文章编号：2095-2163(2023)06-0103-05 中图分类号：TP311 文献标志码：A

基于区块链的公检法电子证据存证模型研究

陈 潮

(浙江警察学院 计算机与信息安全系，杭州 310053)

摘 要：电子证据是司法诉讼中重要证据类型之一，电子证据具有易复制、易篡改、易丢失和易损坏等特点，直接影响到电子证据的可信度。在分析公检法业务流程和研究区块链的基础上，提出一种基于云存储和区块链的电子证据存证模型。云存储服务器存储电子证据原文，区块链存储电子证据的哈希值等元数据和查询电子证据。密码技术确保电子证据的机密性，哈希算法确保电子证据的完整性，云存储和区块链相结合实现电子证据的分布式存储和真实性自动验证，对于提高电子证据的可信度有一定的应用价值。

关键词：电子证据；区块链；云存储；存证

Research on electronic evidence storage model for public security bureau, procuratorate and court based on blockchain

CHEN Chao

(Department of Computer and Information Security, Zhejiang Police College, Hangzhou 310053, China)

【Abstract】 Electronic evidence is one of the important types of evidence in judicial activities. Electronic evidence has the characteristics of easy to copy, easy to modified, easy to lose and easy to damage, which affects the credibility of electronic evidence. On the basis of the analysis of the business process of the public security bureau, procuratorate and court and the research of blockchain, this paper proposes a storage model of electronic evidence based on cloud storage and blockchain. The cloud storage server stores the original text of electronic evidence and the blockchain stores metadata such as the hash value of electronic evidence and queries electronic evidence. The cryptographic technology ensures the confidentiality of electronic evidence, and hash algorithm ensures the integrity of electronic evidence. The combination of cloud storage and blockchain to realize the distributed storage and automatic verification of electronic evidence provides an applicable way for improving the credibility of electronic evidence.

【Key words】 electronic evidence; blockchain; cloud storage; storage and certification

0 引 言

当今社会信息技术广泛应用于国家、社会和企事业单位等各个领域，人们的工作、学习和生活高度依赖各种各样的电子设备和功能多样的信息系统。电子设备和信息系统产生海量电子数据，其中部分电子数据在公检法的侦查、诉讼和审判活动中成为案件重要的电子证据，电子证据在司法活动中越来越被广泛采用，已经成为八大类证据之一[1-3]。电子证据本身是电子数据，其文档、图片、音频、视频和日志等形式呈现，与传统证据相比，具有易复制、易篡改、易丢失和易损坏等特点，这些特点影响到电子证据的可信度。区块链技术是当前最热门的信息技术之一，具有去中心化、难篡改和可溯源等特点，这些特点适合用于电子证据的存储和验证。研究和提出一种基于区块链的公检法电子证据存证模型，实现电子证据的安全可靠存储和自动验证，从而确保电子证据在司法活动中的可信度[4-6]。

1 区块链

2008 年一个自称为中本聪的人或组织在密码学论坛发表一篇论文“Bitcoin：a peer-to-peer electronic cash system”，提出一种点对点电子货币系统——比特币，于 2009 年完成代码开发并上线比特币系统，实现在无中心化平台参与下的不可信任节点之间的电子货币交易。比特币系统的可靠运行，验证了比特币理论体系的正确性。区块链技术是支撑比特币系统正常运行的低层技术，区块链是分布

作者简介：陈 潮(1980-)，男，硕士，副教授，主要研究方向：区块链、计算机网络。

通讯作者：陈 潮 Email：chenchaocn@163.com

收稿日期：2023-01-29

式存储、密码学、点对点网络、共识算法和激励机制等技术的集成创新,虽然区块链未提出新的技术,但是通过对现有技术和理论的精妙设计与整合,创造性地进行了集成创新,具有巨大的创新价值。区块链是一种由区块与哈希指针构成的数据结构,哈希指针实现相邻区块之间的连接,哈希指针串连起所有区块形成区块链。区块由区块头和区块体两部分构成,下面以比特币为例说明:

(1)区块头。区块头由版本号、前一区块哈希、时间戳、随机数、难度和梅克尔树根构成,其中前一区块哈希实现与前一区块的连接;时间戳标记区块生成的时间;随机数是用于工作量证明中调整区块哈希值的一个随机整数;难度用于量化生成新区块需要的工作量;梅克尔树根用于验证区块体中存储交易的完整性。

(2)区块体。区块体由经节点验证通过的一定数量交易构成,这些交易以两个交易为一组基于梅克尔树进行哈希计算,最终生成一个哈希值,即为梅克尔树根,同时记录在区块头的梅克尔树根中。区块体中任何一个交易数据被修改,将改变梅克尔树值,同时区块哈希值也改变,导致当前区块与下一个区块的哈希链断开,无法维持原来的区块链,从而保证上链数据难以篡改[7]。

2 共识机制

共识机制通常用于分布式系统,用来实现分布式系统中各节点数据的一致性,而区块链本质上是一个分布式存储的数字账本,众多节点参与记账,生成一个相同的区块链,因此共识机制是区块链实现各节点数据一致性的核心机制。

区块链经过十余年的发展,出现满足各种区块链应用场景的共识机制,最早的比特币采用工作量证明(PoW)机制,早期的以太坊也采用 PoW。但是,PoW 依赖区块链节点的算力,在达成共识过程中消耗了大量的电力资源,面临自然资源大量浪费的问题。因此,以太坊和其它一些数字货币开始采用权益证明(PoS)机制,具有最高权益的节点来生成最新的区块。PoS 解决了资源浪费和算力过于集中的问题,但是也存在区块链易出现分叉、安全性不高和权益节点记账积极性不高等问题。比特股的首席科学家拉里默在研究 PoS 的基础上,于 2014 年提出委托权益证明(DPoS)机制,各节点将本节点的权益委托给可以信任的节点,获得权益最多且愿意进行记账的 101 个节点将成为委托节点。根据区块链系统规则,每个委托节点在规定的时间内轮流生成新的区块,并进行转发和验证,同时获得每笔交易的交易费,DPoS 大幅度减少区块链网络的记账节点,区块链的效率得到显著提高。实用拜占庭容错(PBFT)共识机制是在拜占庭容错(BFT)的基础上发展而来,其有别于 PoW、PoS 和 DPoS 的是,记账节点不通过节点间的竞争产生,而是所有节点通过投票的方式来产生新的区块,不存在区块链分叉的问题,同时 PBFT 通过算法的优化降低计算复杂度,解决 BFT 效率低下的问题[8-9]。

3 电子证据存证模型

区块链根据节点加入区块链是否需要授权分为许可链和非许可链,其中非许可链即公有链,如比特币和以太坊,任何节点无需授权可以加入和离开区块链,而许可链又分为私有链和联盟链,任何节点需要通过授权才能加入区块链,私有链适合一个单位场景,联盟链适合跨单位跨部门场景。由于公检法电子证据存证涉及 3 个单位,因此电子证据存证模型采用联盟链。以公安局、检察院和法院为 3 个节点,以 PBFT 为共识机制,公检法云服务器存储电子证据原文或密文,区块链存储电子证据的哈希值等元数据和查询电子证据,密码技术确保电子证据的机密性,哈希算法确保电子证据的完整性,区块链和云存储服务器相结合实现电子证据在公检法之间的可靠存储和安全共享。

3.1 公检法业务流程

公安局、检察院和法院属于垂直管理单位,3 家单位互不隶属,在司法活动中分别承担案件侦查、起诉和审判的职能,3 家单位协作完成案件的办理,公检法司法业务流程如图 1 所示。公安局负责案件的受理、审查、立案和侦查等工作,检察院负责对公安局提供的案件材料进行起诉前审查和对犯罪嫌疑人提起公诉,法院负责对公安局和检察院提供的案件材料进行开庭前审查和审判,并根据上诉和抗诉情况开展二审和判决[10]。公安局在案件的侦查过程中提取大量电子证据,检察院也可以对案件进行独立侦查,并提取电子证据,法院审理案件的重要依据是电子证据,在整个公检法业务流程中,电子证据需要在 3 家单位之间进行共享。

3.2 电子证据存证模型架构

公安局、检察院和法院 3 家单位已分别建成内部专用网络,政法专用网络实现 3 家单位专用网络的互连,公检法可将电子证据保存在各自专用网络的云服务器中,涉及重要案件的电子证据可加密保存。区块链布置在政法专用网络中,以公安局、检察

院和法院为节点，形成 3 个节点的区块链，区块链存储电子证据的哈希值等元数据，云存储和区块链相结合解决区块链无法存储大容量电子证据的问题，又通过存储在区块链上的哈希值确保云服务器中电子证据的可信度和完整性，电子证据存证模型架构如图 2 所示[11]。

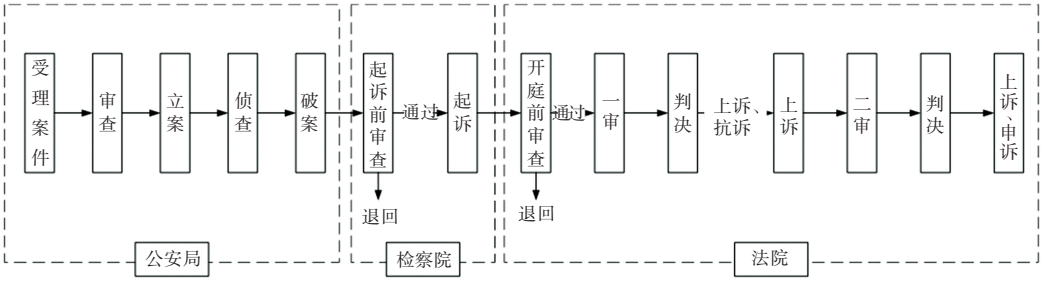

图 1　公检法司法业务流程

Fig. 1　The business process of the public security bureau, procuratorate and court

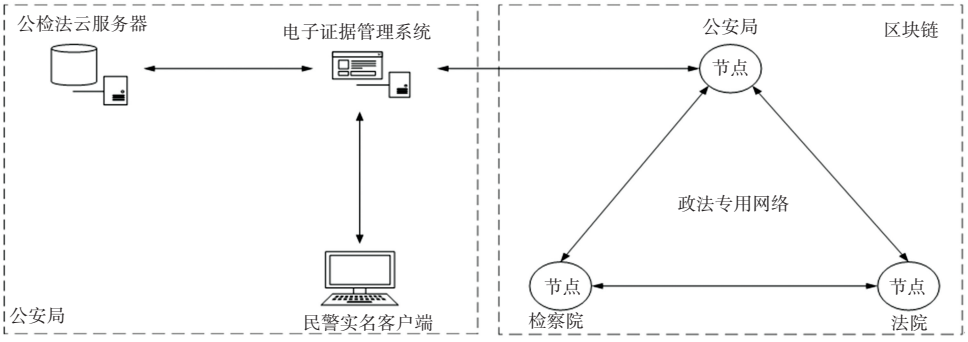

图 2　电子证据存证模型架构

Fig. 2　The framework of electronic evidence storage model

3.3　区块链区块数据结构

区块链区块数据结构跟比特币区块数据结构相似，同样由区块头和区块体构成，区别在于区块体中的交易不再存储交易信息，而是存储电子证据的元数据信息。一个电子证据的元数据对应一个交易，区块数据结构如图 3 所示。在区块 n 的区块体中存储了 8 个交易，即 8 个电子证据的元数据，以两个交易为一组，分别计算出哈希值再合成新的哈希值，再以两个哈希值为一组，再次合成出新的哈希值，用同样的方法向上计算出新的哈希值，最终计算出一个哈希值，存储到区块头中，即梅克尔树根[12]。

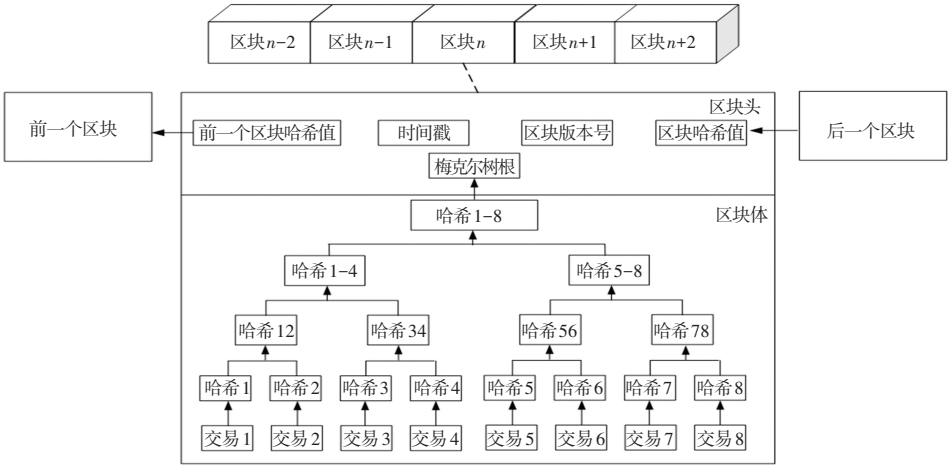

图 3　区块数据结构

Fig. 3　Data structure of blockchain

电子证据的元数据由电子证据编号、电子证据名称、电子证据类型、电子证据数字签名、电子证据哈希值和电子证据存储时间等构成,交易(元数据)的字段构成见表 1。

表 1 区块体交易(元数据)字段

Tab. 1 Blocktransaction (metadata) field

字 段	说 明
电子证据编号	每个电子证据具有唯一的编号,用于标识电子证据
电子证据名称	电子证据的文件名,简要说明电子证据
电子证据类型	标识电子证据类型,例如文档、图片、音频和视频等
电子证据数字签名	电子证据提交过程中涉及的人员和机构对电子证据进行数字签名
电子证据哈希值	采用国密 SM3 算法计算出电子证据的 256 位哈希值
电子证据存储时间	采用北京时间记录电子证据的存储时间

3.4 电子证据存证流程

电子证据存证模型的主要功能包括电子证据的存储、查询、下载和验证等,涉及电子证据的整个生命周期,覆盖了电子证据的存储、提取、出示和共享。

3.4.1 电子证据存储与上链

电子证据原文或密文存储在公检法云存储服务器中,电子证据的元数据上链存储在区块链,电子证据的存储与上链过程如图 4 所示。下面以公安民警存储电子证据为例,民警实名客户端、公安云存储服务器和电子证据管理系统部署在公安专用网络,电子证据管理系统是公安专用网络内电子证据共享的枢纽,具体步骤如下:

(1)公安民警在客户端中通过实名验证后,向电子证据管理系统提交电子证据。

(2)电子证据管理系统向公安云存储服务器提交电子证据,公安云存储服务器返回电子证据的哈希值。

(3)电子证据管理系统将民警 ID、电子证据哈希值、电子证据类型、案件编号和存储时间等元数据提交给区块链中的公安局节点。

(4)公安局节点以元数据构建交易,并通过政法专用网络传输到检察院和法院节点,区块链运行 PBFT 共识机制,各节点打包当前交易汇总生成新的区块。

(5)公安局节点将电子证据元数据上链后,返回存储编号给电子证据管理系统。

(6)电子证据管理系统返回电子证据存储结果给民警实名客户端。

检察院和法院在各自的专用网络和政法专用网络通过类似的流程,同样可以实现电子证据的存储与上链。

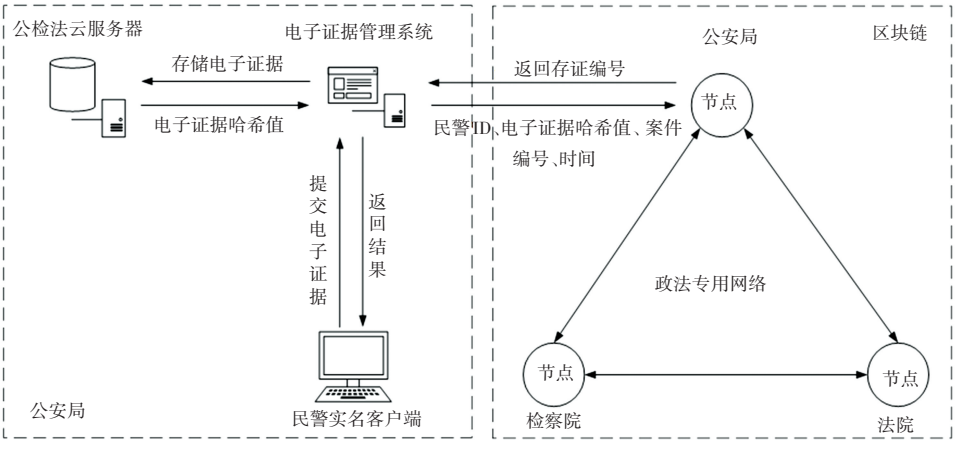

图 4 电子证据存储与上链

Fig. 4 Storage of electronic evidence

3.4.2 电子证据查询与下载

公检法区块链节点根据关键词搜索区块链实现电子证据的查询,电子证据管理系统根据电子证据哈希值,从公检法云存储服务器中提取电子证据原文,并根据电子证据哈希值来验证电子证据的完整性,防止电子证据被篡改,电子证据的查询和下载过程如图 5 所示。下面以公安民警查询和下载电子证据为例,具体步骤如下:

(1)公安民警在客户端通过实名验证后,向电子证据管理系统提交查询电子证据的关键词。

(2)电子证据管理系统将查询信息提交给区块链公安局节点,公安局节点搜索整个区块链,将搜索到的电子证据元数据返回给电子证据管理系统。

(3)电子证据管理系统提交元数据中的电子证据哈希值到公检法云存储服务器,公检法云存储服务器根据电子证据哈希值搜索到电子证据原文,并返回给电子证据管理系统。

(4)电子证据管理系统计算出电子证据的哈希值,并与电子证据元数据中的哈希值进行一致性判断,判断一致,则返回电子证据给民警实名客户端,民警即可提取出经过验证的电子证据,从而完成电子证据的查询与下载;否则,则说明电子证据已经被修改,返回错误信息给民警实名客户端。

公安民警若需要跨单位下载电子证据,则利用政法专用网络用同样的方法即可实现。检察院和法院通过类似的流程,同样可以实现电子证据的查询与下载。

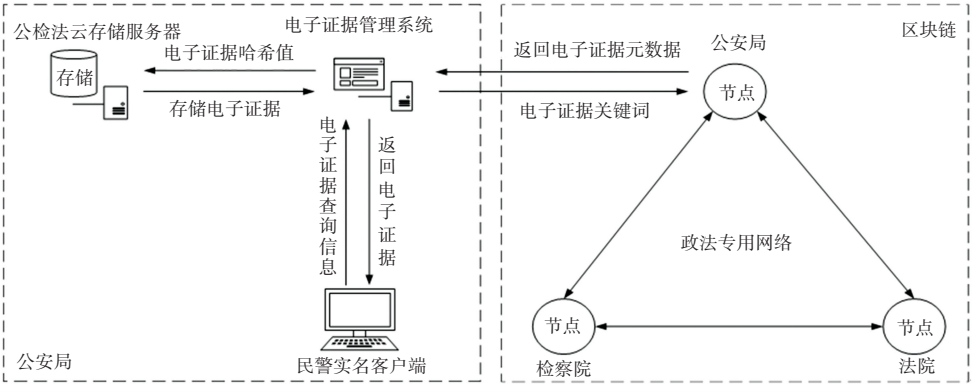

图 5　电子证据查询与下载

Fig. 5　Inquiry and download of electronic evidence

4　结束语

电子证据属于计算机、手机等电子设备运行中产生的各种电子文件,传统的中心化电子证据管理系统存在电子证据的存储安全性低、验证难和共享困难等问题,影响到电子证据的可信度。在分析公检法业务流程和研究区块链的基础上,结合区块链去中心化、难篡改和可溯源等特性,提出一种基于区块链的电子证据存证模型,电子证据分布式存储在公检法云服务器,电子证据的元数据存储在由公检法三家单位构建的区块链中,区块链实现电子证据的查询与验证,较好地解决传统中心化存储电子证据存在的问题,实现电子证据的可靠存储、安全共享和自动验证,对于提高电子证据在司法活动中的可信度有一定的应用价值。

参考文献

[1] 陆一鸣, 丁姝萌, 江舒涵,等. 基于链区块链的电子数据存证技术研究[J]. 网络安全技术与应用, 2022(11):4.

[2] 冒小乐, 陈鼎洁, 孙国梓. 基于区块链的电子数据存证的设计与实现[J]. 中兴通讯技术, 2018, 24(6):7.

[3] 杨坤桥. 基于区块链的电子数据存证平台研究[J]. 现代计算机, 2021(9):36-40.

[4] 沈玉东, 费凡, 吴名. 基于区块链和 IPFS 技术的公检法证据链平台设计[J]. 信息与电脑, 2022,34(6):1-3.

[5] 孙国梓, 冒小乐, 陈鼎洁,等. 基于区块链技术的电子数据存证系统[J]. 西安邮电大学学报, 2018, 23(4):82-87.

[6] 郑清安, 程仲汉. 基于区块链的电子数据存证系统[J]. 莆田学院学报, 2022, 29(5):5.

[7] 王群, 李馥娟, 王振力,等. 区块链原理及关键技术[J]. 计算机科学与探索, 2020, 14(10):23.

[8] 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.

[9] 王群, 李馥娟, 倪雪莉,等. 区块链共识算法及应用研究[J]. 计算机科学与探索, 2022, 16(6):1214-1242.

[10] 荆兆星. 面向公检法司链上存证的安全存储技术研究[D]. 海南:海南大学,2021.

[11] 苗志坤. 基于区块链的电子证据存储与共享研究[D]. 西宁:青海师范大学,2022.

[12] ZHONG Botao, XU Haitao, DING Lieyun, et al. Hyperledger fabric based consortium blockchain for construction quality information management [J]. Frontiers of Engineering Management, 2020, 7(4):512-527.