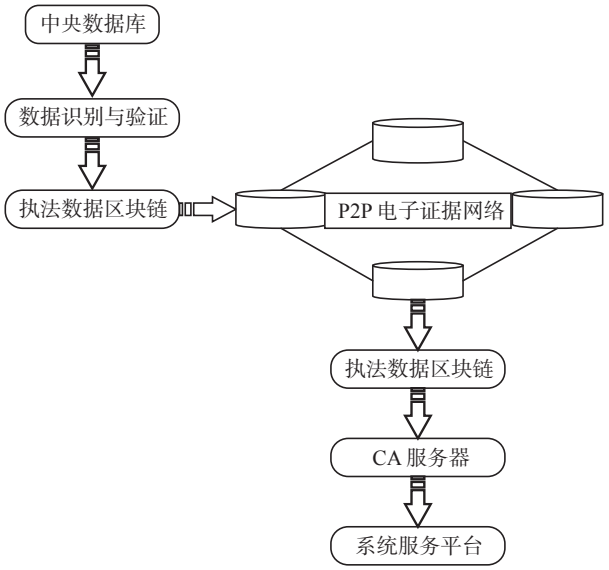

图 2　公安执法电子证据区块链系统的服务子系统结构

Fig. 2　Service subsystem structure of the electronic evidence blockchain system for public security law enforcement

在公安执法电子证据区块链系统的服务子系统中，由市公安局作为服务中心进行统一部署，区县局及所属各派出所机构的数据业务部门应以统一的方式服务于各级领导、警务人员、公安执法办案人员、场所管理员等，并将各级公安局内的执法数据进行统一的管理，从而实现市、区/县、派出所三级监管和应用，为执法办案中心提供系统总体呈现，具体如图 3 所示。

2　PBFT 共识算法的改进及其应用实现

2.1　基于 PBFT 共识算法的改进

本小节主要对 PBFT 共识算法做了改进，为了使共识的量化指标能够更清晰地展示，在这里还与 RAFT 算法进行了对比，从而找到了一个更适合该场景应用的算法。

在 PBFT 算法中，共识节点不仅需要与主节点通信，还需要与其他共识节点进行通信，共识协议流程图如图 4 所示。

在该过程中，需要经历预准备–准备–提交 3 个阶段。成功完成一轮共识之后，接着开始进行下一轮的共识过程。

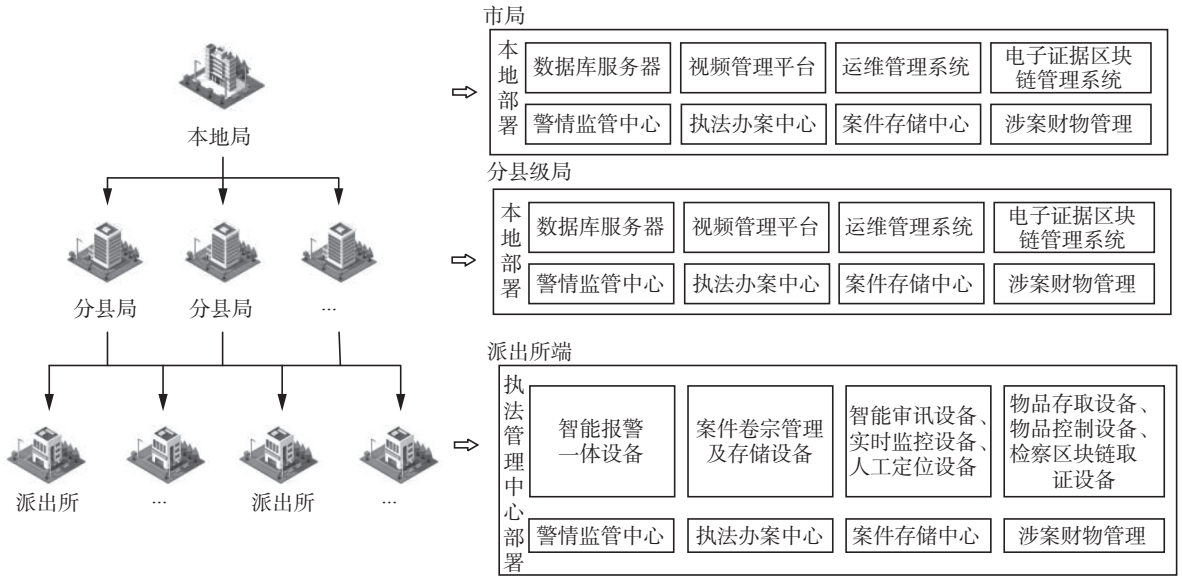

图 3　公安执法电子证据区块链服务子系统总体部署

Fig. 3　Overall deployment of the electronic evidence blockchain service subsystem for public security law enforcement

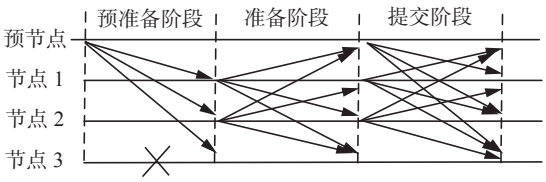

图 4　PBFT 共识协议流程图

Fig. 4　PBFT consensus protocol flow chart

而 RAFT 算法, 共识协议只需要领导者选举、日志复制两阶段即可, 共识协议流程图如图 5 所示。

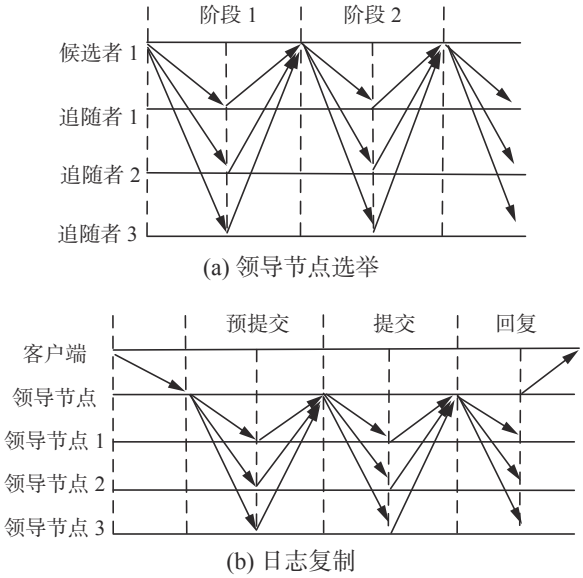

图 5　RAFT 共识协议流程图

Fig. 5　RAFT consensus protocol flow chart

在领导者选举过程中, 通过强调领导者来简化整个共识过程; 在日志复制过程中, 如果追随者收到了由客户端发出的集群, 会直接转发给领导者, 从而确保所有节点状态的一致性。

在公安执法电子证据区块链系统中, 因为出警的执法记录数据是需要到达业务层的, 所以在准备阶段不需要其他节点向主节点发送数据, 同时在主节点投票阶段, 向n个本级节点和$n-1$个上级节点发送共识请求, 若出现故障或超时未响应, 则上级的两个节点可以取代本级节点投票, 这样既可以保证安全性, 又避免了节点因出现故障时导致无响应共识减缓办事效率的问题。对改进算法的共识过程如图 6 所示。

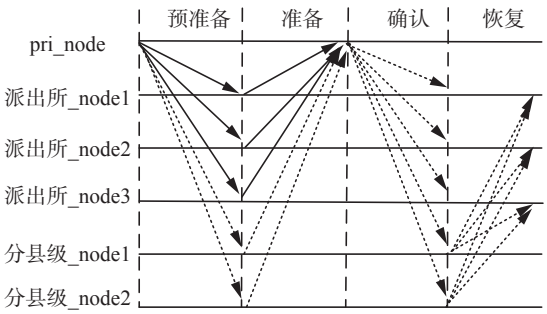

图 6　改进后算法的共识过程

Fig. 6　Consensus process of the improved algorithm

具体流程(以派出所和分县级为例):

预准备: pri_node 向派出所_node 及上级分县级_node 广播预准备消息。通过后主节点 pri_node 进入准备状态。

准备: pri_node 接收来自所有发送广播的节点反馈, 若是本级节点出现故障则直接考虑上级节点(图 6 中虚线部分), 若本级节点全反馈则不接收其他节点反馈。

确认: pri_node 选择性地给确认阶段发送接收的反馈的节点, 并非提交全部节点。

恢复:(此项为可选,当且仅当上述步骤中本级节点宕机、由上级节点代理参与共识时)pri_node 提交给上级节点后,由上级节点给原本需要参与共识的节点进行数据恢复并保持一致性。

现对当前适用于本场景应用的算法就吞吐量和时延做了如下实验。

将共识节点数量固定为 7 个,系统从 0~500 s 不断发出请求下的吞吐量,重复进行了 5 000 次测试,取平均值,实验结果如图 7 所示。

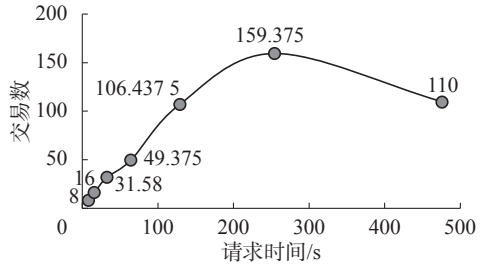

图 7　吞吐量实验

Fig. 7　Throughput experiment

可以看到,随着访问请求时间的加快,每秒交易次数也随之增加。当请求时间约超过 260 s 后吞吐量呈下降趋势。

同样保证 7 个共识节点,在相同的出块间隔内进行了 5 000 次测试,实验结果如图 8 所示。

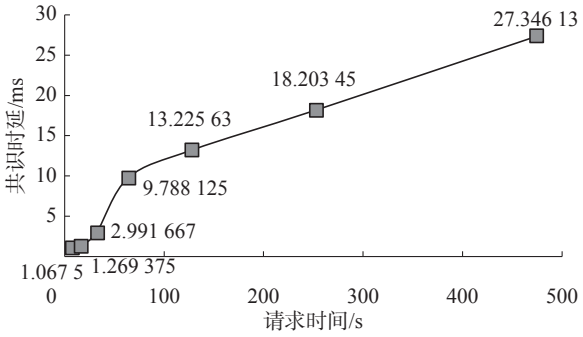

图 8　共识时延实验

Fig. 8　Consensus delay experiment

可以看到,在应用到公安执法系统网络环境中,随着每秒访问请求的增加,单次共识所需的时延不会大幅度增加。这说明在实际的应用过程中,就算在短时间内需要对大量信息进行处理,系统内的时延也能有较好的表现。

此外,利用层级监管特性进行“备用”共识节点设置,以提高整体效率。当有故障节点存在时,系统内会自动出现候补节点进行补充,为了更清晰直观地展示,用改进后的算法与 PBFT、RAFT 算法做了对比,进行了 10 轮共识测试,实验结果如图 9 所示。

为了保证活性,PBFT 算法中需要有$2f+1$个正常节点 (其中f为故障节点),即能够容忍故障节点的数量不超过1/3,并且延迟不会无限增长。RAFT 算法能够容忍故障节点的最大数量为$(N-1)/2$(其中N为节点总数量)。可以看到,当出现 1 个故障节点时,PBFT 算法在共识测试中耗时为 0 ms,即系统不工作;当故障节点大于 2 开始,PBFT 和 RAFT 算法因故障节点数超过了最低限度,所以不再进行工作。而改进后的算法因为出现候补节点,在系统内依然可以正常运作。

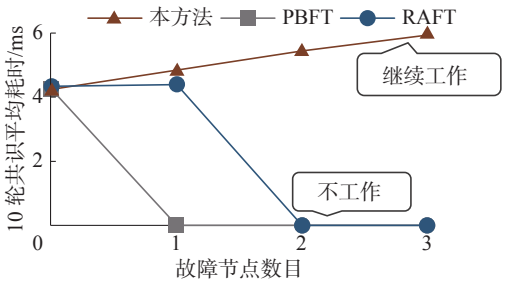

图 9　故障节点数对比

Fig. 9　Comparison of the number of failed nodes

通过上述实验,将基于 PBFT 改进后的算法应用到公安执法系统中验证了改进算法的可行性。

2.2　基于改进 PBFT 算法在实际场景下的应用

本节主要结合区块链 PBFT 共识算法对公安执法做相关应用,防止有警员增删执法记录仪内容的风险,实现对执法记录仪的进一步追溯与高效管控。警员出警回办案大厅后,将涉案警员与相应人证同时分隔在不同的房间内(为了遵循案件排他原则,回避与该警员有关人证),利用共识算法,对该警员的出警内容进行校验,若大于 2/3 的人证赞同此警员的出警记录,系统将自动对其进行容错,说明该记录无问题,提交该内容;若低于 2/3 的人证对此记录进行否认,根据共识算法,系统将不再运行,该记录不被通过,投入新一轮的验证,有效保证了执法信息在上传数据过程中的透明性与完整性,使可篡改几乎成为不可能。

本节基于改进的 PBFT 算法,在单机环境下模拟了 1 个主节点和 3 个从节点进行加入和离开。分别进行了存在一个故障节点和两个故障节点这两组实验。

1) 当存在一个故障节点 (N_1) 时。客户端发送警员赵一清的执法数据信息,这时若有一个人证对赵一清的执法信息给出了否认意见,根据客户端的运行结果,且由公式$n \geqslant 3f+1$和 PBFT 算法的容错性,虽然显示故障节点N_1连接失败,但系统仍然会保持顺利运行。具体如图 10、11 所示。

主节点已接收到客户端发来的request ...
已将request存入临时消息池
正在向其他节点进行进行PrePrepare广播 ...
PrePrepare广播完成
本节点已接收到N_3节点发来的Prepare ...
本节点已接收到N_2节点发来的Prepare ...
本节点已收到至少2f个节点(包括本地节点)发来的Prepare信息 ...
正在进行commit广播
commit广播完成
本节点已接收到N_3节点发来的Commit ...
本节点已接收到N_2节点发来的Commit ...
本节点已收到至少2f+1 个节点(包括本地节点)发来的Commit信息 ...
N_0节点已将msgid:6897843394存入本地消息池中,消息内容为：'20210314002', '赵一清', '云A****2', '002', '云南省昆明市西山区'
正在reply客户端 ...
reply完毕
2021/03/24 04:49:24 connect error dial tcp 127.0.0.1:8001: connectex: No connection could be made because the target machine actively refused it.
2021/03/24 04:49:24 connect error dial tcp 127.0.0.1:8001: connectex: No connection could be made because the target machine actively refused it.

图 10　主节点运行效果且故障节点连接失败

Fig. 10　Running effect of the master nodes showing connection failure to the faulty node

本节点已接收到主节点发来的PrePrepare ...
已将消息存入临时节点池
正在进行Prepare广播 ...
Prepare广播完成
本节点已接收到N_3节点发来的Prepare ...
本节点已收到至少2f个节点(包括本地节点)发来的Prepare信息 ...
正在进行commit广播
commit广播完成
本节点已接收到N_3节点发来的Commit ...
本节点已接收到N_0节点发来的Commit ...
本节点已收到至少2f+1 个节点(包括本地节点)发来的Commit信息...
N_2节点已将msgid:6897843394存入本地消息池中,消息内容为：'20210314002', '赵一清','云A****2', '002','云南省昆明市西山区'
正在reply客户端...
reply完毕
2021/03/24 04:49:24 connect error dial tcp 127.0.0.1:8001: connectex: No connection could be made because the target machine actively refused it.
2021/03/24 04:49:24 connect error dial tcp 127.0.0.1:8001: connectex: No connection could be made because the target machine actively refused it.

图 11　故障节点存在下从节点效果

Fig. 11　Running effect of the slave node with faulty nodes

2) 当存在两个故障节点 (N_2、N_3) 时。即客户端发送警员赵一清的执法信息记录, 有两个人证对赵一清的执法信息数据持有否定意见, 根据共识算法, 这时客户端会直接显示未接收到相应的返回数据, 主节点也会显示连接失败的两个故障节点。不难看出, 如果有大于 2/3 的人对其信息内容持有怀疑态度时, 由于超出节点数量, 消息进行到准备阶段后, 不会再接收到满足数量的节点信息, 系统内不会对此信息进行确认, 客户端接收不到回复, 故达不成一致, 说明赵一清警员的执法记录信息是有问题的。具体如图 12、13 所示。

主节点已接收到客户端发来的request ...
已将request存入临时消息池
正在向其他节点进行进行PrePrepare广播...
PrePrepare广播完成
本节点已接收到N_2节点发来的Prepare ...
2021/03/24 04:51:33 connect error dial tcp 127.0.0.1:8001: connectex: No connection could be made because the target machine actively refused it.
2021/03/24 04:51:33 connect error dial tcp 127.0.0.1:8003: connectex: No connection could be made because the target machine actively refused it.

图 12　主节点效果且显示连接失败的两个故障节点

Fig. 12　Running effect of the master node showing connection failure with two faulty nodes

本节点已接收到主节点发来的PrePrepare ...
已将消息存入临时节点池
正在进行Prepare广播...
Prepare广播完成
2021/03/24 04:51:33 connect error dial tcp 127.0.0.1:8003: connectex: No connection could be made because the target machine actively refused it.
2021/03/24 04:51:33 connect error dial tcp 127.0.0.1:8001: connectex: No connection could be made because the target machine actively refused it.

图 13　其中一个从节点运行效果

Fig. 13　Running effect of a slave node

2.3　对较大数据量上链实验的研究与分析

本节主要基于星际文件系统 (interplanetary file system, IPFS) 来测试在面对较大数据量时数据上链的实验。在本次实验中本文构建了一个私有的 IPFS 网络，仅针对授权的各级别警务人员使用。

本次实验涉及到相对规模从小、中、大 3 种数据记录文件作为实验集，分别将大小为 275 MB 的派出所端电子存证信息、844 MB 的分县局级电子存证信息以及 1.2 GB 的市局电子存证信息上传至 IPFS 端。

派出所端电子存证信息的唯一标识符为 QmUg…e3j6 (46 位)，如图 14 所示，在 IPFS 系统中检查可以看到 links 等更多信息；分县局级电子存证信息的唯一标识符 QmU2…87j9 (46 位)，如图 15 所示，在 IPFS 系统中检查可以看到 links 等更多信息；市级电子存证信息的唯一标识符为 Qmdz…9sCd (46 位)，如图 16 所示。

```
ipfs add 派出所端电子存证信息.sql
275 MiB / 275 MiB [=============================================================]
added QmUg6oJjNDQccgFVwpw1eUvEAUM4PU5LyLc8K7VL2qe3j6 派出所端电子存证信息.sql
275 MiB /275 MiB[=============================================================]
```

图 14　派出所端电子存证信息获取唯一标识

Fig. 14　Unique identification for polices station electronic information access

```
ipfs add 分县局级电子存证信息.sql
844.59 MiB / 844.59 MiB [=============================================] 100.00%
added QmU2Dh1BG5WfACAzRAyXa6WR5CjJrLmb39gkVaAQhW87j9 分县局级电子存证信息.sql
844.59 MiB / 844.59 MiB[=============================================] 100.00%
```

图 15　分县局级电子存证信息获取唯一标识

Fig. 15　Unique identification for sub-county bureau level electronic storage information access

```
ipfs add 市级电子存证信息.sql
1.2 GB / 1.2 GB [=============================================================] 100.00%
added Qmdz3n6fCAZznybVpvaPzEpUpQUY9aafDNXM1JaZYd9sCd 市级电子存证信息.sql
1.2 GB / 1.2 GB[=============================================================] 100.00%
```

图 16　市级电子存证信息获取唯一标识

Fig. 16　Unique identification for municipal electronic storage information access

各级别警务人员在 IPFS 系统中上传执法信息后，得到对应数据的唯一 CID，对其进行校验检查可以发现大型数据文件上传到 IPFS 后会被分成多个 links，links 下还会有更多子集，直到数据被分为 250 kb 的小块进行分布式存储。数据存证的安全性是通过聚合哈希来加以保障，各级部门对某一数据进行取证时仅需通过对应的 CID 即可进行下载查询，并且分布式存储的天然优势可以抵御单点攻击带来的破坏。

此实验结合了 IPFS 和区块链，用户通过 IPFS 处理大量警务数据信息，将其对应的加密哈希存储进区块链内，无需再将数据放在链上，节省网络带宽的同时还能够对数据加以保护，也证明了 IPFS 可填补区块链系统在文件存储方面的短板。

3　公安执法电子证据区块链系统的数据模型与系统功能测试

公安执法电子证据区块链（blockchain of electronic evidences of law enforcement police, BELEP）模型设计的目标是：1) 防范在执法办案中可能出现的刑讯逼供、伪造和篡改电子证据等行为；2) 保证办案过程的电子记录得以真实、完整地保留；3) 保证数据备份和证据链的完整性、电子证据记录发生改变的可溯源性。

在此模型下，每个节点都是整个系统的一部分，通过 P2P 网络对区块中各节点完成数据的传输，使新区块追加到原有区块中，完成区块的确认工作。

在数据模型中，存证人员需向中央数据库上传数据，输入 ID 号、执法的案件名称和电子证据进行权限验证，一旦通过系统中的校验，就可以直接与公安执法电子证据系统服务平台进行交互，系统服务平台向各节点提供由存证人员上传的出警任务序号、警用车牌号、执法记录仪编号和执法人员姓名这四类信息。一方面，存证人员和中央数据库之间的操作须有系统服务平台提供的权限认证；另一方面，公安人员向系统平台提

供执法信息的 ID 号、执法的案件名称和现实证据, 经权限验证, 通过后即可上传至系统服务平台, 同时管理员也可以进行相应的取证, 存储到中央数据库中。具体模型如图 17 所示。

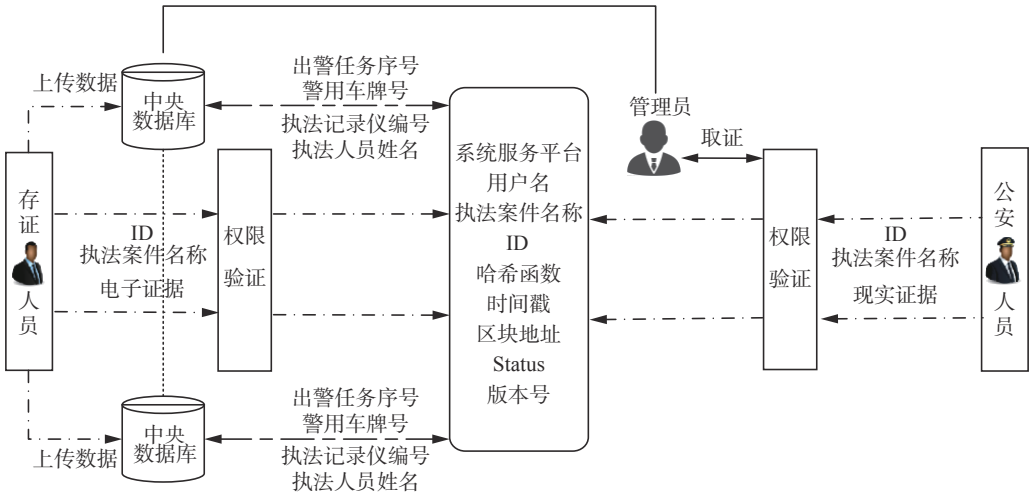

图 17　BELEP 模型

Fig. 17　Model of BELEP

进入系统中, 首先确定需要读取哪一级的公安数据库, 把全部信息都加载进区块链内, 通过 Hash 函数来验证是否上链成功。接着在系统中输入相应的出警任务号、警用车牌号和其他执法信息, 系统会自动进行逐块检验, 如验证成功, 则直接将数据信息传至链上, 载入进区块中, 最终写入服务器, 完成对此执法信息的加载。具体流程如图 18 所示。

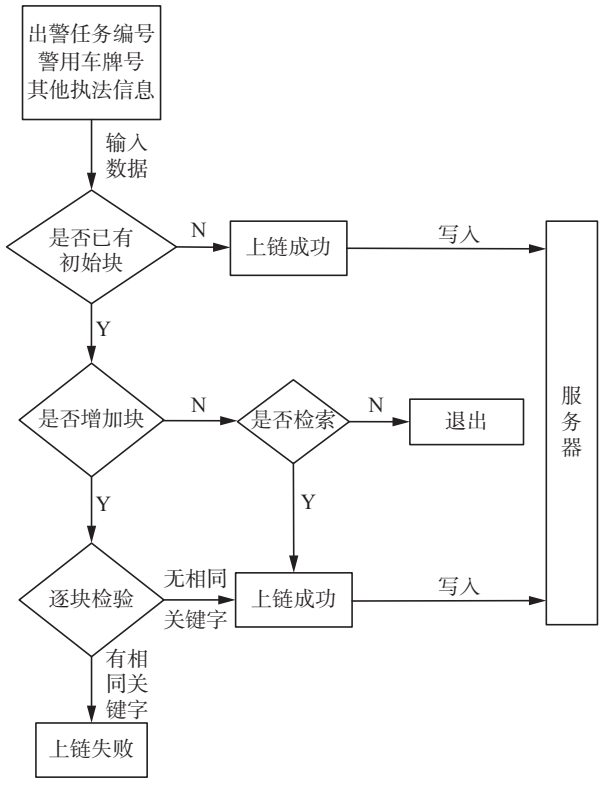

图 18　系统对数据信息的检验与存储

Fig. 18　Data verification and storage of the system

为了验证基于区块链电子证据公安执法模型设计的可行性, 整个系统体系将依赖于公安数据库和现有的数据仓库架构[23-24], 且遵从电子证据在法律上的要求和规定, 再利用区块链技术对数据进行分布式存储。

现以数据库中截取五位公安执法人员的信息为例, 来进行模拟实验的验证及展示系统的运行效果。截取人员的信息整理如表 1 所示。

以系统中对市、县、派出所这三级公安数据库端来说, 在出警前, 执法人员把各自对应的出警任务编号输入到系统中, 系统会自动对出警人员的执法记录号进行取模运算, 由此来判断调用的是哪一级的数据库。警员输入各自的姓名与密码, 待验证通过后, 进入系统的登录界面, 进行身份的验证。首先, 将截取的五位公安执法人员的每条信息分别形成一个节点区块, 数据库中的其他人员信息(节点区块)会对其进行共识认证及校验, 通过验证后会自动将此节点添加至链的尾端, 形成新的最长链。按照系统的总体部署, 从公安各级派出所端、分县局端和市局端, 将数据库中现有的数据上链, 加载进区块链中。加入过程分别如图 19~21 所示。

根据区块链的不可篡改性, 无论是哪一级数据库中的数据信息, 管理员都无权进行增删[25], 若想试图尝试对链上的数据进行修改, 则 Hash 函数会立马发生变化, 校验不通过, 修改信息失败。此外, BELEP 模型还支持自定义存储数据库, 即可以在链上添加新数据, 数据库会进行同步跟进。

表 1　数据库信息表

Table 1　Database information table

出警任务编号	警用车牌号	执法记录仪编号	执法人员姓名	执法地点
20210310001	云A****1	1	王明	云南省昆明市呈贡区
20210310002	云A****2	2	李江	云南省昆明市西山区
20210310003	云A****3	3	赵雷	云南省昆明市呈贡区
20210310004	云A****4	4	王一泽	云南省昆明市五华区
20210310005	云A****5	5	张浩	云南省昆明市西山区

注: 表中信息都为参考数据, 不是真实数据

图 19　派出所端证据区块链

Fig. 19　Police station evidence blockchain

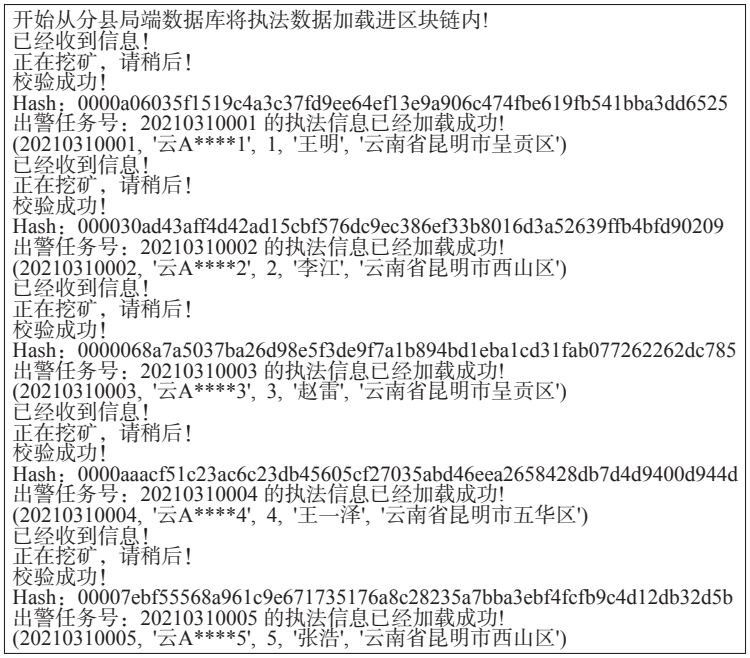

图 20　分县局端证据区块链

Fig. 20　County bureau evidence blockchain

```
开始从市局端数据库将执法数据加载进区块链内!
已经收到信息!
正在挖矿，请稍后!
校验成功!
Hash：0000eba6154b7b2b2304cab48e3c47389a858d4993ece73e375b3ab39c685df8
出警任务号：20210310001 的执法信息已经加载成功!
(20210310001, '云A****1', 1, '王明', '云南省昆明市呈贡区')
已经收到信息!
正在挖矿，请稍后!
校验成功!
Hash：0000c161c805d0e7eefd63ba521a446c257b2d706e5cab90c581f3bfbe14b6ee
出警任务号：20210310002 的执法信息已经加载成功!
(20210310002, '云A****2', 2, '李江', '云南省昆明市西山区')
已经收到信息!
正在挖矿，请稍后!
校验成功!
Hash：0000256e923a4c4c0d25963a8542e45ff0151bdb7a5fc8923196c1b148db2701
出警任务号：20210310003 的执法信息已经加载成功!
(20210310003, '云A****3', 3, '赵雷', '云南省昆明市呈贡区')
已经收到信息!
正在挖矿，请稍后!
校验成功!
Hash：00002d5a87242fa2d2acab7b7df81ce769b721e58f76f2552ef6e43d3539ee42
出警任务号：20210310004 的执法信息已经加载成功!
(20210310004, '云A****4', 4, '王一泽', '云南省昆明市五华区')
已经收到信息!
正在挖矿，请稍后!
校验成功!
Hash：0000337503e24d2b835feb5234295e175a4c9d3f8432dedb8f5fe439993f988e
出警任务号：20210310005 的执法信息已经加载成功!
(20210310005, '云A****5', 5, '张浩', '云南省昆明市西山区')
```

图 21　市局端证据区块链

Fig. 21　City bureau evidence blockchain

4　结束语

本文的主要研究与贡献如以下: 1) 将区块链技术与电子证据结合并应用到公安执法办案中。区块链技术弥补了电子证据的不足, 同时其不可篡改性在公安执法过程中避免会出现的非法操作问题, 在公安执法的透明化、规范化方面具有巨大的应用价值; 2) 就警务系统中容易出现未及时响应状况的特点做出基于 PBFT 共识的改进方法, 利用层级监管特性设置备用共识节点以提高整体效率, 表征为系统中出现故障或超时未响应节点, 则上级节点可以取代本级节点投票, 既可保证系统的安全性, 又可避免因出现故障节点导致系统无响应的问题; 3) 基于 IPFS 分布式存储技术对超大文件实现上链技术并存储, 提高数据安全性与可靠性, 有利于公安系统在处理大型数据信息时做到及时、安全与高效; 4) 根据公安执法的环境和业务流程, 提出了 BELEP 模型, 并设计了公安执法电子证据区块链应用系统原型, 且支持自定义存储数据库, 只需将证据信息、相应的哈希摘要和密钥传至链上, 即可完成相应的数据存储及后期验证。实验以模拟截取数据库中部分数据信息为例, 结果与预期一致, 并通过模拟恶意行为对系统进行安全性检测。

通过上述技术创新, 在公安执法场景中充分发挥了区块链技术的优势。一方面, 通过区块链技术的应用, 提高了公安执法电子证据的法律效力, 提供了大数据时代公安执法体系反腐倡廉技术措施。另一方面, 通过区块链共识算法对执法记录信息进行复认和关联, 保障数据的真实和完整性, 并为公安案件侦破的串并案智能化奠定坚实的数据基础, 从而实现更高效的执法办案。

参考文献:

[1] 刘品新. 论电子证据的定位—基于中国现行证据法律的思辨 [J]. 法商研究, 2002, 19(4): 37–44.
LIU Pinxin. On the positioning of electronic evidence-based on the speculation of the current evidence law in China[J]. Studies in law and business, 2002, 19(4): 37–44.

[2] LOSAVIO M, ADAMS J, ROGERS M. Gap analysis: judicial experience and perception of electronic evidence[J]. Journal of digital forensic practice, 2006, 1(1): 13–17.

[3] 宁勇. 电子证据的基本问题与取证初探 [D]. 北京: 清华大学, 2005: 39−42.
NING Yong. An analysis of basic issues and collection of electronic evidence[D]. Beijing: Tsinghua University, 2005: 39−42.

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2018−04−10)[2021−12−15]. http: //bitcoins. info/bitcoin. pdf.

[5] Lynch N A. Distributed Algorithms[M]. Berlin: Springer, 1991.

[6] 张玉洁, 何明, 孟祥武. 基于用户需求的内容分发点对

点网络系统研究 [J]. 软件学报, 2014, 25(1): 98–117.
ZHANG Yujie, HE Ming, MENG Xiangwu. Research on CDN-P2P system over user requirements[J]. Journal of software, 2014, 25(1): 98–117.

[7] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE transactions on information theory, 1976, 22(6): 644–654.

[8] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展 [J]. 自动化学报, 2019, 45(3): 445–457.
OUYANG Liwei, WANG Shuai, YUAN Yong, et al. Smart contracts: architecture and research progresses[J]. Acta automatica sinica, 2019, 45(3): 445–457.

[9] LAMPORT L, SHOSTAK R, PEASE M. The byzantine generals problem[J]. Acm transactions on programming languages and systems, 1982, 4(3): 382–401.

[10] Ethereum White Paper. A next-generation smart contract and decentralized application platform[EB/OL]. (2015−11−12)[2021−12−15].https://github.com/ethereum/wiki/wiki/White-Paper.

[11] 刘学在, 阮崇翔. 区块链电子证据的研究与思考 [J]. 西北民族大学学报(哲学社会科学版), 2020(1): 52–59.
LIU Xuezai, Ruan Chongxiang. Research and reflection on blockchain electronic evidence[J]. Journal of Northwest Minzu University(philosophy and social sciences edition), 2020(1): 52–59.

[12] 于戈, 聂铁铮, 李晓华, 等. 区块链系统中的分布式数据管理技术-挑战与展望 [J]. 计算机学报, 2021, 44(1): 28–54.
YU Ge, NIE Tiezheng, LI Xiaohua, et al. Distributed data management technology in blockchain system-challenges and prospects[J]. Chinese journal of computers, 2021, 44(1): 28–54.

[13] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术 [J]. 计算机学报, 2021, 44(1): 84–131.
CAI Qiaoqing, DENG Yao, ZHANG Liang, et al. The principle and core technology of blockchain[J]. Chinese journal of computers, 2021, 44(1): 84–131.

[14] 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 Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: architecture and research progress[J]. Chinese journal of computers, 2018, 41(5): 969–988.

[15] 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 Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta automatica sinica, 2016, 42(4): 481–494.

[16] 袁勇, 王飞跃. 区块链理论与方法 [M]. 北京: 清华大学出版社, 2019: 36.
YUAN Yong, WANG Feiyue. Blockchain theory and methods[M]. Beijing: Tsinghua University Press, 2019: 36.

[17] 许韬, 梁亮. 法治语境下公安执法新要求探析 [J]. 人民论坛, 2012(11): 70–71.
XU Tao, LIANG Liang. An analysis of the new requirements of public security law enforcement in the context of rule of law[J]. People's tribune, 2012(11): 70–71.

[18] 毛荣. "区块链+电子证据保全"制度研究 [D]. 成都: 四川省社会科学院, 2019: 19−20.
MAO Rong. Research on the "blockchain + electronic evidence preservation" system[D]. Chengdu: Sichuan Academy of Social Sciences, 2019: 19−20.

[19] 赵雷. 网络证据保全公证存在的问题与策略研究 [J]. 法制与社会, 2016, 19: 129–130.
ZHAO Lei. Research on the existing problems and strategies of notarization of network evidence preservation[J]. Legal system and society, 2016, 19: 129–130.

[20] 许曼青. 浅谈互联网电子证据保全公证 [J]. 法制与社会, 2018, 1: 106–107.
XU Manqing. On the internet electronic evidence preservation notarization[J]. Legal system and society, 2018, 1: 106–107.

[21] 李萌, 刘文奇, 米允龙. 基于区块链的公共数据电子证据系统及关联性分析 [J]. 智能系统学报, 2019, 14(6): 1127–1137.
LI Meng, LIU Wenqi, MI Yunlong. An electronic evidence system based on blockchain and correlation analysis[J]. CAAI transactions on intelligent systems, 2019, 14(6): 1127–1137.

[22] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望 [J]. 自动化学报, 2018, 44(11): 2011–2022.
YUAN Yong, NI Xiaochun, ZENG Shuai, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta automatica sinica, 2018, 44(11): 2011–2022.

[23] 刘文奇. 复杂网络上的公共数据演化博弈与数据质量控制 [J]. 中国科学:信息科学, 2016, 46(11): 1569–1590.
LIU Wenqi. Public data evolution games on complex networks and data quality control[J]. Scientia sinica informationis, 2016, 46(11): 1569–1590.

[24] 刘文奇. 中国公共数据库数据质量控制模型体系及实证 [J]. 中国科学:信息科学, 2014, 44(7): 836–856.
LIU Wenqi. Modeling data quality control system for Chinese public database and its empirical analysis[J]. Scientia sinica informationis, 2014, 44(7): 836–856.

[25] 刘欣亮, 黄涛, 张志勇. 面向开放互联网的多媒体数字

版权保护系统 [J]. 计算机工程与设计, 2015, 36(2): 363–368.

LIU Xinliang, HUANG Tao, ZHANG Zhiyong. Multimedia digital rights management system for open internet[J]. Computer engineering and design, 2015, 36(2): 363–368.

作者简介:

王琪, 硕士研究生, 主要研究方向为区块链、电子证据相关技术。

张嘉政, 硕士研究生, 主要研究方向为区块链技术、可信计算。

刘文奇, 教授, 博士生导师, 主要研究方向为数据博弈、数据质量控制、复杂系统建模。发表学术论文 20 余篇。

活动预告丨“数字法学冬令营”（SAIL-2022）将于 11 月 22–25 日在线举办

11 月 22–25 日, 由中国人工智能学会、人民法院数字法治研究基地、浙江大学光华法学院主办, 中国人工智能学会人工智能逻辑专业委员会(筹)、浙江大学数字法治研究院、浙江大学数字法治实验室承办的数字法学冬令营(SAIL-2022)将在线举办。活动邀请了八位国内外数字法学领域的知名学者前来讲授本领域的前沿动态。届时, 课程将通过中国人工智能学会的微信视频号等渠道提供线上直播, 敬请关注。

“数字法学冬令营”(The School on Artificial Intelligence and Law)是由荷兰格罗宁根大学人工智能系巴特·维赫雅(Bart Verheij)教授与浙江大学光华法学院熊明辉教授共同发起的公益性学术课程。数字法学涉及法律世界数字化和数字世界法律化。冬令营的前身是“法律人工智能春季工作坊”, 先后于 2018 年、2019 年在中山大学(SAIL-2018)、中南大学(SAIL- 2019)举办。

主办单位: 中国人工智能学会、人民法院数字法治研究基地、浙江大学光华法学院

承办单位: 中国人工智能学会人工智能逻辑专业委员会(筹)、浙江大学数字法治研究院、浙江大学数字法治实验室