体的共识机制,能够满足效率和安全性要求的共识机制都是可以的.对于可信第三方,以 CertChian 为例的 PKI 系统使用的是基于 PoS 的共识[48],并且其研究者已经证明了用区块链构建 CA 系统效率是足够的,能够提供毫米级的证书验证服务.本文提出的分布式可信验证者在设计中只需要5个节点,常见的PBFT等共识协议在目前已经主流的区块链基础平台上都能够实现每秒 1 000 笔级别的共识效率,完全可以适用.对于 LogChain,日志更加追求的是不可篡改的特性,对于共识效率的要求相对较低.但是日志本身的数据量大,数据产生的参与方多,可以考虑基于有向无环图 DAG 的共识协议构建大规模分布式网络的日志系统.但共识机制的选取和实际应用场景密切相关.

2) 远程证明

B-TNC 中的远程证明过程比传统的可信网络连接远程证明的过程更加复杂.远程证明的性能损失来自于两个方面:一是共识协议本身的运行速度,二是 DPoS 中的 21 个见证者分别运行可信验证的过程.上一节已经说明了共识机制本身的性能是足够的,能够在秒级完成验证确认.验证过程的性能开销主要来自于可信验证者对完整性证据的确认以及 CA 对于身份的确认.21 个见证者可以执行并行化的认证,时间开销并不是一个 21 倍的关系.并且领导节点只要收到 2/3 节点的通过验证的消息就能够认定验证通过,不需要等待所有节点结束.所以,即使有恶意节点故意拖延验证时间,也无法同时控制 2/3 的节点同时撒谎.所以和传统可信网络连接架构相比,基于区块链的远程证明带来的效率损耗不大,主要取决于对于证据的验证过程,这和 TNC 架构是相同的.假设完成证据验证的时间是 10s,那么远程证明过程的效率约为 3s+10s=13s.由于共识效率是高于网络通信频率的,所以不会产生交易堆积的情况,只要有证明需要,就可以立即运行证明过程.

3) 访问控制

区块链作为分布式数据存储,其数据量本身很大,可以达到 TB 级.但是在数据查询的时候,并不是直接面对整个数据.区块链数据库的增长速度约为 1MB/s,在 B-TNC 中的每一个节点都维护一个区块链高速引擎,能够实时解析区块链数据库,以结构化的方式存储在本地.区块链数据更新后,系统会根据新区块的内容及时更新本地的访问控制列表,以实现快速的数据查询.在本文的设计中,一个平台的最新状态总会被保存在后面的区块中,并且区块是经常更新的,那么这一过程在最新的一部分区块中就能较快地完成.对于普通的计算终端,并不需要维护全部的区块链数据,只需要去超级节点申请数据更新访问控制列表即可.所以当计算节点之间进行网络通信时,能够在秒级的时间开销内完成访问控制决策过程.

5 结束语

本文在对安全实际信任问题的分析基础之上,提出了基于区块链构建分布式信任根的思想,进而提出了基于区块链的分布式可信网络连接架构.其核心思想是:用区块链对可信网络中的中心化认证部件进行分布式改造,主要包括可信第三方、访问控制和日志审计.分析表明,B-TNC 能够有效解决传统架构下面临的访问控制单点化、策略决策中心化的问题.基于区块链的结构能够将二值化的信任模型扩展为网状的整体信任模型,更加符合实际的网络运行环境.本文在提出总体架构设计、抽象描述和运行流程的基础之上,对核心问题展开描述.最后进行了正确性,安全性和效率分析.

下一步工作将从两个方面展开:一是研究更加适合分布式环境下的可信验证模型,进一步弱化二值化信任判断模型的约束;二是原型系统的设计与实现,由于工作量较大,需要展开更广泛的合作.

References:

[1] Shen CX, Chen XS. Construction of the information security infrastructure based on trusted computing. Journal of Sichuan University, 2014,46(1):1−7 (in Chinese with English abstract).

[2] Feng DG, Qin Y, Wang D, Chu XB. Research on trusted computing technology. Journal of Computer Research & Development, 2011,48(8):1332−1349 (in Chinese with English abstract).

[3] Tan L, Xu ZW. Development of the transitive trusted chain based on TPM. Computer Science, 2008,35(10):15−18 (in Chinese with English abstract).

[4] Chen L, Li J. Flexible and scalable digital signatures in TPM 2.0. In: Proc. of the ACM Conf. on Computer and Communications Security. 2013. 37−48. [doi: 10.1145/2508859.2516729]

[5] Zhao S, Xi L, Zhang QY, *et al*. Security analysis of SM2 key exchange protocol in TPM2.0. Security & Communication Networks, 2015,8(3):383−395. [doi: 10.1002/sec.987]

[6] Winter J. Trusted computing building blocks for embedded linux-based ARM trustzone platforms. In: Proc. of the ACM Workshop on Scalable Trusted Computing. DBLP, 2008. 21−30. [doi: 10.1145/1456455.1456460.]

[7] Santos N, Raj H, Saroiu S, Wolman A. Using ARM trustzone to build a trusted language runtime for mobile applications. In: Proc. of the Int'l Conf. on Architectural Support for Programming Languages and Operating Systems. 2016. 67−80. [doi: 10.1145/2541940.2541949]

[8] Jain P, Desai S, Kim S, Shij MW, Lee J, Choi C, Shin Y, Kim TS, Kang BB, Han D. OpenSGX: An open platform for SGX research. In: Proc. of the NDSS. 2016. [doi: 10.14722/ndss.2016.23011]

[9] Schwarz M, Weiser S, Gruss D, Maurice C, Mangard S. Malware guard extension: Using SGX to conceal cache attacks. In: Polychronakis MZ, ed. Proc. of the Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2017). New York: Springer-Verlag, 2017. 3−24. [doi: 10.1007/978-3-319-60876-1_1]

[10] Moghimi A, Irazoqui G, Eisenbarth T. CacheZoom: How SGX amplifies the power of cache attacks. In: Proc. of the Int'l Conf. on Cryptographic Hardware and Embedded Systems; Fischer W, ed. Proc. of the Cryptographic Hardware and Embedded Systems (CHES 2017). New York: Springer-Verlag, 2017. 69−90. [doi: 10.1007/978-3-319-66787-4_4]

[11] Shen CX, Zhang DW, Liu JQ, Ye H, Qiu S. The strategy of TC 3.0: A revolutionary evolution in trusted computing. Engineering Sciences, 2016,18(6):53−57 (in Chinese with English abstract). [doi: 10.15302/J-SSCAE-2016.06.011]

[12] Zhang HG, Chen L, Zhang LQ. Research on trusted network connection. Chinese Journal of Computers, 2010,33(4):706−717 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00706]

[13] Luo AA, Lin C, Wang YZ, Deng FC, Chen Z. Security quantifying method and enhanced mechanisms of TNC. Chinese Journal of Computers, 2009,32(5):887−898 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00887]

[14] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 2009,25(6):599−616. [doi: 10.1016/j.future.2008.12.001]

[15] Chen M, Mao S, Liu Y. Big data: A survey. Mobile Networks and Applications, 2014,19(2):171−209. [doi: 10.1007/s11036-013-0489-0]

[16] Lazer D, Kennedy R, King G, *et al*. The parable of Google Flu: Traps in big data analysis. Science, 2014, 343(6176):1203. [doi: 10.1126/science.1248506]

[17] Zhou MT, Tan L. Progress in trusted computing. Journal of University of Electronic Science & Technology of China, 2006,35(4):116−127 (in Chinese with English abstract).

[18] Li M, Li Q, Zhang GQ, Yan X. The implementation and application of trusted connect architecture. Journal of Information Security Research, 2017,3(4):332−338 (in Chinese with English abstract). [doi: 10.3969/j.issn.2096-1057.2017.04.007]

[19] Yuan Y, Ni XC, Zeng S, Wang FY. Blockchain consensus algorithms: The state of the art and future trends. Acta Automatica Sinica, 2018,44(11):2011−2022 (in Chinese with English abstract). [doi: 10.16383/j.aas.2018.c180268]

[20] Berger S, Caceres R, Goldman KA, Perez R, Sailer R, Doorn LV. vTPM: Virtualizing the trusted platform module. In: Proc. of the Conf. on Usenix Security Symp. USENIX Association, 2006. 305−320.

[21] Danev B, Masti RJ, Karame GO, Capkun S. Enabling secure VM-vTPM migration in private clouds. In: Proc. of the 27th Computer Security Applications Conf. DBLP, 2011. 187−196. [doi: 10.1145/2076732.2076759]

[22] Jin X, Chen XS. Rapid restoration of migrated trusted chain between physical machines. Journal of Wuhan University, 2016,62(2):103−109 (in Chinese with English abstract). [doi: 10.14188/j.1671-8836.2016.02.001]

[23] Liu MD, Cao HY, Shi YJ, Ma LY. Building trusted virtual environment by TCM hardware virtualization based on SR-IOV. Journal of Wuhan University, 2017,63(2):117−124 (in Chinese with English abstract). [doi: 10.14188/j.1671-8836.2017.02.004]

[24] Eyal I, Gencer AE, Sirer EG, Renesse RV. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th Usenix Conf. on Networked Systems Design and Implementation. USENIX Association Berkeley, 2015. 45−59.

[25] Vukolić M. the quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: Camenisch J, ed. Proc. of the Int'l Workshop on Open Problems in Network Security. New York: Springer-Verlag, 2015. 112−125. [doi: 10.1007/978-3-319-39028-4_9]

[26] Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proc. of the 3rd Symp. on Operating Systems Design and Implementation. ACM Press, 1999. 173−186. [doi: 10.1145/571637.571640]

[27] Douceur JR. The sybil attack. In: Druschel P, ed. Proc. of the Int'l Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002. 251−260. [doi: 10.1007/3-540-45748-8_24]

[28] Barak B, Canetti R, Lindell Y, Pass R, Rabin T. Secure computation without authentication. Journal of Cryptology, 2011,24(4): 720−760. [doi: 10.1007/s00145-010-9075-9]

[29] Yoshida M, Obana S. On the (in)efficiency of non-interactive secure multiparty computation. In: Proc. of the Designs Codes & Cryptography. 2018. 1−13. [doi: 10.1007/s10623-017-0424-7]

[30] Blockchain. https://en.wikipedia.org/wiki/Blockchain

[31] Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Trans. on Computers, 2002,51(5):541−552. [doi: 10.1109/tc.2002.1004593]

[32] Fromknecht C, Velicanu D. CertCoin: A NameCoin based decentralized authentication system. Technical Report, Massachusetts Institute of Technology, 2014.

[33] Fromknecht C, Velicanu D. A decentralized public key infrastructure with identity retention. IACR Cryptology ePrint Archive, 2014:803, 2014. https://eprint.iacr.org/2014/803.pdf

[34] Chen J, Yao SX, Yuan Q, He K, Ji S, Du RY. CertChain: Public and efficient certificate audit based on blockchain for TLS connections. In: Proc. of the IEEE INFOCOM. 2018. 1−9.

[35] Kuhn U, Selhorst M, Stuble C. Realizing property-based attestation and sealing with commonly available hard- and software. In: Proc. of the 2007 ACM Workshop on Scalable Trusted Computing. Alexandria, 2007. 50−57. [doi: 10.1145/1314354.1314368]

[36] Brickell E, Camenisch J, Chen L. Direct anonymous attestation. In: Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2004. 132−145. [doi: 10.1145/1030083.1030103]

[37] Liu MD, Shi YJ. Remote attestation model based on blockchain. Computer Science, 2018,45(2):48−52,68 (in Chinese with English abstract). [doi: 10.11896/j.issn.1002-137X.2018.02.008]

[38] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):2092−2115 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[39] Maesa DDF, Mori P, Ricci L. Blockchain based access control. In: Chen L, ed. Proc. of the IFIP Int'l Conf. on Distributed Applications and Interoperable Systems. New York: Springer-Verlag, 2017. 206−220. [doi: 10.1007/978-3-319-59665-5_15]

[40] Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the IEEE Security and Privacy Workshops. Washington: IEEE Computer Society, 2015. 180−184. [doi: 10.1109/SPW.2015.27]

[41] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: A new blockchain-based access control framework for the Internet of things. Security & Communication Networks, 2016,9(18):5943−5964. [doi: 10.1002/sec.1748]

[42] Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA. Access control in the Internet of things: Big challenges and new opportunities. Computer Networks, 2017,112:237−262. [doi: 10.1016/j.comnet.2016.11.007]

[43] Ouaddah A, Elkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha Á, ed. Europe and MENA Cooperation Advances in Information and Communication Technologies. 2017. 523−533. [doi: 10.1007/978-3-319-46568-5_53]

[44] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: Proc. of the IEEE Int'l Conf. on Pervasive Computing and Communications Workshops. Washington: IEEE Computer Society, 2017. [doi: 10.1109/PERCOMW.2017.7917634]

[45] Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of things: Challenges and solutions. Technical Report, University of NewSouth Wales (UNSW), 2016.

[46] Cucurull J, Puiggalí J. Distributed immutabilization of secure logs. In: Barthe G, ed. Proc. of the Int'l Workshop on Security and Trust Management. Cham: Springer-Verlag, 2016. 122−137. [doi: 10.1007/978-3-319-46598-2_9]

[47] Cai YQ, Zhang E, He JY. (*t*,*n*) threshold signature scheme withstanding the conspiracy attack. Journal of Beijing University of Technology, 2011,37(8):1231−1235 (in Chinese with English abstract).

[48] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Katz J, ed. Proc. of the Int'l Cryptology Conf. New York: Springer-Verlag, 2017. 357−388. [doi: 10.1007/978-3-319-63688-7_12]

附中文参考文献:

[1] 沈昌祥,陈兴蜀.基于可信计算构建纵深防御的信息安全保障体系.四川大学学报(工程科学版),2014,46(1):1−7.

[2] 冯登国,秦宇,汪丹,初晓博.可信计算技术研究.计算机研究与发展,2011,48(8):1332−1349.

[3] 谭良,徐志伟.基于可信计算平台的信任链传递研究进展.计算机科学,2008,35(10):15−18.

[11] 沈昌祥,张大伟,刘吉强,叶珩,邱硕.可信 3.0 战略:可信计算的革命性演变.中国工程科学,2016,18(6):53−57. [doi: 10.15302/J-SSCAE-2016.06.011]

[12] 张焕国,陈璐,张立强.可信网络连接研究.计算机学报,2010,33(4):706−717. [doi: 10.3724/SP.J.1016.2009.00706]

[13] 罗安安,林闯,王元卓,邓法超,陈震.可信网络连接的安全量化分析与协议改进.计算机学报,2009,32(5):887−898. [doi: 10.3724/SP.J.1016.2009.00887]

[17] 周明天,谭良.可信计算及其进展.电子科技大学学报,2006,35(4)::116−127.

[18] 李明,李琴,张国强,颜湘.可信网络连接架构 TCA 的实现及其应用.信息安全研究,2017,3(4):332−338. [doi: 10.3969/j.issn.2096-1057.2017.04.007]

[19] 袁勇,倪晓春,曾帅,王飞跃.区块链共识算法的发展现状与展望.自动化学报,2018,44(11):2011−2022. [doi: 10.16383/j.aas.2018.c180268]

[22] 金鑫,陈兴蜀.可信链跨物理主机迁移及快速恢复方法.武汉大学学报(理学版),2016,62(2):103−109. [doi: 10.14188/j.1671-8836.2016.02.001]

[23] 刘明达,曹慧渊,拾以娟,马龙宇.基于 SR-IOV 的 TCM 硬件虚拟化构建可信虚拟环境.武汉大学学报(理学版),2017,63(2):117−124. [doi: 10.14188/j.1671-8836.2017.02.004]

[37] 刘明达,拾以娟.基于区块链的远程证明模型.计算机科学,2018,45(2):48−52,68. [doi: 10.11896/j.issn.1002-137X.2018.02.008]

[38] 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.软件学报,2018,29(7):2092−2115. http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[47] 蔡永泉,张恩,贺警阳.抗合谋攻击的(*t*,*n*)门限签名方案.北京工业大学学报,2011,37(8):1231−1235.

刘明达(1991－),男,山东齐河人,博士生,主要研究领域为信息安全,区块链.

陈左宁(1957－),女,博士,中国工程院院士,博士生导师,CCF 会士,主要研究领域为软件理论,操作系统,信息安全.

拾以娟(1977－),女,博士,副研究员,主要研究领域为信息安全,区块链,系统安全.