HZ BOOKS
华章IT

远光软件区块链首席科学家/中国电子学会区块链专委会专家撰写，6位业界专家联袂推荐

4个行业，5个案例，从总体设计、业务设计、功能接口设计、架构设计4个维度给出完整的行业解决方案，以及实现方案需要的技术和方法

区块链技术丛书

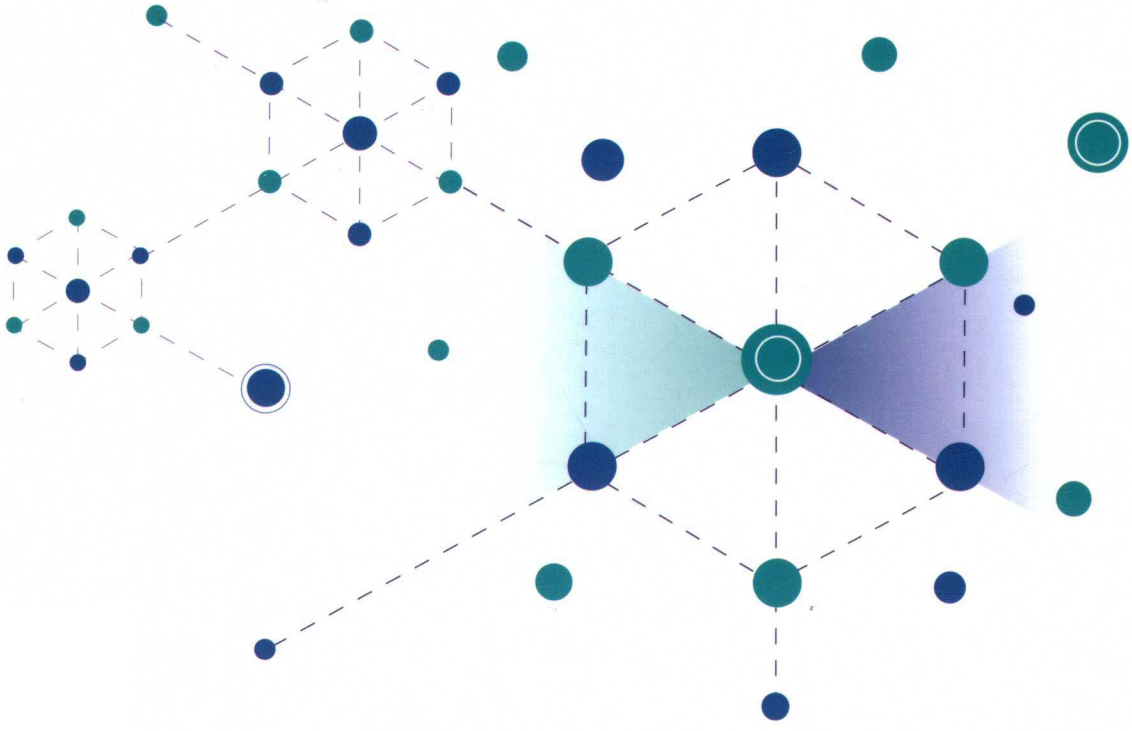
BLOCKCHAIN ENGINEERING PRACTICE

Industry Solutions and Key Technologies

区块链工程实践

行业解决方案与关键技术

鲁静 ◎著



机械工业出版社
China Machine Press

区块链
技术丛书

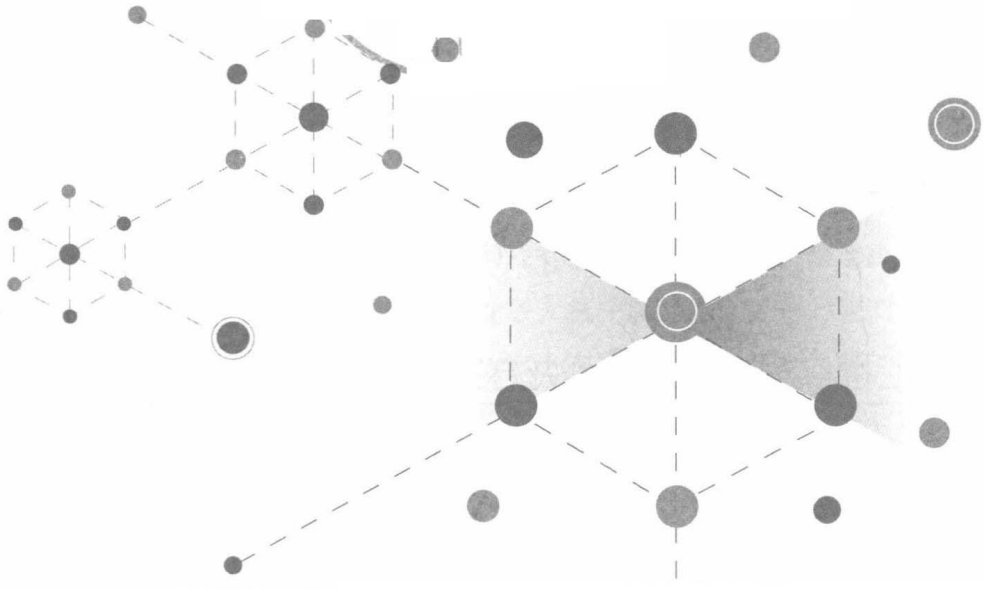
BLOCKCHAIN ENGINEERING PRACTICE

Industry Solutions and Key Technologies

区块链工程实践

行业解决方案与关键技术

鲁静 ◎著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链工程实践：行业解决方案与关键技术 / 鲁静著 . —北京：机械工业出版社，2019.6

（区块链技术丛书）

ISBN 978-7-111-63109-5

I. 区… II. 鲁… III. 电子商务 – 支付方式 – 研究 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2019）第 133730 号

区块链工程实践：行业解决方案与关键技术

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）

责任编辑：孙海亮　　责任校对：殷　虹

印　　刷：北京文昌阁彩色印刷有限责任公司　　版　　次：2019 年 7 月第 1 版第 1 次印刷

开　　本：186mm × 240mm　1/16　　印　　张：11.5

书　　号：ISBN 978-7-111-63109-5　　定　　价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88379426　88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　　读者信箱：hzit@hzbook.com

Preface 前　言

为什么要写这本书

当我 5 年前第一次接触区块链时，马上就被它组织自治、群体协作、大众智慧的运作模式吸引住了。于是我整理了一份资料，向我的朋友、同事甚至客户介绍这门新技术。遗憾的是，当他们听我讲完对等网络、默克尔树、非对称加密、共识算法、智能合约这些拗口的专业术语后，仍然搞不清楚区块链可以为他们带来什么好处。直到一次宣讲课后，移动互联部门的同事主动找到我，说他们正在做一款电子证照产品，遇到了数据库壁垒、权限设计、隐私保护的问题，问我有没有可能用区块链来解决。要知道，这正是可以发挥区块链特长的地方！经过和业务人员一周的深入讨论，我们形成了公司第一个区块链应用——可信电子证照的初步方案；在之后的三个月内，我们完成了可信电子证照的产品演示，并获得了首届中国区块链技术创新应用大赛的二等奖。这件事情让我明白，一个成功的区块链应用需要解决的最核心的问题是，区块链对于解决业务痛点是否是必要和可行的。

自从“区块链”大热以来，社会上各类区块链应用层出不穷。一时间，这门新技术似乎成为各行各业的必需品，网络上甚至出现了“区块链马桶”的恶搞段子。从经济角度考虑，一个区块链系统相比于原生系统多出至少 7 倍的成本，这些多出的成本能为我们带来什么回报？这个回报是不是值得我们付出 7 倍的成本？我想这是每一个区块链应用在构建之初就需要解答的问题，也是我们在每一个项目开始之前就要分析业务和区

块链的匹配度的原因。区块链的根本在于通过技术手段将信息交换和价值交换的信任成本降到最低，这不仅是技术上的创新，更是对生产关系的革新。作为价值互联网的基础设施，区块链最先改变的是金融体系，因为这里信任的代价最大，规则也最容易被写死并合约化。未来，随着共识效率的提升、加密算法的演变、物联网与人工智能的协同发展，区块链将逐步渗透到各行各业，从金融的自我监管过渡到社会的自治。

我所关注的能源互联网是区块链的天然土壤，对区块链有着刚性需求。2016 年国家发改委、能源局和工信部共同发布了《关于推进“互联网 +”智慧能源发展的指导意见》，提出建立一种互联网与能源生产、传输、存储、消费及能源市场深度融合的能源产业发展新形态，实现“设备智能、多能协同、信息对称、供需分散、系统扁平、交易开放”等目标。人与人、人与物、物与物、园区与园区之间的能源共享会越来越普遍。也许就在未来 5 年，你就可以像发红包一样，用 App 发一个能量块给你的邻居，发一个能量块给你的特斯拉，再发一个能量块给你的扫地机器人；随着机器智能飞速演进，也许你的特斯拉能精准地嗅到商业气息，将它的剩余电力共享给别的特斯拉，为你挣钱！那么，用什么来保障这种能源共享经济里的信任环境呢？用什么让陌生人、物之间不用相互猜忌、也不依赖第三方，遵从一致的游戏规则自由地进行能源交换呢？答案就是运行在区块链上的智能合约。正如陈利浩先生在《区块链与“自由人的联合体”》一文所说，人类的天性是渴望和追求自由，没有任何人愿意被强制管理，而区块链是“自由人的联合体”理想的信息实现形式。

虽然任何变革都不是一步到位的，也许能源公链在目前看来还遥不可及，但是电改 9 号文标志着电力市场化全面放开，并且一旦开始就将无法回头，只会势不可挡地朝着更加透明、公平、自由的市场化交易模式演变。这种模式对市场成员、交易品种、交易合同都提出了新的要求：市场成员增多、交易品种趋于复杂化、交易规则趋向于定制化，结算压力较传统模式大大增加。这就要求结算系统能够灵活拓展，账目能够在不同主体间保持一致性和实时性。我们目前开发的几个应用都是围绕着电力行业展开的，如电力市场交易结算智能合约、购售电云合同，通过在不同组织之间构建联盟链，达到规则的共享和价值的协同。在未来的分布式商业模式下，公司的边界将被重新定义，取而代之的将是一些去中心化的自治组织和分布式自主运作企业，公司间的竞争将演变为组织与组织间、行业与行业间的竞争。在这个演进的过程中，区块链是协调分布式组织（如供

应链）中每个参与者的权利和义务，发挥群体协作和群体智慧的良好解决方案。

本书结合我和我所在团队的项目实践经验，通过 5 个具体的区块链案例说明区块链技术是如何一步步和实际业务相结合，服务于集团管理、智慧能源和社会互联的。在每一个案例中，都会分析区块链技术和当前业务痛点的匹配程度，梳理国内外的研究进展和应用落地情况，然后给出我们的解决方案。方案一般包括总体设计、业务设计、功能接口设计和架构设计，有的给出了系统交互和实施方案。在每个案例的末尾还提供了我们使用的关键技术和方法，以及部分实现代码和实验结果。希望通过本书，能够帮助读者理解区块链可以用在何处，能够发挥什么作用，以及如何构建一个具体的区块链应用。

读者对象

本书的读者对象包括但不限于：

- ❑ 区块链应用设计者；
- ❑ 区块链应用开发者；
- ❑ 区块链爱好者；
- ❑ 能源互联网关注者；
- ❑ 集团和社会治理者；
- ❑ 使用区块链参与业务应用的公司与集体；
- ❑ 开设相关课程的大专院校师生。

本书特色

与同类书籍比较起来，本书的特色体现在：

（1）笔者及其团队多年区块链实战经验的精华总结；

（2）通过 5 个具体的区块链案例说明区块链技术如何应用到实际业务中；

（3）侧重实用性，迅速提高读者的实战能力；

（4）缜密的匹配性分析，真正体现区块链价值，不是为了区块链而区块链；

（5）从落地案例和学术层面分析区块链在具体领域的应用情况和研究进展；

（6）介绍实际应用中与区块链相关的技术，如数据上链方式、可信智能电表、能源终端交互方式、小额电费支付方法、云存储与区块链、数据交互智能合约、微服务与区块链、物联网设备与区块链等。

勘误和支持

除封面署名外，参加本书编写工作的还有王超、向智宇、宋斌、张建冬、程晗蕾、吴士泓。由于笔者的水平有限，编写时间仓促，书中难免会出现一些错误或者不准确的地方，恳请读者批评指正。如果你有宝贵意见，也欢迎发送邮件至邮箱 lujing@ygsoft.com，期待能够得到你们的真挚反馈。

致谢

首先要感谢“中本聪”先生发明了区块链技术，并开创了区块链的第一个应用——比特币，将这个伟大的、改变世界的技术带入人们的视野。

其次要感谢远光软件股份有限公司为我提供的良好的学习、工作环境和资源，让我组建团队挑战一个又一个区块链项目。感谢董事长陈利浩先生，您对人类理想社会的孜孜追求和对区块链技术的高度认可是指引我前进方向的明灯。

感谢客户对我们的信任，把区块链项目交给我们团队来完成。这些项目实践经验是本书创作的基础。

感谢远光区块链团队的黄昭慈、王超、向智宇、宋斌、张建冬、何畅、李毅、程晗蕾、镇华、何威、龚强、瞿威、何乐、徐银、张志明、孔智、陈娇阳、仝建华、陈磊、万行、任枭、王波、喻攀黎、杨帅、郭超、杨志、杨骥、许文柱、张欣、钟俊、李浩、邓江坤、徐学章、程欢、高诗阳、胡蝶、陈浩罡、杨晓珊、李洪富、谌艺文、邓肯、钟华欣、杨庆、刘亚建、黄越、邱永星、张航，以及给予我支持和帮助的部门和同事们，

区块链项目的一个个落地离不开大家的共同努力。感谢黄建元先生、黄笑华先生、李美平先生、向万红先生对本书提出的宝贵意见和建议。

感谢国家留学基金委和滑铁卢大学（University of Waterloo），让我有机会远赴加拿大进行为期一年的访问学习，并在滑大区块链社区（UW Blockchain Club）认识了许多区块链爱好者。我的大部分书稿都是在访学期间整理完成的。

感谢机械工业出版社华章公司的编辑杨福川老师、孙海亮老师，在这一年多的时间中始终支持我的写作，你们的鼓励和帮助引导我顺利地完成全部书稿。

深深感谢我的父母对我生活上的关怀和无微不至的照顾，感谢我的先生对我学术和生活上的帮助，感谢我可爱的女儿给我带来的欢乐，你们的幸福一直是我奋斗的动力。

谨以此书献给区块链的爱好者们，献给所有崇尚自由的灵魂！

鲁　静

目　录 *Contents*

第 1 章 Chapter 1

基于区块链的可信电子证照

证件作为个人从事社会活动和企业生产经营的一种具有法定效力的文件，是现代生活中必不可少的工具。在严谨的证件审批管理体制下，烦琐的程序和庞杂的材料证明使得“证件多、办证难、用证烦、核查慢”等办证问题频现，既影响民众生活，阻碍企业正常运营，又降低了行政效率，成为长期以来民众诟病的大问题。与此同时，传统的纸质证照不仅会造成资源浪费，促使重复性证明成为常态，更重要的是难以杜绝证件伪造现象，造成信任危机，同时还存在证照信息分享不畅、易丢失、易损毁等一系列问题。随着信息技术的发展，电子证照应运而生。电子证照不仅可以提高相关人员办事效率，还可以解决纸质证照无法解决的资源浪费和易伪造等问题，甚至可以打通不同的电子政务系统，从而更好地为民众服务。

1.1 背景与现状

1.1.1 电子证照的发展历史

自党的十八大召开以来，利用信息手段解决“证件多”和“用证难”等问题已成为社会共识。国务院办公厅《关于促进电子政务协调发展的指导意见》（国办发 [2014]66

号）明确指出："积极推动电子证照、电子文件、电子印章、电子档案等在政务工作中的应用"；澳门在2005年年底正式推出《电子政务发展纲领（2005—2009）》，提出"运用资讯科技及行政现代化手段，提高政府部门施政质素和效率，降低行政运作成本，持续令公民得到贴身且满意的公共服务"的愿景。自2016年以来，国务院先后发文提出构建电子证照库，并明确要求积极推动电子证照、电子公文、电子签章等在政务服务中的应用，实现"一号一窗一网"，为居民提供"记录一生，管理一生，服务一生"的服务。目前，国内已有80多个试点城市在不同程度地建设电子证照库，但各地都建有自己的信息系统，信息化水平也存在差异，电子证照库的实施困难重重。如何打通不同的信息系统、令证照互认，是亟须解决的技术问题。

国内目前的电子证照管理平台主要采用集中共享模式，由中心数据库来完成证照的制作、存储、信息查询和交换共享，数据库的拥有者掌握着数据库的访问和更新权限。但由于需要管理的人口众多、社会发展水平不均衡，短时间内把不同地区、部门的公民信息完全集中并实时联网，建立"集中的公民信息库"很难实现，因为建立"集中的公民信息库"需要通过体制改革与机构合并实现数据集中和信息联网，在当前条件下，这在管理和技术上的实现都相当困难，存在跨地区、跨部门应用流程复杂、管理性能不高等问题，无法适应大规模、多样化电子证照管理和验证服务需求。同时集中式数据库并没有有效控制证照信息的保密制度，或者有目的性的指定授权，使其对所有办事机构公开，这样证照持有人的信息没法得到有效保护，被攻击篡改和泄露的风险较大，致使证照可靠性打了折扣。

近几年各类研究机构、企业对电子证照也展开了日渐深入的研究。《一种电子证照信息交互的系统及方法》[1]公开了一种电子证照信息交互系统，包括主控端、存储端、签发端、授权端、查验端和服务端，证照持有人可以根据不同的办事流程对不同的办事机构进行电子证照的授权查验；《一种非介质电子证照系统》[2]包括远程信息数据库系统、通信网络和系统终端，提供了一种能克服现有介质证照不足且能基于GPS、智能手机满足社会智能管理条件的非介质证照系统；《电子认证在可信电子证照中的应用》[3]通过在电子证照中增加带有数字签名的二维码形成可信电子证照，保证了证照的真实性和不可篡改性；《基于数字证书互联互通的身份认证支撑平台及认证方法》[4]公开了

一种基于数字证书互联互通的身份认证支撑平台以及身份认证方法，将各应用系统需要进行数字证书认证的请求统一集中到基于数字证书互联互通的身份认证支撑平台进行处理。以上研究均对信息系统进行了不同程度的优化，也取得了一定效果，但其基本思路仍是依托第三方认证机构，建立中心数据库存储数据，然后进行各部门共享，这并不能从根本上解决信息壁垒及证照信息互信互通的问题。

1.1.2　区块链在电子证件和身份认证领域的国内外发展现状

区块链（blockchian）技术[5]是随比特币等数字加密货币兴起的一种新型分布式数据组织方法及运算方式，通过去中心化来集体维护一个可靠数据库的技术。该技术将一段时间内的两两配对数据（比特币中指交易）打包成数据块（block），然后利用具有激励性质的共识算法让点对点对等网（p2p 网络）中的所有节点产生的数据块保持一致，并生成数据指纹验证其有效性然后链接（chain）下一个数据块。在这个过程中，所有节点的地位都是对等的，没有所谓的服务器和客户端之分，因此被称为去中心化的方式，这很好地解决了数据在存储和共享环节中存在的安全和信任问题。通过区块链技术，在数据共享过程中可明确数据的来源、所有权和使用权，达到数据在存储上不可篡改、在流通上路径可追溯、在数据管理上可审计的目的，保证数据在存储、共享、审计等环节中的安全，实现真正意义上的数据全流程管理，进一步拓展数据的流通渠道、促进数据的共享共用、激发数据的价值挖掘、增强数据在流通中的信任。同时，基于区块链的分布式共享“总账”这一特点，在平台安全方面，可达到有效消除单点故障、抵御网络攻击的目的。这些特点使得区块链技术特别适合应用于具有保密要求的大数据运算领域。

近年来，国外已有一些研究机构和企业将区块链应用在电子证件认证和身份认证领域（见图 1-1）。2015 年 7 月，区块链初创公司 ShoCard 获 150 万美元投资，将实体身份证件的数据指纹保存在区块链上。用户用手机扫描自己的身份证件，ShoCard 应用会把证件信息加密后保存在用户本地，把数据指纹保存到区块链。区块链上的数据指纹受一个私钥控制，只有持有私钥的用户自己才有权修改，ShoCard 本身无权修改。同时，为了防范用户盗用他人身份证件扫描上传，ShoCard 还允许银行等机构对用户的身份进行背书，确保真实性。2015 年 9 月，去中心化的管理项目比特国 (Bitnation) 在区块链

上实施“电子公民”（e-Residents）计划。用户在其官网上通过区块链登记成为 Bitnation 的“公民”，并获得 Bitnation“世界公民身份证”。2015 年 12 月，Bitnation 与爱沙尼亚政府签署协议，将为“电子公民”项目提供公证服务，无论他们身居何处，在何处做生意，都可以在区块链上享受结婚证明、出生证明、商务合同和其他服务。区块链是一个公共账本，全世界数以千万计的计算机都存储着其副本，具备公开公证的可复制性与不可更改性，比目前各国使用的传统公证方法更安全。2016 年 6 月，美国国安局向区块链初创公司 Factom 拨款 19.9 万美元用于物联网设备数字身份安全性开发，利用区块链技术来验证物联网设备，阻止因设备欺骗而导致的非授权访问，以此来确保数据完整性；美国区块链公司 Certchain 为文档建立数据指纹，提供去中心化的文件所有权证明；OneName 公司则提供了另一种身份服务，即任何比特币的用户都可以把自己的比特币地址和自己的姓名、Twitter、Facebook 等账号绑定起来，相当于为每个社交账户提供了一个公开的比特币地址和进行数字签名的能力。

图 1-1 区块链在电子证件认证和身份认证领域的应用案例

在国内，有一些研究机构也在开展区块链在电子政务方面的应用研究。闵旭蓉等人[6]设计了一种电子证照共享平台，利用区块链技术的去中心化、不可篡改、分布式共同记账、非对称加密和数据安全存储等特点，实现电子证照的安全可信共享，实现各地、各部门和各层级间政务数据的互联互通，支撑政府高效施政。黄步添等人[7]明确了

电子证照参与者的权利和义务，基于联盟链思想和轮值机制，设计区块链平台的系统架构、数据结构和业务流程，提供电子证照的颁发、存储、更新、验证等功能，实现多中心、协同式电子证照管理，从而为电子证照拥有者以及相关应用系统提供便捷的电子证照服务。蒋海等人[8]提供了一种区块链身份构建及验证方法，有效缓解了因个别认证机构的问题影响用户身份信息准确性的情况，然而其原始数据来源为第三方认证机构，未能解决数据的真实性问题，且其只进行身份验证，未与其他证件锚定，扩展性不强，发挥的作用有限。

此外，有一些教育和科研机构将区块链技术应用于教育证书领域。2015 年，麻省理工学院的媒体实验室（The MIT MediaLab）应用区块链技术研发了学习证书平台，并发布了一个类似“比特币钱包”的手机 App[9]。学习者可以利用该 App 存储和分享自己的学习证书，随身携带、随时展示，且拥有重申成绩的权力。学习者不能擅自更改学习证书的内容，但能自主决定将什么证书展示给哪个访问者。在查询时，将数字证书的密钥点对点地发送给用人单位或学生等有关需求方，确保证书不会被恶意查询。无独有偶，位于旧金山的软件培训机构——Holberton School 从 2017 年开始利用区块链技术记录学历，并在区块链上共享学生的学历证书信息。同样，学分也可以通过这项技术认证和交换。对于学生来说，这一应用拓宽了他们获得教育评价的途径，方便了学习记录和学历信息的保存。从更长远的眼光来看，利用区块链记录跨地区、跨院校甚至跨国学习者的信息，可以使在不同环境中学习的学习者获得同样有效的学习记录。区块链技术在教育证书方面可能的应用方式包括：为在线教育提供有公信力和低成本的证书系统；作为智能合约，完成教育契约和存证；作为分布式的学习记录存储，记录学习轨迹，共享学习学分。从应用规模和范围来看，区块链在教育领域的应用范围可以小到单个教育机构、学校联盟，大到全国甚至全球性的教育互认互通联盟。

1.2　区块链与电子证照的匹配度分析

在电子证照应用中引入区块链技术，可以借助区块链的去中心化同步记账、身份认证、数据加密和数据不可篡改等特征，确保电子证照信息可信任且可追溯，使各社会主体共同建造、共同维护、共同监督，从而满足公众的知情权、监督权，增强电子证照的