DOI:10.16569/j.cnki.cn11-3720/t.2020.09.033

基于区块链技术的数字证书溯源防伪系统的设计

□李娜　周熹丽　胡敏

区块链是一个去中心化运行的共享数据库，具有很高的透明度、效率和安全性；以数学难题为基础，使用非对称加密算法来保证数据安全性。存储在其中的数据或信息，具有全程留痕、不可伪造、可追溯、公开透明、集体维护等特征。这些特征为区块链技术奠定了坚实的信任基础，并创造了可靠的合作机制，具有很广阔的应用前景。本文以数字签名技术、区块链技术为基础，构造数字证书溯源防伪系统，实现数字证书防篡改，以及证书生成、修改、废弃等过程的高效可追溯查询。

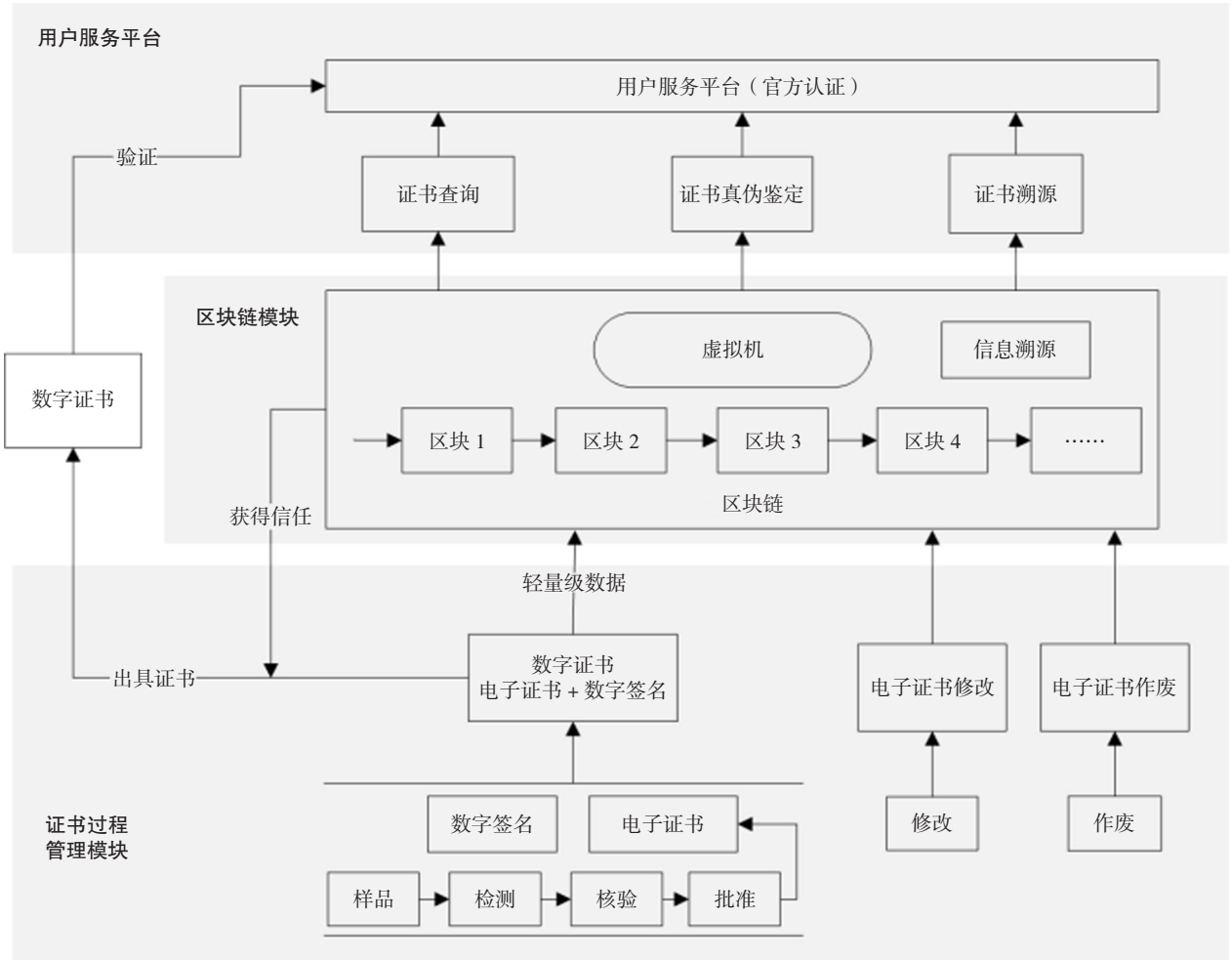

图 1　数字证书溯源防伪系统设计图

一、溯源防伪系统的设计

本系统包括证书过程管理、区块链认证、用户服务平台三个模块。总体设计如图 1 所示。

1. 证书过程管理模块

证书过程管理模块是证书生成、修改、作废等流程的管理模块，直接与检测检验系统接口。被检样本经过检测、核验、批准，生成电子证书；使用哈希算法生成电子证书中关键信息的数据摘要，然后利用非对称加密算法进行签名（数字签章），与电子证书一起组成数字证书，可以实现证书防篡改效果。

数字证书包含电子证书和数字签名，输出轻量级数据到区块链模块，如证书中关键信息等，减少网络中流通的数据量，节省网络资源。

证书修改、作废完成后及时更新到区块链模块，保证区块链模块信息的完整性、准确性。

2. 区块链模块

区块链模块由多个互不信任区块组成，具有去中心化、公开透明及不可篡改性，其中区块链不可篡改的特点可以实现数字证书的防伪功能。区块链中的各个区块可通过虚拟机实现，减少物理机投入，降低成本。

信息溯源：区块记录了样品受理、检测、核验、批准、修改及作废等证书整个生命周期的信息，便于用户查询电子证书制作过程。

数字证书的关键信息和数字签名通过区块链技术获取信任后，发布数字证书给客户。区块链模块提供证书查询、真伪鉴定和证书溯源接口。

证书查询：提供证书查询接口，可查询本机构出具的任意证书，输入相关关键字可查询证书。

证书真伪鉴定接口：通过证书编号等信息可以验证证书的真伪，向区块链的各个区块发送验证消息，只有 51% 以上的区块验证成功后才能保证证书的存在性，接下来可以进一步通过数字证书中的数字签名验证证书内容是否被篡改。

证书溯源接口：溯源信息查询需要首先验证证书的真伪，验证成功后可以进行溯源信息查询；同样地，51% 以上的区块中的溯源信息相同才能认定为溯源信息有效，返回证书制作过程信息给用户，实现证书全过程可追溯，公开透明。

3. 用户服务平台

用户服务平台是机构对外提供的官方认证查询平台，是区块链模块和用户之间交互的桥梁，向用户提供证书查询、真伪鉴定、证书溯源服务，用户输入证书编号等信息，平台通过相关接口向区块链各区块发送验证消息，将查询或验证结果显示给用户。

二、预期效果

本系统利用区块链技术，基于 hash 算法、数字签名、时间戳、分期账本和共识机制等实现电子证书的防伪、溯源功能，当证书出现疑问时，可通过用户服务平台进行查询、鉴定，为计量行业的证书电子化提供了技术保障。本系统实施后预计可达到以下效果：

1. 提高证书可信度

区块链特有的分布式账本和共识机制，将证书各阶段信息记录于区块之中。任何记录信息和数据只有通过区块链各个区块的核实和确认之后，才能被写入区块链之中，保证了数据的真实性和完整性。用户通过用户服务平台可以验证证书并获取溯源信息，实现了证书报告制作的全过程透明，大大提高了证书的可信度。

2. 提高证书查询鉴定效率

本系统提供的网络平台自助查询功能，可以方便用户查询证书信息、鉴定证书真伪，还可以获取证书溯源信息、最新状态信息，让用户全方位了解证书相关信息。相较于传统的纸质证书邮寄、人工查询、查询结果反馈，查询鉴定效率大大提升。

3. 节省证书成本

因检定 / 校准和检测证书数量庞大，纸质证书制作过程复杂，需要专门人员负责打印、寄取证书，导致证书成本及人工成本非常高。检定 / 校准和检测数字证书推广使用后，纸质成本及证书打印、寄取工作人员将被解放出来，大大节省了证书制作成本。

作者单位【浙江省计量科学研究院】