DOI:10.13878/j.cnki.jnuist.2019.05.003

王伟光[1]

区块链技术在电子商务信息安全领域的应用综述

摘要

区块链技术是近年来最受欢迎的技术之一,因其去中心化、去信任、匿名等特点,在电子商务信息安全领域有着广泛的应用.本文首先从区块链的基本原理和关键技术、应用领域、目前存在的安全隐患等几个方面介绍了区块链技术;然后从数据加密技术、基于区块链的身份认证、基于区块链的防火墙技术等几个角度阐述了区块链技术在电子商务信息安全领域的应用;最后分析了区块链技术的在电子商务信息安全领域的应用挑战,并进行了总结与展望.

关键词

区块链技术;电子商务;信息安全

中图分类号 TP309

文献标志码 A

0 引言

区块链技术最早是由中本聪的一篇关于比特币的论文[1]提出的.数字货币面临着“拜占庭将军”问题[2-3]和双重支付问题[4-5],区块链技术[6]作为数字加密货币[7]的关键技术,能够有效地解决上述问题.由于区块链的开放共识、去中心化、去信任、匿名性、不可篡改、可追溯性、可编程性等特点,其在电子商务信息安全[8]领域应用广泛.

电子商务[9]是指通过电子渠道(主要是互联网)购买和销售商品以及服务.电子商务的应用包括在线书店、电子银行、在线机票预订(铁路、航空、电影等)、买卖商品、在线资金转账等.在电子商务交易期间,机密信息存储在数据库中,并通过网络渠道进行通信.电子商务信息安全主要的威胁包括身份验证攻击、完整性攻击、机密性攻击、病毒、特洛伊木马、蠕虫、数据库威胁[10].

1 区块链技术

1.1 基本原理和关键技术

1.1.1 基本原理

区块链技术包含密码学、数学、算法和经济模型,结合点对点网络和使用分布式一致性算法来解决传统的分布式数据库同步问题,它是一个集成的多领域基础设施构建[11-13].区块链技术由6个关键要素组成:分散、透明、开源、自治、不可改变的、匿名.图1所示为区块链的结构.其中,区块是一种数据结构,用于记录交易,由区块头和区块主体组成.

如图2所示,区块主体只负责记录前一段时间内的所有交易信息,区块链的大部分功能都由区块头实现.

1.1.2 关键技术

1)密码学

区块链技术以多种不同的方式使用加密技术,将其用于钱包、交易、安全和隐私保护协议.许多人每天使用加密技术,却没有意识到密码学是通过复杂的数学来伪装和揭示(也称为加密和解密)信息的方法.密码学的早期例子是凯撒密码,由朱利叶斯·凯撒用来保护罗马军事机密.尽管现代密码学复杂程度要高得多,但其工作原理与之类似.现代加密系统使用众所周知的数学算法,并且已经公开测试,依赖于所使用的密钥的安全性[14].区块链使用哈希算法和非对称加密技术

收稿日期 2019-07-14

资助项目 山东省自然科学基金(ZR201807100307)

作者简介

王伟光,男,硕士,讲师,主要研究方向为信息安全.wwgxl@163.com

1 山东管理学院,济南,250357

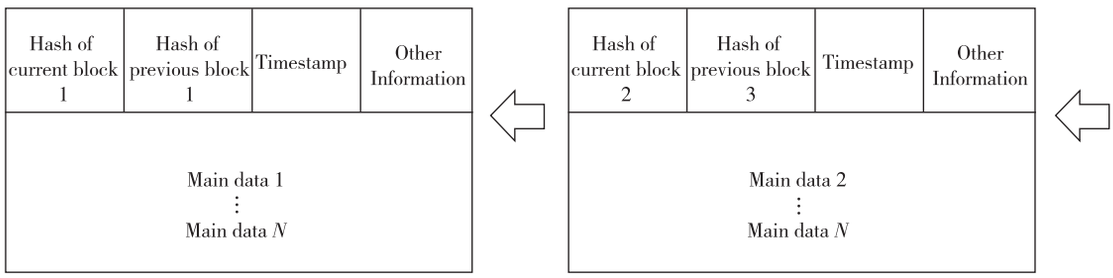

图 1　区块链的结构

Fig. 1　Structure of blockchain

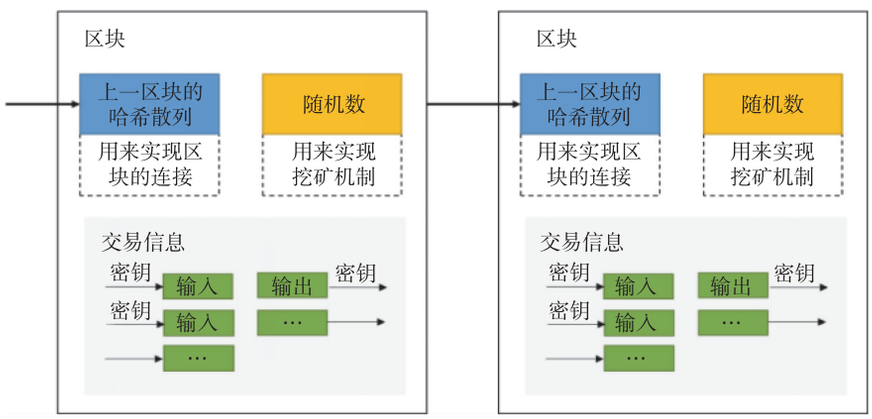

图 2　区块链的区块结构

Fig. 2　Block structure of the blockchain

来确保其完整性和安全性[15].例如,比特币中使用的加密是椭圆加密,最简单的一类用于椭圆的椭圆曲线如式(1)所示:

$$y^2 = x^3 + ax + b. \tag{1}$$

2)分布式存储

目前出现很多的分布式存储系统,例如,IPFS是从先前的P2P 系统发展而来的一种分布式文件系统.然而,作为在多个主机中传播数据的结果,分布式存储系统面临的主要问题是当多个操作同时访问数据时保持数据的一致性.虽然比特币和以太坊采用的点对点技术并不新鲜,但它的实施在过去几年中一直是一项突破性的技术成就[16].

3)共识机制

共识机制是一种容错机制,用于计算机和区块链系统[17-18],是在分布式进程或多代理系统之间实现对单个数据值或网络的单个状态的必要协议.在区块链这种动态变化的状态下,这些公共共享分类账需要一个高效、公平、实时、功能、可靠和安全的机制,以确保网络上发生的所有交易都是真实的[19].

4)智能合约

智能合约是一种计算机程序,可直接控制某些条件下各方之间数字货币或资产的转移[20].由于智能合约存储在区块链上,因此它们继承了一些基于分布式分类账技术(Distributed Ledger Technology,DLT)的网络的关键属性.业务合作中,智能合约的优势突出.并且,通过某种机制,所有参与者可以确定结果而无需中间人参与.智能合约不仅能够实现流程自动化,还能够控制行为,以及通过实时审计和风险评估实现潜力[21].

1.2　区块链的应用

1)金融

区块链金融服务正在重新定义我们当前金融市场基础设施的现有轨道[22].该行业经历重大活动的领域包括后端清算和结算以及全球资本市场架构.在某些情况下,分布式分类账系统不需要完全分散,一些金融机构正在考虑创建自己的“私有区块链”.

2)政府

区块链技术是改善政府服务和促进更加透明的政府与公民关系的潜在工具[23].分布式技术可以通

过更有效和安全的数据共享来显著优化业务流程.

3)健康

区块链技术彻底改变了医学研究人员与用户之间的关系.有人预言,区块链将成为"医疗保健领域的下一个重大创新".健康问题对应的医疗行业存在新人、透明度、激励调整等问题,显然,区块链非常适用于解决这些问题[24].区块链技术对医疗保健生态系统的利益相关者具有广泛的影响.利用这项技术有可能连接分散的系统,以产生洞察力并更好地评估护理的价值.从长远来看,全国范围的电子病历区块链网络可以提高效率并为患者提供更好的健康结果.

4)身份验证

区块链技术为数字身份提供了理想的引擎.虽然数字身份正在成为互联世界不可避免的一部分,但如何保护我们的在线信息这一问题正受到严格的审查[25].基于区块链的身份系统可以通过强化加密和分布式分类账为该问题提供解决方案.

5)物联网

区块链技术提供了理想的引擎,为新的互联世界提供了一个新的概念:物联网.物联网市场的消费预计在未来几年将超过1万亿美元大关[26].研究者提出的基于区块链的物联网架构,这些架构在考虑物联网设备资源限制的基础上用于处理大多数安全和隐私威胁.集中式架构是传统物联网的特点,并且,物联网设备中的可信执行环境(Trusted Execution Environment,TEE)可以证明数据来自特定设备.基于区块链的系统中,一旦来自特定设备的数据存储在区块链中,这些数据就是不可变和可追踪的.

6)保险

区块链保险允许整个保险业通过以高效、安全和透明的方式共享数据以显著优化业务流程[27-28].利用区块链彻底改变保险政策,将系统转变为在对等网络上自主运行的智能合约,逐步淘汰过时的笔和纸流程,并消除保险行业所带来的繁文缛节.

1.3 目前存在的安全隐患

虽然,区块链技术已经足够安全,然而,数字货币被盗事件依然会出现,可以说明,区块链技术依然存在安全隐患.下面,分别从链上和链下这两个方面来讨论.

1)链上

链上,即存储区块链资产的区块链,其主要存在两个漏洞如下:

a. 51%攻击:若某一方占据了全网51%的算例,那么,就取得了一定的新区块产生的支配权.对区块链的51%攻击是指矿工或一组矿工试图控制超过50%的网络挖掘能力、计算能力或哈希率.控制这种采矿权的人可以阻止新的交易发生或被确认.

b. 人为欺诈性上传:没有验证机制的情况下,一旦链上确认了人为造假的上传链下资产或者交易数据,那么,区块链机制便会保护后续的交易.

2)链下

a. 端点漏洞:DLT最可能的漏洞之一来自区块链本身之外,因为其反映了区块链技术的整体安全性,因此必须予以解决.

b. 供应商风险:避免与供应商相关的区块链缺陷需要对每个为区块链生态系统做出贡献的供应商进行彻底审查.

c. 公钥和私钥安全:访问区块链需要公钥和私钥.如果没有公钥和私钥的正确组合,基本上不可能访问区块链中的数据,这代表了区块链技术的优势和劣势.

2 区块链技术在电子商务信息安全领域的应用

2.1 数据加密技术

加密技术是电子商务信息安全领域里区块链技术应用的关键.比特币区块链协议用于使用公钥加密技术进行数字签名和加密哈希函数,其细节将在下面解释.比特币中使用的加密算法称为椭圆曲线加密.与传统的RSA密码术[29]相比,它是一种被认为更有效的非对称密码术.虽然椭圆曲线加密提供与RSA相同的安全级别,但它需要较少的计算和较小的密钥大小,因此降低了存储和传输要求.对于公钥加密[30]:加密密钥,如果两个或更多人想通过互联网安全地进行交易,该技术允许他们使用一组加密密钥证明自己的身份:私钥和公钥.

RSA的加密方式如式(2)所示:

$$A = B^a \% b \ , \tag{2}$$

其中A表示密文,B表示明文,密文是将明文的a次方对b求余数的结果.

RSA的解密方式如式(3)所示:

$$B = A^c \% b \ , \tag{3}$$

其中B是明文,A是密文,而c和b则共同构成了RSA的私钥.

图3所示是简易的比特币区块链.加密货币钱包不存储任何硬币,只存储与用户比特币地址相关联的公钥-私钥对.这同样适用于其他加密货币钱包,钱包只是充当安全密钥存储,并作为区块链的通信工具.当用户发送或接收比特币时,用户使用加密货币钱包用存储在钱包中的公钥-私钥对来签署交易.

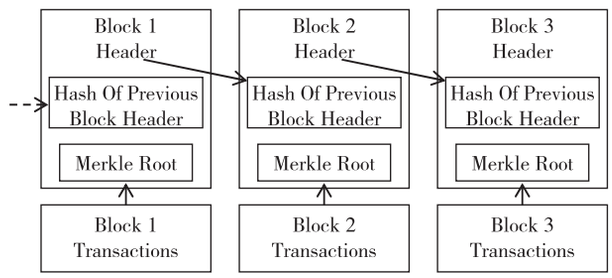

图3 简易的比特币区块链

Fig. 3 Simplified bitcoin blockchain

2.1.1 数字签名

哈希通常与签名结合使用.区块链使用签名来签署交易[31].签名用于证明,例如,某个用户是对应于某个哈希的输入的所有者.签名输入效率不高,因此签名用于签名哈希值[32].一般来说,签名就是这样的:

1)用户A生成事务的哈希.

2)使用私钥用户A加密哈希,从而签署文档.

3)签名的散列与用户A的公钥一起发送给用户B.

4)用户B获取在生成散列之前使用的输入并重新生成散列.此哈希将用作比较.

5)使用加密算法,用户B能够使用提供的公钥解密来自用户A的签名散列.

6)用户B比较哈希值并验证用户A是否拥有输入.

在该系统中,公钥是自由分配的,并且与私钥秘密配对.如果知道公钥,这不是问题,但私钥必须始终保密.即使这两者是成对的,根据公钥计算某人的私钥在计算上也是如此具有挑战性,以至于它在财务上和技术上都是不可行的.如果您丢失了私钥,则会丢失资金.

2.1.2 哈希算法

哈希算法是区块链中用得最多的一种算法.加密散列是区块链技术的另一个基本要素,它直接负责产生不可变性——区块链最重要的特征之一[33].哈希是一个计算机科学术语,意味着获取任意长度的输入字符串并产生固定长度的输出.某个散列函数的输入是3或100个字符无关紧要,输出的长度始终相同.加密哈希函数是具有以下关键属性的哈希函数:

1)确定性:无论您为函数提供多少次特定输入,它都将始终具有相同的输出.

2)不可逆:无法确定函数输出的输入.

3)碰撞阻力:没有两个输入可以具有相同的输出.

哈希函数如式(4)表示:

$$h = H(m)\ , \tag{4}$$

其中,m表示任意长度消息,H表示哈希函数,h表示固定长度的哈希值.

加密散列函数的另一个重要特性是改变输入中的任何数据位将极大地改变输出.例如,111111和111112的散列输出将是完全唯一的并且彼此没有关系.

对于上下文,树[34]是用于以分层树状结构存储数据的计算机科学术语,其中数据位被称为节点.有一个单根(顶部)节点,其下面链接有“子”节点,它们本身有子节点,依此类推.说明典型树数据结构如图4所示.

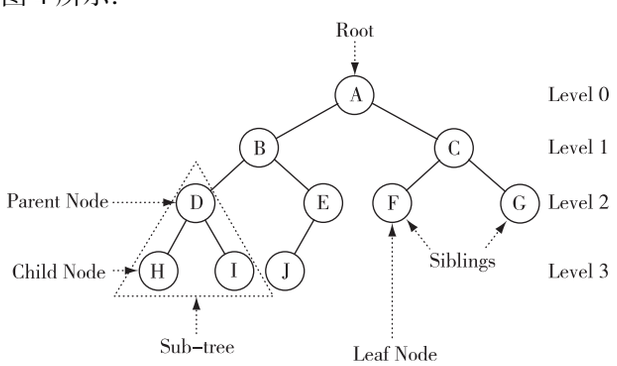

图4 典型树数据结构

Fig. 4 Typical tree data structure

2.1.3 非对称加密

非对称加密是一种加密形式,其中密钥成对出现.一键加密,只有另一个可以解密[35].用户可以通过使用私钥加密来“签名”消息.任何消息接收者都可以验证用户的公钥以解密消息,从而证明用户的密钥是用于加密该消息,因此这很有效.如果用户的私钥是秘密的,那么是用户而不是某些冒名顶替者发送了该消息[36].用户可以通过使用收件人的公钥加密邮件来发送秘密邮件,在这种情况下,只有预期的收件人才能解密该邮件,因为只有该用户才能访问所需的密钥.

例如比特币的数据结构和交易系统是通过区块链技术构建的,使比特币成为数字货币和在线支付系统.比特币使用公钥地址发送和接收比特币,记录交易和个人 ID 是匿名的.如图 5 所示,在比特币中,每个用户都有一对密钥(公钥和私钥).

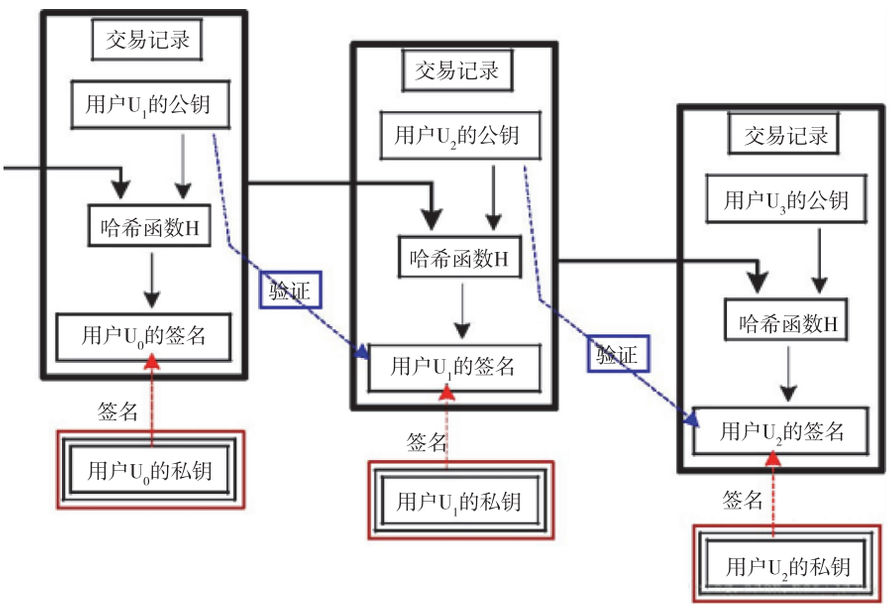

图 5　比特币系统

Fig. 5　Bitcoin system

2.1.4　基于区块链个人数据保护

电子商务信息安全领域,个人数据保护非常重要[37].最近调查的监视和安全漏洞事件发生率的增加导致用户的隐私安全性受到质疑,这使得当前模式受到质疑.Zyskind 等[38]描述了一个分散的个人数据管理系统,确保用户拥有和控制他们的数据.并且实施了一个协议,将区块链转变为自动访问控制管理器[39].这些应用程序的提供者,由于操作和业务相关的原因需要处理个人数据[40](例如,有针对性的广告、个性化服务).图 6 所示是 Zyskind 等[38]给出的区块链的分散式平台.

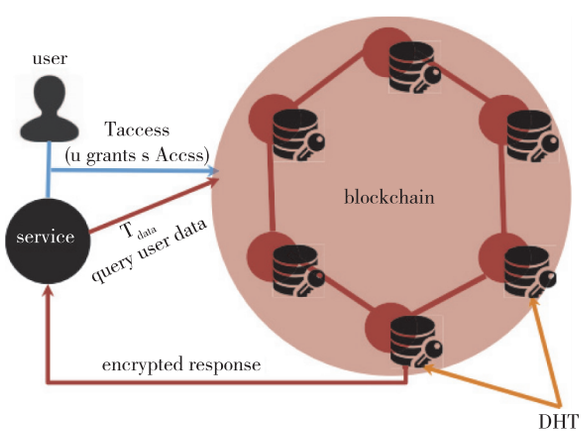

图 6　分散式平台[38]

Fig. 6　Decentralized platform[38]

从法律的角度,区块链存储加密的个人可识别数据是完全正确的,只要所有者可以按照自己的意愿控制、修改和删除它.但是,由于大多数公共区块链依赖于分散且不可改变的记录历史,因此大多数记录都不符合通用数据保护条例(General Data Protection Regulation,GDPR),并且他们有可能被“隐私中毒”.隐私中毒是指个人数据被添加到公共区块链中,使得所涉及的区块链违反了隐私保护法.如果区块链上的个人信息无法更改、不再需要或不再准确,那么区块链就违法了.如果所涉及的区块链揭示了个人的身份,那么它也违反了法律[41].当然,这只是一个考虑,到目前为止,还没有任何记录的区块链被隐私中毒的案例,但这并不意味着它没有发生.

区块链同样可以作为数据保护的催化剂,在实践中,区块链数据库在多大程度上适用于实现隐私的七项基本原则仍有待观察.但是流行的加密货币比特币通常被称为具有数据保护潜力的区块链数据库的一个例子,因为比特币提供了“匿名的、不可持久的”支付手段.

2.2 基于区块链的身份认证

在区块链方面,最常听到的与技术优势相关的词是“安全性”.身份管理是行业的一个部门,其前提是为那些依赖它来保证数据安全的人提供顶级安全性.然而,客户的安全并不总是百分之百受到保障的.进入数字时代已经建立了一种新的身份盗用模式.

区块链身份管理提供分散且安全的解决方案,通过分布式信任模型让用户重新掌控自我主权身份(Self Sovereign Identity,SSI)[42].现有的身份管理系统既不安全也不可靠,在任何时候,都会要求用户通过多个政府授权的身份证明自己,如护照和 Pan Card 等.然而,共享多个 ID 会导致隐私问题和数据泄露.因此,区块链可以有效地解决这一问题.自我主权身份可以确保数据隐私,身份文件由获得许可的参与者进行保护、验证和认可.

默认情况下,底层身份数据应该是私有的,因此核心声明信息需要在分类账簿之外.当然,也可以简单地“散列”声明,并将其与指向核心声明的指针一起存储在链上或作为智能合约的一部分.这充分体现了自我主权身份的不断增长的主张[43].

2.3 基于区块链的防火墙技术

隐私或参与要求更受限制的应用程序不能依赖公共区块链[44-45].首先,可以随时下载整个区块链,从而使数据可供公众使用.其次,任何人都可以部署节点,加入区块链网络并参与到共识建立过程.如图 7 所示,为了提供给区块链节点额外的安全性,ChainGuard 利用 SDN 功能对网络流量进行过滤,从而为区块链应用实施一个防火墙.ChainGuard 与其保护的区块链节点进行通信,以确定流量的来源是合法的.如果流量的来源是非法的,那么来自非法来源的数据包将会被截获,因此不会对区块链产生影响.实验显示,ChainGuard 提供的访问控制功能可以有效地缓解来自多个来源的“洪水攻击”.

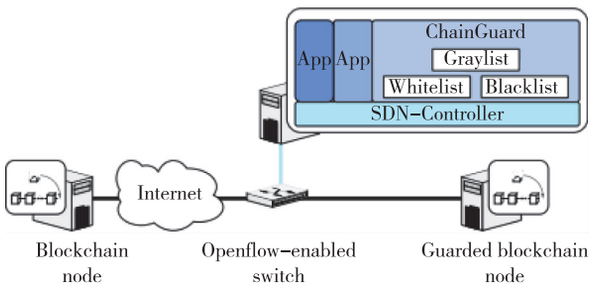

图 7 基于 Openflow 实施区块链防火墙示例

Fig. 7 Using Openflow to implement a firewall for the blockchain

3 应用挑战及展望

首先,把商业链条中的隐形环节摆到前端,即他们都有互相指责的权利.各个环节既独立又捆绑在一起,因此有彼此监督的责任,最终在共同努力下呈现结果.但品牌溢价降低是肯定的,原因是基于对中间环节的了解.平台结算体系,即供应量中的各个服务商有不同的服务体系与结算方式,互相不统一,影响了商业流通的顺畅性,而在区块链电商中,平台采用数字货币置换,统一了每一个供应商的结算方式,这样所有的供应链不存在强势与弱势.

其次,从区块链安全的角度,一旦它保持 51%的计算能力,它就可以控制这个区块链.显然,这会导致安全问题[46].如果某人拥有超过 51%的计算能力,那么他/她可以比其他人更快地找到 Nonce 值,这意味着他/她有权决定允许哪个块.它能做的是:

1)修改交易数据,可能导致双重攻击[47];

2)停止块验证交易;

3)停止矿工开采任何可用的区块.

事实上,区块链真正具有革命性的是它在处理比特币交易之外的应用潜力.虽然区块链技术影响着大量行业,但是,区块链在电子商务信息安全领域的应用依然具有很多挑战[48].如下列挑战:

1)初始成本

虽然区块链技术的采用有望在生产率、效率、及时性和降低成本方面带来长期利益,但最初将其付诸实施仍然是昂贵的.

2)与遗留系统集成

为了转移到基于区块链的系统,组织必须彻底检修其先前的系统,或者找到将现有系统与区块链解决方案集成的方法.但是,区块链解决方案可能难以处理所有功能,使得难以完全根除遗留系统.

3)能源消耗

比特币和以太网网络都使用工作量证明机制来验证区块链上的交易.该机制需要计算复杂的数学问题以验证和处理事务并保护网络.这些计算需要大量的能量来驱动计算机解决问题.除了用于运行计算机的能量之外,还需要相当大的能量来冷却计算机.

4)公众感知

大多数公众仍然不了解这项技术的存在和潜在用途.为了使区块链技术成为主流,首先必须公开支持其利益.

5)隐私和安全

区块链可以公开显示.以比特币区块链为例,该区块链旨在让所有在网络上进行交易的人都可以访问.但是,对于政府和企业来说,这会产生许多问题.由于种种原因,政府和公司需要能够保护和限制对其数据的访问.这意味着在满足此挑战之前,区块链技术无法在具有敏感数据的空间中工作.

4 结束语

区块链技术优点突出,虽然也有链上、链下安全隐患,但可以认为是用于电子商务信息安全非常有前途的技术.区块链技术使得所有交易都会被记录而不会被改变,不需要有任何征信系统.电子商务信息安全领域虽然存在身份验证、数字签名、防火墙等诸多方面的挑战,但去中心化去除了第三方机构的参与,使得交易双方直接进行交易,这就大大缩短了时间,提高了效率.因此,区块链不仅在金融上有着颠覆性改变,而且对社会生活也产生了难以想象的影响.区块链广泛应用于电子商务信息安全领域的身份验证、数字签名、防火墙和数据保护领域,保障了电子商务的信息安全.

参考文献

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].[2019-07-01].https://bitcoin.org/bitcoin.pdf

[2] Antonopoulos A M. Mastering bitcoin: unlocking digital cryptocurrencies[M]. Sebastopol, CA: O'Reilly Media, Inc.,2014

[3] 范捷,易乐天,舒继武.拜占庭系统技术研究综述[J].软件学报,2013,24(6):1346-1360
FAN Jie,YI Letian,SHU Jiwu.Research on the technologies of Byzantine system[J].Journal of Software,2013,24(6):1346-1360

[4] Dwyer G P.The economics of bitcoin and similar private digital currencies[J]. Journal of Financial Stability,2015,17:81-91

[5] Karame G O, Androulaki E, Roeschlin M, et al. Misbehavior in bitcoin[J].ACM Transactions on Information and System Security,2015,18(1):1-32

[6] Swan M.Blockchain:blueprint for a new economy[M]. Sebastopol,CA:O'Reilly Media,Inc.,2015

[7] Mukhopadhyay U,Skjellum A,Hambolu O,et al.A brief survey of crypto currency systems[C]// 2016 14th Annual Conference on Privacy, Security and Trust (PST),2016.DOI:10.1109/PST.2016.7906988

[8] 牛荣.电子商务信息安全[J].商场现代化,2008(2):169-170
NIU Rong.E-commerce information security[J].Market Modernization,2008(2):169-170

[9] 刘敖迪,杜学绘,王娜,等.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(7):2092-2115
LIU Aodi, DU Xuehui, WANG Na, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7):2092-2115

[10] 沈鑫,裴庆祺,刘雪峰.区块链技术综述[J].网络与信息安全学报,2016,2(11):11-20
SHEN Xin, PEI Qingqi, LIU Xuefeng. Survey of blockchain[J]. Chinese Journal of Network and Information Security,2016,2(11):11-20

[11] Baliga A. Understanding blockchain consensus models[M].India:Persistent Systems Limited,2017

[12] Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: analysis and applications[M]// Advances in Cryptology-EUROCRYPT2015. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 281-310. DOI: 10.1007/978-3-662-46803-6_10

[13] Gervais A,Karame G O,Capkun V,et al.Is bitcoin a decentralized currency?[J]. IEEE Security & Privacy, 2014,12(3):54-60

[14] Böhme R, Christin N, Edelman B, et al. Bitcoin: economics, technology, and governance[J]. Journal of Economic Perspectives,2015,29(2):213-238

[15] Kosba A, Miller A, Shi E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE Symposium on Security and Privacy (SP),2016.DOI:10.1109/SP.2016.55

[16] Davidson S, de Filippi P, Potts J. Economics of blockchain[J]. SSRN Electronic Journal, 2016. DOI: 10.2139/ssrn.2744751

[17] Sharma P K,Chen M,Park J H.A software defined fog node based distributed blockchain cloud architecture for IoT[J].IEEE Access,2018,6:115-124

[18] Cachin C,Vukolić M.Blockchain consensus protocols in the wild[J].arXiv e-print,2017,arXiv:1707.01873

[19] Wang W, Hoang D T, Xiong Z, et al. A survey on consensus mechanisms and mining management in blockchain networks[J]. arXiv e-print, 2018, arXiv:1805.02707

[20] Watanabe H,Fujimura S,Nakadaira A,et al.Blockchain contract:securing a blockchain applied to smart contracts[C]//2016 IEEE International Conference on Consumer Electronics (ICCE), 2016. DOI: 10.1109/ICCE.2016.7430693

[21] Clack C D,Bakshi V A,Braine L.Smart contract templates:foundations,design landscape and research directions[J].arXiv e-print,2016,arXiv:1608.00771

[22] Watanabe H,Fujimura S,Nakadaira A,et al.Blockchain contract:a complete consensus using blockchain[C]// 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE),2015.DOI:10.1109/GCCE.2015.7398721

[23] Fanning K, Centers D P. Blockchain and its coming impact on financial services[J].Journal of Corporate Accounting & Finance,2016,27(5):53-57

[24] Nguyen Q K.Blockchain:a financial technology for future

sustainable development[C]// 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD),2016.DOI:10.1109/GTSD.2016.22

[25] Linn L A,Koo M B.Blockchain for health data and its potential use in health IT and health care related research[C]//ONC/NIST Use of Blockchain for Healthcare and Research Workshop,2016

[26] Wu L F,Du X J,Wang W,et al.An out-of-band authentication scheme for internet of things using blockchain technology[C]//2018 International Conference on Computing,Networking and Communications (ICNC),2018.DOI:10.1109/ICCNC.2018.8390280

[27] Samaniego M,Deters R.Blockchain as a service for IoT[C]//2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber,Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),2016.DOI:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

[28] Raikwar M,Mazumdar S,Ruj S,et al.A blockchain framework for insurance processes[C]//2018 9th IFIP International Conference on New Technologies,Mobility and Security (NTMS),2018.DOI:10.1109/NTMS.2018.8328731

[29] Lamberti F,Gatteschi V,Demartini C,et al.Blockchain or not blockchain,that is the question of the insurance and other sectors[J].IT Professional,2017.DOI:10.1109/MITP.2017.265110355

[30] Bleichenbacher D.Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1[M]// Advances in Cryptology:CRYPTO'98.Berlin,Heidelberg:Springer Berlin Heidelberg,1998:1-12.DOI:10.1007/bfb0055716

[31] Boneh D,di Crescenzo G,Ostrovsky R,et al.Public key encryption with keyword search[M]//Advances in Cryptology:EUROCRYPT2004.Berlin,Heidelberg:Springer Berlin Heidelberg,2004:506-522.DOI:10.1007/978-3-540-24676-3_30

[32] 张彤.区块链安全性问题中数字签名潜信道分析[C]//第十二届全国信号和智能信息处理与应用学术会议论文集,杭州,2018
ZHANG Tong.Analyses for the subliminal channel in digital signature of the blockchain security issues[C]//Proceedings of the 12th National Conference on Signal and Intelligent Information Processing and Applications,Hangzhou,2018

[33] 田海博,何杰杰,付利青.基于公开区块链的隐私保护公平合同签署协议[J].密码学报,2017,4(2):187-198
TIAN Haibo,HE Jiejie,FU Liqing.A privacy preserving fair contract signing protocol based on blockchains[J].Journal of Cryptologic Research,2017,4(2):187-198

[34] 周致成,李立新,李作辉.基于区块链技术的高效跨域认证方案[J].计算机应用,2018,38(2):316-320,326
ZHOU Zhicheng,LI Lixin,LI Zuohui.Efficient cross-domain authentication scheme based on blockchain technology[J].Journal of Computer Applications,2018,38(2):316-320,326

[35] 李传湘.树数据结构[J].数学物理学报,1983,3(3):283-302
LI Chuanxiang.Tree data structure[J].Acta Mathematica Scientia,1983,3(3):283-302

[36] 蒋春凤.非对称加密算法[J].内江科技,2012,33(8):148
JIANG Chunfeng.Asymmetric encryption algorithm[J].Neijiang Science & Technology,2012,33(8):148

[37] 王明.概述基于比特币和SAT认证加密的延时释放协议[J].信息系统工程,2016(5):55
WANG Ming.Overview of delayed release protocol based on bitcoin and SAT authentication encryption[J].Information Systems Engineering,2016(5):55

[38] Zyskind G,Nathan O,Pentland A.Decentralizing privacy:using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops,2015:180-184

[39] 祝烈煌,董慧,沈蒙.区块链交易数据隐私保护机制[J].大数据,2018,4(1):46-56
ZHU Liehuang,DONG Hui,SHEN Meng.Privacy protection mechanism for blockchain transaction data[J].Big Data Research,2018,4(1):46-56

[40] 刘文杰,刘保汛,刘亚军.基于区块链技术保护个人数据[J].科技资讯,2018,16(9):29-31
LIU Wenjie,LIU Baoxun,LIU Yajun.Protection of personal data based on blockchain technology[J].Science and Technology Information,2018,16(9):29-31

[41] Liang G Q,Weller S R,Luo F J,et al.Distributed blockchain-based data protection framework for modern power systems against cyber attacks[J].IEEE Transactions on Smart Grid,2019,10(3):3162-3173

[42] 王皓,宋祥福,柯俊明,等.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(7):32-39
WANG Hao,SONG Xiangfu,KE Junming,et al.Blockchain and privacy preserving mechanisms in cryptocurrency[J].Netinfo Security,2017(7):32-39

[43] 詹煜.区块链数据库与传统数据库的对比[J].电脑知识与技术,2018,14(23):44-45
ZHAN Yu.Comparison between blockchain database and traditional database[J].Computer Knowledge and Technology,2018,14(23):44-45

[44] 康双勇.区块链中的身份认证问题研究[J].保密科学技术,2018,92(5):34-37
KANG Shuangyong.Research on identity authentication in blockchain[J].Security Science and Technology,2018,92(5):34-37

[45] 夏友清.基于区块链技术的Anti-APT型防火墙技术研究[J].信息与电脑,2016(14):30-32,45
XIA Youqing.Research on Anti-APT firewall technology based on blockchain technology[J].China Computer & Communication,2016(14):30-32,45

[46] 杨翊,彭扬,矫毅.基于区块链的DDoS防御云网络[EB/OL].北京:中国科技论文在线[2016-11-04].http://www.paper.edu.cn/releasepaper/content/201611-59
YANG Yi,PENG Yang,JIAO Yi.DDoS defense cloud network based on blockchain[EB/OL].Beijing:Chinese Sciencepaper Online[2016-11-04].http://www.paper.edu.cn/releasepaper/content/201611-59

[47] Opara E U,Soluade O A.Straddling the next cyber frontier:the empirical analysis on network security,exploits,and vulnerabilities [J]. International Journal of Electronics and Information Engineering,2015,3(1):10-18

[48] Gervais A,Ritzdorf H,Karame G O,et al.Tampering with the delivery of blocks and transactions in bitcoin[C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security,2015. DOI:10.1145/2810103.2813655

A survey of application of blockchain in e-commerce information security

WANG Weiguang[1]

1 Shandong Management University,Jinan 250357

Abstract Blockchain technology is one of the most popular technologies in recent years.It has been widely used in the field of e-commerce information security because of its characteristics of decentralization,trustworthiness and anonymity.Firstly,this paper introduces the blockchain technology from its basic principles,key technologies,application fields,and existing security risks.Secondly,the application of blockchain technology in the field of e-commerce information security is elaborated from several perspectives,such as data encryption technology,blockchain-based identity authentication,blockchain-based firewall technology,etc.Finally,the application challenges of blockchain technology in the field of e-commerce information security are analyzed,and the conclusions and prospects are summarized.

Key words blockchain technology;e-commerce;information security