基于区块链的隐私安全保护可行性分析

邓 毅,陈秀清,王志豪,王东升

(徐州医科大学 医学信息学院,江苏 徐州 221004)

摘 要:随着人们对信息安全越来越重视,区块链技术近年来发展迅速。介绍了区块链关键技术,对基于区块链的隐私保护方式及优缺点进行了系统概述,分析基于区块链隐私安全保护的可行性。得出结论:区块链作为一种去中心化、不可篡改的记录技术,可在一定程度上为用户提供隐私安全保障。因此,基于区块链的隐私安全保护是可行的,也为传统隐私保护提供了新思路。

关键词:区块链;隐私保护;密码学

DOI:10. 11907/rjdk. 181917

中图分类号:TP309 **文献标识码**:A **文章编号**:1672-7800(2019)001-0166-03

Blockchain-based Privacy Security Protection Feasibility Analysis

DENG Yi, CHEN Xiu-qing, WANG Zhi-hao, WANG Dong-sheng

(*School of Medical Information*, *Xuzhou Medical University*, *Xuzhou* 221004, *China*)

Abstract: Based on the overview of blockchain and key technologies, this article proposes a concept of blockchain-based privacy protection, systematically summarizes the advantages, advantages and disadvantages of blockchain-based privacy protection and analyzes the feasibility of privacy protection based on blockchain. The results show that, to some extent, blockchain-based privacy protection can provide users with privacy protection, and it also brings new inspiration for traditional privacy protection. It is concluded that blockchain, as a decentralized and non-tampered recording technology, can provide certain protection for privacy security, and it also shows that blockchain-based privacy protection is feasible.

Key Words: blockchain; privacy protection; cryptography

0 引言

2008年10月,中本聪提出比特币设计白皮书[1],并于2009年公开了最初的实现代码。2014年开始,作为比特币底层技术的区块链技术受到人们广泛关注。由于区块链具备去中心化、不可篡改、匿名性等特点,目前已被应用于金融、贸易、征信、共享经济等诸多领域。2015年10月,美国纳斯达克(Nasdaq)证券交易所推出区块链平台 Nasdaq Linq[2],通过该平台进行股票发行的发行者将享有“数字化”所有权。2016年1月20日,中国中央银行专门组织了“数字货币研讨会”,邀请花旗、德勤等公司的区块链专家,针对数字货币发行总框架与演进过程,以及国家加密货币等话题进行研讨。

最早的区块链技术出现在比特币项目中,作为比特币背后的P2P网络分布式记账平台[3]。公认的最早关于区块链的描述性文献是2008年中本聪撰写的《比特币:一种点对点的电子现金系统》[4],但该文献重在讨论比特币系统,并未提出明确的区块链定义与概念。目前区块链利用密码学中的hash算法等技术,使比特币形成了一个不依赖于发行方的货币系统,保证了各地参与者的交易安全。

针对区块链的安全问题,张宪等[5]对当前主流的隐私解决方案进行了介绍;祝烈煌等[6]详细介绍了区块链的层次构架,分析了现有区块链技术存在的缺陷;Meiklejohn

收稿日期:2018-06-10

基金项目:国家自然科学基金重大国际合作项目(81320108026);江苏省“六大人才高峰”科研项目(2014-WLW-023);江苏省现代教育技术研究立项项目(2017-R-54844,2017-R-57185);江苏省教育改革项目(2015JSJJG261);江苏省博士后科研资助计划项目(1701061B);江苏省高校自然科学研究面上项目(16KJB180028);江苏省高等学校大学生实践创新训练计划项目(20161031308H,201610313043Y);徐州医科大学博士后基金项目(183822,53120225);徐州医科大学优秀人才引进项目(D2016006,53591506)

作者简介:邓毅(1998-),男,徐州医科大学医学信息学院学生,研究方向为医学信息工程;陈秀清(1982-),女,博士,徐州医科大学医学信息学院讲师,研究方向为信息安全;王志豪(1998-),男,徐州医科大学医学信息学院学生,研究方向为物联网工程;王东升(1998-),男,徐州医科大学医学信息学院学生,研究方向为物联网工程。本文通讯作者:陈秀清。

等[7]通过启发式聚类分析技术分析区块链中的交易记录。本文介绍区块链关键技术,提出基于区块链的隐私保护构想,并通过实例论证该构想的可行性。

1　区块链概述

区块链主要分为3种:私链、联盟链、公有链。私链用于机构内部,性能上相对弱于现有分布式系统;联盟链建立于多个联盟机构之间,且每个机构间有一个核心节点;公有链对社会公开,用于资源共享等方面。Baas平台可以面向用户群体提供联盟链与公开链。区块链结构分为数据层、网络层、共识层、激励层、合约层与应用层[8],功能分别为:①数据层封装底层数据区块的链式结构,采用相关非对称公钥数据加密技术以及时间戳技术,通过哈希算法与Merkle数据结构,将一定时间内接收到的数据和代码封装到一个带有时间戳的数据区块中,并链接到最长的主链中,形成新的区块;②网络层建立在IP通信协议与P2P网络基础上,包括分布式组网机制、数据传播机制以及数据验证机制,使区块链系统的每个节点都能参与区块链数据的校验与记账过程。仅当数据通过全网大部分节点验证后,才能写入区块链;③共识层为封装网络节点的各类共识机制算法,在去中心化的系统中,其能够使各节点更高效地针对区块数据的有效性达成共识;④激励层集成了经济因素,主要用于公有链中。它使共识节点可采取最大化自身收益的行为,并且保障了去中心化区块链系统的安全性与有效性,在具备适度经济激励机制的情况下,可形成对区块链历史的稳定共识;⑤合约层封装各类脚本、算法与智能合约,目前已出现以太坊等图灵完备的、实现较为复杂的脚本语言,是可编程特性的基础,并使区块链可以支持各种金融与社会系统的应用;⑥应用层封装区块链各种应用场景与案例,提供可编程环境,通过智能合约将业务规则转化成平台自动执行合约。区块链功能机制见图1。

多中心化应用		应用层		
智能合约		合约层	虚拟机	
发行机制		激励层	分配机制	
PBFT	PoS	共识层	DPoS	PoW
P2P网络	传播机制	网络层	数据验证机制	
区块数据	链式结构	数据层	链上链下数据结合	……

图1　区块链功能机制

2　区块链隐私保护

个人用户隐私信息通常指数据拥有者不愿披露的敏感数据或数据所表征的特性[9],而为了维持分散节点间的数据同步性并对交易达成共识,必须公开一些信息。所以必须对用户敏感信息进行处理,以减少隐私泄露的风险。

2.1　区块链隐私保护方式

在区块链上实现隐私保护,主要通过区块链的多个节点验证每笔交易,但如果存在恶意用户验证,则有交易信息泄露的风险。因此,Vitalik提出4种解决方案:①通道(见图2)。只有通信或交易双方才能掌握其中详细信息,与票据交易类似,经过双方共同验证、签名才能最终确认。若要继续通信,需要经过双方再次确认信息并签名。签名次数越多,说明通信发生得越晚。对于有冲突的交易,才会被放到链上(双方确认的信息都在链下进行)。通过"通道"方式发起交易,其安全性与区块链上发起的交易基本一致,可有效保障交易方的隐私性;②混合器[10]。在交易前设置好一个连接所有交易方的中心平台,左侧交易方A1将需要交易的货币与地址发送给该平台后,B1、C1以及右侧的A2、B2、C2也执行相同操作。交易方将需要的货币发送到一个相连的中心平台,以保证将其联系打乱后可发送到事先指定的地址上。在链上参与方看来,只知道A1、B1、C1用户与A2、B2、C2用户发生了交易,却不知具体对应关系。这也意味着需要一个中心化的服务器存贮货币,且告诉中心处理器应该发送的位置。但是该方式需要充分信任中心处理器,即对于第三方的信任。为了削弱中心化趋势,Vitalik等[11]又引入了智能合约(见图3),在一定程度上兼顾了安全性与隐私性;③环匿名[12]。它是一种特殊的群签名组成的协议,只需证明拥有环签名中任意一个签名的签署权即可;④零知识证明。在区块链公有链中,运用零知识证明使其不需要添加或向外界透露更多信息即可完成整个交易流程。

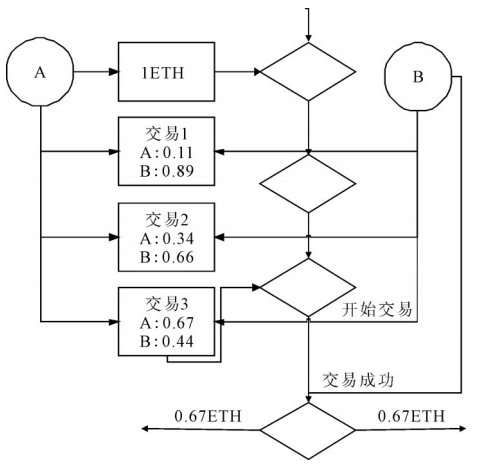

图2　通道

图3　智能合约

2.2　区块链技术在隐私保护方面优缺点

区块链能解决一些中心化服务器面临的隐私泄露问题,但由于区块链技术采取的去中心化架构与数据存储机制,也为隐私保护带来一些不利因素。

在区块链隐私保护方面,张宪在文献[5]中提及了达氏币(Dash)、门罗币、零币。其中达世币具有可保护隐私的主节点,且引入了链式混合(chaining)[13]及盲化(blinding)技术[14]。但由于达氏币依旧存在主节点被控制的风险,所以又提出不依赖中心节点的加密混合方案;门罗币

的两个重要技术分别为隐蔽地址(stealth address)与环签名(ring signature),由于在环签名技术中需与其他用户的公钥混合,有隐私暴露的风险,所以又提出零币概念。但区块链提供的匿名方式仍有隐私泄露的风险。因此,如何增强区块链匿名性是研究中的一大难点。目前主流研究方法有P2P混合机制[15]、分布式混淆网络[16]与零知识证明[17]等。

基于区块链的隐私保护优势如下:①信息不可篡改。信息经过验证后添加到区块链上,则会永久存贮起来,除非超过51%的节点(即51%攻击[18])受到控制,否则对单个节点的数据修改无效,因此区块链稳定性较强;②匿名性。节点之间的数据交换遵循固定算法,且不需第三方参与,交易双方无需公开自己的身份以取得信任。另外,区块链地址空间一般较大,出现碰撞的概率非常低,从而充分避免了隐私泄露的风险;③区块链网络稳定。区块链网络是一种P2P网络,在P2P网络环境中,计算机既可作为服务器,又可作为工作站。在网络中的每一个节点地位都是对等的,节点之间采用中继转发的模式进行通信。信息的传输分散在各节点之间,而不需要经过集中环节,从而降低了信息被窃听的可能性,能够更好地保护用户隐私。

基于区块链的隐私保护劣势如下:①区块链网络中的数据不可更改,在公有链上的交易数据也是透明的,因此容易受到攻击。攻击者可通过推断区块链之间的交易数据找出敏感信息。尽管是匿名交易,但通过分析全局账本交易信息的关联性,可降低区块链中个人信息的匿名性效果,甚至泄露匿名信息内容。如Meiklejohn等通过启发式的聚类分析技术分析区块链中交易记录,可发现同一用户的不同地址;②与传统中心化架构相比,由于区块链去中心化的特点,使每个节点储存的信息等效,攻击者很容易找到安全性相对薄弱的节点入侵;③随着数据量增大,区块链的应用会出现延迟。因每一次交易都有相应不可更改的记录,随着时间推进,每次交易都需要下载并读入历史上所有交易记录才能正常进行,另外每一笔交易都需要全网告知,因而产生记账周期(比特币控制在10min左右)。

3 结语

区块链技术近年来得到了迅速发展,麦肯锡研究报告指出,区块链技术是最有潜力触发第五轮颠覆性革命浪潮的核心科技。未来可能深入应用区块链的场景包括金融服务、征信与权属管理、资源共享以及投资管理等领域,但相应的用户隐私安全问题也日益突出。如何增强区块链的匿名性,以及加强节点保护等问题都是目前面临的难题,而且运用隐私保护也需要采用合理的系统设计方案,以规避硬件限制。虽然目前区块链底层技术还不够成熟,但相关技术发展迅速。

通过对区块链隐私保护方式的介绍与分析,表明基于区块链的隐私保护方案是可行的。同时,针对区块链节点易被攻击的情况,考虑对区块链中的节点进行差分隐私保护[19],并对各个节点进行加噪。为了更加直观地反映节点特征,还可采用路径前缀树代替节点信息,这也是下一步的研究方向。

参考文献:

[1] LIPPINCOTT E R. Infrared spectra of inorganic and coordination compounds[M]. New Jersey: John Wiley,1986.

[2] The blockchain revolution: new opportunities in equity markets[EB/OL]. http://hdl.handle.net/1721.1/104522.

[3] 朱云鹏,陆余良. P2P对等网络分布式服务应用研究[J]. 计算机工程与设计,2007,28(12):2858-2862.

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted,2008.

[5] 张宪,蒋钰钊,闫莺. 区块链隐私技术综述[J]. 信息安全研究,2017(11):981-989.

[6] 祝烈煌,高峰,沈蒙,等. 区块链隐私保护研究综述[J]. 计算机研究与发展,2017,54(10):2170-2186.

[7] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names[C]. Conference on Internet Measurement Conference. ACM, 2013:127-140.

[8] MAESA D D F, MORI P, RICCI L. Blockchain based access control[M]. Distributed Applications and Interoperable Systems,2017.

[9] 胡持. 云计算环境中面向密文计算的同态加密方法研究[D]. 南京:南京邮电大学, 2016.

[10] TARAVATI S, CALOZ C. Mixer-duplexer-antenna leaky-wave system based on periodic space-time modulation[J]. IEEE Transactions on Antennas & Propagation, 2016, 65(99):1.

[11] WATANABE H, FUJIMURA S, NAKADAIRA A, et al. Blockchain contract: Securing a blockchain applied to smart contracts[C]. IEEE International Conference on Consumer Electronics. IEEE,2016.

[12] MALAVOLTA G, SCHRÖDER D. Efficient ring signatures in the standard model[M]. Hongkong:springer,2017.

[13] BELLARE M, KILIAN J, ROGAWAY P. The security of cipher block chaining[C]. International Cryptology Conference on Advances in Cryptology. Springer-Verlag, 1994:341-358.

[14] SAARINEN M J O. Arithmetic coding and blinding countermeasures for lattice signatures [J]. Journal of Cryptographic Engineering, 2017, 8(3):1-14.

[15] RUFFING T, MORENO-SANCHEZ P, KATE A. P2P mixing and unlinkable bitcoin transactions[C]. Network and Distributed System Security Symposium, 2017.

[16] JAGFELD G, VU N T. Encoding word confusion networks with recurrent neural networks for dialog state tracking[C]. Proceedings of the First Workshop on Speech-Centric Natural Language Processing, 2017:7-11.

[17] RACKOFF C, SIMON D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack[J]. Proceedings of Crypto, 1991, 576(12):433-444.

[18] JI R, SCHWAMM L H, PERVEZ M A, et al. Ischemic stroke and transient Ischemic attack in young adults: risk factors, diagnostic yield, neuroimaging, and thrombolysis.[J]. Jama Neurol, 2013, 70(1):51-57.

[19] 夏英,毛鸿睿,张旭,等. 面向位置推荐的差分隐私保护方法[J]. 计算机科学,2017,44(12):38-41,57.

(责任编辑:黄 健)