4.3.2 性能测试

由于链内隐私保护方法主要面向小数据量、小群体之间的隐私保护需求,因此该方法注重的是隐私交易的延迟而非吞吐量.本文选择在 6 节点情况下,分别设置 1~6 个节点作为隐私参与方,测试不同参与方数量下隐私交易请求与隐私交易回执查询的延时.为了防止网络波动对本测试的影响,本测试选择在夜间无网络负载的情况下进行,且所有节点均处在同一机房同一内网.同时,为了作为对比,也将相应的公开交易请求与公开交易回执查询的延迟画在了图中.图 10 展示了隐私请求延迟对比图.

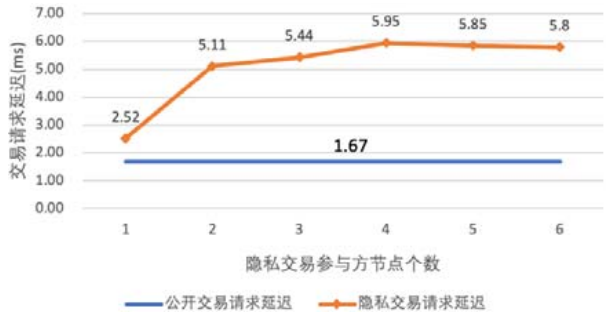


Fig.10 Comparison of transaction's request latency

图 10 交易请求延迟对比

从图 10 可以看出,相比于正常公开交易的请求延迟(1.67ms),所有隐私交易的请求延迟都略有上升.其中,当参与方只有 1 个时(该节点必然为中转节点),由于中转节点已经无需将隐私交易同步至其他的参与方节点,因此该场景只比公开交易场景多了一次隐私交易验签的时间加上隐私交易本地持久化的时间,延迟上升约 0.85ms;当参与方有 2 个时,中转节点除了自身需要进行隐私交易验签加本地持久化之外,还需要将隐私交易同步至其余的 1 个隐私参与方节点,等待该隐私参与方节点进行验签、本地持久化以及返回确认消息的时间,因此延迟上升了约 2.59ms;后续,随着参与方的增多,隐私同步的总时间也基本上稳定在了 5ms~6ms 之间,总体的延迟时间在用户可接受的范围内.

图 11 展示了隐私交易回执查询延迟对比图.

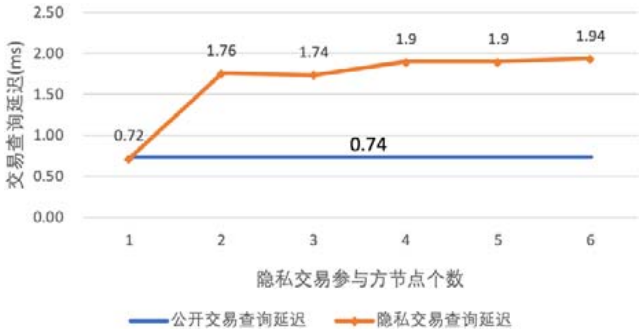


Fig.11 Comparison of transaction's query latency

图 11 交易查询延迟对比

从上图可以看出,相比于正常公开交易的查询延迟(0.74ms),隐私交易的查询延迟略有上升.特别地,当参与方只有 1 个时(该节点即为接收节点),由于接收节点已经无需向其他参与方查询回执了,因此该场景下只需要接收节点查询本地数据库的结果即可,相比于公开交易查询时一样的要从本地数据库查询交易回执,该场景反而比公开交易查询快了 0.02ms;当参与方有 2 个时,接收节点除了自身需要进行本地数据库的查询外,还需要向其他 1 个参与方节点请求回执信息,等待该隐私参与方节点进行本地查询加返回查询结果,因此延迟上升了约

1.04ms;后续,随着参与方的增多,隐私查询的总时间也基本上稳定在 1.7ms~2ms 之间,总体的延迟时间在用户可接受的范围内.

## 5 结 论

随着区块链技术的火热发展,越来越多的区块链应用开始落地实施,随之而来的问题也逐渐暴露出来.本文主要着手研究了联盟区块链中的隐私保护问题,具体工作内容包括:

(1) 设计并实现了链间隐私保护方法.

通过对不同业务流的数据进行分流处理、分区存储实现了业务流之间的数据隔离保护,所有分区的信息通过统一的分区管理器 NSM 进行管理,所有节点在启动完之后,需要首先加入到全局分区,以便进行后期节点的管理.一个分区的生命周期包括注册、启动、停止、注销.需要注意的是,为了保证分区参与方变动时共识机制的完备性,分区注册之前需要进行分区名与分区配置项的线下协商,分区启动时需要进行协议版本的线上协商,分区注销之前需要进行删除节点操作.

(2) 设计并实现了链内隐私保护方法,具体包括隐私交易与隐私合约的保护.

通过在交易体中嵌入 Collection 字段,用户可以指定分区参与方的任意子集作为一笔隐私交易的参与方,实现了灵活的交易级别隐私保护.为了简化隐私交易同步存储的流程,本文将第 1 个接收隐私请求的区块链节点记为中转节点,并由其负责进行隐私数据的同步存储;同时,本文设计了独特的双签名交易,使得中转节点可以直接构造合法的公开交易进行上链操作,而无需由客户端进行二次的交易请求.为了实现隐私交易与隐私合约数据的隔离存储,节点需要为每一个分区维护两份账本数据:一份是正常的公开交易及公开状态的数据,一份是隐私交易及隐私状态的数据.公开账本与隐私账本之间隔离存储,保证了两者之间的互不影响.

最后,本文分别对链间隐私方法吞吐量以及链内隐私保护方法的延迟性进行了测试与对比,结果表明,通过结合粗粒度的链间隐私保护与细粒度的链内隐私保护,在满足了隐私需求的同时也保证了可观的性能,为区块链平台的隐私性与安全性做出了贡献.

**References**:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. 1–9. https://bitcoin.org/bitcoin.pdf

[2] Buterin V. A next-generation smart contract and decentralized application platform. 2014. 1–36. https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[3] Szabo N. The Idea of Smart Contracts. Nick Szabo's Papers and Concise Tutorials, 1997. 1–2. https://nakamotoinstitute.org/the-idea-of-smart-contracts

[4] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper. 2014. 1–34.

[5] Cachin C. Architecture of the hyperledger blockchain fabric. In: Proc. of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016. 1–4.

[6] Zheng Z, Xie S, Dai H, Chen X, Wang H. Blockchain challenges and opportunities: A survey. Int'l Journal of Web and Grid Services, 2018,14(4):352–375.

[7] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In: Proc. of the IEEE Int'l Congress on Big Data (BigData Congress). 2017. 557–564.

[8] Vujičić D, Jagodić D, Ranđić S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In: Proc. of the 17th Int'l Symp. on Infoteh-Jahorina (infoteh). IEEE, 2018. 1–6.

[9] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 2018, 82:395–411.

[10] Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, Rousseau F, Tourancheau B, Veltri L, Zanichelli F. IoTChain: A blockchain security architecture for the Internet of Things. In: Proc. of the IEEE Wireless Communications and Networking Conf. (WCNC). 2018. 1–6.

[11] Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. 2019. 1–46. https://doi.org/10.6028/NIST.IR.8202

[12] Eyal I, Sirer E G. Majority is not enough: Bitcoin mining is vulnerable. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2014. 436−454.

[13] Marcus Y, Heilman E, Goldberg S. Low-resource eclipse attacks on Ethereum's peer-to-peer network. IACR Cryptology ePrint Archive, 2018.

[14] Kalra S, Goel S, Dhawan M, Sharma S. Zeus: Analyzing safety of smart contracts. In: Proc. of the 25th Annual Network and Distributed System Security Symp. (NDSS). 2018. 1−12.

[15] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 2018,39:283−297.

[16] Praitheeshan P, Pan L, Yu J, Liu J, Doss R. Security analysis methods on Ethereum smart contract vulnerabilities: A survey. arXiv preprint arXiv:1908.08605, 2019.

[17] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys (CSUR), 2019,52(3):1−34. https://doi.org/10.1145/3316481

[18] Feng Q, He D, Zeadally S, Khan MK, Kumar N. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 2019,126:45−58.

[19] Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 2019, 19(2):326. https://doi.org/10.3390/s19020326

[20] Reid F, Harrigan M. An analysis of anonymity in the Bitcoin system. In: Proc. of the Security and Privacy in Social Networks. New York: Springer, 2013. 197−223.

[21] Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. Sok: Research perspectives and challenges for Bitcoin and cryptocurrencies. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2015. 104−121.

[22] Bonneau J, Narayanan A, Miller A, Clark J, Kroll J A, Felten EW. Mixcoin: Anonymity for Bitcoin with accountable mixes. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2014. 486−504.

[23] Ruffing T, Moreno-Sanchez P. ValueShuffle: Mixing confidential transactions for comprehensive transaction privacy in Bitcoin. In: Brenner M, *et al*., eds. Proc. of the Financial Cryptography and Data Security (FC 2017). LNCS 10323. Cham: Springer-Verlag, 2017. 133−154.

[24] Miers I, Garman C, Green M, Rubin AD. Zerocoin: Anonymous distributed e-cash from Bitcoin. In: Proc. of the IEEE Symp. on Security and Privacy. 2013. 397−411.

[25] Maxwell G. CoinJoin: Bitcoin privacy for the real world. In: Proc. of the Post on Bitcoin Forum. 2013. https://bitcointalk.org/index.php?topic=279249.0

[26] Maurer FK, Neudecker T, Florian M. Anonymous CoinJoin transactions with arbitrary values. In: Proc. of the 2017 IEEE Trustcom/BigDataSE/ICESS. 2017. 522−529.

[27] Heilman E, Alshenibr L, Baldimtsi F, Scafuro A, Goldberg S. TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub. In: Proc. of the Network and Distributed System Security Symp. 2017. 1−37.

[28] Heilman E, Baldimtsi F, Goldberg S. Blindly signed contracts: Anonymous on-blockchain and off-blockchain Bitcoin transactions. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2016. 43−60.

[29] Noether S. Ring signature confidential transactions for Monero. IACR Cryptology ePrint Archive, 2015,1098:1−34.

[30] Möser M, Soska K, Heilman E, Lee K, Heffan H, Srivastava S, Hogan K, Hennessey J, Miller A, Narayanan A, Christin N. An empirical analysis of traceability in the Monero blockchain. Proc. on Privacy Enhancing Technologies, 2018,(3):143−163.

[31] Borggren N, Yao L. Correlations of multi-input Monero transactions. arXiv preprint arXiv:2001.04827, 2020.

[32] Van Saberhagen N. CryptoNote v 2.0. 2013. 1−20. https://cryptonote.org/whitepaper.pdf

[33] Gai K, Wu Y, Zhu L, Qiu M, Shen M. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. on Industrial Informatics, 2019,15(6):3548−3558.

[34] Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of Medical Systems, 2018,42(8):Article No.140.

[35] Androulaki E, Barger A, Bortnikov V, *et al*. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proc. of the 13th EuroSys Conf. 2018. 1−15.

[36] Sousa J, Bessani A, Vukolic M. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In: Proc. of the IEEE 48th Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN). 2018. 51−58.

**蔡亮**(1976－),男,博士,副教授,CCF 高级会员,主要研究领域为计算机应用.

**端豪**(1994－),男,硕士,主要研究领域为区块链技术与应用.

**鄢萌**(1989－),男,博士,研究员,博士生导师,CCF 专业会员,主要研究领域为智能软件工程,软件仓库挖掘,软件维护与演化.

**夏鑫**(1986－),男,博士,讲师,博士生导师,CCF 专业会员,主要研究领域为软件仓库挖掘,经验软件工程.