软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链技术在安全软件领域的研究与应用*

黄家承[1], 杨振国[1], 刘文印[1]

[1](广东工业大学 计算机学院,广东 广州 510006)

通讯作者: 刘文印, E-mail: liuwy@gdut.edu.cn

摘 要: 区块链技术是一种源于数字加密货币的分布式数据库技术方案,该技术方案整合了数学、密码学、计算机科学领域的成果,具有去中心化、不可篡改、去信任化等优势。安全软件指辅助用户管理计算机安全的软件,是计算机防御系统的重要组成部分,其作用包括但不限于防止病毒传播和防护网络攻击。安全软件降低了用户遭受网络攻击的风险,但现阶段,安全软件的发展面临着两个问题:恶意安全软件泛滥和用户安全意识不足。本文从区块链的底层实现、关键技术等方面阐述了区块链技术应用在安全软件领域的优势和思考,提出了区块链技术用于安全软件辨识和用户安全意识量化与激励的解决方案,旨在对区块链技术在网络安全相关领域的研究提供方向和帮助。

关键词: 区块链;安全软件;用户安全意识;智能合约

中图法分类号: TP311

中文引用格式: 黄家承等.区块链技术在安全软件领域的研究综述.软件学报. http://www.jos.org.cn/1000-9825/ 0000.htm

英文引用格式: Huang JC, etc. Research and Application on Blockchain Technology in Security Software, 2018 (in Chinese). http://www.jos.org.cn/1000-9825/0000.htm

Research and Application on Blockchain Technology in Security Software

HUANG JiaCheng[1], YANG Zhen-Guo[1], LIU Wen-Yin[1]

[1](School of Computer Science and Technology, Guangdong University of Technology, Guangzou 510006, China)

Abstract: Blockchain technology is a distributed database technology solution originating from digital cryptocurrency. This technology integrates the achievements from the fields of mathematics, cryptography and computer science, and has the advantages of decentralization, non-tampering and trustworthiness. Security software refers to software that assists users in managing computer security. It is an important part of the computer defense system, functions include, but are not limited to, preventing virus propagation and protecting against network attacks. Security software reduces the risk of users being attacked by cyber attacks, but at this stage, the development of security software faces two problems: the proliferation of malicious security software and the lack of user security awareness. This paper expounds the advantages and considerations of blockchain technology application in network security from its bottom layer implementation and key technologies, and proposes solutions for blockchain technology for security software identification and user security awareness quantification and incentive, aiming at providing direction and assistance to the research of blockchain technology in the field of network security.

Key words: blockchain; security software; user's security awareness; smart contract

自 2008 年中本聪发表论文《Bitcoin: A peer-to-peer electronic cash system》[1]以来,随着比特币、以太坊等数字加密货币的流行与发展,作为其底层技术的区块链引起了人们的广泛关注,麦肯锡报告指出区块链是目前最有潜力触发第 5 轮颠覆性革命浪潮的核心技术[2]。区块链是由区块链网络中所有节点共同维护的一种分布式共享数据库,结合了密码学、数学和计算机科学等多个领域的研究成果,利用去中心化和去信任的方式对数据进行修改,具有不可篡改和完全可追溯的安全特性[3]。区块链除了在货币上的应用外,还有各

基金项目:国家自然科学基金(No.61703109);广东创新研究团队计划(No.2014ZT05G157)

收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00

CNKI 在线出版时间: 0000-00-00

种衍生应用，如文件存储、电子商务、智能合约系统等。

软件认证机制是网络安全中不可或缺的一环。传统的软件认证机制为摘要认证机制，软件开发商将程序二进制文件的信息摘要公开，用户在执行程序前，在本地计算出程序的信息摘要并与开发商公布的摘要进行比对。这种认证方式只能认证软件是否遭到篡改，并不能认证软件的真伪，无法防御钓鱼软件和恶意软件的攻击。随后，软件认证引入了数字签名认证的机制，用户可以通过查看数字签名的方式来确定软件开发商、发布时间等信息，一但应用被篡改，软件数字签名信息就会被破坏，这样就可以在一定程度上保证用户获取到应用程序的安全。相较于信息摘要认证机制，数字签名认证机制在一定程度上解决了钓鱼软件的认证问题，但是面对无签名信息或伪造签名的恶意软件或钓鱼软件依然束手无策，目前已有专门的产业链为恶意软件颁发数字签名[4]。而且这种认证机制本身也存在着许多安全问题：数字签名的生成、存储与颁发过程由认证机构服务器执行，这种中心化的认证机制带来了极大的安全风险，攻击者可以通过窃取认证机构的证书为恶意软件进行签名[5]。；虽然数字签名采用了非对称密钥进行加密，但是密钥对不曾变更或变更周期较长，具有被暴力破解的隐患。除了这两种认证方式外，还有基于外部设备的认证机制，如基于 USBKey 的软件认证保护机制[6]，这类认证方式虽然安全性得到了保证，但是成本高、使用不便，在可用性方面差强人意。

安全软件是杀毒软件，系统工具和反流氓软件的统称。安全软件对维护网络信息安全[7]具有及其重要的意义，大多数互联网用户都依赖安全软件来保护自己的设备不受网络攻击的侵害。然而这种依赖被攻击者加以利用，伪装成安全软件的恶意软件应运而生，泛滥全球，侵害了许多安全意识不足的用户的权益。随着互联网的规模不断扩大，互联网设备所面临的安全风险将不断上升，安全软件的重要性愈发凸显。然而，现阶段安全软件的发展面临着以下两个问题：

(1) 恶意安全软件泛滥

恶意安全软件是伪造成合法安全软件的外观的恶意软件。用户安装恶意安全软件后，其将通知用户称计算机感染了恶意软件，诱使用户付费并解锁软件的“高级功能”以解除安全威胁[8]。恶意安全软件的危害不仅限于诈骗用户的钱财，还会窃取用户账户信息和危害设备安全。恶意安全软件可以在用户设备上执行多种恶意操作，比如在用户的计算机上安装击键记录软件或者用于盗取密码的木马病毒软件以窃取用户的个人资料，或者安装将伪造信息传播给别人的恶意软件进行传播。恶意安全软件波及范围广，危害大。知名安全软件公司 McAfee 警告称：全球每天有 100 万人受到恶意安全软件的侵害[9]；FBI 亦警告称某恶意安全软件一年可以获得 1.5 万美元的非法牟利[10] 。恶意安全软件不仅会威胁用户设备安全，也会令安全软件公司利益受损，比如造成客户流失，收集到虚假的用户数据等。恶意安全软件的泛滥造成了用户和安全软件公司双输的局面。

(2) 用户安全意识薄弱

使用安全软件的用户安全意识良莠不齐，即使安全软件具有极佳的防护效果，如果用户安全意识不足，攻击者依然能通过多种方式来绕过安全软件的防护，比如通过弱密码获取设备管理员权限，亦或是通过系统漏洞来获取设备的控制权，进而令安全软件失效。用户安全意识不足是引发网络攻击事件的诱因，原因有三：首先，安全意识弱的用户通常会使用弱密码以方便记忆，据威瑞森发布的《2017 年的数据泄露调查报告》，在外部攻击所导致数据泄露的众多网络安全事件中，81%的数据泄露涉及到撞库或弱口令[11]，随着互联网技术的发展，特别是人工智能的广泛应用，此类针对弱密码的用户账户攻击将更加精确和有效。其次，安全意识不足也体现在使用过时的软件或系统上，截至今年 4 月 3 日，失去微软官方安全支持的 Windows XP 系统目前市场份额为 4.59%[12]，使用该系统的用户极易遭受最新系统漏洞的攻击。再者，由于用户缺乏安全意识，会做出一些危险的举动，为攻击者提供了极大的便利：如打开来历不明的网页、电子邮件链接或附件所引发的钓鱼攻击，未对下载的文件进行病毒扫描所导致的病毒感染等，根据 Gemalto 公布的最新报告，2018 上半年用户账户信息被盗数量增长了 133%，而所有被盗事件中，超过半数是攻击者瞄准了用户不良的使用习惯，通过漏洞或者恶意软件等方式完成攻击 [13]。随着物联网和互联网技术的发展，网络中的用户数量和设备数量会不断增长，用户安全意识在网络安全体系中将变得愈发重要。

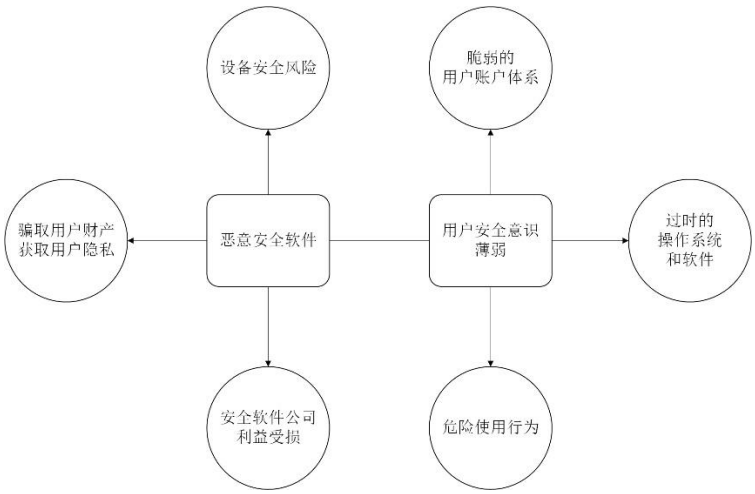

图 1　安全软件所面临的两个问题

解决以上两个问题的关键在于建立一个有效的安全软件辨识与认证机制，激励用户提高安全意识并养成良好的使用习惯。区块链在解决安全软件问题方面具有极大的技术优势。在软件认证方面，区块链技术可以提高传统认证机制的可用性和安全性，利用区块链去中心化和去信任化的技术特性可以低成本、自动化地辨识安全软件的真伪，共识机制和不可篡改性保证了认证数据的安全性。智能合约的应用让用户安全意识量化整个过程自动化、透明化，可为激励用户提高安全意识提供良好的解决方案。

本文第 1 节对区块链技术原理进行梳理。第 2 节阐述了区块链应用在安全软件领域的技术优势，提出了结合区块链技术的安全软件认证和用户安全意识量化与激励的解决方案。第 3 节提出了区块链技术在应用中遇到的问题与不足，为网络安全相关领域的研究提供方向和思路。最后一节为全文总结。

1　区块链技术简介

1.1　区块链的底层架构

区块链的底层架构是区块。区块，是区块链网络中用于存储信息的数据结构，包含两个部分：区块元数据[14]和区块体。区块元数据包含了用于区块链中用于认证和溯源的必要信息，包括父区块的哈希值、版本号、Merkle 树根、时间戳和计数器。区块体中记录了一段时间内所有的交易记录的哈希值和交易数量。区块的结构如图 2 所示

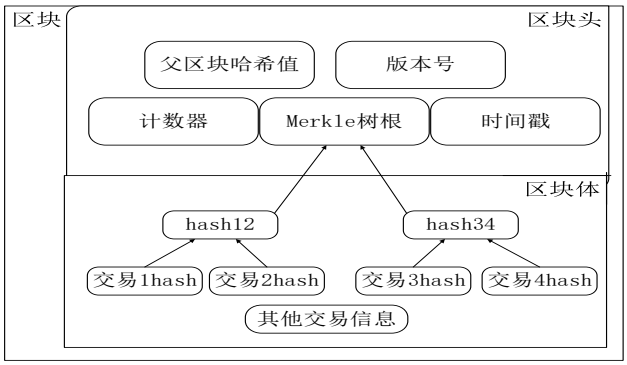

图 2　区块结构

当前区块通过存储前一区块的哈希值与前一区块相连，形成链式结构[15]，任意区块都可通过链式结构追溯到并获取到从创世区块至当前区块所包含的所有交易信息。版本号、计数器分别标识区块链所使用软件/协议的版本和当前区块的序号，时间戳记录了区块通过共识机制认证并加入区块链的时间（UNIX 纪元秒）。Merkle 树根归纳了一段时间内所有交易的哈希值，用于认证交易信息的真伪。区块头信息可以按照共识机制发展进行扩展，如在 POW 共识机制下，区块头中添加了随机数和难度控制信息以筛选区块。

1.2 区块链的关键技术

1.2.1 分布式结构

区块链使用了点对点技术，它没有中心服务器，数据存储分布于网络中各个节点上。每个节点在记录数据的同时，也对其他节点发送的数据进行验证。每个节点相对独立，单个节点的失效对整个系统几乎没有影响。这种去中心化的存储结构让区块链的安全性和容错性得到了保证。

1.2.2 共识机制

区块链网络中所有节点都在记录数据，产生区块。共识机制的作用是使系统各节点达成共识，选出唯一一个区块加入区块链中。通过共识机制，区块链实行了去信任化的存储方式，节点间无需依赖可信的第三方即可建立信任关系，若想篡改某一区块的数据，必须得修改该区块和其后续区块的数据，同时还需要网络中所有节点达成共识，承认篡改的数据。去信任化赋予了区块链上数据不可篡改的特性。目前共识机制主要分为三类：工作量证明机制、权益证明机制和强一致共识机制。不同的共识算法都有其优劣，目前还没有一种共识够机制能够解决“不可能三角”问题[16]。

1.2.3 非对称加密技术

非对称加密也称公开密钥加密，是密码学的一种算法，由公钥和私钥配对组成。用公钥加密的数据只能用私钥解密，私钥加密的数据只能用公钥解密，虽然两个密钥在数学上相关，但如果知道了其中一个，并不能凭此计算出另外一个[17]。区块链中，非对称加密技术主要应用于数据加密和数据签名，为区块链提供了安全性、不可否认性和匿名性。

1.2.4 智能合约

在区块链中，智能合约的定义为：由事件驱动的，具有状态的，运行在一个可复制和共享的账本上，且能够保管账本上资产的程序[18]。智能合约内封装了预置的触发条件、响应条件和执行的操作等内容，以代码的形式部署在区块链上，当满足合约的条件触发时，合约内预置的操作将自动执行。智能合约极大地提升了区块链的拓展性，通过部署智能合约，区块链可以应用于各种场景，如投票、金融、博彩等。

2 区块链技在安全软件领域的应用

2.1 区块链技术应用于安全软件领域的动机

区块链的底层数据结构为基于时间戳的链式结构[19]，每个区块都包含着前一区块的哈希值，并通过密码学的方式来保证区块中的数据不可被篡改与伪造，每一笔交易在节点达成共识后，区块数据将和区块生成的时间戳一起永久性地存储在区块体中。这种数据结构保证了区块链上数据的不可否认性和可追溯性，这些特性为低成本、自动化认证安全软件提供了可能。

区块链应用具有极强的可塑性，开发人员可以通过在区块链上部署脚本来进行应用层服务的拓展，也可以通过构建智能合约来实现更为复杂的区块链应用[20]。区块链的共识机制能够监督并确保智能合约的执行。通过部署恰当的智能合约，可以实现自动化、智能化的软件辨识和激励方式。

区块链使用非对称加密技术对用户个人数据进行信息加密和数字签名，保障了用户的隐私。同时区块链中的用户的身份辨识仅与其私钥地址有关，与用户自身或用户设备无任何关系，用户运行区块链应用时不会暴露自己的个人信息。对数据的加密和区块链的匿名性可以让攻击者无法从区块链上的数据中定位到有价值的攻击目标。

下面从安全软件认证和用户安全意识量化与激励两个个方面来探讨使用区块链解决安全软件问题的方法与思路。

2.2 结合区块链技术的安全软件认证机制

在用户安装安全软件时，需要对安全软件的真实性进行认证，认证分为两个方面：一是认证软件公司是否真实可信，二是认证软件本身是否被篡改。使用区块链技术结合公钥密码数字签名机制[21]可以便捷地解决这个认证问题。认证信息为软件的信息摘要。认证信息通过两轮加密，与以往的固定密钥不同，通过对智能合约的应用，可以在使用随时间变化的密钥进行加密以降低被暴力破解的风险的同时，保证系统的可用性。利用区块链技术的共识机制，整个认证过程可以自动进行，不需人工筛选辨别，在保证了安全性的同时极大地降低了用户与安全公司的辨识成本，一举两得。以下是认证方案的具体说明：

安全软件公司使用散列算法，根据软件的二进制文件、软件版本、软件发布时间、软件公司信息生成信息摘要，并使用软件公司的私钥对信息摘要进行加密，将公司写入区块链中。通过智能合约的方式，在区块链网络中生成随时间变化的临时公钥-密钥对。生成临时密钥对后在区块中添加临时公钥信息，使用临时私钥对加密后的信息摘要进行二次加密。使用两个不同的密钥对进行二次加密可以提升安全性[22]。将二次加密后的信息摘要放置于区块中，并向全网广播。

用户在安装安全软件后，节点生成软件的信息摘要，并确认本地生成的摘要是否在区块链中失效摘要列表中，如果存在，则认证失败。随后，节点根据安全软件的公司信息，在最新的区块中寻找软件对应的加密信息摘要、临时公钥和安全软件公司的公钥，如果没有对应安全软件公司信息，认证失败，提醒用户该安全软件为恶意安全软件。最后，节点使用区块中的临时公钥进行第一轮解密，使用软件公司公钥进行第二轮解密，获取软件的信息摘要，将解密后的信息摘要与本地运算得出的信息摘要进行比对。比对成功，说明软件没有被篡改，与安全软件公司发布的一致，可以信任。解密失败或比对失败则认证失败，提醒用户软件已被他人篡改。在进行软件认证的同时将认证失败的摘要加入区块的失效摘要列表，以简化后续的验证流程。

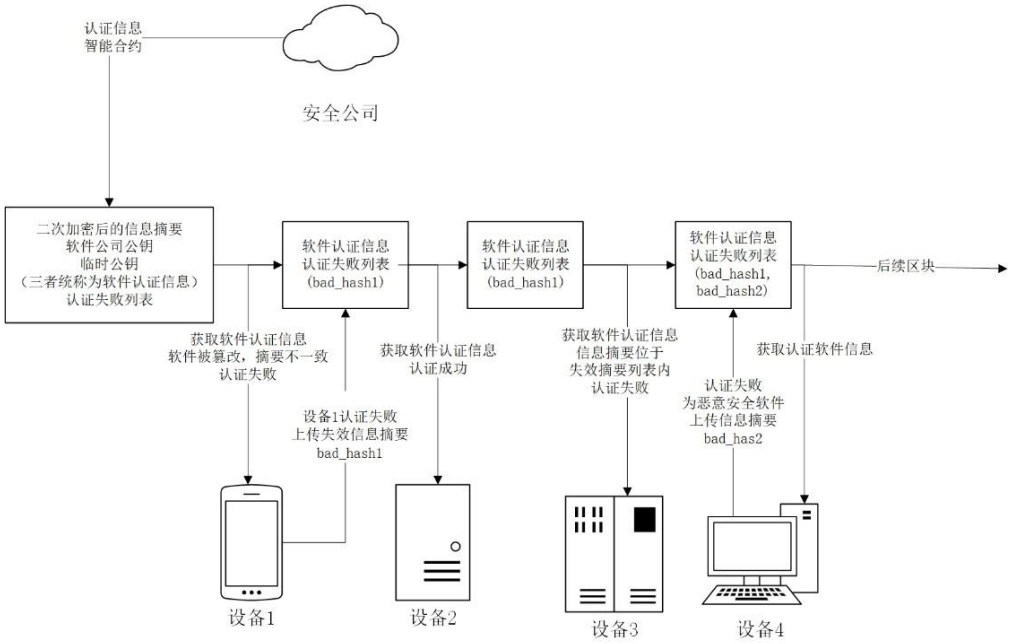

图 3　安全软件认证解决方案

制作恶意软件的攻击者在该认证机制下极难获得成功，原因有二：

- 理论上，恶意安全软件制作者虽然可以获取到安全软件的信息摘要，将篡改或伪造后的软件摘要信息替换为真实软件的摘要以通过验证，但是由于缺少安全软件公司的私钥，攻击者的信息摘要无法通过区块中的公司公钥进行解密，因此无法通过验证。即使攻击者通过某些手段获取到了安全软件公司的私钥，并使用该私钥对恶意安全软件进行签名，由于智能合约的作用，攻击者还需要获取随时间不断变化的私钥来对软件信息摘要进行二次加密。由于公开密钥体系的特性，攻击者要想在短时间内根据区块链中的临时公钥推导出私钥，在理论上极难实现。
- 区块链中的失效摘要列表存储了认证失败软件的摘要信息，攻击者制作的软件一经认证失败，其摘要将加入封禁列表，永远无法通过认证。攻击者每尝试一次攻击，都需要对软件的信息进行一次修改，大幅增加了攻击的时间成本。

由此可见，区块链技术的加入极大地提升了传统软件认证机制的安全性和可用性。

2.3 结合区块链技术的用户安全意识量化与激励机制

Token 是区块链领域中运用密码学技术确认权属，基于共识机制发行和流通的私人信用凭证[23]。用户的安全意识由用户 Token 呈现。用户 Token 以节点安全性评分为核心，结合其他因素，量化了用户安全意识，为激励机制提供了评价标准。用户节点安全性评分的评判依据分为两个方面：系统环境和行为分析。每个节点都有相同的初始评分，根据系统环境和行为分析的结果对评分进行扣除，得到与节点绑定的最终的评分。得益于区块链的匿名性，攻击者无法确定安全评分低的节点位置和详细信息。同时，智能合约和共识机制的作用可令整个过程自动化和透明化，不可篡改性保证了节点评分和用户 Token 的可信度。下面将对系统环境和行为分析这两个方面的评分机制，和基于用户 Token 的激励机制做出概述。

2.3.1 系统环境评分机制概述

系统环境的评分依据的是用户设备上的软件，包括操作系统、驱动、浏览器、邮箱等常用软件是否为最新版。在大多数情况下，软件更新的内容为增加功能、提升性能，更重要的是修补软件漏洞以防止黑客利用。2017 年 5 月肆虐全球的勒索软件 Wanacry 利用了些版本的微软服务器消息块（SMB）协议中的数个漏洞，然而漏洞补丁已于 3 月份放出，通过升级系统打补丁的方式可以免疫此次攻击[24]。谷歌公司每月都会对安卓系统推送安全补丁以修复漏洞， 2018 年 8 月的安全补丁修复了 37 个高级别、6 个严重级别的漏洞，漏洞的类型类型涉及任意代码执行和远程信息泄露，与驱动相关的漏洞多达 22 个，极度危险[25]。浏览器、邮箱等常用软件若不及时更新，其漏洞亦会引发安全事件，如 Chrome 浏览器地址栏欺骗漏洞(CVE-2016-1707)，该漏洞存在于版本号低于 v52.0.2743.82 的 chrome 浏览器，攻击者可以利用这个漏洞发起网络钓鱼攻击[26]。因此及时更新软件，修复漏洞对维护设备安全极为重要，以软件版本号作为评判用户安全意识的一环是合理的。

节点收集用户设备的系统版本S_L、驱动数量n_1和版本D_L、常用软件数量n_2和版本号N_L，同时生成本地的信息摘要，与区块中对应版本的信息摘要进行比对以防止版本号伪造。随后，节点与区块中的最新版本信息（S_C、D_C、N_C）进行比对，根据版本号的差对扣分项进行累积，得出系统环境扣分F_1。

$$F_1 = (S_C - S_L) + \sum_{i=1}^{n_1}(D_C - D_L)_i + \sum_{p=1}^{n_2}(N_C - N_L)_p$$

2.3.2 用户行为分析评分机制概述

用户实体行为分析(UEBA)是 Gartner 认为 2016 年十大信息安全技术之一，它通过收集用户、系统、应用等多方面的信息进行分析，找出异常情况并进行告警[27]。用户实体行为分析通常采用监督和非监督的机器学习技术来检测异常行为和发现威胁[28]，监督的机器学习模型用以提供快速的行为分析结果，非监督的机器学习模型的自学习能力能够随着用户行为习惯的变化持续、自适应地准确识别用户不安全的行为。行为分析需要在网络中广泛采集行为数据，区块链的不可否认性令了用户无法否认节点上传的数据，确保数据的真实性；通过在区块中存储模型和模型信息摘要，杜绝了攻击者或用户修改模型以伪造评分、隐匿恶意数据的可能。

在该情境下，节点结合了 EDR、NGFW 的功能，对用户的操作进行信息收集并导入模型，得到的模型分

析结果作为评分的依据。模型收集的信息如下图所示：

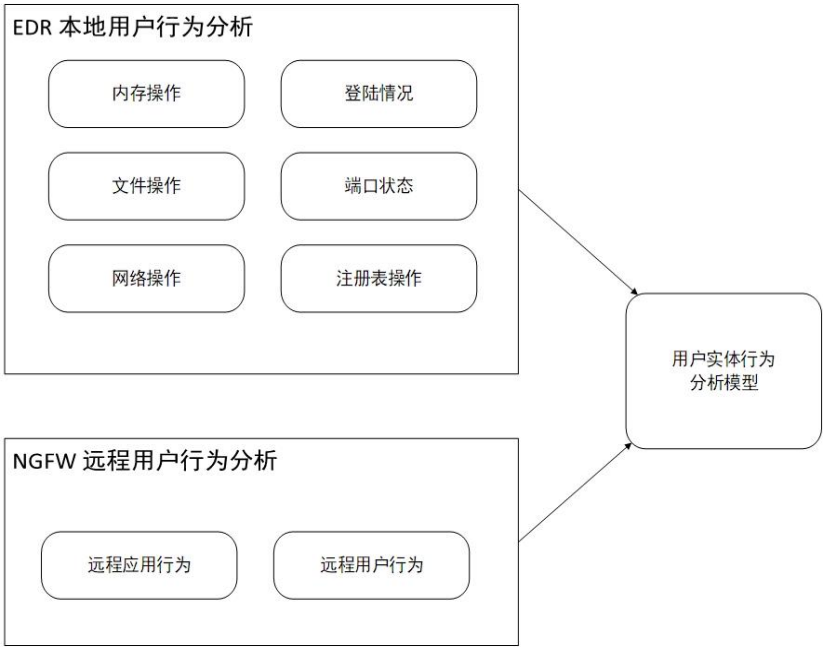

图 4　用户实体分析模型概述

如果用户的某个行为被模型判定为不安全行为，会根据行为中包含的操作类型O和操作数量N扣除节点的安全评分。比如用户点击了钓鱼邮件内的链接并下载安装了钓鱼软件，该行为中包含了内存操作、文件操作和网络操作，在计算节点评分时会对这三项操作的评分进行扣除。节点随后将不安全行为的操作内容经用户节点私钥加密后上传至安全公司服务器中，供优化模型和安全事件分析所用。用户行为分析评分F_2的计算公式为：

$$F_2 = \sum_{i=1}^{n} O_i \times N_i$$

2.3.3　用户 Token 与激励机制概述

用户的安全意识通过 Token 呈现，节点安全性评分对 Token 有着决定性的影响。每个节点的初始评分F减去系统环境与用户实体分析模型的扣分项得到最终的评分，该评分不仅体现了节点是否易遭受攻击，而且结合各项分析结果可以根据不同的用户情况提出针对性的解决方案。用户可以通过完成解决方案来提高节点评分，通过智能合约在区块链上部署相应的解决方案并与安全软件公司/软件供应商合作，可以自动化地为用户解决安全隐患，提升节点的安全水平。下面是常见的扣分项目和对应的解决方案示例：

扣分项目	解决方案
软件版本过时	升级软件
存在软件漏洞	安装漏洞补丁
异常的文件/内存/网络/注册表操作	使用安全软件进行扫描
异地登陆/执行敏感操作	提醒用户确认，如非本人登陆应修改密码，并运行安全软件排除可能的恶意软件威胁
系统或组件中开启了不安全的设置项	关闭设置项

表 1 常见扣分项目和对应解决方案

除节点安全性评分外，Token 还与以下因素关联：由安全软件上报的用户遭受攻击记录A和危险操作警告记录W、用户安全知识积累K等因素。

$$\text{Token} = \text{F} - \text{F}_1 - \text{F}_2 - \text{A} - \text{W} + \text{K}$$

用户可以通过学习安全课程、养成良好的使用习惯、维持节点安全评分来获得 Token。得益于智能合约的拓展性，Token 的影响因素可以随着项目的发展依需进行扩充和修改。

Token 量化了用户的安全意识，以此为评价标准，可以衍生出多种激励方式：如对 Token 高的节点奖励虚拟货币奖励、给予节点用户实物奖励、参与安全事件分析的资格等等。对用户来说，提升 Token 不仅能够提升设备的安全性和自身的安全意识，而且能够获得收益，一举两得。于安全软件公司而言，可以依据用户 Token 来筛选出更有价值的行为分析数据，针对不同安全意识的用户开发不同的产品或制定更有针对性的解决方案，提升产品的竞争力。量化用户安全意识，并以此为基础制定激励机制，是一个用户与安全软件公司双赢的解决方案。

3 问题与展望

虽然区块链应用于安全软件领域具有许多优势，但是仍然有诸多问题仍需解决，如共识机制、数据存储方式等。下面对区块链技术应用于安全软件领域所遇到的问题和研究方向进行展望，以供研究探讨。

3.1.1 共识机制方向

区块链的运行离不开共识机制的支撑，当前最流行且应用最广泛的是基于算力的 POW 共识机制，但该机制需要“矿工”挖矿以维持系统运转，浪费了许多节点的算力。不基于算力的 POS 等共识机制的安全性有待证明，PBFT 等强一致性算法存在这算法复杂度高、中心化程度大的问题。因此，要将区块链应用至安全软件领域，需要研究出轻量化、去中心化和安全性强的共识机制以确保系统稳定、安全而高效地运行。

3.1.2 数据存储方向

区块链中的数据只增不减，同步完整区块链所需存储空间不断递增。截至 2018 年 9 月，比特币已经记录了超过 50 万个区块[29]，完整区块链大小已超过 100GB。如此大的数据容量不仅对用户的带宽造成了负担，同时也对节点的性能有着极高的要求。在后续的研究中，如何对区块链中的数据轻量化，提升存储效率和传输速度，是一个急需解决的问题。

3.1.3 用户身份辨识方向

传统的用户身份辨识方式是帐号密码体系，当用户丢失帐号信息时，可以通过有效的身份证明找回帐号密码，通过身份验证。而在区块链中，用户身份的证明依赖于用户私钥，当私钥丢失时，用户会丢失其所有数字资产和个人帐号信息，无法找回。通过私钥进行身份辨识虽保证了安全性，但可用性方面仍有极大的提升空间。在后续的研究中对私钥认证机制进行改进，在方便用户使用，提供找回机制的同时保证安全性，将对区块链于网络安全领域的应用具有极大的促进作用。

4 结论

用户安全意识不高和恶意安全软件泛滥是网络安全所面临的两个重要问题。得益于去中心化、去信任化的技术特性和智能合约带来的拓展性，区块链在解决上述问题时具有极大的技术优势。相较于传统的软件认证机制，区块链技术的融入极大地提升了既有认证机制的安全性和可用性，智能合约与用户行为分析技术结合亦为用户安全意识的量化与激励提供了高效透明的解决方案。区块链技术目前仍处在发展阶段，在共识机制、存储方式和用户身份辨识可用性方面存在着许多不足，在实际应用中依然有许多问题亟待解决。本文对区块链技术应用于安全软件领域提出了思考与解决方案，以期对未来相关领域的研究提供有益的启发与借鉴。

References:

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf

[2] MCKINSEY COMPANY. Blockchain in insurance—opportunity or threat?[EB/OL]. [2016-07]. https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat

[3] 谢辉,王健.区块链技术及其应用研究[J].信息网络安全,2016(09):192-195.

[4] FreeBuf. 黑市热卖杀器 GovRAT：恶意软件数字签名平台[EB/OL]. http://www.freebuf.com/news/84126.html

[5] HackerNews. APT 组织窃取 D-Link 公司数字证书签署其恶意软件[EB/OL]. http://hackernews.cc/archives/23520

[6] 马征宇,严迎建.基于 USBKey 的软件保护增强策略[J].计算机工程与设计,2017,38(01):53-58.

[7] 马雪晶.计算机安全软件在网络安全视角下的开发[J].电子技术与软件工程,2017(22):218.

[8] Anubhav Savant. Method and system for detecting rogue security software that displays frequent misleading warnings. US Grant, US9009819B1

[9] McAfee: A million 'scareware' victims a day [EB/OL]. https://www.cnet.com/news/mcafee-a-million-scareware-victims-a-day/

[10] FBI: Rogue Antivirus Scammers Have Made $150M [EB/OL]. https://www.pcworld.com/article/184468/article.html

[11] 华住 1.3 亿用户数据疑被泄 拷问 AI 时代数据安全[EB/OL]. http://capital.people.com.cn/n1/2018/0903/c405954-30268079.html

[12] Windows XP 仍然没有消亡 市场份额反而有所提升[EB/OL]. https://www.cnbeta.com/articles/soft/713315.htm

[13] DBSEC. 2018 上半年有 45 亿账号被盗 平均每分钟 4822 个[EB/OL]. http://www.dbsec.cn/zx/20181012-1.html

[14] 何蒲,于戈,张岩峰,鲍玉斌.区块链技术与应用前瞻综述[J].计算机科学,2017,44(04):1-7+15.

[15] 刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展[J].软件学报,2018,29(07):2092-2115.

[16] 陈一稀.区块链技术的“不可能三角”及需要注意的问题研究[J].浙江金融,2016(02):17-20+66.

[17] Wikipedia. 公开密钥加密[EB/OL]. [2018-5-10]. https://zh.wikipedia.org/wiki/公开密钥加密

[18] BROWN A R. A SIMPLE MODEL FOR SMART CONTRACTS[EB/OL]. https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/

[19] 何渝君,龚国成.区块链技术在物联网安全相关领域的研究[J].电信工程技术与标准化,2017,30(05):12-16.

[20] 蔡维德,郁莲,王荣,刘娜,邓恩艳.基于区块链的应用系统开发方法研究[J].软件学报,2017,28(06):1474-1487.

[21] 王克,邹嘉,戴一奇.基于软件实名认证的系统安全机制[J].清华大学学报(自然科学版),2008(07):1169-1172.

[22] 闫茂昌,华中,宋占杰,饶刚,杨爱萍.一种面向广电运营商的 Android 软件认证系统[J].电视技术,2013,37(10):23-26.

[23] 8BTC. 昌用：通证的性质[EB/OL]. https://www.8btc.com/article/253659

[24] Wikipedia. WannaCry[EB/OL]. [2018-8-17]. https://zh.wikipedia.org/wiki/WannaCry

[25] Google. Android 安全公告 - 2018 年 8 月[EB/OL]. https://source.android.com/security/bulletin/2018-08-01

[26] 51CTO. Chrome 浏览器地址栏欺骗漏洞(CVE-2016-1707)[EB/OL]. http://netsecurity.51cto.com/art/201610/519002.htm

[27] 陈剑锋,陈天莹.走向体系智能的网络空间安全自动化研究[J].信息安全与通信保密,2016(08):111-116.

[28] 陈捷,丛键,张海燕.基于机器学习的行为分析技术在下一代智能化网络安全体系中的应用[J].通信技术,2018,51(08):1956-1960.

[29] BLOCKCHAIN. Blocks mined on:01/09/2018[EB/OL]. https://www.blockchain.com/btc/blocks/1535826051241