密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2017,4(2):199–208

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

基于区块链技术的防伪系统的设计与实现*

安 瑞[1], 何德彪[2], 张韵茹[2], 李 莉[3]

1. 武汉大学数学与统计学院, 武汉 430072
2. 武汉大学计算机学院软件工程国家重点实验室, 武汉 430072
3. 武汉大学国际软件学院, 武汉 430072
通讯作者: 何德彪, E-mail: hedebiao@whu.edu.cn

摘 要: 随着国民经济的高速发展和人民生活水平的不断提高, 假冒伪劣产品日益增多, 给市场经济造成很大的破坏, 并影响着国民诚信素质, 为了解决这个问题, 防伪技术得到了广泛关注. 作为目前使用最广泛的防伪手段, 二维码制作简单, 极易伪造, 并不能提供不可伪造性. 为了促进市场经济的健康发展, 亟待一种有效的防伪技术来阻止目前的破坏行为. 区块链技术具有去中心化、开放、自治、匿名和不可篡改等特性, 这用来做产品防伪具有天然优势. 同时, IC 卡芯片具有存储量大、安全性高、使用方便等特性. 本文将区块链技术和 IC 卡芯片相结合, 设计了一种安全的防伪系统, 并给出了具体实现细节. 实现结果表明:由于区块链技术和 IC 卡芯片的高安全性, 该系统具有极高的不可伪造性质, 且成本低廉、易于实施, 具备相当不错的竞争力. 在目前区块链实际落地的应用相对较少的情况下, 此系统作为一个已经实现的比较完善的系统, 对于目前的区块链落地以及防伪市场给出了一个技术参考.

关键词: 区块链; IC 卡芯片; 防伪系统; 数据完整性
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000174

中文引用格式: 安瑞, 何德彪, 张韵茹, 李莉. 基于区块链技术的防伪系统的设计与实现[J]. 密码学报, 2017, 4(2): 199–208.
英文引用格式: AN R, HE D B, ZHANG Y R, LI L. The design of an anti-counterfeiting system based on blockchain[J]. Journal of Cryptologic Research, 2017, 4(2): 199–208.

The Design of an Anti-Counterfeiting System Based on Blockchain

AN Rui[1], HE De-Biao[2], ZHANG Yun-Ru[2], LI Li[3]

1. School of Mathematics And Statistics, Wuhan University, Wuhan 430072, China
2. The State Key Lab of Software Engineering, School of Computing, Wuhan University, Wuhan 430072, China
3. International School of Software, Wuhan University, Wuhan 430072, China
Corresponding author: HE De-Biao, E-mail: hedebiao@whu.edu.cn

Abstract: With the rapid development of the national economy and the continuous improvement of people's living standard, the increasing number of fake and shoddy products have caused great damage to the market economy and effects the national quality. Thus, anti-counterfeiting techniques, as a solution to the problem, has attracted wide attention. The QR codes, which are the most widely used security techniques, are so easy to forge. To promote the healthy development of the market economy, effective Anti-counterfeiting techniques are urgently needed to prevent the current sabotages. The blockchain technology possess varieties of properties such as the

* 基金项目: 国家自然科学基金项目(61402339, 61572379, 61501333)
收稿日期: 2017-02-11 定稿日期: 2017-04-02

perfect characteristics of openness, de-centralization, autonomy and non-tampering, etc. It shows natural advantages to do anti-counterfeiting stuffs. IC card chip has a large storage capacity, high security and easy to use. Combine the blockchain technique with IC card chips, a new safety security system is designed in this paper. The specific implementation details are described in this paper. The result shows that the system has high unforgeability, low cost and easy implementation because of the high security of blockchain technique and IC card chip, having fairly good competitiveness. Owning to the limited applications of blockchain technique, this system as an implemented one gives a technical reference to the application of blockchain and the current anti-counterfeiting market.

Key words: blockchain; IC card chip; anti-counterfeiting system; data integrity

1 引言

随着国民经济的高速发展和人民生活水平的不断提高, 人们对于物质生活等方面有了更高的追求. 为了满足人们的需求, 市场上各式高档商品层出不穷. 与此同时, 市面上制造假劣品的行为日益猖狂, 食品、副食品、医药、保健品等行业的造假行为, 不仅损害了生产者的利益, 同时也威胁着人们的身体健康和心理健康. 很多名包、珠宝等贵重物品也出现许多的高仿品, 既损害了消费者的切身利益, 也影响着市场诚信[1]. 甚至让消费者对名优品的购买失去了信心, 丧失对品牌的信任, 对个人以及市场都造成了难以估计的影响.

为了增加消费者对产品的可信度, 维护商家的利益, 防伪技术开始进入人们的视线. 目前防伪技术中应用的最广泛的是二维码防伪技术[2]. 二维码防伪技术是将每个产品的相应信息编码成一个二维码, 消费者可以通过扫描这个二维码获取产品信息来核对产品真假. 然而目前由于二维码的生成方式简单, 有太多的方法可以便于人们生成二维码, 并且二维码复制的代价低廉, 假冒品的二维码扫出来的依然是商家发布的真实产品信息. 这使得假货依然横行, 因此急需一些更安全、可靠的技术手段来达到防伪的目的.

IC 卡芯片是一个集成了许多密码学算法的装置, 内置独立的密钥生成、加解密装置, 拥有独立的处理器和存储单元. 它可以存储密钥、数字证书、指纹等信息, 并且其安全保密性很好, 很难被复制与伪造. 目前市场上使用区块链进行防伪所用的是一个可复制芯片, 相比而言, 我们所采用的技术更优: 写入安全芯片内的数据同时还写入区块链上, 安全芯片内加密数据的不可破解性和区块链上数据的不可更改性, 这两者结合可以真正地达到高端防伪的要求.

在 2009 年, 区块链首次被中本聪[3]提出用来作为一个不涉及第三方的记录比特币交易的公共账本. 在区块链上, 其中的每个区块都存储了一些信息, 包括上一个区块的区块哈希值, 这就形成了从创世块到当前区块的链[4]的形式. 区块链的这种特性保证了数据的完整性和不可更改性并且能被用来验证数据的真实性[5].

区块链主要依赖于两种密码学方法: 数字签名和密码学哈希函数. 数字签名是证明数字消息本真性的一种方法, 它被用来验证数据的完整性以及不可抵赖性. 消息发送者用自己的私钥签名发送的消息. 当接收者收到消息后, 他用消息发送者的公钥来验证这条消息. 这条消息可以被任何知道消息发送者的公钥的人验证[6]. 密码学哈希函数是给定一个输入然后计算其哈希值的一个数学运算. 哈希函数是确定性的, 即同样的输入一定会产生同样的输出. 根据哈希函数的抗碰撞性——即不同的输入肯定会得到不同的输出, 在只知道函数输出的条件下, 输入内容是无法被求出的. 比特币区块链和以太坊区块链中, 分别使用的是 SHA2-256 算法和 SHA3-256 算法[7].

区块链的不可更改性, 使其形成了一个不可篡改、不可伪造的分布式数据库; 它的去中心化运行, 使其在很大程度上提高透明度、安全性和效率; 它以数学难题为信任基础, 使用非对称加密算法来保证交易的安全. 区块链作为一个分布式数据库, 记录着区块链从创世块到当前块的所有交易, 相比于传统数据库, 区块链具有去中心化、不可更改性、匿名性、可审计性这几个特点.

2 预备知识

2.1 区块链

比特币自面世到现在, 成为现在最受欢迎的数字货币[8,9], 其设计就是允许比特币区块链上的两个地址账户进行点对点的交易, 而不通过第三方机构. 在 2014 年的时候, 通过比特币改进方案[10], 每个比特币交易可以附加一个不超过 40 个字节的信息, 因此我们可以往比特币区块链中写入自己想写的任意数据. 现在比特币区块链数据变得越来越大, 而且交易确认时间也变得越来越长. 由于我们的项目要往区块链中写入的证书数量比较庞大, 因此比特币区块链不是我们的一个合适选择.

以太币是搭建去中心化应用平台以太坊中的数字货币, 相比比特币区块链, 以太坊区块链由于它作为一个能搭建去中心化应用的平台, 使得其具备很高的竞争性. 以太坊区块链上的写入数据字节无限制以及交易确认相对较快, 因此我们的项目实施就是通过在以太坊区块链上以交易的形式将宝石鉴定证书写入区块链中, 证书数据写入区块链上后, 可以保证完全安全[11−13].

区块链总体上可以分为三种类型: 公有链、联盟链和私有链.

在联盟链中, 区块链的区块和交易的有效性由预先设定的一个验证者群体决定, 这个验证群体, 形成一个联盟. 例如, 要使得联盟链中的一个区块有效, 需要联盟中 50%以上的成员签名通过, 新区块才有效. 区块链上的信息可以是公开的, 也可以只对联盟成员可见.

私有链是一个完全中心化的区块链, 只有私有链的创建者才有能往区块链中写入信息, 这个对于想进行内部审计的组织会是一个很好的选择.

在公有链上, 所有的数据对任何人都是公共可见的, 一个区块链地址相关的所有交易信息都能被公众查看. 然而很多金融领域的交易并不想对所有人可见[14], 因此公有链上的数据隐私性是一个比较短板的问题. 在公有链上将一个证书的 32 字节的哈希值通过交易写入区块链中, 大概花费 0.0004 个以太币, 以目前以太币单价 70CNY 为准, 公链上发布一个证书需要人民币 0.1 元, 成本比较高, 因此我们采用的是在自己搭建的私有链上发布我们的证书.

由于我们的项目只涉及以太坊区块链[4], 因此这里只介绍以太坊区块链地址的生成方法. 以太坊区块链上每个节点都拥有自己的一个密钥对——私钥 sk 和公钥 pk, 区块链地址 $\text{Add} = \text{SHA3}(\text{pk} - \text{'04'})$, 即公钥去掉第一个字节'0x04'后, 进行 SHA3 运算, 得到区块链地址 Add.

在我们本地的一个完整以太坊节点上, 与区块链进行交互, 使用的就是 Add, 以及另外一个 password. password 是用来加密用户本地的以太坊钱包, 而钱包里存用户的个人私钥. 因此相当于私钥被 password 加密. 真正在区块链网络上使用的是一个以太坊区块链地址以及这个 password.

2.2 智能卡

智能卡是一个集成了许多密码学算法的装置, 内置独立的密钥生成、加解密装置, 拥有独立的处理器和存储单元. 智能卡所起的作用相当于一个“保险柜”[15], 存储在其上的数据会进行加密处理, 因此, 可将密钥和重要数据存在智能卡中, 因而, 要想窃取到其中的数据必须破解这个智能卡的加密算法, 而这个加密算法的核心是由一个目前不可解决的数学难题构成, 从而保护商业隐私和数据安全. 根据智能卡的设计原理, 加密数据只能输出, 不能输入, 这样加密和解密以及签名的运算都在智能卡内部完成, 只是将结果输出到上层, 避免了密码被破解的机会.

Near Field Communication(NFC)[16]是一种短距高频的无线电技术, 由非接触式射频识别演变而来. 在单一芯片上结合感应式读卡器、感应式卡片和点对点的功能, 能在短距离内与兼容设备进行识别和数据交换. 项目中就是利用手机的 NFC 功能来读取智能卡芯片内的数据.

我们采用的智能卡支持 SM2, SM3, SM4, AES, DES 等密码学算法, 并且嵌入了椭圆曲线电子签名算法(ECDSA)来实现通过智能卡输出签名, 只有签名结果才出智能卡, 私钥这些重要数据存储在智能卡内部.

3 防伪系统设计

目前市面上运用的最广泛的是基于二维码的防伪系统, 但是就现在看来它主要存在如下五点缺陷:

(1) 不法商家可以直接盗取正牌商品的二维码, 将该二维码复制数以千份;

(2) 不法商家通过分析正牌商品的序列号各字段内容, 即可伪造出类似的序列号, 也就是能伪造或复制正牌商品的数据库;

(3) 扫描二维码后就能立即跳转到相应的网页页面(或者商家官方主页), 输入相关的查询信息, 便可以获取商品的信息等;

(4) 不良商家通过修改链接, 伪造出与正牌网站内容相似的恶意网站, 伪装正品商家, 从而欺骗消费者;

(5) 由于商家掌握着数据库的更改权力, 商家可自行操纵数据库, 让在线验证不再可信.

区块链宝石防伪系统包括两大部分: **宝石防伪证书发行系统**和**宝石防伪证书验证系统**. 证书发行系统的总体架构如图 1 所示:

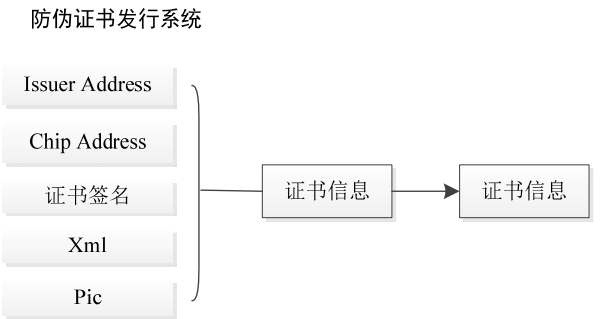


图 1 证书发行系统

Figure 1 The certificate issuing system

证书验证系统的总体架构如图 2 所示:

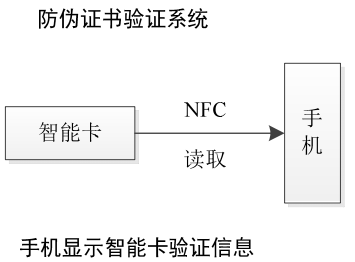


图 2 证书验证系统

Figure 2 The certificate verifying system

宝石防伪证书发行系统主要实现系统初始化、宝石鉴定证书信息录入、宝石鉴定防伪证书生成、宝石鉴定防伪证书发行、NFC 防伪芯片管理等功能, 其产品形态为软硬件结合, 硬件包含服务器、NFC 读卡器、NFC 芯片, 软件为产品防伪证书发行系统, 为宝石鉴定机构人员提供 WEB 管理界面供其操作.

我们开发的区块链宝石防伪系统是集芯片技术、区块链技术、Android 技术于一体的具有高可靠性的安全防伪系统. 该防伪系统主要涉及以下几个方面:

自主发行证书芯片

首先我们对自己的出厂卡片进行验证，并且初始化，提供给客户进行写卡．客户对我们提供的卡片进行防伪验证，验证卡片是否确实是我们提供的芯片卡，验证通过，则对卡片进行写卡操作．图 3 表示卡片验证通过:

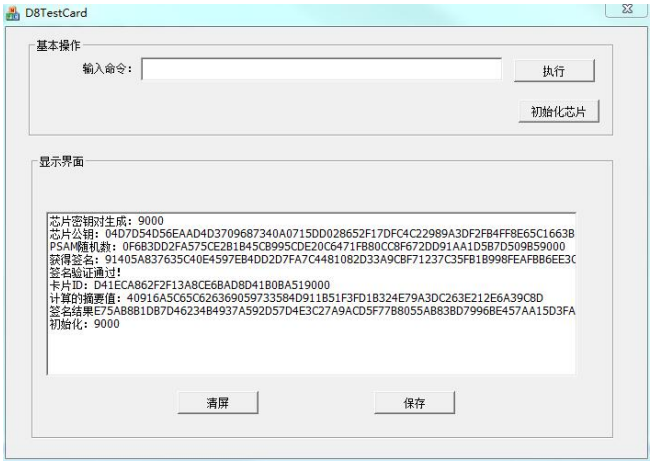


图 3　卡片验证通过

Figure 3　The verification of smart card passed

图 4 是往卡片写入宝石信息的操作界面:

图 4　卡片写入信息

Figure 4　Write information into smart card

写卡完成之后,就会生成每个产品对应的证书,客户将证书摘要通过交易放进以太坊区块链上，证书就存储在区块链上了.

属性防伪证书

由于宝石的属性影响到宝石的价值，所以每块宝石应该都会配有经鉴定中心鉴定后的“属性身份证”，用来描述宝石的大小、色泽、硬度、比重等通过物理专业手段鉴定出的物理属性. 首先，我们将每个产品的“属性身份证”通过软件写入到相应的芯片中，防伪证书生成及发行流程如下:

(1) 获取宝石防伪证书发行者区块链地址 Issuer Address;

(2) 调用 NFC 防伪芯片提供的生成密钥对接口，生成密钥对，导出公钥，并生成 NFC 防伪芯片的区块链地址 NFC Chip Address;

(3) 获取宝石鉴定原始证书信 xml 文件和 pic 文件;

(4) 对上述信息进行组包，组包格式为 Issuer Address||Chip Address||xml||pic;

(5) 将步骤(4)生成的组包信息先进行 SHA3 运算计算其摘要值，然后利用宝石防伪证书发行者私钥对摘要值进行 ECDSA 签名，生成签名信息;

(6) 调用 NFC 防伪芯片提供的写数据接口，将步骤(1)的发行者区块链地址 Issuer Address、步骤(2)的 NFC 防伪芯片的区块链地址 NFC Chip Address、步骤(3)的原始证书信 xml 文件和 pic 文件、步骤(5)生成的签名信息写入 NFC 防伪芯片中. 信息一经写入不可更改. 将防伪芯片附在实体证书上.

产品信息写入之后，鉴定中心和芯片本身分别会有一个密钥对，公钥以及私钥，每个公钥对应一个区块链地址. 该“属性身份证”加上鉴定中心地址以及芯片地址就构成了对应产品的证书，由于区块链上存储数据的能力有限，那么将证书原始数据存放在区块链上就不是一个较好的选择. 由于哈希函数的特殊性质，通过哈希函数，我们将原始证书数据通过哈希求值，得到证书的唯一哈希值，即证书摘要，我们要做的就是将此摘要存放于区块链上. 鉴定中心拥有自己的密钥对，它用自己的私钥对此证书摘要进行签名，生成鉴定中心签名过得证书. 签名过程都是通过安全芯片，在芯片内部完成，送出签名，芯片内部使用的签名算法为 ECDSA. 用户使用鉴定中心的公钥即可实现链下的证书真伪验证.

宝石防伪证书验证系统产品形态为验证 APP，验证 APP 内置宝石防伪证书发行者公钥信息，证书验证方式分为离线验证和在线验证两种方式. 图 5 是产品通过所有鉴定的结果，图 6 是由鉴定为非法中心的显示结果.

图 5 产品通过鉴定

Figure 5 The product passed verification

图 6 鉴定为非法中心

Figure 6 Verified that issued by illegal center

离线验证方式流程如下:

(1) 验证APP调用NFC防伪芯片提供的接口获取防伪证书信息, 并对防伪证书信息进行解析, 获取鉴定证书原始信息、签名信息、NFC Chip Address、Issuer Address;

(2) 验证APP调用NFC防伪芯片提供的导出公钥接口, 保存公钥后期使用, 生成区块链地址, 并与步骤(1)中的NFC Chip Address比较, 如果一致, 则继续下一步, 否则验证失败;

(3) 验证APP调用NFC防伪芯片提供的数字签名接口, 使用NFC芯片私钥对随机数进行签名, 返回签名结果给验证APP;

(4) 验证APP从利用芯片公钥对步骤(5)中的数字签名进行验证, 验证通过则该证书为真, 否则验证失败.

(5) 验证APP利用内置的公钥信息生成区块链地址, 并与步骤(1)中的Issuer Address比较, 如果一致, 则继续下一步, 否则验证失败;

(6) 验证APP利用内置的公钥将步骤(1)中的信息作为原文, 验证签名信息的正确性, 验证通过继续下一步, 否则验证失败.

图7是离线验证的部分代码:

```
cardVerifyFlag = cardVerifySignature(randomTerminator, cardSignx, cardSigny);
System.out.println("cardVerifyFlag=====================================================" +cardVerifyFlag);
byte[] sigX = Arrays.copyOfRange(addressStrArr, 40, 72);

System.out.println("sigX=" +Hex.toHexString(sigX));
byte[] sigY = Arrays.copyOfRange(addressStrArr, 72, 104);

System.out.println("sigY=" +Hex.toHexString(sigY));
System.out.println("allMsgHash=" +toHexString(allMsgHash));
certVerifyFlag = certVerifySignature(allMsgHash, new BigInteger(Hex.toHexString(sigX), 16), new BigInteger(Hex.toHexString(sigY), 16));
System.out.println("certVerifyFlag=====================================================" +certVerifyFlag);

byte[] getIssueAdd = Arrays.copyOfRange(addressStrArr, 0, 20);
issAddVerifyFlag = Arrays.equals(issueAddress, getIssueAdd);
System.out.println("issAddVerifyFlag=========================================" + issAddVerifyFlag);
byte[] getCardAdd = Arrays.copyOfRange(addressStrArr, 20, 40);
System.out.println("getCardAdd:" + toHexString(getCardAdd));

cardAddVerifyFlag = Arrays.equals(chipAddress, getCardAdd);
System.out.println("cardAddVerifyFlag=========================================" + cardAddVerifyFlag);
```

图 7　离线验证的部分源代码

Figure 7　Parts of source code of off-line verifying

在线验证方式流程如下:

(1) 验证APP调用NFC防伪芯片提供的读取数据接口, 获取防伪证书信息, 并对防伪证书信息进行解析, 获取鉴定证书原始信息、NFC Chip Address、Issuer Address;

(2) 验证APP调用NFC防伪芯片提供的读取数据接口, 获取防伪证书信息(或摘要值)和签名信息

(3) 验证 APP 调用 NFC 防伪芯片提供的导出公钥接口，生成区块链地址，并与步骤(1)中的 NFC Chip Address 比较，如果一致，则继续下一步，否则验证失败；

(4) 验证 APP 利用内置的公钥信息生成区块链地址，并与步骤(1)中的 Issuer Address 比较，如果一致，则继续下一步，否则验证失败；

(5) 验证 APP 通过芯片区块链地址在区块链中查找该笔交易的信息，验证该笔交易中嵌入的信息是否与步骤(1)中的防伪证书信息(或摘要值)、步骤(2)中的防伪证书信息(或摘要值)是否一致，如果一致，则继续下一步，否则验证失败；

(6) 验证 APP 调用 NFC 防伪芯片提供的读取数据接口，读取签名信息，利用内置的公钥将步骤(1)中的信息作为原文，验证签名信息的正确性，验证通过继续下一步，否则验证失败；

(7) 验证 APP 调用 NFC 防伪芯片提供的数字签名接口，使用 NFC 芯片私钥对随机数进行签名，返回签名结果给验证 APP；

(8) 验证 APP 从 NFC Chip Address 中计算出公钥，利用此公钥对步骤(6)中的数字签名进行验证，验证通过则该证书为真，否则验证失败.

用户的手机界面显示真伪全部通过之后,我们的手机 APP 可以通过 webservice 查询到每个证书在区块链上的相关信息. 这些信息包括交易发送者账户随机数，代表中心发证数量；发证中心区块链地址；每个证书对应芯片的区块链地址以及证书存储在区块链上的区块号.

图 8 是离线验证所显示的结果，图 9 是增加了在线查询的显示结果.

图 8 离线验证
Figure 8 Off-line verify

图 9 在线查询
Figure 9 On-line query

图 10 是 APP 调用 webservice 查询区块链上该证书所在交易的信息的部分代码:

```
do {
    HttpURLConnection conn = (HttpURLConnection) url.openConnection();
    conn.setRequestMethod("GET");
    conn.setConnectTimeout(3000);
    conn.setReadTimeout(3000);
    conn.connect();
    if (conn.getResponseCode() == HttpURLConnection.HTTP_OK) {
        InputStream iS = conn.getInputStream();
        BufferedReader bR = new BufferedReader(new InputStreamReader(iS));
        String line;
        StringBuilder sB = new StringBuilder();
        while ((line = bR.readLine()) != null) {
            sB.append(line);
        }
        bR.close();
        String txResultJson = sB.toString();

        net.sf.json.JSONObject jsonObject = JSONObject.fromObject(txResultJson);
        JSONArray jsonArray = jsonObject.getJSONArray("data");
        JSONObject jsonObject1 = (JSONObject) jsonArray.get(0);
        sender[0] = jsonObject1.getString("sender");
        recipient[0] = jsonObject1.getString("recipient");
        blockId[0] = jsonObject1.getString("block_id");
        accountNonce[0] = jsonObject1.getString("accountNonce");

        System.out.println("txResultJson=======" + txResultJson);
        System.out.println("sender:" + sender[0]);
        System.out.println("recipient:" + recipient[0]);
        System.out.println("blockId:" + blockId[0]);
        i.onGetTxResult(1,accountNonce[0],sender[0],recipient[0],blockId[0]);
```

图 10　webservice 查询交易信息的部分源代码

Figure 10　Parts of source code of querying the transaction information by webservice

如果用户还是不放心，可以找第三方鉴定机构，重新鉴定产品.

4　结论

随着造假行为的日益猖獗，防伪需求的不断增加，然而能满足这样需求的防伪技术确是少之又少，因而目前市面上的防伪需求这一块还有着很大的市场空间. 通过结合我们研发出来的智能卡以及当前科技前沿的区块链技术，可以完美地满足这一需求. 文章首先介绍区块链，说明区块链是一个适合用来防伪的技术；其次，从成本角度分析，采用私有链对于我们是更好的选择；然后介绍智能卡，说明智能卡的一些特性，并且它与区块链的数据不可更改性类似，写入智能卡的数据也不可更改.

文章详细说明了利用区块链进行防伪的一套开发系统，这套系统整合了芯片技术、区块链技术以及 Android 技术，其中 Android 技术就是实现手机 APP 通过 Webservice 能够访问到每个产品证书在区块链上的相关信息，整套系统完成之后，我们提供给用户的就是一个需要用户自主安装在手机上的 Android 程序了，对于用户来说非常方便. 通过结合智能卡与区块链技术，能够达到产品真正地防伪目的. 由于区块链的数据可追溯性及不可更改性，可以预见未来市场上高端物品的防伪都会在区块链平台上进行.

References

[1] BÖHME R, CHRISTIN N, EDELMAN B, et al. Bitcoin: Economics, technology, and governance[J]. The Journal of Economic Perspectives, 2015, 29(2): 213–238.

[2] WANG Z M. Anti-counterfeiting of two dimensional code[J]. China Brand and Anti-counterfeiting, 2001(3): 61.
王志民. 二维码防伪[J]. 中国品牌与防伪, 2001(3): 61.

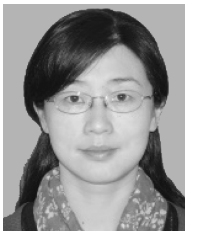
[3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. 2008.
[4] Ethereum Homestead Documentation[OL]. http://ethdocs.org/en/latest/
[5] Blockchain Bitcoin Wiki[OL]. https://en.bitcoin.it/wiki/Block_chain
[6] BADEV A, CHEN M. Bitcoin: technical background and data analysis[S]. Federal Reserve Board.
[7] BIDER D, BAUSHKE M. SHA-2 data integrity for the secure shell (SSH) transport layer protocol[R]. IETF RFC 6668.
[8] KUMARESAN R, MORAN T, BENTOV I. How to use bitcoin to play decentralized poker[C]. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015: 195–206.
[9] ØLNES S. Beyond bitcoin enabling smart government using blockchain technology[C]. In: International Conference on Electronic Government and the Information Systems Perspective. Springer International Publishing, 2016: 253–264.
[10] Bitcoin Improvement Proposals[OL]. https://github.com/bitcoin/bips.
[11] MILLER A, JUELS A, SHI E, et al. Permacoin: repurposing bitcoin work for data preservation[C]. In: 2014 IEEE Symposium on Security and Privacy. IEEE, 2014: 475–490.
[12] HERRERA-JOANCOMARTÍ J. Research and challenges on bitcoin anonymity[C]. In: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. Springer International Publishing, 2015: 3–16.
[13] Michael B, Nicolas C, Benjamin J, et al. Financial Cryptography and Data Security[M]. Springer Berlin Heidelberg, 2015.
[14] KAYE J, VERTESI J, FERREIRA J, et al. # CHImoney: financial interactions, digital cash, capital exchange and mobile money[C]. In: CHI'14 Extended Abstracts on Human Factors in Computing Systems. ACM, 2014: 111–114.
[15] LIU D G. Discussion on the factors of Chinese safety chip technology research and development[J]. China Science and Technology Information, 2014(6): 130–131.
刘德国. 浅谈中国安全芯片技术研发的要素——以联想“恒智”为例[J]. 中国科技信息, 2014(6): 130–131.
[16] BREITFUß K, HASELSTEINER E. Security in near field communication[C]. In: Proceedings of the Workshop on RFID Security. IEEE, 2006.

作者信息

安瑞(1992–), 湖北咸宁人, 硕士研究生. 主要研究领域为密码学.
E-mail: ruia.math@whu.edu.cn

何德彪(1980–), 山东阳谷人, 博士, 副教授, 博士生导师. 主要研究领域为公钥密码学.
E-mail: hedebiao@whu.edu.cn

张韵茹(1992–), 湖北襄阳人, 硕士研究生. 主要研究领域为密码学.
E-mail: zuozhe2@sina.com



李莉(1979–), 安徽芜湖人, 博士, 副教授. 主要研究领域为数据安全、嵌入式安全.
E-mail: lli@whu.edu.cn