基于联盟区块链的中国福利彩票系统设计*

李梦炜

(中国科学技术大学 网络空间安全学院,安徽 合肥 230026)

摘 要:针对目前中国福利彩票系统存在的数据安全程度有限、公开透明力度不足问题,结合实际情况,采用哈希函数和联盟链技术,对传统彩票系统中数据传输记录、开奖号码产生方面进行了改进,设计了一种具有可实践性的彩票系统。该系统具有的优点:分布式存储保障数据安全;节点权限的层次化降低了联盟链中心化程度,维护购买者隐私;全体购买者均可参与数据监督,对开奖号码随机性进行验证。

关键词:区块链;联盟链;福利彩票;哈希函数

中图分类号:TP309 文献标识码:A DOI:10.19358/j.issn.2096-5133.2020.08.003

引用格式:李梦炜. 基于联盟区块链的中国福利彩票系统设计[J].信息技术与网络安全,2020,39(8):9-14.

China welfare lottery system based on the consortium blockchain

Li Mengwei

(School of Cyber Security, University of Science and Technology of China, Hefei 230026, China)

Abstract: To solve the problems of the limited data security and fairness in the current China welfare lottery system, combining with the actual situation, we use the hash function and consortium blockchain technology to improve the data transmission records and the generation of lottery numbers. The advantages of the system include distributed storage guarantees data security, and the hierarchical level of node authority reduces the degree of centralization and maintains the privacy of purchasers, at the same time, all purchasers can participate in data supervision and verify the randomness of lottery numbers.

Key words: blockchain; consortium blockchain; welfare lottery; hash function

www.pcachina.com

0 引言

2014 年至 2018 年,中国福利彩票总销量已连续 5 年超越 2 000 亿元,截至 2018 年 12 月 31 日,中国福利彩票累计发行销售量为20 197.26 亿元,筹集公益金 6 022.97 亿元,惠及数亿人次,创造税收数百亿元,创造就业岗位 40 多万个。中国福利彩票已经成为中国公益事业和社会福利事业发展不可或缺的重要力量,保障中国福利彩票健康稳固发展具有十分重要的意义。

然而,福彩系统一直风波不断。彩票造假、暗箱操作时有发生,2009 年深圳福彩巨骗案,据深圳警方披露案情,一男子利用职务之便,恶意篡改开奖后的彩票数据,企图伪造一等奖中奖事实,所涉金额高达 3 305 万元;彩票销售、开奖等环节屡屡遭受质疑,原定于 2015 年 1 月 25 日晚 21:30 开奖直播的第 15011 期中国福利彩票双色球游戏(以下称双色球)[1],未能进行开奖直播,也未给出具体“失联”原因;多名中国福利彩票发行管理中心(以下称中福彩中心)主要管理人员连续落马,2018 年中央纪委国家监委网站公布了被查处的福彩领域 4 名局级领导干部的忏悔视频,共有 14 人涉案,更是引发公众质疑。这些事件都对中国福利彩票的公信力造成了极大的负面影响。

2008 年,中本聪(Satoshi Nakamoto)发表了题为《比特币:一种点对点式的电子现金系统》的论文[2],提出了一种基于密码学的电子货币,并命名为比特币,其中最核心的技术就是区块链技术。区块链具有数据不可篡改、公开透明等特征,非常适合于需要保证数据高可信度以及透明度的场景。

目前国内外对区块链在中国福利彩票上的应

*基金项目:安徽省量子通信与量子计算机重大项目引导性项目(AHY150200)

用研究较少,且多集中在互联网彩票上[1,3-6]。然而互联网彩票在监管问题上形式非常严峻,几经波折,目前中国彩票法规中将违规互联网售彩明确为非法彩票[7],各彩票网站均暂停售彩,购买彩票需至线下实体销售网点(以下称销售网点)。同时部分彩票基层工作人员和部分购买者受教育程度不高,对新型销售和购买方式的接受和认可上可能出现问题。

2019 年 4 月 4 日,中国政府采购网发布了《中国福利彩票发行管理中心基于区块链智能合约技术的可公证性电子开奖技术研究与应用公开招标公告》[8],预算金额 284.87 万元,表现了中福彩中心对因地制宜的区块链技术的迫切需求。

本文首先对当前中国福利彩票系统和区块链关键概念进行简要介绍,再提出基于联盟区块链的新型彩票系统的节点结构和具体流程,最后对新系统的性能进行了分析。新系统相较于传统彩票系统和联盟链,有以下三点突破:

(1)在满足监管需求和保护隐私的同时,降低了联盟链的中心化程度,数据被篡改、伪造后更容易被发现、核查。区块链中记录的数据是加密后的数据,保护了隐私;多级节点的设计,对中心节点的权限进行了分割,提高了去中心化的程度;在联盟链中引入了无需授权即可加入但权限有限的自由节点,提高了数据安全程度,且实现了全民监督。

(2)开奖号码不可作伪。以全部购买数据信息为数据源,数据源记录在区块链中“不可篡改”,再利用哈希函数对数据源进行处理后得到的开奖号码,具有可验证性、不可预测性和不可操纵性。

(3)充分考虑实际,易于落地落实。新系统基本没有对现行的线下售票、购票、兑奖环节进行改变,易于被广大购买者和销售网点基层工作人员接受。

1 预备知识

1.1 彩票基本信息

乐透数字型彩票是中国福利彩票的重要组成部分,其规则简单来说就是从多个号码中选择一定号码。2018 年福彩乐透数字型彩票共销售 1 655.65 亿多元,占全年福彩总销量2 245.56 亿多元的 73.73%。其中双色球销售 532.58 亿多元,占全年福彩乐透总销量的 32.17%,是占比最大的乐透型彩种。双色球 2019 年第 39 期至第 138 期这 100 期,平均每期销售额超过 3.5 亿元,体量巨大,具有代表性[9]。以双色球为例,对其开奖方式进行简要介绍。

当期销售结束,在公证人员封存销售数据资料之后,并在其监督下通过摇奖器确定开奖号码。开奖号码由 1~33 中随机选择的 6 个不同数字与 1~16 中随机选择的 1 个数字共同组成。根据购买者所选投注号码与当期开奖号码的相符情况,确定相应的中奖资格。

1.2 当前彩票规则下存在的弊端

(1)所有数据信息中心化集中于中福彩中心,数据安全完全依赖中福彩中心信息安全程度,一旦遭到恶意攻击,交易数据被篡改的后果极为严重;

(2)使用摇号机产生开奖号码并进行直播的方式存在有黑幕的可能性,可信力度不够;

(3)无法完全避免内部工作人员修改数据库或开奖号码;

(4)以实体彩票票券作为中奖唯一凭证过于单一,存在伪造彩票的可能性。

1.3 哈希函数

哈希函数 H 可将任意有限长度的输入映射到固定长度的输出,同时具有以下性质:

(1)单向性:对 $H(x)=y$,已知 y,要找出 x 是困难的;

(2)二原像攻击:已知 x,找出另一个 x',使得 $H(x)=H(x')$ 是困难的;

(3)强抗碰撞性:找出任意两个不同的 x 和 x',使得 $H(x)=H(x')$ 是困难的;

(4)雪崩效应:即使输入发生最微小的变化,输出也会发生剧变;

(5)谜题难解(Puzzle Friendliness)[10]:如果想产生一些特殊的哈希值,同时哈希函数的一部分输入固定、另一部分输入随机,则很难找到那样的随机值,使得计算出来的哈希值正好等于想产生的特殊哈希值。

SHA 是一类由美国国家标准与技术研究院发布的密码学哈希函数。比特币系统中广泛使用的 SHA-256 算法为比特币提供了重要保障,目前仍没有出现明显弱点。本文后续涉及的哈希函数,均采用 SHA-256 算法,后续亦可根据实际情况进行调整,例如可以混合使用多种哈希函数算法。

1.4 Merkle 树

Merkle 树是一种哈希二叉树,其基本结构如图1所示。

利用 Merkle 树可以实现信息快速便捷的完整性验证。底层节点数据的任何变动,都会逐级向上

www.bcachina.com

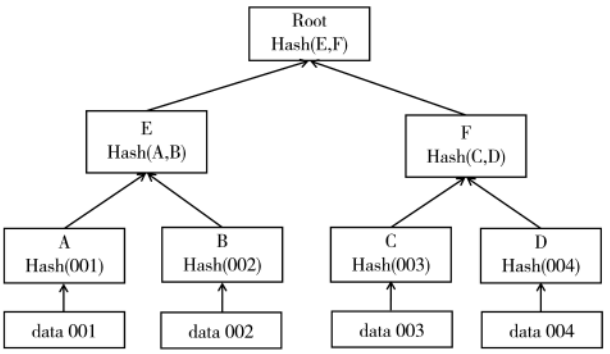

图 1 Merkle 树结构

传递到其父节点,一直到 Merkle 树的根节点,使其根节点的哈希值发生变化。因而可以利用一个节点出发到达 Merkle 树的根节点所经过的路径上存储的哈希值,进行一个 Merkle 证明。

在处理完整性验证的场景中,特别对于分布式环境,Merkle 树可大幅减少数据的传输量和计算的复杂度。以图 1 为例,data 001、002、003、004 的哈希值分别存储在 A、B、C、D 中,不同节点只需验证根节点值是否一致,即可验证数据完整性。若 data 003 遭到篡改,根节点、节点 F、节点 C 对应的哈希值都会发生变化,通过 Merkle 树可迅速进行定位,定位的时间复杂度为 $O(\log(n))$。

1.5 区块链分类

根据管理模式、节点权限、节点规模等方面,区块链分为公有链、联盟链和私有链三种类型。公有链完全去中心化,任何人都可以成为参与者,所有节点权限相同,由全体参与者共同维护。联盟链部分去中心化,由选定的多方共同管理,节点需要许可后才能获得相应的权限[11]。私有链完全封闭,中心化,仅使用区块链的记账功能,记账权由个人独享,不适合应用到彩票系统中。表 1 为公有链和联盟链具体对比。

表 1 公有链与联盟链主要差异

类型	公有链	联盟链
中心化程度	完全去中心化	部分去中心化
激励机制	必备	可选
参与者	任何人	需要许可
记账人	所有参与者	协商决定
共识确认方式	多次确认	立即确认
一致性	大概率一致性	确定性一致性
常用共识算法	PoW、PoS 等	Paxos、PBFT 等
交易处理时间	长(分钟级别)	短(秒级别)
承载能力	3~20 次/秒	1 000 次/秒以上

在中国福利彩票应用方面,联盟链是优于公有链的,原因如下:

(1)公有链所有人都可以自由参与,且所有节点都平等地拥有权限,于监管不利,而联盟链每个节点均有准入机制,参与共识、写入及查询数据均可由授权控制,可满足监管要求。

(2)公有链常用的共识机制,PoW 速度慢且耗能巨大,PoS 存在马太效应的问题,且主链有概率分叉,对交易处理需要等待主链确认,速度较慢,而联盟链采用的共识机制速度较快,而且具有确定性一致性,不存在分叉的情况。

(3)公有链承载能力较低,不能满足彩票交易的需求,而联盟链承载能力较公有链大大增加。

2 系统设计

2.1 节点结构

定义以下 4 种节点类型:

1 级节点:对应中福彩中心,亦可根据实际情况增设。负责按时间戳顺序整理联盟链内数据,打包成区块发送给 2 级节点,同时负责 2 节点的管理授权。

2 级节点:对应各省福彩机构与监管机构,亦可根据实际情况增设。参与共识,负责接收 1 级节点发送的区块,接收 3 级节点发送的交易数据,同时负责 3 级节点的管理授权。

3 级节点:对应销售网点。负责向 2 级节点发送交易产生的数据信息。

4 级节点:对应购买者。不需要授权,所有人都可自由参与,只有下载权限,可在任意时间从 1、2 级节点下载区块链到本地。

2.2 具体流程

2.2.1 准备阶段

当期彩票销售开始前两个小时,所有 2 级节点向证书颁发机构发出申请,经 1 级节点审核通过后,证书颁发机构为每个 2 级节点生成一组公钥和私钥,每个 2 级节点保存自己的私钥,1 级节点保存所有 2 级节点的公钥,在一个小时内完成密钥分配。

当期彩票销售开始前一个小时,所有 2 级节点已完成密钥分配,所有 3 级节点向证书颁发机构发出申请,经 2 级节点审核通过后,证书颁发机构为每个 3 级节点生成一组公钥和私钥,每个 3 级节点保存自己的私钥,2 级节点保存所有 3 级节点

www.pcachina.com

的公钥,在一个小时内完成密钥分配,准备开始彩票销售。

2.2.2 销售阶段

交易数据传输情况如图 2 所示。

当期彩票开始销售后,购买者在一个 3 级节点对应的销售网点进行了一笔彩票交易,该 3 级节点即将本次彩票的交易数据(包括时间戳、3 级节点编号、购买种类、购买数量、购买号码)用分配的私钥进行数字签名后,得到数字签名 3,将交易数据和数字签名 3 发送给数个被配置的受信任的 2 级节点。同时,销售网点内的投注机将交易数据和数字签名 3 等信息均打印在纸质彩票上,提供给购买者。

2 级节点接收到 3 级节点发送的数据后,根据 3 级节点编号,用相应的公钥进行验证,验证通过后,用分配的私钥对时间戳、2 级节点编号、3 级节点编号、数据签名 3 进行数字签名,得到数字签名 2,将时间戳、2 级节点编号、3 级节点编号、数字签名 3、数字签名 2 发送给 1 级节点。

1 级节点接收到 2 级节点发送的数据后,根据 2 级节点编号,用相应的公钥进行验证,验证通过足够数量的 2 级节点签名后[13],记录下时间戳、3级节点编号、数字签名 3,按照时间戳对记录下的数据进行排序,并每隔 5 分钟将数据打包生成一个区块,每个区块包括区块体和区块头两部分。区块体存放前一区块生成之后记录的批量数据,区块头存放区块编号、区块时间戳、前块哈希、基于块内交易数据哈希生成的 Merkle 根。区块发送给所有 2 级节点,每个 2 级节点对区块进行核验,核验通过后将区块下载到本地,链入主链。

销售时间截止后,所有 3 级节点停止彩票销售,等待 1、2、3 级节点处理完所有待处理数据后,1 级节点将剩余未打包的数据全体进行打包,生成本期最后一个区块,发送给所有 2 级区块,所有 2 级区块记录完毕后,销售阶段结束。

2.2.3 开奖阶段

销售阶段结束后,不再产生新的区块,核查 1级节点和所有 2 级节点区块链信息。核查无误后,对区块链上所有区块的块哈希数据进行两次哈希,得到一个哈希值 HASH。

以双色球为例,符合双色球游戏规则的所有号码组合共有 $C_{33}^{6}\cdot 16=17\ 721\ 088$ 种,对全体号码组合进行排序,用哈希值 HASH 模去 17 721 088,以所得的余数为序号的号码即为当期的开奖号码。

3 系统性能分析

3.1 数据安全

所有数据分布式存储在中彩票中心、各省福彩机构和监管机构,恶意攻击且成功篡改数据的难度极大;联盟链的准入和权限控制机制,从源头上避免了恶意节点的介入;任意一个环节出现问题后,可以利用 Merkle 树进行排查,迅速准确地定位问题所在;所有人都能够在任意时间下载区块链,数据公开透明。

3.2 节点权限分级

利用多级节点设计,将系统职能进行分割。与

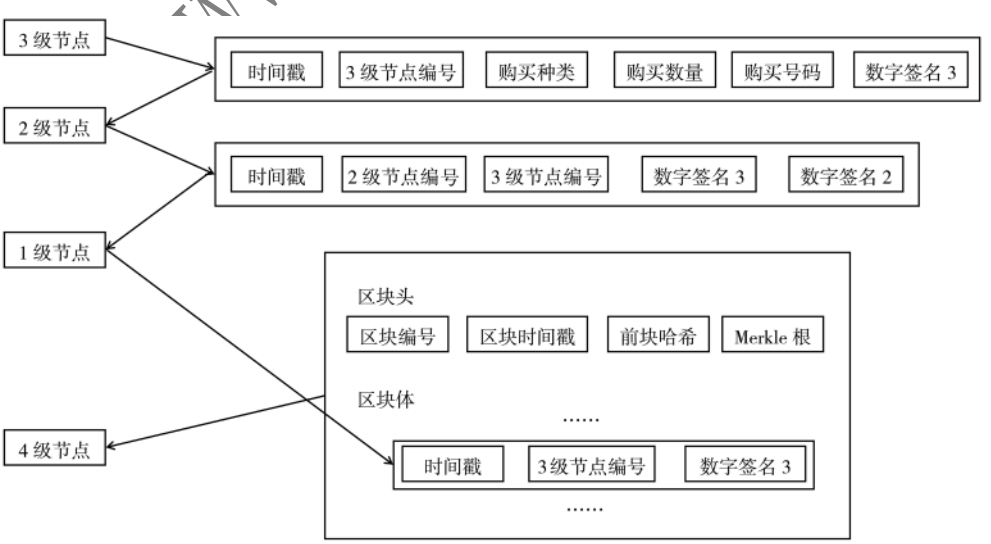

图 2 交易数据传输

www.bcachina.com

普通联盟链相比,去中心化程度更高。1级节点作为拥有记账权的节点,接收不到最原始的交易数据,接收到的是被3级节点的私钥数字签名后的数据,而1级节点并没有3级节点的公钥。这一设计让1级节点极难进行数据伪造,即使伪造了数据,也极易被2级节点识破,基本不可能由此牟利。

3.3 有效保护隐私

系统没有在区块中直接记录交易数据,而是记录加密后的交易数据,这样即使数据可以被任意下载,也不会泄露购买者的隐私信息。

3.4 开奖号码随机且可验证

(1)可验证性

每位购买者,均可根据所持彩票上的交易数据和数字签名3,准确在区块链中定位到自己交易产生的记录,即可验证购买者的确参与了开奖号码的产生。

(2)不可预测性

产生开奖号码的数据源来自数量众多的购买者的自由意志,每位购买者在购买种类、购买数量、购买号码、购买时间、选择的销售网点等方面均由每位购买者自己决定,为真随机数据源。且数据经过了多次哈希运算,由哈希函数的单向性和雪崩效应,任一位购买者的抉择发生任何微小的变化,开奖号码都会随之变化。

(3)不可操纵性

考虑到最极端的情况,假设某攻击者可以确定自己将成为当期彩票的最后一名购买者,同时已获得了当期之前所有区块链数据,还盗取了即将投注的销售网点的私钥信息。若该攻击者先确定购买号码等交易数据,进行一次哈希运算得到最后一个区块的块哈希数据,和之前所有块哈希数据一起,再进行两次哈希运算,所得到的哈希值经过模运算后,获得的开奖号码需要恰好对应攻击者先前确定的购买号码。根据谜题难解可知,这个求解是极难的。同理,若该攻击者先确定开奖号码,也是极难求解的。

3.5 周期短

目前支撑比特币的区块链运行历史最长,从2009年开始,而根据比特币的设计,还需要100多年才能挖完全部比特币,10年的实验案例很难说明未来100年能否安全运行。本文为中国福利彩票设计的新系统,每期只需运行2至3个自然日,10年的案例来说明如此短期运行的安全,是非常有说服力的。

3.6 可操作性高

充分考虑了当前部分销售网点基层工作人员和部分购买者文化程度不高的实际情况,本系统在基层工作人员销售和购买者购买、兑奖环节基本没有做出改变,贴合实际,易于落实推广。

此外,中国彩票系统硬件设施均为统一配置,也可考虑采用硬件加密技术,进一步提高系统安全性和运行效率。

3.7 全民监督

每位购买者都可以参与保障数据安全不可篡改,确认自己参与了开奖号码的产生,每位购买者都可以成为监督者,亲自认证了新型彩票系统的公平公开公正。数据不可篡改保证了彩票每期总销售额不会遭到虚报少报,从资金源头进行了控制,一定程度上维护了公益金的安全,变相遏制了部分贪腐行为。

4 结束语

本文分析了中国福利彩票系统面临的风险与弊端,设计了一个基于联盟区块链的新型彩票系统。该系统强有力的保障了彩票交易数据的安全,通过新型开奖号码产生方式与全民监督的模式,可以提高购买者对中国福利彩票的信任程度,还在一定程度上维护了公益金的安全,具有较强的实用性,为中国福利彩票系统的革新提供了参考价值。

参考文献

[1] YONGRAE J, CHANIK P. BlockLot: blockchain based verifiable lottery[J]. arXiv: 1912.00642, 2019.

[2] NAKAMATO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. https://www.bitcoincash.org/bitcoin.pdf.

[3] LIAO D Y, WANG X H. Design of a blockchain-based lottery system for smart cities applications[C]. Color Imaging Conference, 2017: 275-282.

[4] MILLER A, BENTOV I. Zero-collateral lotteries in bitcoin and ethereum[C]. 2017 IEEE European Symposium on Security and Privacy Workshops(EuroS&PW), 2017.

[5] 梅颖. 一种分布式互联网彩票安全策略[J]. 武汉大学学报(工学版), 2017(5): 790-794.

[6] 李聪, 刘新, 李梦磊, 等. 一种基于区块链的数字彩

www.bcachina.com

票发行系统[J].信息安全研究,2018(12):1142-1148.
[7] 互联网售彩明文列为非法彩票[J].理财,2018(10):8.
[8] 曾祥昌.从"福彩延迟开彩"事件看待彩票监管制度存在的问题及完善[J].法制博览,2015(28):188-189.
[9] 邹均,于斌,庄鹏,等.区块链核心技术与应用[D].北京:机械工业出版社,2018.8.
[10] KIAYIAS A,ZHOU H S,ZIKAS V. Fair and robust multi-party computation using a global transaction ledger[C].The Annual International Conference on the Theory and Applications of Cryptographic Tech niques,2016:705-734.
[11] ANDROULAKI E,BARGER A,BORTNIKOV V,et al. Hyperledger Fabric:a distributed operating system for permissioned blockchains[C].Proceedings of the Thirteenth EuroSys Conference.ACM,2018:30.

(收稿日期:2020-07-01)

作者简介:

李梦炜(1993-),男,硕士研究生,主要研究方向:区块链。

(上接第 5 页)

Systems,2018,9(1):1-20.
[16] MARY J,MATTHIEUDE L,VINCENZO P,et al.Use cases for blockchain in the energy industry opportunities of emerging business models and related risks.[J].Computers & Industrial Enginering,2019(137):1-9.
[17] European Commission.Blockchain now and tomorrow[R].Brussels, 2019.
[18] Bundesministerium fur Wirtschaft und Energie,Bundesministerium der Finanzeen.Blockchain-Strategie der bundesregierung[R].Berlin,2019.
[19] BUNZ B,BOOTLE J,BONEH D,et al.Bulletproofs:efficient range proofs for confidential transactions[C].IEEE Symposium on Security and Privacy,2018.
[20] SASSONE B,CHIESA A,GARMAN C,et al.Zerocash:decentralized anonymous payments from bitcoin[C].IEEE Symposium on Security and Privacy,2014.
[21] 中国信息通信研究院.区块链白皮书[R].北京,2018.
[22] Center for A New American Security.Indo rising to the China challenge:renewing American competitiveness in the Indo-Pacific[R].Washington D.C.,2019.
[23] WEF.Inclusive deployment of blockchain for supply chains:part 6-a framework for blockchain interoperability[R].Geneva,2020.
[24] GAUR V,GAIHA A.Building a transparent supply chain[EB/OL].[2020-07-01].https://hbr.org/2020/05/building-a-transparent-supply-chain.

(收稿日期:2020-07-29)

作者简介:

郭滕达(1982-),女,博士,副研究员,主要研究方向:区块链技术与绿色技术创新。

周代数(1985-),通信作者,男,博士,主要研究方向:区块链技术与数字货币。E-mail:zhoudaishu@126.com。

(上接第 8 页)

[4] 程斌琪.金融科技对金融服务贸易自由化的影响研究[D].北京:对外经济贸易大学,2019.
[5] 中国工商银行河北省分行课题组,宋颖新,韩长征,申克敏.商业银行在雄安新区建设中的市场机遇与对策[J].河北金融,2019(1):27-32.
[6] 李朋林,董一一.区块链技术在商业银行业务模式创新中的应用[J].财会月刊,2018(21):46-52.
[7] 程华,杨云志.区块链发展趋势与商业银行应对策略研究[J].金融监管研究,2016(6):73-91.

(收稿日期:2020-05-14)

作者简介:

宫延新(1982-),男,硕士,工程师,主要研究方向:国际结算电子化。

宣奇(1984-),男,硕士,经济师,主要研究方向:国际结算电子化。

陈志明(1986-),男,博士,工程师,主要研究方向:金融科技创新。

www.pcachina.com

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所