文章编号:1671-4598(2023)10-0228-05 DOI:10.16526/j.cnki.11—4762/tp.2023.10.035 中图分类号:TP311.564 文献标识码:A

实用拜占庭容错共识算法在医疗信息泄露防控及共享中的研究与应用

陈 洁
(南京医科大学 附属无锡人民医院,江苏 无锡 214023)

摘要:目前电子病历在多客户端数据共享上依然存在分享困难和患者隐私无法保护等的问题,因此医疗信息泄露防控及共享问题迫在眉睫;为了解决该问题对PBFT算法进行了分析,以此提出了afBFT共识算法,并对其有效性进行了验证;实验结果表明,连续运行时可插拔共识算法(CPBFT)算法和拜占庭容错算法(PBFT)算法的通信量的平均值十分相近,而afBFT共识算法的通信量平均值为3.47千字节,比PBFT算法高14.1%左右,但处于可接受的范围内;同时出块时间的平均值可以稳定在2.4 s左右;同时数据加密与搜索的时间处于较低的范围,分别为350 ms内和140 ms内;并且在实际应用中数据上链与查询接口的平均响应时间分别为2 120 ms和1 020 ms;综合来看,提出的afBFT共识算法在电子病历管理应用上具备有效性,其对保障多客户端医疗信息共享安全性具有重要意义。

关键词:afBFT算法;医疗信息;主节点;安全性;惩罚措施;智能合约

Research and Application of Byzantine Fault-Tolerant Consensus Algorithm in Prevention and Sharing of Medical Information Leakage

CHEN Jie
(Wuxi People's Hospital Affiliated to Nanjing Medical University, Wuxi 214023, China)

Abstract: At present, electronic medical records still face difficulties in sharing data on multiple clients and the inability to protect patient privacy. Therefore, the prevention and control of medical information leakage and sharing issues are urgent; In order to solve this problem, the PBFT algorithm was analyzed and the afBFT consensus algorithm was proposed, and its effectiveness was verified; The experimental results show that the average traffic of the Pluggable Consensus based on PBFT (CPBFT) algorithm and the Practical Byzantine Fault Tolerance (PBFT) algorithm during continuous operation is very similar, while the average traffic of the afBFT consensus algorithm is 3.47 kilobytes, which is about 14.1% higher than the PBFT algorithm, but within an acceptable range; The average value of simultaneous block out time can be stable at around 2.4 seconds; At the same time, the time for data encryption and search is in a relatively low range, within 350 ms and 140ms respectively; And in practical applications, the average response time of the data uplink and query interface is 2 120 ms and 1 020 ms, respectively; Overall, the proposed afBFT consensus algorithm is effective in electronic medical record management applications, and it is of great significance in ensuring the security of multi client medical information sharing.

Keywords: afBFT algorithm; medical information; master node; safety; punishment measures; smart contracts

0 引言

病历是患者在医疗机构就诊后所形成的一份书面记录,是医生为患者做出诊断的重要依据[1-3]。信息发展推动着传统纸质病历向线上电子病历转变,同时区块链技术的应用使得电子病历的管理愈发容易,共享性更强[4-6],同时泄露的风险也加大。Abbas A等人针对医疗信息泄露防控的问题,在对医疗系统进行详细分析的基础上提出了有效的替代方案[7]。牛淑芬等人为了保障电子病历共享中数据的安全性,在区块链技术的基础上提出了一种新的数据共享方案[8]。张剑等人针对电子病历数据分享中的信息泄露、篡改等问题,在区块链技术的基础上构建了电子病历数据存储的系统[9]。区块链技术的出现,很好地解决了传统模式下因互不信任而导致的合作难题。而从这一点上来看,区块链技术的作用是显而易见的。随着区块链技术的不断发展和广泛应用,其在电子医疗档案管理方面也得到了广泛的应用。利用区块链技术的数据不可更改、去中心化等特点来管理电子病历具备各种优点。与传统的电子病历管理系统相比,其优势在于病历更加容易管理、电子病历存档更加安全可靠且更容易实现共享,从而在保证医疗信息共享安全性以及患者隐私性具备有效性。尽管当前,区块链技术已经取得了较大的进展,但还有许多问题有待于进一步研究和完善。并且,当前应用区块链技术的电子病历在

收稿日期:2023-04-24; **修回日期**:2023-04-26。
作者简介:陈 洁(1978-),男,大学本科,高级工程师。
引用格式:陈 洁.实用拜占庭容错共识算法在医疗信息泄露防控及共享中的研究与应用[J].计算机测量与控制,2023,31(10):228-232,239.

多客户端数据共享上仍然存在医疗信息泄露的问题，同时传统意义上的共识算法的抗攻击预测能力明显不足。基于此，针对以往共识算法的缺陷，研究在实用拜占庭容错算法（PBFT，practical byzantine fault tolerance）的基础上引入抵抗预测攻击（anti-forecast）机制，提出了 afBFT 共识算法。其目的是有效保证医疗信息共享的安全性并保护患者的隐私，同时也有效加强患者医疗信息在多客户端中的共享性，以此为提升医疗技术的发展提供帮助。

1　afBFT 共识算法整体设计

针对医疗数据中的电子病历在多客户端信息共享中的困难与隐私安全性问题，研究在 PBFT 的基础上引入 anti-forecast 机制，提出了 afBFT 共识算法。共识算法中的共识指的是在一个更加分布式的非中心化点到点网络中，网络中的所有节点都可以在没有任何非信任第三方的帮助下达到一致[10-12]。在区块链网络中，随着节点数量的减少和分散性的降低，安全问题也会随之增加。随着网络中节点数量的增加和分散，单个节点所拥有的唯一决策权力变得更少，这也会导致系统性能下降[13-15]。基于分布式思想的一致性算法为 P2P 网络中节点间的互信提供了一种有效的解决方案。研究选择了目前作为主流的 PBFT 共识算法作为基础算法。

在实际的网络共识过程中，传统的 BFT 算法在处理交易数据时性能较弱，因此为了解决该问题对其进行改进就得到了 PBFT 算法。PBFT 共识算法通过对网络中节点和视图的标号，使一致性网络成为确定性网络。同时，其引入了主节的概念，从而减少了系统的通信开销，并提高了一致性对交易信息的处理效率[16-18]。其中，PBFT 共识算法会在每一个视图中均存在一个副本节点，并且该节点会被视为主节点。因此，副本节点相应表达如式（1）所示：

$$q = u \bmod m \tag{1}$$

式（1）中，q 表示副本节点的实际标号；u 表示目前视图的标号；m 表示网络中节点的实际数量。在 PBFT 共识算法的前期工作中，若副本节点没有收到当前主节点的相关信息，或发现当前主节点有欺诈行为，就会向另一个主节点发出请求，要求切换视图。该过程的计算表达如式（2）所示：

$$q = (u+1) \bmod m \tag{2}$$

在 PBFT 共识算法的视图切换期间，因为没有一个能够对客户发出的交易要求做出反应，因此此时网络对于交易要求的处理能力是 0。与此同时，在视角切换期间，还会产生更多的数据流量。所以，视角切换会极大地影响一致性网络的整体性能，同时，增加的数据流量也会给整个一致性网络带来很大的压力。另外，在主节点选择的实际过程中，如果其存在一定的顺序，预测性的攻击就难以被规避，以此产生不必要的安全风险[19-20]。因此，为了解决该问题研究提出的 afBFT 共识算法。afBFT 共识算法集成了智能合约（Fabric）中 PBFT 公式算法的相关协议，并将主节点的选择过程进行了无序化处理。其流程如图 1 所示。

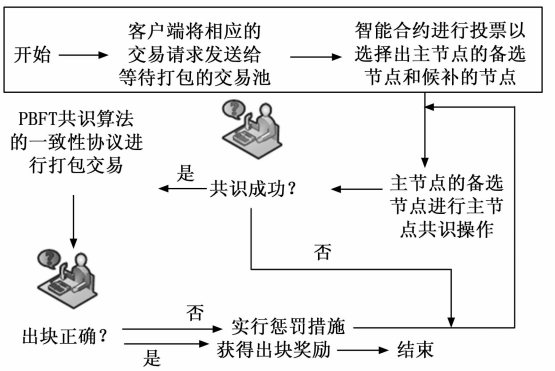


图 1　afBFT 共识算法流程示意图

从图 1 中可以看出，afBFT 共识算法流程中首先是客户端将相应的交易请求发送给等待打包的交易池，同时智能合约进行相应的投票以选择出主节点的备选节点和候补的节点。其次主节点的备选节点进行对应的主节点共识操作，如果共识失败则重新进行共识，如果共识成功则将 PBFT 共识算法的一致性协议进行打包交易。最后开始判定出块是否正确，如果不是则实行惩罚措施重新进行共识，如果是则获得相应的出块奖励并结束流程。afBFT 共识算法确保主节点在共识选择出来之前的不可预测性，以此可以对预先攻击进行规避。同时，等待打包的交易池也有效增加了电子病历系统的并行性，从而主节点无论处于哪种状态下，区块链网络都可以接收到实际交易请求。在奖惩机制中，将由节点出块所产生的挖矿奖励一次性支付给节点，而变成在连续的 6 个区块中每次给予该区块铸造奖励的 1/6，以此减少主节点作恶所造成的损失。

从图 1 的 afBFT 共识算法流程可以看出，其为主节点提供了不可被预测的方案，而在其共识的阶段中，网络中的实际节点被划分了主节点的备选节点、候补节点以及一般的节点，分别用 A、B、C 来表示。在实际的网络中，由于每一个节点真实的网络带宽不一定是一致的，因此造成网络上的信息量是有限的。同时因为 afBFT 算法中添加了一个主节点的一致阶段，所以通信量比 PBFT 稍大一些。节点的网络带宽必须足够大，从而能够在最后一个区块上对整个网络进行广播确认。其中，研究最低的网络带宽表达如式（3）～（6）所示：

$$D = fh \times T^2 + bl \times T + CP + s \tag{3}$$

式（3）中，D 表示网络带宽的实际最小值；fh 表示转发哈希的实际大小；T 表示主节点的实际数目；bl 表示进行相应打包操作后的一个区块的实际大小；CP 表示一致性协议中实际产出的通信总量；s 表示一般节点进行投票操作后生成的备选的主节点产生的通信总量。

$$CP = bl \times T + (pr + v) \times T^2 \tag{4}$$

式（4）中，pr 表示准备阶段中节点广播进行确认的消息的实际大小；v 表示确认阶段节点广播进行确认的消息的实际大小。

$$W = \gamma \times t \tag{5}$$

式（5）中，W 表示一个区块进行打包时的实际交易数目；γ 表示每秒可以打包的交易的实际数目；t 表示前一个区块处于主节点共识阶段的时间与当前处于主节点共识阶段的时间之间存在的时间差。

$$bl = he + \sum_{m=1}^{W} \lambda_m \tag{6}$$

式（6）中，he 表示区块头的实际大小；λ 表示一条交易相关信息的实际大小。依据式（3）至式（6）可以看出，T 的大小直接决定着网络中的最小带宽，将其设置过小会带来较为严重的医疗信息泄露等问题，这违背了 afBFT 共识算法设计的初衷，而如果将其设置过大，则会使得网络中的实际通信量不断增大，以此造成不必要的网路拥堵问题。因此研究利用仿真计算将节点数目设定为 19，以此保证产生的通信总量仅占整个网络带宽的 35～40％之间。在 afBFT 共识算法中，研究加入了一种惩罚机制来避免主节点与多个 C 节点串通一气地使某个节点顺利进入主节点的备用节点队列中作恶。在表决过程中，各节点均需提供相应的通证。如果主节点被发现作恶，那么这个主节点和那些投票给这个节点的 C 节点将会被扣掉通证，这将使其所付出的成本远高于所得到的收益，进而降低了其作恶的概率。惩罚措施的流程如图 2 所示。

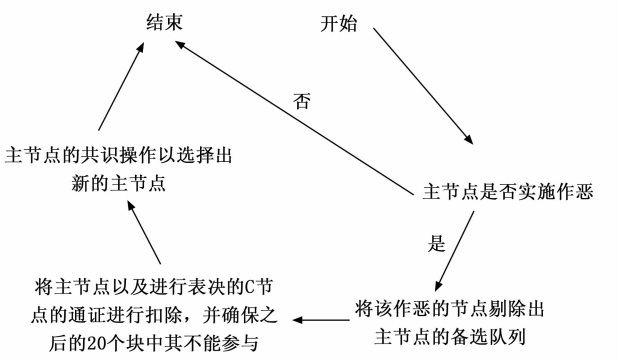


图 2 惩罚措施的流程示意图

从图 2 中可以看出，afBFT 共识算法惩罚措施流程中首先判断主节点是否实施作恶，如果没有则结束流程。如果有则将该作恶的节点剔除出主节点的备选队列中。其次将主节点以及进行表决的 C 节点的通证进行扣除，并确保之后的 20 个块中其不能进行参与。最后进行主节点的共识操作以选择出新的主节点并结束流程。afBFT 共识算法表决过程中，每一个节点都要支付一定的抵押额，每一个被选为“ON”和“SN”的节点都会被记录下来。如果当前的主节点被发现作恶，那么这个主节点与其所票的其他节点将会被扣掉通证，这将使其所付出的成本远高于所得到的收益，进而降低了其所能产生的收益。

在 afBFT 的共识算法中，尽管节点的公钥是可共享的，但在协议产生阶段，网络中的所有节点都是在协议产生阶段通过哈希合成和转发哈希加密，从而在协议产生前网络中的其他节点都不知道被转发哈希的节点是哪一个。此外，在使用 afBFT 共识算法选定出主节点之后，恶意节点无法预知下一次负责出块的是哪一个节点，从而无法发起攻击。基于此，利用 afBFT 算法的多客户端电子病历信息管理与数据共享方案整体框架如图 3 所示。

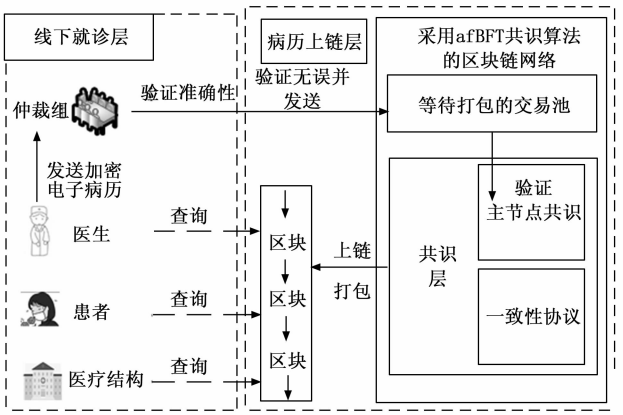


图 3 基于 afBFT 算法多客户端电子病历信息管理与数据共享方案

从图 3 中可以看出，该方案主要包含线下的就诊与线上的链接两个部分。通过该方案可以有效实现医疗机构之间电子病历信息数据共享的安全性与真实性，并加强了医疗信息泄露防控，从而保证了患者的隐私。另外，线下就诊层和病案上链层相互合作，能够实现对电子病案进行加密上链，在加强医疗信息泄露防控的基础上实现了不同的医疗机构之间病案信息的共享。与此同时，因为采用了 afBFT 共识算法，所以能够有效地避免节点通过对其进行预测攻击，以此让其选择主节点，从而对病案信息进行篡改。从总体上看，电子病案管理系统是保存病人病案资料的重要载体，其数据的真实性和正确性要求很高。同时，在电子医疗记录系统中，医疗记录的上载程序不需要实时，因而能够容许一定程度的延时。而在所给出的方案中，研究所使用的 afBFT 共识算法，也是为了确保链上数据的真实性和可靠性而牺牲了一些实时性，将 afBFT 共识算法应用到电子医案管理系统中，完全能够满足系统的要求。

另外，afBFT 共识算法在实际的公式过程中，由于其面向多客户端，因此在每次共识结束后均会进行一次多对多的通信进入新的视图之中。因此，afBFT 共识算法在实际的共识过程中，交互式通信量的计算表达如式（7）所示：

$$\xi_a = l^2 M^2 + 3lm - 4 \tag{7}$$

式（7）中，ξ_a 表示 afBFT 共识算法实际共识过程中的交互式通信总量。lm 表示加入共识的节点。而其与原始的 PBFT 算法通信开销对比表达如式（8）所示：

$$X = \frac{\xi_p}{\xi_a} \tag{8}$$

式（8）中，X 为原始 PBFT 算法与 afBFT 算法通信开销之比；ξ_p 表示 PBFT 算法的通信开销。同时，在进行时延分析时，afBFT 共识算法拜占庭可容忍的最大数量表达如式

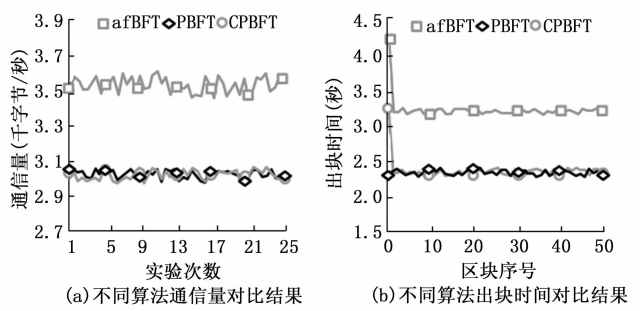
(9) 所示：

$$g=\left[\left(1-\frac{2}{3}l\right)\cdot M-\frac{1}{3}\right] \tag{9}$$

式 (9) 中，g 为 afBFT 共识算法拜占庭可容忍的最大数量。由于研究的共识算法利用了区块链技术，因此需要在实际的应用方案中进行验证。区块链是一种新型的计算机技术，包括分布式数据存储，点对点传输，共识机制，加密算法等。在区块链中，区块是由上一个区块的哈希值所连接起来的，并由创世区块与最近的一个区块相连接而成的一条链，一旦被写进去，就难以更改或删除。实际的区块链系统具备去中心化、难以篡改、匿名以及开放性等特点，在区块链技术中，智能合约是在一个重要的概念，研究提出的方案便是利用此概念构建的。

2　afBFT 算法在医疗信息泄露防控及共享方案中的应用实验

为了验证 afBFT 算法在医疗信息泄露防控及共享方案中应用时的安全性，研究利用模拟实验对其进行了验证，并在南京医科大学附属无锡人民医院进行了实际应用。实验环境中 4 个服务器均采用同样的中央处理器、内存容量以及操作系统，除服务器 2 硬盘 1 TB 外，其余均为 500 GB。同时，研究引入传统的 PBFT 共识算法和在 PBFT 基础上构建的可插拔共识算法 (CPBFT，Pluggable Consensus based on pbft) 作为对比算法。其中，在正常的系统环境中，3 种算法均对 100 个包含区块头的空块进行打包，同时做 50 次实验，最后得到实际通信量的平均值与出块时间，其结果如图 4 所示。

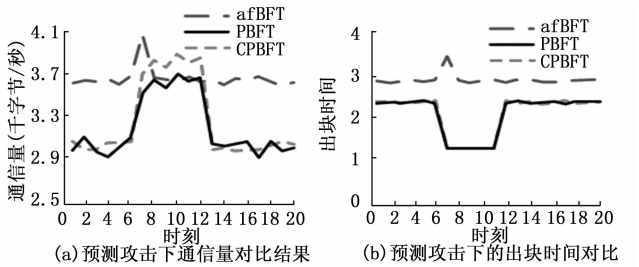


(a) 不同算法通信量对比结果　(b) 不同算法出块时间对比结果

图 4　不同算法的平均通信量与出块时间平均值对比结果

综合图 4 中可以看出，通过对 50 次实验的数据统计后，PBFT 共识算法、CPBFT 共识算法以及 afBFT 共识算法每秒通信量的平均值分别达到 3.04 千字节、3.04 和 3.47 千字节。同时，因为 PFBT 具有较高的出块速度，因此对其改进后得到的 afBFT 算法可以将全局一致性的时间控制在 2.4 s 左右来确保系统的性能。综合来看，在连续运行时，CPBFT 算法和 PBFT 算法的通信量的平均值十分相近，而 afBFT 共识算法的通信量平均值比 PBFT 算法高 14.1%左右。在 afBFT 共识算法中加入了主节点的一致性，使得在一致性过程中，需要进行更多的广播，以此使通信量有所增加。尽管在执行时，afBFT 共识算法的通信量很大，但实际通信量仍然在可以接受的范围之内。

另外，CPBFT 共识算法每个节点的可信度都是按照其信誉度相关系数来进行的，这就导致第一个区块的出块时间比较长。在 afBFT 算法中，节点必须首先对智能契约进行表决，然后再选择一个替代的主结点，这会导致算法耗时很长。PBFT 和 CPBFT 平均出块时间分别为 1.65 s 和 1.7 s，而在 afBFT 共识算法中，因为每个节点在最初的阶段都要对智能合约进行表决，所以第一个区块的出块时间会比较长。在选择了主节点备选队列之后，在主节点选择、普通节点投票以及备选节点进入主节点备选队列都是同步进行的，所以后续出块时间可基本稳定在 2.4 s。在受到预测攻击环境中，研究仿真模拟攻击者早上 7 点开始进行预测性攻击，12 点结束攻击。因此，其通信量对别结果如图 5 所示。



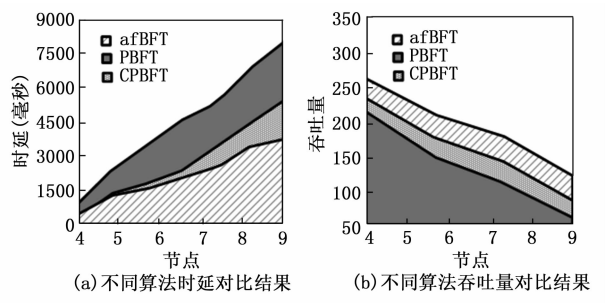
(a) 预测攻击下通信量对比结果　(b) 预测攻击下的出块时间对比

图 5　受到预测攻击环境中不同算法的对比结果

综合图 5 可以看出，PBFT 与 CPBFT 算法的视窗切换策略利用了 A 节点侦测到当前主节点的脱机情况，从而增加了视窗切换的通信量。同时因为主节点和编号在当前主节点之后的 5 个节点都是脱线的，因此系统将会接连触发五次超时，并接连发起五次视图切换请求。afBFT 共识算法中，如果当前的主节点因为受到了恶意节点的攻击而处于脱机状态，则必须重新运行主节点一致性来选择新的主节点。因此在刚刚被攻破的区域，信息流是最多的。但是，因为这种预测攻击是一种固定的攻击方式，所以不会对 afBFT 共识算法的后续出块通信量产生影响。

另外，在受到预测攻击的情况下，afBFT 共识算法的出块时间大致维持在 2.5 s，而 PBFT 算法和 CPBFT 算法在 7 点至 11 点之间时出块时间为 0，其余时间出块时间平均值为 1.7 s 左右。同时，CPBFT 和 PBFT 公式算法均无法在受到预测攻击的时间段内进行打包交易。而 afBFT 共识算法，则是在第一次被预测攻击时，将主结点脱机来使系统恢复到主节点的一致性。因此在第一个被攻击的区块上，每一个被攻击的区块，都会花费更多的时间。但是从实验的结果来看，预测攻击并没有对 afBFT 共识算法的后续分块造成任何影响。综合图 4 和图 5 来看，在正常工作状态下，afBFT 共识算法数据传输速率稍有增大，但在受到攻击时具有较好的稳定性。与 PBFT 和 CPBFT 相比，afBFT 共识算法的出块时间没有明显的变化。因此 afBFT 共识算法在某种程度上具备了对预测攻击的抵抗能力，并且在遇到预测攻击时，其稳定性和安全性都要高得多，即在医疗信息防控上具备较高的性能。为了进一步验证 afBFT 共识

算法的优越性，研究对比 3 种算法在不同节点下的时延与吞吐量，其结果如图 6 所示。



(a) 不同算法时延对比结果 (b) 不同算法吞吐量对比结果

图 6 3 种算法在不同节点下的时延与吞吐量

综合图 6 可以看出，afBFT 共识算法的时延远远低于对比算法，在实验节点中最高为 3 150 ms，仅为 PBFT 算法的一半。另外，其吞吐量也远远大于对比算法。综合来看，研究提出的 afBFT 共识算法无论是时延还是吞吐量上都具备较高的性能。基于此，研究将其应用到实际的医疗信息泄露防控及共享方案中，得到的数据加密与搜索成本结果如图 7 所示。

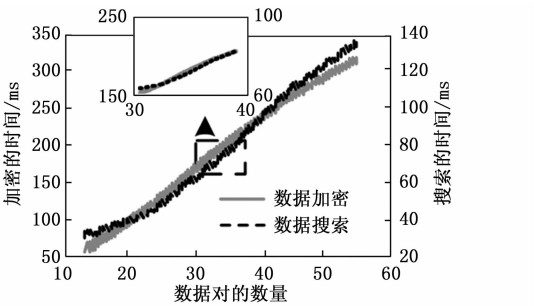


图 7 基于 afBFT 共识算法的方案数据加密与搜索成本结果

综合图 7 可以看出，数据对数量的不断增加促使加密和搜索过程的消耗逐渐变大，但所需要的时间一直都在较低的范围内，其中加密时间维持在 350 ms 内，而搜索时间维持在 140 ms 内。综合来看，运用 afBFT 共识算法后的方案在加密和搜索过程中拥有较低的时延，表明了方案在实际应用中可以及时进行数据加密和搜索，具有一定的可行性。同时也表明了 afBFT 共识算法在医疗信息泄露防控及共享方案中的应用对数据的安全性保证与患者的隐私性保护上具备有效性。为了进一步验证利用区块链技术与 afBFT 共识算法构建的方案的有效性，研究在实际应用中将其应用到系统中，以此验证数据上链的性能和耗时，实验访问用户为 100 个。其结果如表 1 所示。

表 1 研究方案在系统应用下的性能

—	1	2	3	4	5
A	10 000 个	2 120 ms	370 ms	7 100 ms	39.2 个/s
B	10 000 个	1 020 ms	56 ms	3 130 ms	96.4 个/s
	6		7	8	
A	1 815 ms		3 251 ms	3 600 ms	
B	850 ms		1 500 ms	2 000 ms	

表 1 中，1～5 分别表示请求的实际数量、响应时间的平均值、最小值、最大值以及吞吐量；A 和 B 表示数据的上链和查询接口。6～8 表示 50%～95%的用户。从表 1 中可以看出，数据上链与查询接口的平均响应时间分别为 2 120 ms 和 1 020 ms，同时 95%永华下分别为 3 600 ms 与 2 000 ms，基本满足需求。

3 结束语

为了解决医疗信息泄露防控及共享方案中的安全性与隐私性等的问题，研究在 PBFT 共识算法的基础上引入 anti-forecast，提出了 afBFT 共识算法，并利用实验对其有效性进行验证。实验结果表明，在正常无攻击的情况中，PBFT 共识算法、CPBFT 共识算法以及 afBFT 共识算法每秒通信量的平均值分别达到 3.04 千字节、3.04 和 3.47 千字节。PBFT 一致性和 CPBFT 平均出块时间分别为 1.65 s 和 1.7 s。而在 afBFT 共识算法中第一个区块的出块时间会比较长，基本稳定为 2.4 s。同时，afBFT 共识算法的时延远远低于对比算法，在实验节点中最高为 3 150 ms，仅为 PBFT 算法的一半，而吞吐量远远大于对比算法，并且将其应用在实际方案中使得方案的数据加密与搜索时间分别维持在 350 ms 与 140 ms 内，具备较高的可行性。实际应用中，数据上链与查询接口的平均响应时间分别为 2 120 ms 和 1 020 ms。综合来看，研究提出的 afBFT 共识算法在保证系统稳定上具备高性能，即在医疗信息泄露防控及共享方案中的应用具备较高的实用性，同时在数据的安全性保证与患者的隐私性保护上具备较高的有效性。但是，afBFT 共识算法的主节点共识工程比较繁杂，由此造成通信量的不断增长，因此后续需要进行优化。

参考文献：

[1] JOHARI R, KUMAR V, GUPTA K, et al. BLOSOM: BLOckchain technology for Security of Medical records [J]. ICT Express, 2022, 8 (1): 56-60.

[2] 董婉婷. 基于区块链技术的医疗信息安全策略构建与实现 [J]. 电子设计工程, 2021, 29 (15): 63-67.

[3] 刘 扬, 胡学先, 周 刚, 等. 基于多层次区块链的医疗数据共享模型 [J]. 计算机应用研究, 2022, 39 (5): 1307-1318.

[4] 刘 晨, 赵 迪. 基于区块链数据共享技术的可追溯共识机制 [J]. 信息技术, 2021, 45 (12): 112-117.

[5] 颜芬芬, 孙冬杰, 王道雄. 基于区块链技术的医疗器械全流程追溯系统设计探索 [J]. 中国卫生信息管理杂志, 2021, 18 (6): 797-801.

[6] 李 莉, 吴 怡, 杨祉坤, 等. 基于分区型区块链医疗电子病历共享方案 [J]. 计算机应用, 2022, 42 (1): 183-190.

[7] ABBAS A, HAMID M A. Adapting hybrid approaches for electronic medical record management and sharing using blockchain sharding [J]. Periodicals of Engineering and Natural Sciences, 2023, 11 (1): 5-14.

(下转第 239 页)