安全 RFID 和区块链技术在瓶装酒防伪溯源中的应用研究

杨云勇[1]，马纪丰[2]，胡川[1]
（1. 中国贵州茅台酒厂（集团）有限责任公司，贵州 564501；
2. 华大半导体有限公司，北京 100102）

摘要：提出了一种基于安全 RFID 和区块链技术相结合的酒类防伪溯源应用方案。该方案采用安全 RFID 产品和认证节点的联盟链模式，利用安全 RFID 产品高安全、防复制功能和区块链数据不可篡改、数据共享、点对点传输等技术特点，将芯片生产、标签的生产、密钥发行、标签与酒的信息关联等环节加入到联盟链里，所有的节点生产信息透明。该系统从技术上突破了传统的溯源防伪系统易复制、信息不透明、数据容易篡改、安全性差、相对封闭等弊端和弱点，为创造一个全新的酒产品诚信体系打下了坚实的基础。

关键词：安全 RFID；区块链；防伪溯源

中图分类号：TP391.44　文章编号：1674–2583(2018)03–0066–04
DOI：10.19339/j.issn.1674–2583.2018.03.016
中文引用格式：杨云勇，马纪丰，胡川.安全RFID和区块链技术在瓶装酒防伪溯源中的应用研究[J]. 集成电路应用, 2018, 35(03): 66–69.

Study on the Application of Safe RFID and Block Chain Technology in the Anti Counterfeiting and Traceability of Bottled Wine

YANG Yunyong[1], MA Jifeng[2], HU Chuan[1]
(1. Guizhou Moutai distillery (Group) Co., Ltd, Guizhou 564501, China.
2. Huada Semiconductor Co., Ltd, Beijing 100102, China.)

Abstract: An application scheme based on the combination of security RFID and Blockchain technology is proposed in this paper. This scheme adopts alliance chain model with RFIDsecruity products and authentication nodes.It will make the links of die production, tag production, key issueand wine's information are added to the alliance chain with RFID security products of high safety, anti copy function and Blockchain data can notbe tampered with, data sharing and point to point transmission technology,etc.The system breaks through the shortcomings of traditional traceability and anti–counterfeiting system, such as easy copying, opaque information, data falsification, poor security and relatively closed, etc., which lays a solid foundation for creating a new credit system of liquor products.

Key words: security RFID, block chain, anti–counterfeiting and traceability

1 引言

为遏制假酒现象的蔓延，近年来我国监管部门一直保持对制假售假采取高压态势严厉打击，但酒类造假活动依然猖獗。为降低造假给企业形象带来的损害，不少企业纷纷开发防伪技术，然而这些防伪技术都无法根本上解决通过复制和转移防伪标识

作者简介：杨云勇，中国贵州茅台酒厂（集团）有限责任公司信息中心主任，副教授，研究方向：IT架构及网络安全，物联网及RFID应用，作者邮箱：yyunyong@moutaichina.com。
马纪丰，华大半导体有限公司，研究方向：物联网及集成电路设计，通信作者邮箱：majf@hed.com.cn
胡川，中国贵州茅台酒厂（集团）有限责任公司信息中心，研究方向：网络安全及物联网应用，作者邮箱：huchuan@moutaichina.com
收稿日期：2018-2-7 ，修回日期：2018-02-27。

进行造假的问题，造假现象仍然难以遏制，消费者仍然无从辨别产品的真假。而且，中心化的防伪验证设备和运维管理工作消耗了大量的资金和人力，企业迫切期盼一种验伪操作简单、能够防复制、防转移、防篡改、运营成本低的酒类防伪解决方案。

安全 RFID 和区块链技术的产生与发展，为解决上述问题提供了强有力的技术基础。

2 带国密算法的安全RFID产品介绍

高频安全电子标签芯片采用了一款超低功耗、带国产 SM7 算法的高频无源电子芯片，提供唯一识别号码，支持单向认证和双向认证，支持带 NFC 功能的手机识别与防伪验证。

3 区块链概念

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

区块链系统根据应用场景和设计体系的不同，一般分为公有链、联盟链和私有链。其中，公有链的各个节点可以自由加入和退出网络，并参加链上数据的读写，运行时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点。

联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络。各机构组织组成利益相关的联盟，共同维护区块链的健康运转。

私有链的各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放。专有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。

上述三种类型的区块链特性如图 1 所示。

图 1　区块链三种设计体系

4 区块链及物联网应用分析

4.1 物联网应用分析

物联网（The Internet of things），是将物理设备、车辆、建筑物和一些其他嵌入电子设备、软件、传感器等事物与网络连接起来，使这些对象能够收集和交换数据的网络。其核心和基础仍然是互联网，是对现有网络基础设施的延伸和扩展，其远端系统延伸和扩展到了任何物品与物品之间，进行信息交换和通信。

经过二十多年的发展，物联网已经逐步融合到我们的生活中。万物互联已成必然趋势，物联网设备将会呈现几何级数的增长，其应用将大大改变人们现有的生活环境和习惯。但是物联网在给人们的生活带来便利的同时，也会给人们带来种种隐忧，物联网面临着一系列亟待解决的行业痛点。

（1）设备安全。物联网的安全既构建在互联网的安全上，也有因为其业务环境而具有自身的特点。总的来说，物联网安全和互联网安全的关系，体现在以下这几点：物联网安全不是全新的概念，物联网安全比互联网安全多了感知层，传统互联网的安全机制可以应用到物联网，物联网安全比互联网安全更复杂。

近年来，关于网络的安全事件不断攀升。Mirai 创造的僵尸物联网（Botnets of Things）被麻省理工科技评论评为 2017 年的十大突破性技术，据统计，Mirai 僵尸网络已累计感染超过 200 万台摄像机等 IoT 设备，由其发起的 DDoS 攻击，让美国域名解析服务提供商 Dyn 瘫痪，Twitter 、Paypal 等多个人气网站当时无法访问。后续，又有奴役物联网设备、让其比特币挖矿的僵尸网络，还有规模更大、更为活跃的 http81 僵尸网络等。

（2）隐私保护。中心化的管理架构无法自证清白，个人隐私数据被泄露的事件时有发生。

（3）架构僵化。目前的物联网数据流都汇总到单一的中心控制系统，随着低功耗广域技术（LPWA）的持续演进，可预见未来物联网设备将呈几何级数增长，中心化服务成本难以负担。

（4）通信兼容。全球物联网平台缺少统一的语言，容易造成多个物联网设备彼此之间通信受到阻碍，并导致产生多个竞争性标准和平台。

（5）多主体协同。目前很多物联网应用都是运营商、企业内部的自组织网络。涉及到跨多个运营商、多个对等主体之间的协作时，建立互信的成本很高。

4.2 区块链+物联网改进思路

区块链凭借主体对等、公开透明、安全通信、难以篡改和多方共识等特性，对物联网将产生重要的影响：多中心、弱中心化的特质将降低中心化架构的高额运维成本，信息加密、安全通信的特质将有助于保护隐私，身份权限管理和多方共识有助于

识别非法节点，及时阻止恶意节点的接入和作恶，依托链式的结构有助于构建可证可溯的电子证据存证，分布式架构和主体对等的特点有助于打破物联网现存的多个信息孤岛桎梏，促进信息的横向流动和多方协作。图 2，区块链的优势。

图 2　区块链的优势

运用区块链技术，可以为物联网的世界提供一个引人入胜的可能性，当产品最终完成组装时，可以由制造商注册到通用的区块链里面标示着它生命周期的开始，一旦该产品售出，经销商可以把它注册到一个区域性的区块链上（社区、城市或国家），通过创建有形资产和匹配供给和需求，物联网将会创造一个新的市场。

5 安全 RFID 和区块链在瓶装酒防伪溯源中的应用

5.1 安全 RFID+ 区块链的防伪溯源技术优势

5.1.1安全 RFID 技术优势

（1）防复制。采用多重安全防护设计技术基于国密算法的多级分散密钥管理体系，一芯一密，消除技术破解风险，避免芯片复制和批量造假。

（2）防转移。防伪标采用易碎 RFID 标签，开封即毁，有效防止转移造假。

（3）简化验伪操作，可信验伪。使用 NFC 手机进行验伪，操作简单易辨真伪。

（4）验伪 App 从酒厂官网下载，增强验伪结果可信度。

5.1.2 区块链技术优势

区块链不可篡改、数据可完整追溯以及时间戳功能，可有效解决物品的溯源防伪问题。

（1）防回收假冒，防篡改。区块链基于由密码学链接建立分布式数据库，从而形成不可篡改的数据源，避免 RFID 标签回收利用和内部技术人员的数据篡改。

（2）分布式存储，数据安全可靠。区块链采取去中心化的方法，每个节点都仅仅是系统的一部分，每个节点都是存有一个相同的交易备份，部分节点故障对系统的正常运营无任何影响，大大提高了系统的稳定性和抗攻击能力。

5.2 基于安全 RFID 和区块链的酒类防伪溯源应用方案

5.2.1 方案的实现

该系统采用安全 RFID 产品和认证节点的联盟链模式，利用安全 RFID 产品高安全、防复制功能和区块链数据不可篡改、数据共享、点对点传输等技术特点，将芯片生产、标签生产、密钥发行、标签与酒的关联信息等环节加入到联盟链上，链上节点信息全透明（图 3）。

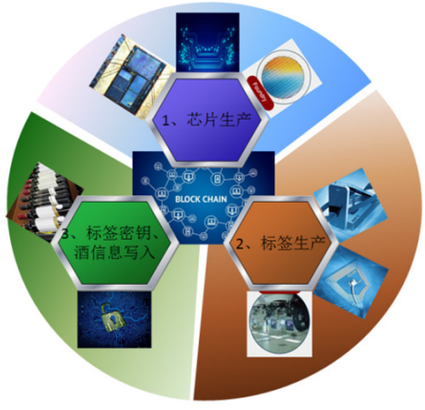

图 3　加入联盟链里的节点

在联盟链中芯片生产节点记录芯片的全球唯一 ID 号，且此 ID 永不可更改。标签生产节点记录芯片的全球唯一 ID 号。标签信息写入和密钥发行节点记录芯片的 ID、密钥或 ID、密钥、产品信息。

结合的区块链技术从架构设计上来说，可以简单地分为三个层次，协议层、扩展层和应用层。其中，协议层又可以分为存储层和网络层，它们相互独立但又不可分割。如图 4 所示。

最终验伪分两部分，除了终端 NFC 等技术的单向认证以外还有联盟链内的各节点方的相互验证。这样一些节点方之间不透明的信息透明起来了，酒生产方可以清晰地知道收到的标签是否是用约定的芯片做成的，发行方也知道标签是否写入了他们所需要的密钥，应用流程如图 5 所示。

图 4　区块链架构

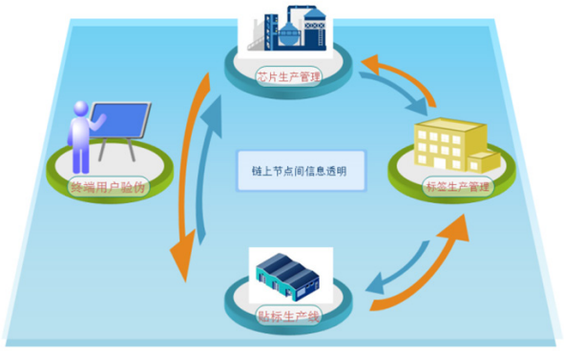

图 5　应用流程

5.2.2 方案的优势

第一，流程公开透明。通过给产品植入识别芯片，并注册到区块链上，使其拥有一个数字身份，再通过共同维护的账本来记录这个数字身份的所有信息，比如来源、流转等，以达到验证效果。

第二，安全 RFID 芯片基于国密算法，采取多重安全防护设计技术，防止复制造假，确保身份标识唯一性。

第三，在产品的生产、仓储、物流、分销等业务过程达成共识并建立信任，形成数据记录，信息存储在区块链网络中，为监管部门、打假部门或消费者提供各个环节的数据信息。

第四，验证过的信息添加至区块链将会被永久储存，单个节点将无法实现对数据的修改，所以区块链的数据稳定性更高，并具有不可篡改性和不可抵赖性。

第五，节约成本，提高效率。区块链上的数据记录在保密的情况下，由监管部门对产品信息储存、传递、核实、分析，并在不同部门之间进行流转，达到统一凭证、全程记录、企业征信，能够有效解决多方参与、信息碎片化、流通环节重复审核等问题。

6 结语

该系统从技术上突破了传统的溯源防伪系统易复制、信息不透明、数据容易篡改、安全性差、相对封闭等弊端和弱点，为创造一个全新的酒产品诚信体系打下了坚实的基础。

参考文献

[1] ASatoshi Nakamoto.Peer-to-Peer Electronic Cash System[M]，Bitcoin，2009.

[2] 中国区块链技术和应用发展白皮书[M].北京：中国工业与信息化部，2016.

[3] 高昀.我国金融区块链应用的法律问题研究[D].甘肃：兰州财经大学，2017.

[4] 物联网操作系统之安全[EB/OL].(2017-04).[2017-11].http://www.veryol.com.

[5] 王皓,宋祥福,柯俊明,徐秋亮.数字货币中的区块链及其隐私保护机制[J].信息网络安全,2017(07)：32-39.

[6] 刘财林.区块链技术在我国社会信用体系建设中的应用研究[J]. 征信，2017，35（08）：28-32.

[7] 宋志国.加强数字货币关键基础设施建设[J].中国金融家,2017(10)：121-122.

[8] 区块链应用场景[EB/OL].(2016-07).[2017-11].http://max.book118.com.

[9] 李淼.区块链模式下金融业创新与监管研究[J].华北金融,2017(09)：54-57.

[10] 陆阳平.被提前催熟的区块链风口[J].经理人,2017(01)：67-71.

[11] 中投顾问.酒类造假猖獗 整治势在必行[EB/OL].(2012-04).[2017-11].http://blog.sina.com.cn.

[12] 黎勇，徐元根，王军.物联网安全框架与风险评估研究[J].电子测试,2015（19）：81-84.

[13] 张冬杨.2017年物联网发展十大趋势[J].物联网技术,2017,7(02)：3-4.

[14] 张琳.信任的机器，看上去很美[N].光明日报，2017-06-25.