基于区块链的铁路工程施工安全监测数据共享关键技术研究

刘玉红[1,2]，杨亮[1]，朴春慧[1,2]，张志国[3]

（1.石家庄铁道大学信息科学与技术学院，河北 石家庄 050043 ；2.河北省电磁环境效应与信息处理重点实验室，河北 石家庄 050043；
3.石家庄铁道大学土木工程学院，河北 石家庄 050043）

摘 要：为了解决铁路工程施工安全监测过程中监测数据易被篡改、事故追责时数据真实性可能遭到质疑的问题，提出了一种基于区块链的铁路工程施工安全监测数据共享模型，利用智能合约自动执行的特点保证监测数据上链过程的透明性。针对实用拜占庭容错（PBFT）算法中拜占庭节点与正常节点被选为主节点概率相同的问题，提出了基于信誉积分的实用拜占庭容错算法；针对流式数据上链可能产生网络拥塞的问题，简化了一致性协议，将协议的时间复杂度由 $O(n^2)$降为 $O(n)$。利用 Hyperledger Caliper 进行了对比实验，证明改进算法的时延低于 PBFT 算法，吞吐量高于 PBFT 算法；进行攻击可能性和攻击成功概率的量化分析，确定智能合约为链上监测数据提供了防篡改性。对比分析结果证明，所提基于区块链的铁路工程施工安全监测数据共享模型在共识效率、吞吐量和区块生成速度方面优于其他模型。

关键词：铁路工程施工；区块链；基于信誉积分的实用拜占庭容错；智能合约；安全共享

中图分类号：TP311

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021076

Research on key technologies of safety monitoring data sharing for railway engineering construction based on blockchain

LIU Yuhong[1,2], YANG Liang[1], PIAO Chunhui[1,2], ZHANG Zhiguo[3]

1. School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang 050043, China
2. Laboratory for Electromagnetic Environmental Effects and Information Processing, Shijiazhuang 050043, China
3. School of Civil Engineering, Shijiazhuang Tiedao University, Shijiazhuang 050043, China

Abstract: In order to solve the problems that the monitoring data was easy to be tampered with in the process of railway engineering construction safety monitoring, and the authenticity of the data might be questioned during the accountability of accidents, a blockchain-based railway engineering construction safety monitoring data sharing model was proposed. The characteristics of automatic execution of smart contracts ensured the transparency of the process of monitoring data on the chain. In the PBFT algorithm, there was a problem that the Byzantine nodes and the normal nodes were selected as the master node with the same probability, a reputation-based practical Byzantine fault tolerance algorithm was proposed. Streaming data on the chain might cause network congestion, which simplified the consensus protocol and reduced the time complexity from $O(n^2)$ to $O(n)$. A comparative experiment was conducted using Hyperledger Caliper to prove that the delay of the improved algorithm is lower than PBFT algorithm, and the throughput is higher than PBFT algorithm. A quantitative analysis of the possibility of attack and the probability of successful attack was carried out, and it was determined that the smart contract provides tamper-proof modification for the monitoring data on the chain. Comparative analysis proves that the proposed blockchain-based railway engineering construction safety monitoring data sharing model is good than other models in terms of consensus efficiency, TPS and block generation speed.

Keywords: railway engineering construction, blockchain, RPBFT, smart contract, safe sharing

收稿日期：2021−01−14；**修回日期：**2021−03−08

通信作者：朴春慧，pchls2011@126.com

基金项目：河北省教育厅在读研究生创新能力培养基金资助项目（No.CXZZSS2020073）

Foundation Item: Graduate Innovation Foundation of Hebei Province (No.CXZZSS2020073)

1　引言

在铁路工程施工过程中，大量带有感知功能的物联网设备被部署到施工项目内的不同结构物上，这些设备产生的数据具有多源异构、规模庞大、时空关联、冗余度高、多维标量等特征[1]。这些数据经过整合、共享，可实现铁路建设过程安全管理和事故后的责任追溯等。但由于传统的信息化平台采用了中心式的云存储方式，该方式使数据脱离了施工参与方的物理控制，无法保证数据的安全性，存在篡改风险，使铁路施工各参与方无法对中心式存储下的监测数据达成共识，且在该模式下无法确保共享过程中数据的有效性以及在不同系统传输过程中数据的一致性[2-4]。

区块链技术起源于文献[5]，是一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记账技术，也称为分布式账本技术，它构建了数据安全保护机制，实现数据所有权与使用权的分离，按智能合约进行数据存储与查询[6-7]。在铁路建设领域内，有学者结合区块链进行研究，如代明睿[8]研究了基于区块链的铁路数据汇集共享过程中的关键技术，分析了铁路数据汇集共享体系架构的安全特性，提出了基于区块链的铁路数据汇集共享体系架构。在铁路建设方面的区块链技术的应用也有一些实际案例，如 2020 年，区块链技术应用于雄安新区工程质量监督管理[9]。综上所述，将区块链应用于铁路工程建设中，已有一些理论研究与实际应用。

基于上述背景，针对铁路工程施工中监测数据的安全问题以及保证监测数据真实性，本文提出一种基于区块链的铁路工程施工安全监测数据共享模型，主要贡献如下。

1) 提出一种基于区块链的铁路工程施工安全监测数据共享模型，利用智能合约自动执行的特点保证监测数据上链过程的透明性，使业主单位、施工单位和监管单位认可链上数据的真实性。采用区块链存储监测数据的关键索引信息、数据中心存储原始监测数据的方式实现监测数据的存储。

2) 设计了监测数据存储与查询智能合约，使施工单位通过智能合约将监测数据的特征值、异常数据等上链存储，监管单位和业主单位通过查询智能合约查看链上数据。

3) 针对铁路施工过程中监测数据的流式特征导致的数据上链过程中产生的网络拥塞问题，提出了一种基于信誉积分的实用拜占庭容错（RPBFT, reputation-based practical Byzantine fault tolerance）算法。通过简化一致性协议的方式，将协议的时间复杂度由 $O(n^2)$降为 $O(n)$；通过加入基于节点行为的奖励机制，降低拜占庭节点作为主节点的概率。

4) 通过攻击可能性和攻击成功概率的量化分析，表明智能合约技术为链上监测数据提供了防篡改性。利用 Hyperledger Caliper 进行对比实验，证明 RPBFT 算法在共识过程中的时延较 PBFT 算法降低约 30%，吞吐量提升约 170%。与同类问题的对比分析表明，本文模型在共识效率与共享速度方面优势明显。

2　基于区块链的铁路工程施工安全监测数据共享模型

区块链按照中心化程度可以分为公有链、联盟链和私有链。公有链由所有参与成员维护，具有完全去中心化的特点；联盟链由一些机构发起，只允许该机构组织内部成员参加，具有部分中心化的特点；私有链的写入权限只受一个实体组织控制，为了追求性能已渐渐演变成中心化的模式[10]。考虑到铁路工程施工中的监测数据共享区块链参与节点是多个参建实体或其他机构组成的组织或联盟，并未面向大众完全公开，且加入区块链的参与者需要经过主管部门的审核，故联盟链是最佳选择。

基于区块链的铁路工程施工安全监测数据共享模型如图 1 所示，模型中区块链节点主要分为业主单位、施工单位和监管单位。

业主单位。业主单位是铁路工程施工的投资主体，是铁路工程施工的发起者，也是施工过程的管理者。

施工单位。在铁路工程施工过程中施工单位广义上包括现场负责施工的单位、监测单位等与铁路建设相关的单位，本文将上述单位统称为施工单位。施工单位是铁路项目的总承包单位，也是铁路项目施工过程的主要负责单位。施工单位负责在项目中的结构体不同部位安装多种物联网感知设备，物联网感知设备的数量根据结构体类型、体积等的不同而变化。

监管单位。监管单位包括负责铁路施工项目建设监管等工作的监理单位、地区铁路监督管理局以及铁路行业信息化工作的主管部门。本文提出的监测数据共享联盟链是由监管单位负责发起与维护的；当铁路

项目施工过程中出现安全事故时，监管单位根据该项目施工监测数据进行责任追溯。

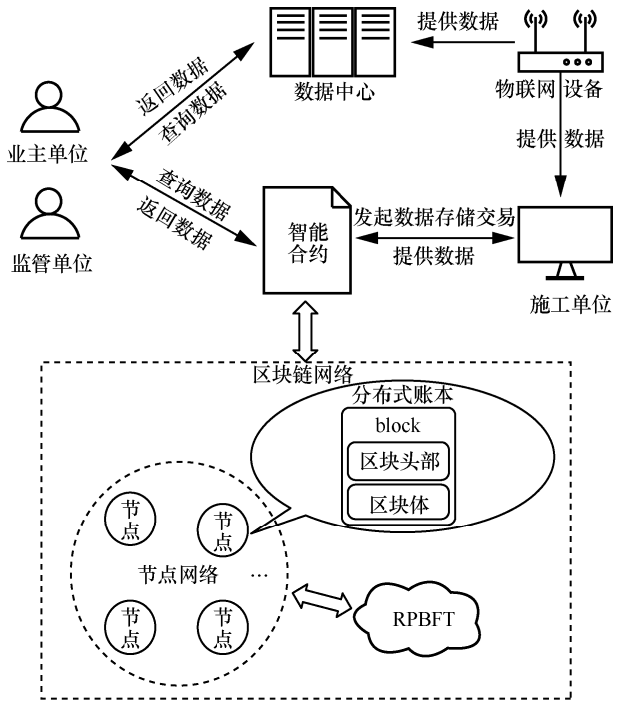


图 1 基于区块链的铁路工程施工安全监测数据共享模型

模型结构主要包括智能合约、区块链网络、数据中心和物联网设备。

智能合约保存在区块链上，链内各节点可以查看并执行智能合约指令，还可以查看节点与智能合约交互日志[11]。通过智能合约，施工单位可以将数据存储在去中心化的区块链网络中，监管单位和业主单位可以监测数据进行查询。

区块链网络主要包括节点网络和共识机制，在节点网络中的节点维护自己的分布式账本。节点网络主要包括共识节点和验证节点，共识节点负责验证数据存储或查询交易并执行共识算法，还在自身分布式账本中记录存储的数据；验证节点负责验证数据存储或查询交易。

数据中心用于存储铁路施工现场传输的原始监测数据，对监测数据进行转换、处理、特征提取等操作，最后将特征值、异常值等构成的监测数据索引与摘要传输给监管单位。

物联网设备指铁路施工现场的监测数据收集与传输设备，由于传感器本身不具备数据的远程传输能力，因此需要借助数据传输单元（DTU, data transfer unit）进行数据的远程传输。

监测数据存储流程如图 2 所示。在铁路施工现场，物联网设备监测到数据后传输至 DTU，DTU 通过运营商网络将监测数据以二进制流的形式分别传输至数据中心和施工单位。1) 监测数据传输至数据中心后，由于监测数据是实时采集的，存在噪声、异常值和缺失值等问题，因此需要在数据中心进行数据处理；处理完成后将监测数据存储至数据中心。2) 监测数据传输至施工单位后，在施工单位的信息化平台使用与数据中心相同的方法对监测数据进行处理，由于区块链的链上状态数据库不适合存储大量数据，故需生成监测数据的索引与摘要，其中包括了监测数据的特征值、异常值等信息；然后通过智能合约将数据索引与摘要存储至区块链平台。施工单位出于成本考虑，不会在本地服务器中存储大量监测数据，因此当上传数据完成后，便将数据删除，继续接收下一阶段监测数据。

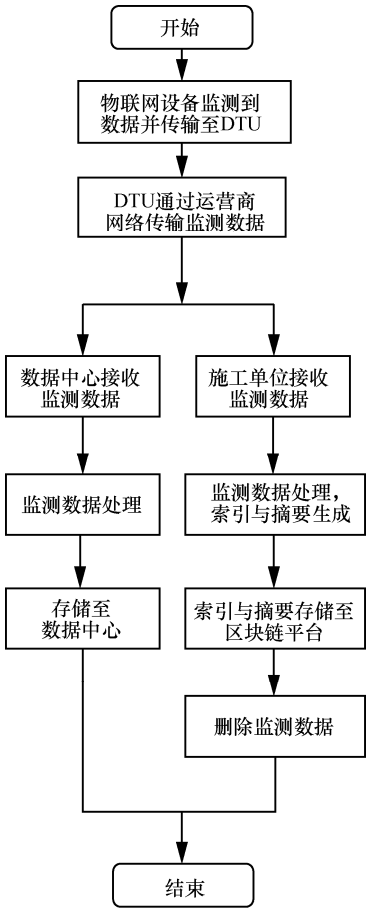


图 2 监测数据存储流程

监测数据查询流程如图 3 所示。当铁路项目在施工过程中出现安全事故时，监管单位可以使用存储于数据中心的监测数据作为责任追溯的依据之一。但由于数据中心数据存在被篡改的风险，因此

需要与区块链中的监测数据进行验证，确定监测数据的真实性。当监管单位提出查询请求时，判断查询请求是否需要调取区块链中的数据。1) 当请求消息发送至数据中心时，数据中心根据请求信息中的项目编号提取相应监测数据传输至监管单位；2) 当请求消息发送至区块链时，智能合约根据请求信息中的项目编号将相应的监测数据索引提取并发送给监管单位。

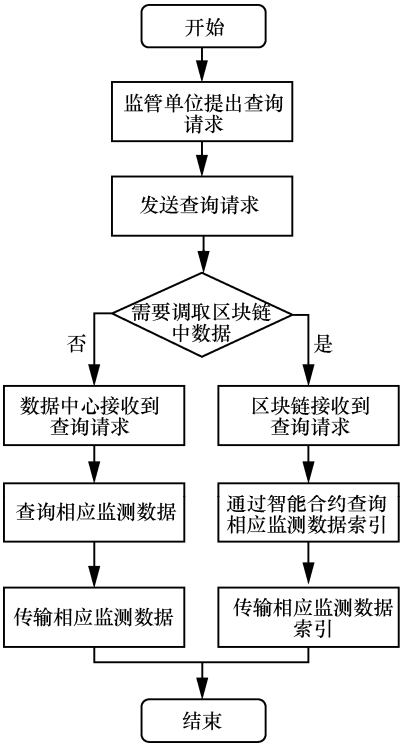


图 3　监测数据查询流程

3　相关合约设计

在本文方案中，参与方将通过联盟区块链的远程过程调用（RPC, remote procedure call）接口实现监测数据索引的存储与查询。据此本文设计了监测数据存储合约和监测数据查询合约。

3.1　监测数据存储合约

监测数据存储合约用于将原始监测数据索引存储到区块链中。当上传原始监测数据索引时，通过区块链向外部提供的 RPC 接口发送索引相关数据；监测数据存储合约监测到有数据传输时，先对传输的数据进行检查，通过后其方可进入联盟链中，作为新区块的区块体，并进行下一步的共识过程。监测数据存储合约设计如算法 1 所示。

算法 1　监测数据存储合约

输入　监测数据索引 MD

输出　存储成功 Req

1) while MD.senderid is exist &&Check (MD.sign==true) //判断上传监测数据索引的用户是否存在

2)　*a*←HASH(MD)

3)　moni.update(‘TIME’: Datatime.now())

4)　moni.update(‘MONIDATASI’: MD)

5)　moni.update(‘HASH’: *a*)

6)　moni.update(‘SIGN’: MD.sign)

7)　Req←Request(‘STORAGE’: moni)

8) end while

9) return Req

3.2　监测数据查询合约

监测数据查询合约为区块链参与方提供查询存储在联盟链的监测数据索引功能。当参与方向联盟链提出查询请求时，区块链系统构造查询请求信息 *R*，如式(1)所示；将 *R* 发送至联盟链节点，等待查询结果。被查询的监测数据索引会被参与方的公钥加密，加密后的结果返回给参与方，参与方使用自己的私钥解密即可得到真实监测数据索引。

$$R=\{\text{TYPE="SHARE",proid,Pub}(\text{key})\} \tag{1}$$

其中，SHARE 表示该命令的请求类型为查询请求，proid 是全局不会重复的项目编号，Pub(key)是参与方的公钥。为了提升查询效率，本文方案的监管方所处的节点会维护一张哈希表 LIST，LIST 用来记录监测数据索引在联盟链中的位置，LIST 的结构如式(2)所示。

$$\text{LIST=\{KEY:proid,VLAUE:(TimeStamp,Blockid)\}} \tag{2}$$

其中，proid 是全局不会重复的项目编号，TimeStamp 是项目编号所对应项目的最新监测数据索引上传时间，Blockid 是项目编号所对应项目的监测数据索引所处区块编号。监测数据查询合约设计如算法 2 所示。

算法 2　监测数据查询合约

输入　查询请求 *R*

输出　查询结果 result

1) while *R*.proid is exist //判断查询的项目是否存在

2)　value←LIST(*R*.proid)

3)　if value!=NULL //判断查询的项目中是否有监测数据

4)　monitordata←Request(“SHARE”, *R*.proid, value.Blockid)

5) result←Encryption(monitordata)
6) else
7) return NULL
8) end if
9) end while
10) return result

4 PBFT 算法的改进

共识机制是区块链的核心技术，它确定新区块是否经过验证以及谁保留记录，影响着整个系统的安全性和可靠性[12]。本文方案采用联盟链，因此选择 Hyperledger Fabric 作为区块链底层框架，该框架采用了 PBFT 算法作为共识算法，但 PBFT 算法存在以下问题。

1) 主节点选择问题。PBFT 算法的各节点成为主节点的概率是相同的，它们轮流成为主节点，承担出块任务。按照上述方式来选择主节点，会让一些性能较低或共识过程中表现较差的节点成为主节点，这样会影响系统中的出块效率，降低系统性能。

2) 通信量问题。在 PBFT 算法的一致性协议准备阶段和提交阶段，每个从节点都会向所有节点广播信息，使共识过程的通信量达到 $O(n^2)$。造成节点通信次数随节点数量增加而呈指数级增长，进而导致共识效率下降，严重影响了系统扩展性。

针对上述问题，文献[13]在共识策略方面改进了 PBFT 算法，通过划分节点簇的方式保证算法的协调性和安全性。文献[14]在节点选择方面改进了 PBFT 算法，根据节点职责划分多个节点集合，使其适用于节点数量不停变化的动态区块链网络中。文献[15]在方法创新方面改进了 PBFT 算法，利用 K-medoids 对节点进行聚类和层次划分，使其适用于较大规模共识节点参与的共识过程。文献[16]在区块结构方面改进了 PBFT 算法，通过设计多主节点的方式，一定程度上降低了恶意节点作为主节点时的高时延问题。上述文献从不同角度对 PBFT 算法进行了改进，以期降低算法复杂度和通信量，提高共识效率，但其针对的数据类型均属于静态数据，对于铁路施工项目安全监测中的流式数据并不适用，且在改进算法时均插入了节点选择算法，在一定程度上增加了算法的复杂度，存在降低共识效率的潜在风险。

因此，本文结合铁路工程施工安全监测数据共享应用场景，提出了 RPBFT 算法，该算法从以下两方面对 PBFT 算法进行了改进。

1) 加入了基于节点行为的奖励机制，奖励或惩罚将通过节点得分体现，RPBFT 根据得分来选择更加值得信任的节点作为主节点和共识节点，以达到提升算法效率的目的。

2) 由于联盟链中大部分节点都是诚实节点，因此在不存在拜占庭节点的情况下通过简化 PBFT 一致性协议，以达到降低节点间的通信量，减少系统开销，减轻带宽压力的目的。

4.1 基于节点行为的奖励机制

1) 节点信誉分数计算

在初始阶段，各个节点的信誉分数设置为 100，分数根据节点在共识过程中的行为改变，每完成一轮共识，各个节点的分数将根据该节点在此轮共识中的表现进行加分或减分。成功参与本轮共识的节点加分；在本轮共识中作恶或者失效的节点减分。对节点行为惩罚严重程度上，方案允许节点偶发失效，即当节点失效时，减分较少；但对节点作恶的行为绝对不允许，若节点作恶则进行严厉惩罚，扣除该节点大部分分数，使其短时间内难以参与共识过程，杜绝其连续作恶情况发生。本文方案对奖惩的相关系数按照 2 的指数级别设置，分数的计算如式(3)所示。

$$\mathrm{Score}_i = \mathrm{Score}_{i-1} + 2S_i - 2^3 F_i - 2^6 E_i, i = 1,2,3\cdots \quad (3)$$

其中，Score 表示节点当前的分数；S 表示节点是否成功参与本轮共识，若成功参与，则 S=1，否则 S=0；F 表示节点在本轮共识中是否出现失效情况，若出现，则 F=1，否则 F=0；E 表示节点在本轮共识中是否出现作恶情况，若出现，则 E=1，否则 E=0。

2) 基于信誉分数的主节点和共识节点选取方案

主节点选取。本文方案的主节点选取方式采用基于信誉分数的选取方式，选取分数最高的节点为主节点，当主节点失效或作恶时，根据视图变更协议选择分数排名第二的节点作为主节点，并开始新一轮共识。

共识节点选取。本文选择的区块链类型为联盟链，参与其中的节点已经通过了身份验证，有力保证了节点的诚实性。使用分数的多少作为节点可靠性排名的依据，进一步确保了节点的可靠性。因此为提升共识效率，本文方案选取部分分数较高的节点作为共识节点，其他节点在共识结束后同步共识结果。

4.2　完整一致性协议分析与简化设计

PBFT 算法要求所有节点处于同一种状态下和行为一致性。达到此目的的方式是运行 3 类基本协议：一致性协议、视图更换协议和检查点协议。一致性协议通过预准备、准备、确认 3 个阶段保证区块链内全部节点的数据一致性；在共识过程中主节点出现失效或作恶情况时，会触发视图更换协议，选择另一节点作为主节点；检查点协议将系统中的服务器同步到某一个相同状态，系统设置了 checkpoint 时间点，定期处理系统内日志，节约网络资源并纠正服务器状态[17]。

1) 完整一致性协议分析

完整一致性协议定义了主节点和共识节点 2 种节点，在每一轮共识过程中，主节点只有一个，共识节点有多个。主节点负责验证一段时间内区块链系统接收到准备上链的数据，验证通过后主节点将这些数据打包进区块并发起共识。完成一次完整的一致性协议需要 3 个阶段，其执行过程如图 4 所示。

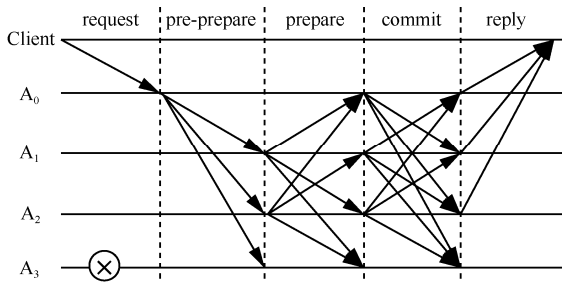


图 4　完整一致性协议执行过程

图 4 中 Client 表示客户端，A_0 是主节点，A_1 和 A_2 是诚实节点，A_3 是拜占庭节点，具体运行过程如下。

预准备阶段（pre-prepare）。主节点将客户端发来的请求生成预准备消息，将其广播给所有共识节点。消息格式为<PRE-PREPARE,*v*,*n*,*d*,*m*>，其中，*v* 是视图编号，*n* 是消息编号，*d* 是对 *m* 进行哈希运算后的结果，*m* 是客户端发来的消息。

准备阶段（prepare）。共识节点收到预准备消息后，生成准备消息并广播，预准备消息和准备消息被同时写入自身日志文件，消息格式为<PREPARE, *v*, *n*, *d*, *i* >，其中 *i* 是节点编号。节点收到其他节点的准备消息后，验证消息的真实性，将收到消息的 *n*, *v*, *m* 和自己日志中准备消息对应字段进行比较，若超过 *f*+1 个准备消息的比较结果是正确的则进入确认阶段。本文将此阶段中共识节点接收预准备消息、发送准备消息、接收并验证其他节点的准备消息称为共识节点在准备阶段的“接收−发送−接收”验证过程。

确认阶段（commit）。所有共识节点生成确认消息，并广播到网络中的其他节点，消息格式为<COMMIT, *v*, *n*, *d*, *i* >。此阶段验证步骤与准备阶段相同，当超过 *f*+1 个节点的确认消息验证成功后，此轮共识过程方可成功。

2) 简化一致性协议设计

在 PBFT 一致性协议运行过程中，完成了两次复杂度为 $O(n^2)$的通信步骤，这是为了解决网络中存在的拜占庭将军问题，使区块链网络中各个节点能够达成共识。RPBFT 中简化一致性协议将完整一致性协议的准备阶段进行转换，把共识节点“接收−发送−接收”的验证过程转移至主节点，由主节点判定所有共识节点的反馈信息是否正确，不需要共识节点再做判断；另外，在选择参与共识节点过程中，选择节点数量超过全网节点数量的一半。简化一致性协议运行的前提是当前共识节点中不存在拜占庭节点，使 RPBFT 算法在完成复杂度为 $O(n)$的共识操作后，区块链网络中各个节点能够达成共识。

简化一致性协议是基于文献[18]，并结合本文研究背景提出的一种一致性协议，其运行过程如图 5 所示。

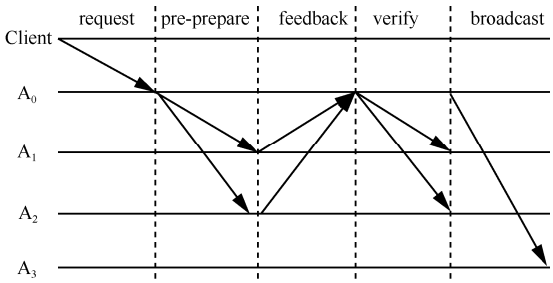


图 5　简化一致性协议运行过程

图 5 中 Client 为客户端，A_0 为主节点，A_1、A_2 为共识节点，A_3 为非共识节点，简化一致性协议具体运行过程如下。

预准备阶段（pre-prepare）。在此阶段，主节点会为打包信息分配一个序列号 *n*，然后将序列号与打包信息共同广播至全网，消息格式为<PRE-PREPARE, *v*, *n*, *m*, *d*, *w*>，其中，*v* 是视图编号，*n* 是消息编号，*m* 是客户端发来的消息摘要，*d* 是对 *m* 进行哈希运算后的结果，*w* 是节点的信誉积分信息。

反馈阶段（feedback）。主节点发送的预准备消息被共识节点接收后，共识节点验证预准备消息

中的交易信息及其信誉积分与本地积分是否相同，若认可该消息且相同，则生成反馈消息并向主节点发送；否则不发送反馈消息，反馈消息格式为<FEEDBACK, *v*, *n*, *d*, *i* >。如果主节点没有收到全部共识节点的反馈消息，则进入完整的一致性协议流程；否则进入验证阶段。此阶段从节点验证以下内容。

① 查看预准备消息的签名是否正确。

② 摘要内容与 *d* 是否一致。

③ 查看视图编号，确定消息是否来自主节点。

④ 该节点是否接收过相同视图编号 *v* 发送的相同信息编号 *n* 的消息。

⑤ 消息序号是否在一定区间中。此处设定一定区间一方面可以方便清除多余的日志信息，另一方面可以防止拜占庭主节点使用大量序列号，消耗序列号空间。

验证阶段（verify）。当主节点接收到所有共识节点的反馈消息后，会验证接收到的所有反馈消息是否相同，若全部相同则生成验证消息并广播，消息格式为<VERIFY, *v*, *n*, *d*, *a*>，其中 *a* 是确认添加的信息。共识节点接收到验证消息后将确认添加的信息保存到本地内存中，若不同，则执行完整一致性协议，至此简化一致性协议完成。

RPBFT 是为铁路施工项目安全监测数据共享联盟链设计的共识算法，在此背景下，参与联盟链的节点绝大多数都是诚实节点，因此 RPBFT 在绝大部分时间内都执行简化一致性协议，缩短了共识时间，使其能够适应铁路施工项目安全监测的流式数据上链速度。通过引入奖励机制，选择信誉分数最高的节点作为主节点，极大地降低了主节点失效或作恶的概率，保证了共识过程的稳定；选择部分节点参与共识的方法，减低了共识时间，提高了共识效率。

4.3 算法的流程

RPBFT 算法在 PBFT 算法基础上增加了基于节点行为的奖励机制，设计了以信誉分数为指标的主节点选择方案，极大地降低了选择拜占庭节点作为主节点的概率；并简化了一致性协议的运行流程，减少了节点间的通信量，节省了通信开销。RPBFT 算法的流程如图 6 所示。RPBFT 算法的具体执行过程如下。

节点初始化。使用整数 0～*N*−1 对节点进行编号（*N* 为节点总数），将各节点信誉值设为 100。随机选取一个节点作为主节点和 $N-\frac{N-1}{3}-1$ 个共识节点。

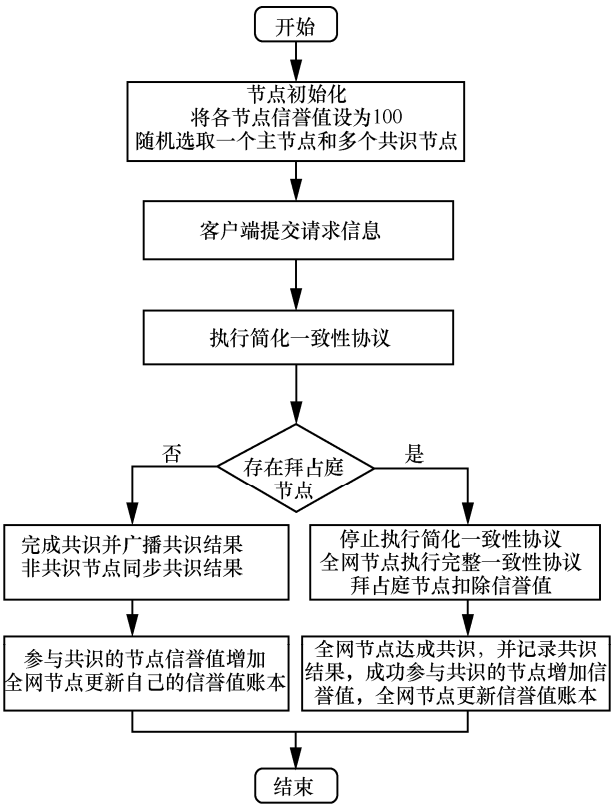


图 6 RPBFT 算法流程

客户端向主节点发送请求信息，主节点接收请求信息后，将请求消息编号，生成预准备消息，并执行简化一致性协议。

所有共识节点执行简化一致性协议，在简化一致性协议的执行过程中，对所有参与共识的节点状态进行判断，算法根据判断结果进行操作，具体如下。

1) 若判断参与共识的节点中无拜占庭节点，则主节点和共识节点会继续执行简化一致性协议，直到完成本次共识。

2) 若判断共识节点中出现拜占庭节点，则主节点终止本次简化一致性协议的运行；全网节点执行完整一致性协议，完成本次请求信息的共识过程。当完整一致性协议完成后，系统扣除拜占庭节点的信誉值，并重新选择主节点和共识节点，在下一次共识过程中继续执行简化一致性协议。

4.4 通信量对比

假设此时区块链网络中有 *n* 个节点，在 PBFT 算法的一致性协议的预准备阶段中，主节点向所有共识节点广播预准备消息，通信次数为 *n*−1 次；准备阶段中，所有共识节点分别向除自身之外的共识节点广播准备消息，通信次数为 *n*(*n*−1)次；

提交阶段中，所有共识节点分别向除自身之外的共识节点广播提交消息，通信次数为 $n(n-1)$次。由此可知，PBFT 算法的一致性协议总通信次数为 $2n^2-n-1$ 次。

在 RPBFT 算法简化一致性协议的预准备阶段中，主节点向所有共识节点广播预准备消息，通信次数为 $n-1$ 次；反馈阶段中，共识节点将反馈消息发送给主节点，通信次数为$(n-1)$次；验证阶段中，主节点将验证消息发送给所有共识节点，通信次数为$(n-1)$次。由此可知，RPBFT 算法的简化一致性协议总通信次数为 $3n-3$ 次。

可以看出，RPBFT 算法的通信次数远小于 PBFT 算法的通信次数，减少了网络带宽的消耗，提高了共识算法的效率。值得注意的是，上述通信次数的计算是建立在区块链网络中不存在拜占庭节点情况下的。当区块链网络中存在拜占庭节点时，RPBFT 算法会执行完整的一致性协议，其通信次数与 PBFT 算法一致。

5　实验结果与分析

本文使用超级账本的子项目 Caliper 对 RPBFT 算法进行实验评估。Hyperledger Caliper 是华为公司参与设计和开发的一个项目，它是一个区块链基准测试工具。为不失一般性，每次实验测试 10 次，取平均值作为测试结果。

5.1　性能测试与结果分析

1) 共识时延测试

共识时延是指从交易提起到交易结束所消耗的时间，是衡量共识算法运行速度的重要指标[17]。为了对比RPBFT算法和PBFT算法在共识时延上的差别，在固定4个共识节点和相同时间间隔的情况下，系统分别发送200条、400条、600条、800条、1 000条交易的对比实验，实验结果如图 7 所示。

图 7 中，当区块链内不存在拜占庭节点时，RPBFT 算法执行简化一致性协议，其共识时延明显低于 PBFT 算法。当交易量增加时，PBFT 算法的交易时延增长迅速，而 RPBFT 算法与之相比增速较慢，在交易量为 1 000 条时，时延降低约 30%。因此，当交易量增多时，RPBFT 算法的优势更为明显，时延更低。

2) 吞吐量测试

吞吐量（TPS, transaction per second）是单位时间内打包的交易数量，是反映共识算法性能的关键指标[13]。为了对比RPBFT算法和PBFT算法在TPS上的差别，本文进行如下实验：固定4个共识节点情况下，相同时间间隔内分别发送1 000条、1 500条、2 000条、2 500条、3 000条交易量，实验结果如图 8 所示。

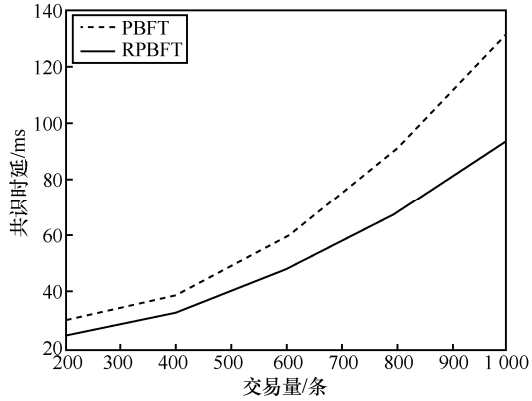


图 7　相同节点数量，不同交易量下共识时延的对比

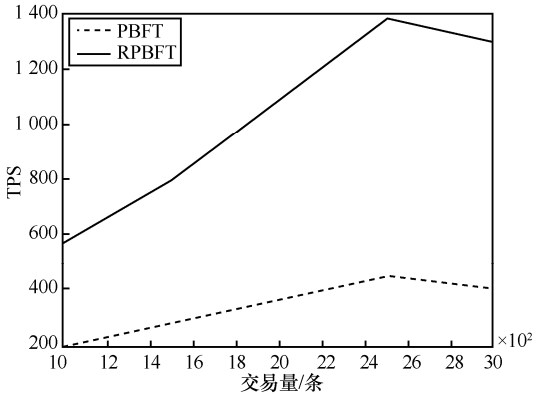


图 8　相同节点数量，不同交易量下 TPS 的对比

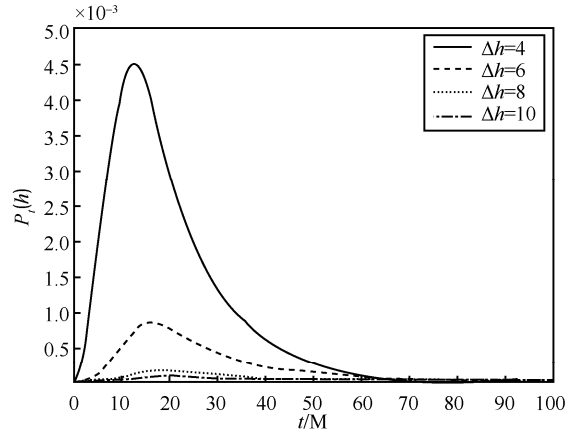
图 8 中，当区块链内不存在拜占庭节点时，RPBFT 算法会执行简化一致性协议，其 TPS 明显大于 PBFT 算法，在交易量为 2 500 条时，RPBFT 的 TPS 较 PBFT 增长了约 250%。当交易量过大，超出系统处理能力时会造成线程堵塞，使 TPS 呈现下降态势，但从整体上看，RPBFT 算法的 TPS 仍旧高于 PBFT 算法。

5.2　安全性分析

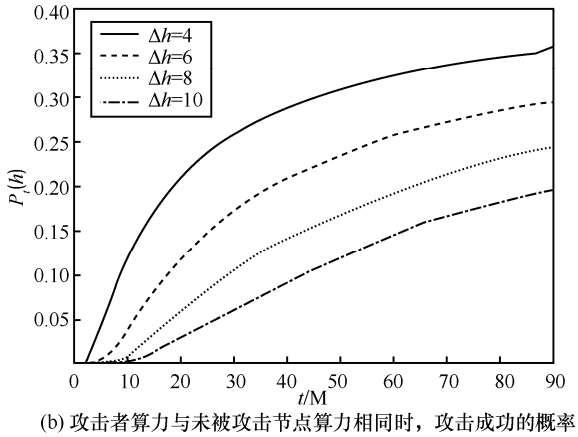
在本文提出模型中，施工单位通过上传监测数据至区块链的行为，将监测数据访问控制权和数据安全性托付给了区块链。在本文模型中施工单位可能成为攻击者，攻击目的是逃避事故后的责任追究，因此攻击者想要成功逃避责任则必须篡改链上数据。本节根据参考文献[19-20]中攻击可能性和攻击成功概率的量化分析方法，对本文模型进行分析。攻击者攻击成功的概率函数表示为

$$P_t(h)=\sum_{n=0}^{\frac{t-1-\Delta h}{2}}\sum_{j=0}^{t-2n-\Delta h-1}\frac{t!P_1^nP_2^{n+\Delta h+1+j}P_3^{t-2n-\Delta h-1-j}}{n!(n+\Delta h+1+j)!(t-2n-\Delta h-1-j)!} \tag{4}$$

其中，Δh 为攻击者想攻击的区块与最新区块的高度差。为了比较高度差不同时的攻击成功概率，本节实验对比了 Δh 分别为 4、6、8、10 的 $P_t(h)$，如图 9 所示。图 9 中横坐标的单位 M 表示未被攻击节点生成一个区块的平均时间。



(a) 攻击者算力为未被攻击节点算力50%时，攻击成功的概率



(b) 攻击者算力与未被攻击节点算力相同时，攻击成功的概率

图 9 攻击成功概率对比

由图 9 可知，攻击者攻击成功的概率随着高度差 Δh 的增大而减小。当攻击者的算力小于未被攻击节点算力时，攻击者首先需要生成攻击区块与最新区块之间的 Δh 个区块，然后才可以与未被攻击的节点竞争产生新区块，攻击成功的概率先增大后减小，最终趋于 0。当攻击者的算力与未被攻击节点相同时，攻击成功的概率会逐渐变大，但变大幅度越来越小[20]。在本文场景中，攻击者攻击区块的目的往往涉及事故后的追责，此时距离区块生成时间间隔较长，区块高度差 Δh 的值至少达到 10^3 的数量级，即使攻击者算力与未被攻击节点算力相同，完成攻击的概率也是极低的。

5.3 对比分析

传统基于中心化云存储的数据共享模型不可避免地存在数据被篡改的安全问题，区块链本身的防篡改特点对能够有效避免该问题，但区块链自身数据库并不支持海量流式铁路施工项目监测数据的存储，因此需辅以其他存储手段，且铁路施工项目监测产生的流式数据对区块链的存储与共享过程中的共识算法效率要求较高。本文将共识机制、共识效率、吞吐量、区块生成速度和算力需求作为对比指标，将本文提出的模型与文献[8, 21-22]进行对比分析，结果如表 1 所示。

根据 5.1 节的实验结果可以看出，RPBFT 算法在共识效率、吞吐量和区块生成速度方面优于 PBFT 算法，且算力需求比 PBFT 低。文献[8]提出的铁路数据汇集共享系统能将铁路数据规范存储、管理和应用，但使用的 PBFT 算法存在通信量大和主节点选择随机的问题。文献[21]使用混合共识的方式解决拜占庭节点问题，导致共识过程复杂，共识效率和吞吐量较低，区块生成速度缓慢，且节点中同时运行 2 种共识算法，对算力的需求较高。文献[22]的 DPCC（disease prevention and control algorithm）是基于 DPoS（delegated proof of stake）算法的改进方案，优化了节点选举方式，共识效率相对较高，但是其每次共识时都需要选择一个出块节点导致其吞吐量有所降低；在区块生成速度方面，DPCC 继承了 DPoS 的快速出块特点[22]。由表 1 可知，本文模型与其他模

表 1 对比分析结果

研究工作	共识机制	共识效率	吞吐量	区块生成速度	算力需求
基于区块链的铁路数据汇集共享系统[8]	PBFT	低	低	慢	高
基于区块链和 DRL 的安全数据共享方案[21]	Paxos/PBFT	低	低	慢	高
双链结构的数据共享区块链模型[22]	DPCC	高	中	快	中
基于区块链的铁路工程施工安全监测数据共享模型	RPBFT	高	高	快	中

型相比，在共识效率、吞吐量和区块生成速度方面表现较优秀。

6　结束语

区块链技术的去中心化、防篡改特点为铁路工程施工安全监测数据共享中的安全问题以及保证监测数据真实性提供了新的解决思路。本文首先提出了基于区块链的铁路工程施工安全监测数据共享模型，并对该模型的框架、参与者和共享流程进行了说明；其次，通过智能合约实现了监测数据的存储与查询功能，施工单位可以通过存储合约实现监测数据的上链存储，监管单位和业主单位可以通过查询合约查询历史监测数据；然后，针对 PBFT 算法的拜占庭节点与正常节点被选为主节点概率相同以及共识过程中通信量较大的问题，结合铁路施工项目监测到的流式数据特点，提出了 RPBFT 算法，降低了通信量和拜占庭节点作为主节点的概率；最后，在 Hyperledger Caliper 中的对比实验证明，RPBFT 算法共识时延与吞吐量均优于 PBFT 算法，时间复杂度由 $O(n^2)$降为 $O(n)$；攻击可能性和攻击成功概率的量化分析结果表明，智能合约技术为链上监测数据提供了防篡改性；与其他模型的对比分析表明，本文模型在共识效率、吞吐量和区块生成速度方面表现较优秀。

参考文献：

[1] LI T, LIU Y, TIAN Y, et al. A storage solution for massive IoT data based on NoSQL[C]//2012 IEEE International Conference on Internet of Things. Piscataway: IEEE Press, 2012: 50-57.

[2] 姜顺荣. 物联网中信息共享的安全和隐私保护的研究[D]. 西安:西安电子科技大学, 2016.
JIANG S R. Research on secure and privacy-preserving of information sharing in Internet of things [D]. Xi'an: Xidian University, 2016.

[3] 杜瑞忠, 谭艾伦, 田俊峰. 基于区块链的公钥可搜索加密方案[J]. 通信学报, 2020, 41(4): 114-122.
DU R Z, TAN A L, TIAN J F. Public key searchable encryption scheme based on blockchain[J]. Journal on Communications, 2020,41(4):114-122.

[4] 马海群, 江尚谦. 我国政府数据开放的共享机制研究[J]. 图书情报研究, 2018, 11(1): 3-11.
MA H Q, JIANG S Q. The sharing mechanism of china's open government data[J]. Library and Information Studies, 2018, 11(1): 3-11.

[5] NAKAMOTO S. Bitcoin：a peer-to-peer electronic cash system [R]. 2008.

[6] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.

[7] 裴庆祺, 马得林, 张乐平. 区块链与社会治理的数字化重构[J]. 新疆师范大学学报(哲学社会科学版), 2020, 41(5): 114-122.
PEI Q Q, MA D L, ZHANG L P. Blockchain and the digital reconstruction of social governance[J]. Journal of Xinjiang Normal University (Edition of Philosophy and Social Sciences), 2020, 41(5): 114-122.

[8] 代明睿. 基于区块链技术的铁路数据汇集共享体系架构研究[J]. 铁道运输与经济, 2020, 42(11): 80-85.
DAI M R. Architecture of the railway data collection and sharing system based on blockchain[J]. Railway Transport and Economy, 2020, 42(11): 80-85.

[9] 韩梅. 雄安新区工地工程监理用上区块链[N]. 北京日报, (2020-07-17) [2021-01-04].
HAN M. Blockchain is used for construction supervision in Xiong'an New District [N]. Beijing Daily, (2020-07-17) [2020-11-28].

[10] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[11] JIANG Y N, ZHONG Y, GE X H. Smart contract-based data commodity transactions for industrial Internet of Things[J]. IEEE Access, 2019, 7: 180856-180866.

[12] 张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12.

[13] 王日宏, 邢聪颖, 徐泉清, 等. 具有监督机制的高效拜占庭容错算法[J]. 计算机工程与应用, 2020(11): 1-9.
WANG R H, XING C Y, XU Q Q, et al. Efficient Byzantine fault tolerant algorithm with supervision mechanism[J]. Computer Engineering and Applications, 2020(11): 1-9.

[14] 王海勇, 郭凯璇, 潘启青. 基于投票机制的拜占庭容错共识算法[J]. 计算机应用, 2019, 39(6): 1766-1771.
WANG H Y, GUO K X, PAN Q Q. Byzantine fault tolerance consensus algorithm based on voting mechanism[J]. Journal of Computer Applications, 2019, 39(6): 1766-1771.

[15] 陈子豪, 李强. 基于 K-medoids 的改进 PBFT 共识机制[J]. 计算机科学, 2019, 46(12): 101-107.
CHEN Z H, LI Q. Improved PBFT consensus mechanism based on K-medoids[J]. Computer Science, 2019, 46(12): 101-107.

[16] 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.
MIN X P, LI Q Z, KONG L J, et al. Permissioned blockchain dynamic consensus mechanism based multi-centers[J]. Chinese Journal of Computers, 2018, 41(5): 1005-1020.

[17] 吴晓彤, 柳平增. 基于备选投票机制的低时延 PBFT 改进研究[J]. 计算机工程, 2020(11): 1-11.
WU X T, LIU P Z. Improvement of PBFT with low delay based on alternative voting mechanism[J]. Computer Engineering, 2020(11): 1-11.

[18] 徐治理, 封化民, 刘飚. 一种基于信用的改进PBFT高效共识机制[J]. 计算机应用研究, 2019, 36(9): 2788-2791.
XU Z L, FENG H M, LIU B. Improved PBFT efficient consensus mechanism based on credit[J]. Application Research of Computers, 2019, 36(9): 2788-2791.

[19] 谭海波, 周桐, 赵赫, 等. 基于区块链的档案数据保护与共享方法[J]. 软件学报, 2019, 30(9): 2620-2635.
TAN H B, ZHOU T, ZHAO H, et al. Archival data protection and sharing method based on blockchain[J]. Journal of Software, 2019, 30(9): 2620-2635.

[20] 盛念祖, 李芳, 李晓风, 等. 基于区块链智能合约的物联网数据资产化方法[J]. 浙江大学学报(工学版), 2018, 52(11): 2150-2158.
SHENG N Z, LI F, LI X F, et al. Data capitalization method based on blockchain smart contract for Internet of Things[J]. Journal of Zhejiang University (Engineering Science), 2018, 52(11): 2150-2158.

[21] LIU C H, LIN Q X, WEN S L. Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3516-3526.

[22] 刘炜, 李阳, 田钊, 等. IDDS：一种双链结构传染病数据共享区块链模型[J]. 计算机应用研究, 2021(2): 1-6.
LIU W, LI Y, TIAN Z, et al. IDDS: double-chain structure infectious disease data sharing blockchain model[J]. Application Research of Computers, 2021(2): 1-6.

[作者简介]

刘玉红（1974− ），男，河北定州人，石家庄铁道大学副教授，主要研究方向为物联网、结构安全监测、施工监测等。

杨亮（1994− ），男，河北石家庄人，石家庄铁道大学硕士生，主要研究方向为区块链技术及应用、大数据与隐私保护、物联网与边缘计算等。

朴春慧（1964− ），女，朝鲜族，黑龙江牡丹江人，博士，石家庄铁道大学教授、硕士生导师，主要研究方向为电子政务、大数据与隐私保护、区块链技术及应用等。

张志国（1971− ），男，河北抚宁人，博士，石家庄铁道大学教授、硕士生导师，主要研究方向为桥梁设计与施工控制、结构安全监测、施工监测等。