doi:10.3772/j.issn.1002-0470.2021.02.004

基于区块链的医疗临床数据防篡改机制及篡改攻击分析①

李晓明②* 黄 慧* 应 毅* 曾 岳**

(*三江学院计算机科学与工程学院 南京 210012)

(**金陵科技学院软件工程学院 南京 210012)

摘 要 医疗临床数据的可靠共享机制对提升智慧医疗水平具有重要意义,防篡改机制可为医疗临床数据交互与共享提供保障。本文首先给出了基于区块链的医疗临床数据防篡改机制,然后设计了两种场景来分析医疗临床数据篡改攻击的实施途径,最后对篡改攻击进行建模并基于马尔科夫链进行了分析。本文研究内容对提升医疗临床数据共享安全性以及智慧医疗水平均具有较高的应用价值。

关键词 区块链;智慧医疗;防篡改机制;篡改攻击;马尔科夫链

0 引 言

医疗行业将逐步融入人工智能技术、传感技术等高科技技术,使医疗服务走向真正意义的智能化,推动医疗事业的繁荣发展。在中国新医改的大背景下,智慧医疗正在走进寻常百姓的生活。智慧医疗通过打造健康档案区域医疗信息平台,利用最先进的物联网技术,实现患者信息在医务人员、医疗机构、医疗设备之间的互动,逐步达到信息化[1-2]。在智慧医疗体系中,医疗临床数据存储及共享机制是首先要关注的问题。数据完整性和来源可追溯性是医疗临床数据交互与共享的关键,医疗科研机构必须能够证明跨机构数据来源的可靠性,以确保临床试验结果从数据捕获到最终分析的可靠性。因此,研究医疗临床数据的可靠共享机制对提升智慧医疗水平具有重要的意义。文献[3]提出了一种基于非标准对角数据聚合方法共享医疗敏感数据的解决方案。文献[4]提出了一种基于上下文感知医疗隐私保护方案。文献[5]提出了一种基于雾计算设施的医疗信息安全模型。然而,上述解决方案都依赖于完全受信的第三方,采用认证和密钥协议方案来提供医学信息共享的安全性[6],容易受到离线密码猜测攻击和特权内线攻击[7],很难实现医疗临床试验数据安全、可追溯共享和管理。

区块链技术最早于文献[8]中有所阐述,目前在全球范围引起了一场新的技术革新和产业变革。狭义来讲,区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证的防篡改和不可伪造的分布式账本。广义来讲,区块链是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式。

区块链技术是分布式数据存储、点对点传输、共识机制、加密算法等多种计算机技术的新型应用模式,其技术体系主要包括非对称加密技术、分布式存储技术、对等网络传输技术和共识机制等。区块链典型特征包括去中心化、去信任、防篡改和匿名。区块链技术主要用于解决交易的信任和安全问题,区块链以其特有的安全性,已在许多领域中得到了应用,国内外学者对区块链的研究也主要集中在区块链技术

① 国家自然科学基金(61902447),江苏省高校自然科学基金(19KJB520049,18KJB520042,18KJB520042)和江苏省高校“青蓝工程”资助项目。

② 男,1978 年生,硕士,副教授;研究方向:区块链技术,大数据应用开发技术;联系人,E-mail:nj_lixiaoming@163.com

(收稿日期:2020-05-19)

的应用层面[9-14]。

基于区块链的数据共享机制可为医疗临床数据提供完整性及可追溯性管理,从而提升医疗临床数据应用安全性和效能,被认为是一种可行的解决方案。本文专注研究基于区块链技术的医疗临床数据共享,首先从理论上分析了基于区块链的医疗临床数据防篡改机制(数据结构层面、传输机制层面和共享机制层面),然后分析了医疗临床数据被封装到区块之前及被封装到区块并入链之后两种场景下可能存在的篡改攻击,最后对篡改攻击进行建模并基于马尔科夫链进行了分析。

1 基于区块链的医疗临床数据防篡改机制

医疗临床数据在采用区块链技术进行共享时,区块链技术可为医疗临床数据提供一个立体的防篡改机制。为了便于分析,把患者个人信息的敏感数据抽象为交易数据。

1.1 数据结构层面上的防篡改机制

从数据结构上看,区块包括区块头和区块体两个部分,其中区块头中包含前一个区块的哈希值、时间戳、Merkle 根等选项,区块体中包含多个交易记录、基于交易生成的 Merkle 树等,如图 1 所示。

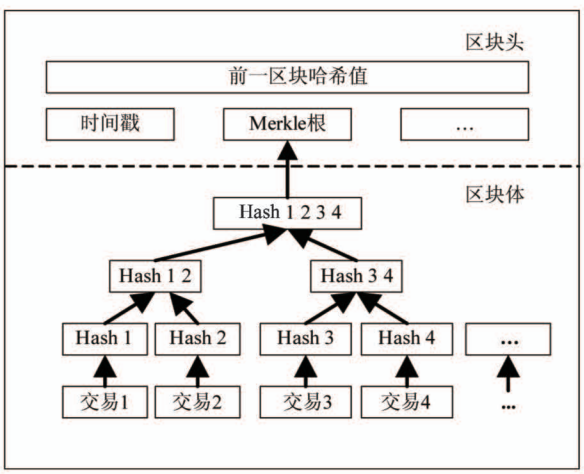


图 1 区块的数据结构

1.1.1 Merkle 树

为了增加篡改攻击的难度,在区块体中使用了 Merkle 树,其作用是快速归纳和校验区块体的交易数据的存在性和完整性。Merkle 树通常包含区块体的交易数据,区块头的根哈希值(即 Merkle 根)以及所有沿交易数据到根哈希值的分支。Merkle 树运算过程一般是将区块体的交易数据进行分组哈希,并将生成的新哈希值插入到 Merkle 树中,如此递归直到只剩最后一个根哈希值,并把其记为区块头的 Merkle 根。区块链系统中大多采用二叉 Merkle 树,其每个哈希节点总是包含两个相邻的交易数据块或其哈希值。

Merkle 树是基于交易数据经过多次哈希运算而生成的,一旦篡改了某个交易数据,将导致整个 Merkle 树异变,在数据结构上进行防篡改。

1.1.2 时间戳

时间戳通常是一个字符序列,用于标识一份数据在某个特定时间之前是已经存在的、完整的、可验证的。区块头中的时间戳用于记录区块的入链时间。区块链使用共识算法实现了一个分布式的时间戳服务,利用时间戳实现在时间上有序的、由一个个区块组成的一根链条。每一个新区块生成时,都会被打上时间戳,最终依照区块生成时间的先后顺序相连成区块链,每个独立节点又通过 P2P 网络建立联系,这样就为信息数据的记录形成了一个去中心化的分布式时间戳服务系统。

1.1.3 前一区块的哈希值

每个区块都在区块头中记录了前一个区块的哈希值,新生成的区块在入链前,会把当前链中最后一个区块的哈希值作为该区块的前一个区块的哈希值,所有区块按照区块哈希值逐个相连就构成一根链条。当前区块的哈希值是由前一个区块的哈希值与当前区块信息再次哈希而生成的。因此,当前区块的哈希值会影响其后所有区块的哈希值。篡改一个区块的信息,会导致区块链中该区块之后所有区块的哈希值发生异变。

1.2 传输过程中的防篡改机制

1.2.1 交易信息的透明性

区块体记录的交易信息是经过加密的,换句话说,交易信息对网络用户是透明的。交易信息密文对网络上所有用户都是公开的,但是关联用户才能

解密并使用交易信息,客观上起到了防篡改效果。

传统的交易,需要知道交易双方的真实信息(如网上购物交易时,需要知道双方的姓名和联系方式)。区块链支持用户进行匿名交易,即在不要求用户真实信息的前提下,通过基于非对称密码技术的数字签名和验证机制来实现匿名交易,避免了用户真实信息的泄露。

1.2.2 交易的签名与验证

根据区块链的运行机制,一个时间间隔内的所有交易数据被广播在网络中,由共识机制产生具有写入链权益的节点产生新区块,并把这些交易数据封装到一个区块中。如何认定该交易数据在传输过程中是否被篡改过?区块链网络使用了基于非对称密码技术的数字签名与验证措施来保证交易数据的安全性。其基本原理是交易双方都有一个私钥和公钥,私钥自己保存,公钥广播给网络的所有用户;交易发起方(发送者)先使用数字摘要技术(Hash 等)将交易数据缩短到某个固定长度,即生成交易数据的数字摘要,然后使用自己的私钥对数据摘要进行加密,这样就得到了一份数字签名;然后把交易数据连同数字签名一块发送,区块链网络上任何人都可以用该交易发起方的公钥来解密数字签名以验证数据是否为该交易发起方发出(如果解密失败则不是),同时可以验证解密后生成的数字摘要和收到的数据的数字摘要是否匹配来验证交易数据是否被篡改过。

通过数字签名技术,可以保证交易数据在传输过程中无法被篡改,实际区块链网络中会在记录数据时通过数字签名验证交易的有效性,只会将验证通过的交易打包到区块中,并且每个客户端在接收到一个新的区块时也会做这个验证。

1.3 基于共识机制的防篡改机制

1.3.1 记账权分配

区块链的自信任主要体现于分布于区块链中的用户无须信任交易的另一方,也无须信任一个中心化的机构,只需要信任区块链协议下的软件系统即可实现交易。这种自信任的前提是区块链的共识机制(consensus),即在一个互不信任的市场中,要想使各节点达成一致的充分必要条件是每个节点出于对自身利益最大化的考虑,都会自发、诚实地遵守协议中预先设定的规则,判断每一笔记录的真实性,最终将判断为真的记录记入区块链之中。换句话说,如果各节点具有各自独立的利益并互相竞争,则这些节点几乎不可能合谋欺骗,而当节点在网络中拥有公共信誉时,这一点体现得尤为明显。区块链技术正是运用一套基于共识的数学算法,在机器之间建立信任网络,从而通过技术背书而非中心化信用机构来进行全新的信用创造。

目前,区块链系统使用的共享机制主要有 4 类:即工作量证明机制、权益证明机制、股份授权证明机制和 Pool 验证池。从实质上看,共识机制用于解决在互不信任的场景下谁拥有当前时间间隔内交易的记账权的问题。只有通过共享机制验证获得记账权的节点,才能把自己生产的区块加入链中。获得记账权需要通过复杂的共享机制验证过程,即获得一次记账权需要花费很大的成本。恶意节点若想篡改交易信息,首先要支付获得记账权的成本,即使获得了记账权,还未必能够实现篡改的企图。从成本效益角度看,共享机制本身就是防篡改的有效保障。

1.3.2 最长链有效原则

区块链系统是分布式系统,不同节点保存的当前区块链副本的长度可能不同,节点在同步区块链系统副本时,遵循最长链有效原则。所谓最长链有效原则,即当节点在同步区块链副本时,若发现系统中存在多个长度不同的链,则相信包含最多区块的长链为系统的有效链。

例如当前区块链中存在 $N+M+1$ 个区块,当某节点把第 N 个区块修改后重新播送到网络上,这相当于创建一个比真实链(长度为 $N+M+1$) 短得多的区块链分支(长度为 $N+1$)。现在有两个互相竞争的区块链, 一个是包含被修改第 N 个区块的区块链(长度为 $N+1$), 另一个长度为 $N+M+1$ 的区块链。系统中其他的节点在同步区块链副本时,会丢弃长度为 $N+1$ 的链,因为它们已经知道存在一个现有的更长的区块链。

若想使第 N 个区块修改后重新播送到网络上且能够成功入链,则必须至少重新生成 $M+2$ 个区块,使新链长度大于 $N+M+1$。在分布式环境下,要

重新生成 $M+2$ 个区块，则需要控制全网一半以上的节点，否则几乎是不可能的。而在分布式环境下，控制网络 50% 以上的节点，成本是难以估量的。这从成本效益角度，规避了被篡改的风险。

2 医疗临床数据共享的篡改攻击

采用区块链技术作为医疗临床数据共享机制，下面对可能遇到的篡改攻击进行理论分析。为了便于分析，把患者个人信息的敏感数据抽象为交易数据。区块链系统被设计成只能对链进行追加区块，即对区块链唯一的操作就是把生成的新区块追加在链的尾部。当交易数据被封装在某个区块中且该区块被验证通过加入链后，无法通过修改或删除该区块的方式来达到修改交易数据的目的。防篡改性是区块链技术的核心特征之一，其本意是交易数据一旦被封装到区块并入链后，被成功篡改的可能性极小，几乎可以忽略。但事实上，区块链系统的交易数据仍然存在被篡改的可能性。下面分析可能发生篡改攻击的场景以及攻击成功的可能性。

假设用户 A、B 之间进行了一笔交易，记用户 A 和用户 B 的公钥和私钥分别为 $public\_keyA$、$private\_keyA$、$public\_keyB$、$private\_keyB$；用户 A 和用户 B 产生的原始数据分别为 MA、MB，交易数据为 $M'(M' = MA' + MB')$，其中，$MA' = private\_keyA(public\_keyB(MA))$，$MB' = private\_keyB(public\_keyA(MB))$；该交易数据 M' 在第 t_1 时刻被广播到网络中，等待被封装到区块，在第 t_2 时刻某恶意节点窃取了该交易双方的私钥和公钥；区块链系统每隔时间周期 T 封装一个区块。

场景 1 若 $t_2 - t_1 < T$，即在交易数据被封装到区块前，恶意节点窃取了交易双方的私钥和公钥，实施篡改攻击。下面分析篡改攻击的可能性。

当 $t_2 - t_1 < T$ 时，该交易数据尚未被封装到区块中，恶意节点将执行以下操作：

$public\_keyB(private\_keyA(MA')) \rightarrow MA$

$public\_keyA(private\_keyB(MB')) \rightarrow MB$

$M_A \rightarrow M_A*$

$M_B \rightarrow M_B*$

$private\_keyA(public\_keyB(M_A*)) \rightarrow M_A'*$

$private\_keyB(public\_keyA(M_B*)) \rightarrow M_B'*$

$M_A'* + M_B'* \rightarrow M'*$

$M'*$ 就是篡改后的交易数据。

然后，该恶意节点把篡改后的交易数据 $M'*(M'* = MA'* + MB'*)$ 广播到网络上。此时，用户 A、B 之间的一次交易，却在网络上存在两份不同的交易数据 M' 和 $M'*$。

由于记账节点是通过共识机制来获得记账权的，即各个记账节点随机获得本次记账权。恶意节点难以推测出是哪个记账节点获得本次记账权，就无法实施把篡改后的交易数据 $M'*$ 直接推送给本次记账节点的企图。

场景 2 若 $t_2 - t_1 \geqslant T$，即在交易数据被封装到区块后，恶意节点窃取了交易双方的私钥和公钥，实施篡改攻击。

设该交易数据 M' 在第 $t_{12}(t_1 < t_{12} < t_2)$ 时刻被封装到第 B_N 区块中并入链（此时链长为 $N+1$），如图 2 所示。

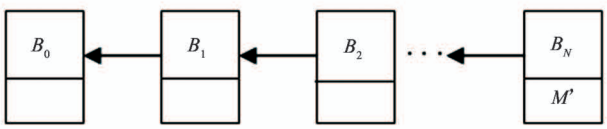


图 2 区块链（最后一个区块为 B_N，链长为 $N+1$）

下面分析篡改攻击的可能性。

若 $t_2 - t_{12} < T$，恶意节点将执行以下操作：

获取当前时间周期的记账权来产生区块 B_N*；

恶意节点篡改 M' 生成 $M'*$；

把 $M'*$ 重新封装在区块 B_N*；

试图把区块 B_N* 链接到第 B_{N-1} 区块后入链；

此时链中产生短分支（如图 3 所示）。

此时，按照最长链有效原则，恶意节点产生的分支在系统同步时会被其他节点丢弃。理论上，该恶意节点必须从当前时间周期起至少连续获得 3 个周期的记账权，使得分支链长度为 $N+3$，而从当前时间周期起第 4 周期由正常记账节点产生区块后，正常链的链长为 $N+2$，由最长链有效原则，使得含有篡改数据的区块入链，如图 4 所示。

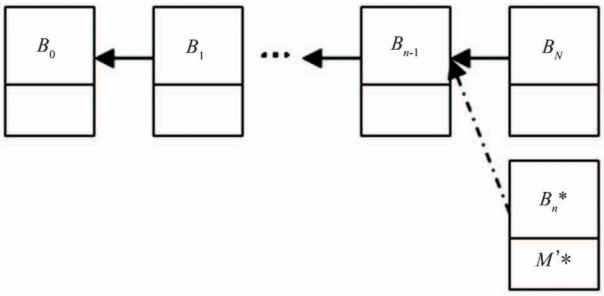
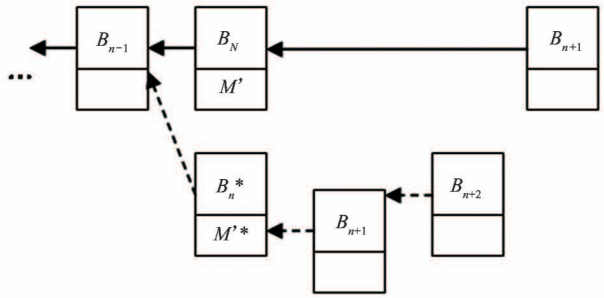


图3　区块链(含短分支)



(恶意节点连续获得3次记账权)

图4　含有篡改数据的区块入链

设网络中存在 $W(W \to +\infty)$ 个记账节点,单个节点获得1次记账权的概率为 $1/W$,连续获得3次记账权的概率为 $(1/W)^3$。也就是说,在交易数据被封装到区块并入链后,单个恶意节点实施篡改攻击的成功概率是极小的,几乎是不可能的。

若 $t_2 - t_{12} \geqslant T$,交易数据 M' 被记账节点封装到区块并入链后,又至少有1个新区块入链,此时区块链的链长至少为 $N+2$。

由上面的分析可知,在更加复杂的情景下,单个恶意节点实施篡改攻击的成功概率几乎为0。

3　医疗临床数据共享的篡改攻击建模分析

3.1　篡改攻击的定义

攻击者企图对交易数据(患者个人信息的敏感数据)进行篡改,把篡改后的交易数据封装在区块中,并使该区块出现在最长链上,称之为篡改攻击。区块链系统在运行时,诚实节点通过共识机制验证后获得记账权,把产生的区块正常加入主链所形成的链,称之为诚实链。攻击节点把产生的含有篡改交易数据的区块加入主链后,将在主链上产生分支链,称之为攻击链。诚实链和攻击链的速率类似于二项式随机游走。

设主链上区块高度为 i 的区块 B_i 中封装了交易数据 M',对交易数据 M' 进行篡改攻击后,产生的新区块 B_i*,对篡改攻击成功 $Success_{M'}$ 定义如式(1)所示。

$$Success_{M'} = \begin{cases} 1 & \text{若 } B_i* \text{ 加入主链} \\ 0 & \text{若 } B_i \quad \text{加入主链} \end{cases} \tag{1}$$

若含有区块 B_i* 的攻击链的游走速率大于含有区块 B_i 的诚实链,此时攻击链长度大于诚实链,按照最长链有效原则,节点同步时,攻击链被并入主链,封装有篡改交易数据的区块 B_i* 加入主链,封装有原始交易数据的区块 B_i 被丢弃,篡改攻击成功;若含有区块 B_i 的诚实链的游走速率大于含有区块 B_i* 的攻击链,此时诚实链长度大于攻击链,按照最长链有效原则,节点同步时,把攻击链丢弃,篡改攻击失败。

3.2　篡改攻击建模

由第2节可知,篡改攻击发生的时刻 t_2 与交易数据处理时刻 t_1 之间的时间差,其值的大小对篡改攻击成功率有影响。本文对篡改攻击成功概率 $P_{M'}$ 的定义如式(2)所示。

$$P_{M'} = f(t_2 - t_1) \tag{2}$$

式中,$P_{M'}$ 是关于 $(t_2 - t_1)$ 的函数,对函数值与区块链记账周期 T 的关系,本文定义如式(3)所示。

$$f(t_2 - t_1) = \begin{cases} \dfrac{1}{2}e^{-(t_2-t_1)} & \text{若 } t_1 \text{ 时刻交易数据被封装} \\ \dfrac{1}{2}e^{-(t_2-t_1)^3} & \text{若 } t_1 \text{ 时刻交易数据被入链} \end{cases} \tag{3}$$

式(3)中,若在第 t_1 时刻,交易数据被封装到区块,区块尚未入链,此时模拟的是第2节的攻击场景1,当 $(t_2 - t_1)$ 趋于0时,篡改攻击成功的概率趋于50%,当 $(t_2 - t_1) > T$ 时,篡改攻击成功的概率趋于0;若在第 t_1 时刻,交易数据被封装到区块且区块入链,此时模拟的是第2节的攻击场景2,当 $(t_2 - t_1) > T$ 时,篡改攻击成功的概率以指数倍速率趋于0。

3.3　篡改攻击的马尔科夫链分析

区块链系统在一个记账周期内记账一次,把一

个区块加入链中。设第 i 个记账周期，交易数据为 M'_i，入链的区块为 B_i，记账周期结束时区块链所处的状态为 s_i（s_i 与记账后区块链当前的长度正相关）。由于每个记账周期内产生的交易数据是随机的，每个记账周期内入链的区块也是随机的，区块链的状态是随机的，即 $\{s_i,\ i \in I\}$ 是一个随机过程。对于区块链来说，在第 i 个记账周期开始时其状态为 s_{i-1}，由于区块 B_i 入链，该记账周期结束时其状态变为 s_i，由此可见，区块链在第 i 个记账周期结束时的状态仅与其在第 $i-1$ 个记账周期结束时的状态有关，而与其在第 $i-2$ 个记账周期结束时的状态及以前的状态无关。区块链的状态序列 s_0，s_1，s_2 …构成了一个马尔科夫链（Markov chain），记状态序列集合为 $S = \{s_0, s_1, s_2 \cdots\}$ 或 $S = \{s_i \mid i \in I\}$。

区块链状态序列马尔可夫链是满足下面两个假设的一种随机过程。

假设 1 区块链在第 i 个记账周期结束时刻的状态的概率分布只与在第 $i-1$ 个记账周期结束时刻的状态有关，与第 $i-1$ 个记账周期结束时刻以前的状态无关。

假设 2 区块链从第 i 个记账周期结束时刻的状态 s_i 到第 $i+1$ 个记账周期结束时刻的状态 s_{i+1}，这个状态转移与 i 的值无关。

区块链状态序列马尔可夫链模型可表示为 $BC\_MerkovChain = \langle S, \boldsymbol{P}, Q\rangle$，其中各元的含义如下：

S 是区块链系统所有可能的状态所组成的非空的状态集，也称之为系统的状态空间，它可以是有限的、可列的集合或任意非空集。本文中假定 S 是可数集（即有限或可列），用 s_i 来表示状态。

$\boldsymbol{P}$ 是系统的状态转移概率矩阵，记作 $\boldsymbol{P} = \{p_{i,j} \mid i \in I, j \in I\}$，其中 $p_{i,j}$ 表示系统从第 i 个记账周期结束时刻的状态 s_i 到第 j 个记账周期结束时刻的状态 s_j 的转移概率。

Q 是系统的初始概率分布，q_i 是系统在第 0 个记账周期结束时刻处于状态 s_i 的概率。由于区块链系统在第 0 个记账周期结束时刻只可能有一个创世块，故 $q_0 = 1$，$\forall i \neq 0 \wedge i \in I$，$q_i = 0$。

下面分析节点在同步系统账本时的情形。

若某诚实节点在第 i 个记账周期内产生一个区块 B_i，把交易数据 M'_i 封装在新区块 B_i 中广播给所有相邻节点进行验证，验证通过后接入主链。其他节点在同步时，发现当前系统的账本比自己保存的账本副本多出一个区块，会用最新的系统账本替换自己的账本副本，即自己存储的区块链的状态进行更新（由 s_{i-1} 更新为 s_i）。此时 $p(s_{i-1} \rightarrow s_i) = p_{i-1,i} = p(B_i)$，$p(B_i)$ 是区块 B_i 通过验证的概率，$p(B_i) \in [0,1]$。

若某恶意节点在第 i 个记账周期内产生一个区块 B_i，把篡改后的交易数据 $M'_{i-1}*$ 封装在 B_i 中，此时若广播区块 B_i，无法通过其他节点的验证。为了实施篡改企图，该恶意节点必须至少连续获得第 $i+1$ 个记账周期和第 $i+2$ 个记账周期的记账权，此时主链产生攻击链分支。其他节点在同步时，发现当前系统的账本比自己保存的账本副本多出多个区块，在对自己存储的区块链的状态更新时需由 s_{i-1} 更新为 s_{i+2}。由马尔科夫链的性质可知，状态 s_{i+2} 与状态 s_{i+1} 有关，而与状态 s_{i-1} 无关，即 $p(s_{i-1} \rightarrow s_{i+2}) = 0$，$p_{i-1,i+1} = 0$，此时诚实节点会发现恶意节点的篡改攻击行为，导致篡改攻击被识破，即篡改失败。

4 结 论

医疗临床数据的可靠共享机制对提升智慧医疗水平具有重要意义，防篡改机制可为医疗临床数据交互与共享提供保障。本文对基于区块链技术的医疗临床数据共享防篡改机制，从数据结构、传输机制、共识机制 3 个层面进行了分析，帮助研究者解决医疗临床数据共享安全方面的问题。另外，本文还通过从篡改攻击发生的时间维度模拟了可能发生的攻击场景，并对篡改攻击难度及成功概率进行了理论分析。通过分析可知，诚实节点在同步区块链时，若利用区块链状态序列马尔科夫链的性质，可以发现恶意节点的篡改攻击行为。本文研究内容对提升医疗临床数据共享安全性以及智慧医疗水平均具有较高的应用价值。

参考文献

[1] 糜泽花，钱爱兵. 智慧医疗发展现状及趋势研究文献综述[J]. 中国全科医学，2019，22(3)：366-370

[2] 徐玲玲,徐婷婷. “互联网+”背景下智慧医疗应用现状研究[J]. 智能计算机与应用,2020,10(1):207-210

[3] Singh K, Batten L. Aggregating privatized medical data for secure querying applications[J]. *Future Generation Computer Systems*, 2017 ,7(72):250-263

[4] Jabeen F, Hamid Z, Wadood A, et al. Enhanced architecture for privacy preserving data integration in a medical research environment[J]. *IEEE Access*, 2017,29(9): 308- 326

[5] Al Hamid H A, Rahman S M M, Hossain M S, et al. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography[J]. *IEEE Access*, 2017, 29(12): 313-328

[6] Arshad H, Rasoolzadegan A. Design of a secure authentication and key agreement scheme preserving user privacy usable in telecare medicine information systems[J]. *Journal of Medical Systems*, 2016, 40(11): 237

[7] Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy[J]. *Journal of Big Data*, 2018, 5(1): 1-5

[8] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. http://www.btcpapers.com/bitcoin.pdf: Bitcoin, 2008

[9] 闵新平,李庆忠,孔兰菊,等. 许可链多中心动态共识机制[J]. 计算机学报, 2018,41(5):1005-1020

[10] 高峰,毛洪亮,吴震,等. 轻量级比特币交易溯源机制[J]. 计算机学报,2018,41(5):989-1004

[11] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J]. 计算机学报,2018,41(5):969-988

[12] 任彦冰,李兴华,刘海,等. 基于区块链的分布式物联网信任管理方法研究[J]. 计算机研究与发展,2018,55(7):1462-1478

[13] Yin W, Wen Q Y, Li W M, et al. An anti-quantum transaction authentication approach in blockchain[J]. *IEEE Access*, 2018,30(5):393-401

[14] Kosba A, Miller A. The blockchain model of cryptography and privacy-preserving smart contracts[J]. *Security and Privacy*, 2018,10(26): 839-858

Research on tamper-proof mechanism and tampering attacks of medical clinical data based on block chain

Li Xiaoming*, Huang Hui*, Ying Yi*, Zeng Yue**

(*School of Computer Science and Engineering, Sanjiang University, Nanjing 210012)

(**School of Software Engineering, Jinling Institute of Technology, Nanjing 210012)

Abstract

The reliable sharing mechanism of medical clinical data is of great significance to improve the level of intelligent medical treatment, and tamper-proof mechanism can provide guarantee for the interaction and sharing of medical clinical data. In this paper, the tamper-proof mechanism of the medical clinical data based on block chain system is analyzed , two scenarios are designed to analyze the implementation of tamper attack and the probability of success, the tamper attack is modeled and analyzed based on Markov chain. The research content of this paper has a good application value for improving the security of medical clinical data sharing and the level of intelligent medical treatment.

Key words: block chain, intelligent medical treatment, tamper-proof mechanism, tampering attack, Markov chain