计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.181202409

基于区块链的环境监测数据安全传输方案

周万锴[1]　龙　敏[1,2]
1 长沙理工大学计算机与通信工程学院　长沙 410114
2 长沙理工大学综合交通运输大数据智能处理湖南省重点实验室　长沙 410114
(799796288@qq.com)

摘　要　随着物联网的飞速发展,环境监测系统极大地提高了政府日常运作的效率和透明度。但是,大多数现有的环境监测系统都是以集中的方式提供服务,并且严重依赖人工控制。高度集中的系统架构容易受到外部攻击;此外,不法分子破坏数据真实性相对容易,导致公众对环境监测数据的信任度不高。针对这些问题,文中首先提出一种基于区块链的环境监测数据传输方案,监测设备获取的数据经过签名发送至数据采集终端,数据采集终端验证数据后将其写入区块链,智能合约对公众关心的数据进行实时分析并对外发布结果;其次,提出一种基于分组的PBFT共识算法,以提高系统的可扩展性。文中对方案进行了分析,结果表明,环境监测区块链保障了环境监测数据的安全性、真实性、完整性;同时结合具体案例验证了该方案的可行性。

关键词:区块链;智能合约;环境监测;密码学;实用拜占庭容错算法
中图法分类号　TP309

Secure Transmission Scheme for Environmental Monitoring Data Based on Blockchain

ZHOU Wan-kai[1] and LONG Min[1,2]
1 School of Computer and Communication Engineering,Changsha University of Science and Technology,Changsha 410114,China
2 Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation,Changsha University of Science and Technology,Changsha 410114,China

Abstract　With the rapid development of the Internet of things,environmental monitoring system has greatly improved the efficiency and transparency of government's daily operation. However,most existing environmental monitoring systems currently provide services in a centralized manner and rely heavily on human control. Highly centralized system architectures are vulnerable to external attacks. In addition,it is relatively easy for criminals to destroy the authenticity of data,resulting in the public trust in environmental monitoring data is not high. To resolve these problems,this paper proposed an environmental monitoring data transmission scheme based on blockchain. The data acquired by the monitoring device is delivered to the data collection terminal by signature,and the data collection terminal verifies the data and writes it to the blockchain. Smart contracts analyze the data in real time and then issue the results. Then,PBFT consensus algorithm based on grouping was proposed to improve the scalability of the system. This paper analyzes the scheme and the results show that the environmental monitoring blockchain can ensure the security,authenticity and integrity of environmental monitoring data and verifies the feasibility of the scheme with specific cases.

Keywords　Blockchain,Smart contract,Environmental monitoring,Cryptography,Practical Byzantine Fault Tolerance algorithm

1　引言

目前,中国环境监测产业发展迅速。在政府环保政策的指引下,我国环境监测产业逐渐从以"污染源监测"为主转变为以"环境质量监测"为主。物联网技术大大提高了环境监测的工作效率和管理效率,加快了环境监测的信息化进程。目前,中国从事环境监测业务的企业共有约200家。据预测,环境监测产业市场空间价值将超1200亿元。

无线传感器网络(Wireless Sensor Network,WSN)是环境监测网络的重要组成部分。WSN由许多微型传感器构成,能够协作实时监测、感知、采集网络分布区域内的各种环境或监测对象的信息,并对这些信息进行处理以获得详尽、准确的信息,再将这些信息传送给需要这些信息的用户[1]。

随着环境监测产业的发展,人们对环境监测数据的高效

到稿日期:2019-01-23　返修日期:2019-04-23　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61572182);湖南省自然科学基金(15JJ2007)
This work was supported by the National Natural Science Foundation of China (61572182) and Natural Science Foundation of Hunan Province (15JJ2007).
通信作者:龙敏(80951404@qq.com)

安全传输产生了担忧。无线传感器从监测环境中收集数据信息，数据随后被发送到数据中心进行存储和分析，并为环境管理、污染源控制、环境规划等提供科学依据，同时展示公众关心的环境监测数据；然而，环境监测数据对于黑客或不法分子来说是一个利润丰厚的目标。此外，环境监测数据的不安全性会降低政府的公信力，也将影响相关管理部门决策的正确性。因此，必须保证环境监测数据的安全性、真实性、完整性。

针对环境监测数据的安全性，文献[2]采用 Kolmogorov 水印技术保护 WSN 数据。该技术将 WSN 节点采集的传感数据转换为二进制矩阵后，依照 Kolmogorov 规则，同步生成水印信息，能抵抗数据攻击(如数据删除、Sybil 包复制和选择性转发攻击等)。文献[3]为了保护环境监测系统的信息安全，提出了一种撤销用户的安全机制。如果用户对系统执行非法操作，则使用带撤销机制的 CP-ABE 来撤销非法访问系统的用户。通过带时间戳的数字签名 RSA2048，在数据中添加认证功能，可以保证数据的完整性。上述两种方案都是数据中心化存储，存在破坏数据的风险，且容错能力较差，各个实体有被合谋攻击的可能。

近年，区块链技术引起了广泛的关注，其是以 Bitcoin[4] 为代表的数字加密货币体系的核心支撑技术。区块链网络提供了一个“无信任”环境，用户可以在不依赖中央信任机构的情况下进行交易。目前，区块链技术已被应用于政府[5]、医疗[6]、版权[7]、物联网[8-9]等领域。根据应用需求，可将区块链分为公共链、联盟链和私有链。公共链是完全去中心化的区块链，分布式系统的任何节点均可参与链上数据的读写、验证和共识过程；联盟链则是部分去中心化(或称多中心化)的区块链，适用于由多个实体构成的组织或联盟；私有链则是完全中心化的区块链[10]。其中，联盟链在效率和灵活性上更有优势。智能合约是构成区块链的核心要素，是由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的计算机程序，能够实现主动或被动地处理数据，接收、储存和发送价值，以及控制和管理各类链上智能资产等功能。文献[11]提出一种使用区块链技术处理 EMR 的小型分散式记录管理系统，其针对患者、医院和医学研究人员的需求，利用区块链技术来验证身份、授予权限、共享数据及保护隐私。文献[12]为后期供应链提出了一种基于区块链的产品所有权管理系统，伪造者由于不能证明在该系统上拥有真实产品，因此无法克隆真实标签。文献[13]提出一种基于区块链的智能电网数据保护系统，其利用区块链不可篡改、可追溯和集体维护的特征来解决智能电网上参与者之间的信任问题。文献[14]提出了基于联盟区块链的新型自动食品交易系统，其利用联盟区块链技术为食品交易中的不同角色设置权限和认证，以保护多利益相关者的隐私。以上研究表明，区块链技术在数据的安全传输、存储及共享等方面具有较好的应用可行性和有效性。

基于上述方案，本文提出一种环境监测数据的安全传输方案，其利用区块链去中心架构持续记录进出 WSN 节点的传输数据，以保证环境监测数据的安全性、真实性、完整性。根据每种环境监测数据的自定义阈值，通过智能合约分析 WSN 设备收集的环境监测数据来确定当前环境状况的等级。该方案可以实现环境监测数据的分类记录和安全传输，并自动确定环境等级，为专业人员提供当前环境情况的实时数据，从而进行精准、安全的环境管理。

2 环境监测区块链方案设计

本文方案采用一个联盟主导的区块链，在该区块链中，只有授权的个体才能读取区块、执行智能合约并验证新的区块。限制个体仅限于与环境监测相关的政府管理部门和监测站点。

2.1 系统组成

本文提出的环境监测区块链方案如图 1 所示。

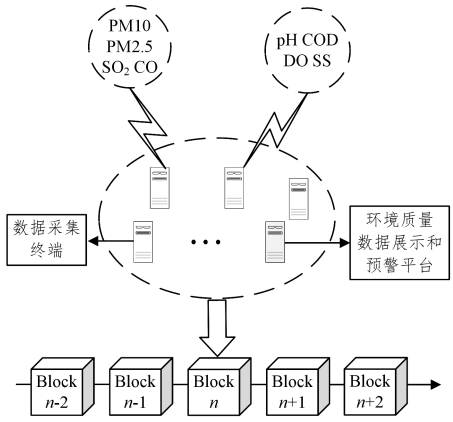


图 1 环境监测区块链方案

Fig. 1 Scheme for environmental monitoring blockchain

1)环境监测设备：不同的环境会有各式各样的监测设备，这些设备主要对大气、水、噪声环境进行监测。环境空气质量监测因子包括 PM10，PM2.5，SO_2，CO 等；污水监测因子包括 pH，COD，DO，SS 等；噪声监测因子包括噪声的强度和噪声的特征等。自动监测空气、水质、噪声的设备将监测数据通过无线网络传至数据采集终端。一组环境监测设备记为 $D=\{D_1, D_2, \cdots, D_n\}$，$D_i \in D$。

2)数据采集终端：数据采集终端将从环境监测设备中采集的数据发送到环境监测区块链上。共识算法对这些数据进行处理后，记账节点将其添加到区块链中。除此之外，数据采集终端还根据采集数据的类型创建自定义的智能合约。一组数据采集终端记为 $TN=\{TN_1, TN_2, \cdots, TN_n\}$，$TN_i \in TN$。

3)环境质量数据展示和预警平台：对于公众关心的环境质量数据，数据采集终端创建相应的智能合约并对原始数据进行分析。智能合约根据自定义阈值发布结果，当数据超过预定值时，触发智能合约发出警告通知。一组环境质量数据展示和预警平台记为 $WN=\{WN_1, WN_2, \cdots, WN_n\}$，$WN_i \in WN$。

4)区块链：各个节点上传的数据、部署的智能合约经共识算法审核后都会被写入区块链。环境监测区块链记为 EMB(Environmental Monitoring Blockchain)，区块链中各节点记为 N，$TN \subset N$，$WN \subset N$。

2.2 系统运行

2.2.1 上传数据

本文采用 BLS 短签名[15]技术来确保系统的数据传输安全。已知双线性映射 $e:G_1\times G_2=G_T$，其中 G_1，G_2，G_T 为乘法群，生成元为 P，选择 hash 函数 $h:\{0,1\}^*\rightarrow G_1^*$。监测设备随机选取 $sk\in Z_q^*$，sk 即为私钥；随机选择 $P\in G_2^*$，计算 $pk=P^{sk}$，pk 即为公钥。

对于待传输的数据 $data$，监测设备计算 $sig=h(data)^{sk}$。监测设备将 $s=data\parallel sig$ 上传至数据采集终端。数据采集终端计算 $e(sig,P)$ 和 $e(h(data),pk)$ 的值并比较其大小。如果两值相等则签名合法，否则忽略。若验证成功，则将监测数据上传至环境监测区块链。

2.2.2 区块结构

环境监测区块链的基本架构如图 2 所示，每个区块引用前一个区块头的散列并存储于链表形成区块链，区块结构包括区块头(Block header)和区块体(Block body)。

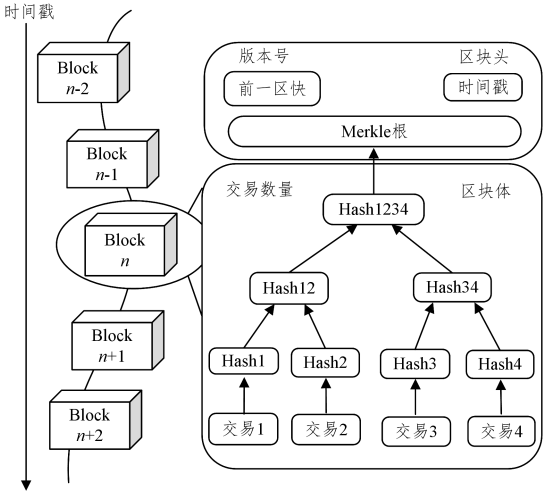


图 2 区块的结构

Fig. 2 Structure of block

区块头包含前一区块的地址(Prev-block)，其功能是把当前新的区块与前一区块相连。时间戳(Timestamp)表示此区块的创建时间，Merkle 根(Merkle-root)是由区块创建过程中的交易记录通过 Merkle 树的哈希过程生成的，区块体由交易和交易数量组成。交易包括了设备类型(DT)、监测内容(MC)、监测数据(MD)、监测时间(MT)、处理节点(BN)、处理节点签名(BN_{sig})。

2.2.3 共识算法

实用拜占庭容错(Practical Byzantine Fault Tolerance，PBFT)[16]共识机制由 Miguel 和 Barbara 于 1999 年提出，其具体步骤如下。

1)Request：客户端各节点发送服务操作请求。

2)Pre-prepare：主节点广播请求到备份节点。

3)Prepare：副本节点发送预准备消息的验证结果至主节点和其他副本节点。

4)Commit：当主节点和副本节点接收到 $2f+1$(f 为可容忍的拜占庭节点数)个一致的准备消息后，执行请求并将结果发送至客户端。

5)Reply：客户端收到 $f+1$ 个相同的回复后，判定该消息已被所有副本节点承认并执行，因此共识结束。

PBFT 算法的过程如图 3 所示。

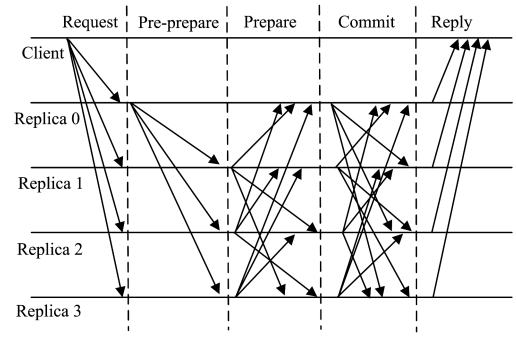


图 3 PBFT 算法的过程

Fig. 3 Process of PBFT algorithm

由图 3 可以看出，随着 PBFT 算法中共识节点数的增多，系统的通信开销大大增加。为了克服 PBFT 算法扩展性较差的缺点，本文在 PBFT 算法的基础上改进共识机制。改进的环境监测区块链采用分组实用拜占庭容错(Group Practical Byzantine Fault Tolerance，GPBFT)，具体改进如下：

1)PBFT 算法中，所有存储副本的节点担任主节点的概率均等，但恶意节点担任主节点会极大地破坏系统全网节点的共识。因此，本文根据系统当前的节点数量，将所有节点分为数量均等的 m 个小组，小组中的节点轮流担任小组的主节点，以此降低恶意主节点所造成的危害。

2)PBFT 算法通过消息广播的形式传递消息，一次完整的 PBFT 共识需要完成两次复杂度为 $O(n^2)$ 的通信过程。本文将共识节点分组，整个系统的节点只需要在小组内进行一次 PBFT 共识，一次完整的 GPBFT 共识需要完成两次复杂度为 $O(\frac{n^2}{m})$ 的通信过程，因此极大地减少了通信开销。

GPBFT 算法的过程如图 4 所示。

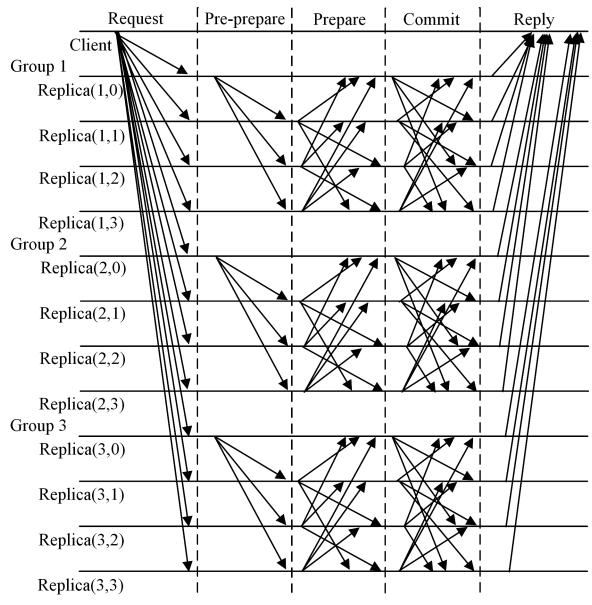


图 4 GPBFT 算法的过程

Fig. 4 Process of GPBFT algorithm

2.2.4 智能合约

所有监测设备都会有各自的智能合约，智能合约本身将为环境监测数据及其响应事件进行模块化和定制化。智能合约里有数据采集终端事先制定好的阈值，只有智能合约管理方享有上传数据的权限，通过阈值分析监测数据，然后根据分析结果发布环境状况等级，并将该等级和监测数据一起发送至环境质量数据展示和预警平台。

该合约设计如下：

```
Input:data,the object of transaction
Output:rank
1. List [ ]CustomThreshold;
2. Procedure analyze (data)
3.    if data.sender=owner then
4.    rank= CustomThreshold [data];
5.    sendTo(data,rank,WN);
6.    return rank;
7.    end if
8. end Procedure
```

智能合约处理的逻辑流程如图 5 所示。数据采集终端根据管辖监测设备所传数据进行合约制定，随后将创建好的智能合约上传至环境监测区块链。合约在部署后不能再次编辑，若要更新或替换合约，必须让原合约“死亡”并部署新的合约。因此，这种模块化结构可以很容易地替换设备的合约，而不会影响其他合约的运作。监测设备通过无线网将监测数据上传至数据采集终端，数据采集终端将数据发送到相应的智能合约。智能合约分析过后，会把结果写入环境监测区块链，同时会将结果发送至环境质量数据展示和预警平台。

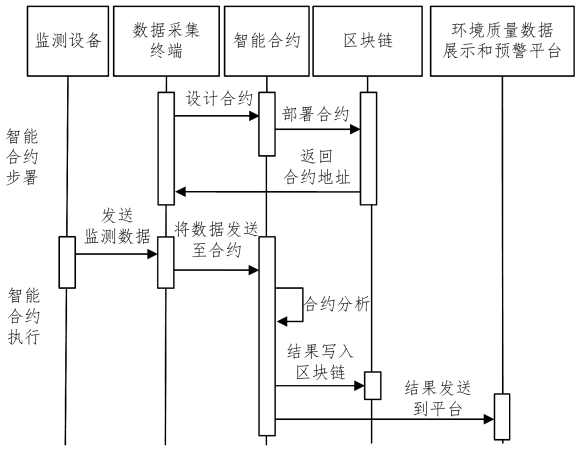


图 5 智能合约执行的逻辑流程

Fig. 5 Logical process of smart contract

3 方案分析

3.1 安全分析

本文提出的环境监测区块链方案与现有的中心化监测系统有显著的不同。下面将从 3 个方面对环境监测区块链方案进行安全分析。

1)去中心化。采用去中心化的网络架构，所有的交易信息由全部节点进行验证，并最终形成环境监测区块链。传统的中心化系统中，因系统架构过于集中而容易遭受攻击(如 DDoS 攻击、SQL 注入攻击等)。去中心化的所有节点上都存储着完整的环境监测数据，即使部分节点失效或被黑客攻击，故障节点仍可以从其他正常节点处恢复区块链数据，不会影响故障节点发布交易和验证新的区块。系统中任意节点的权利和义务都是均等的，不存在任何中心化的特殊节点和层级结构。

2)不可篡改性。一方面，在监测数据上传阶段，监测设备用 BLS 签名数据，并将签名上传至数据采集终端。如果该终端能伪造一个有效签名，则推测它有能力伪造 BLS 签名，但现已证明 BLS 签名在随机语言模型下能够抵抗伪造攻击[17]，因此数据具有不可篡改性。另一方面，方案使用的区块链为联盟链，区块链查看权限仅限于授权方，只有通过共识机制，数据才能被写入区块链。本文的区块链采用 GPBFT 共识机制，设当前共有 n 个节点，其中恶意节点 f 个，当 $n>3f+1$ 时，就可以抵挡恶意节点发起的攻击。假设每个节点都有 50%的概率成为恶意节点，若当前网络中存在 100 个节点，其中包括 50 个恶意节点，则其篡改数据的成功率仅为 $\frac{1}{2^{50}}\approx 8.9\times10^{-16}$。

3)可追溯性。共识节点会验证交易的真实性，只有通过验证的交易才会被写入区块链。在环境监测区块链中，每个区块都存有上一个区块的哈希值，可以追溯到源头。当恶意节点删除、修改一个区块的内容，不再承认原有的监测数据时，监管机构可以在区块链系统中方便地还原、追溯出所有的交易数据，因此恶意节点的行为对方案的实现不会产生影响。此外，依托区块链，监管机构对监测数据可以执行可追溯性管理和责任追究，公众可以获得环境状况等级的全部信息，这有利于建立健康的监测环境。

3.2 PBFT 性能分析

3.2.1 通信开销对比

PBFT 共识机制存在的问题就是共识过程需要大量的节点间通信。GPBFT 将整个系统进行了分组，这大大降低了系统的通信开销。在不同分组情况下，系统通信开销量的比较如图 6 所示。图中横坐标为系统节点数量，纵坐标为系统通信次数。选取 $m=1$，$m=3$，$m=8$ 进行测试，当 $m=1$ 时，系统不分组并直接运行 PBFT 算法。由图 6 可以看出，系统分组后大大降低了系统的通信开销。同时，在共识节点数相等时，分组数 m 的值越大，通信开销越小。

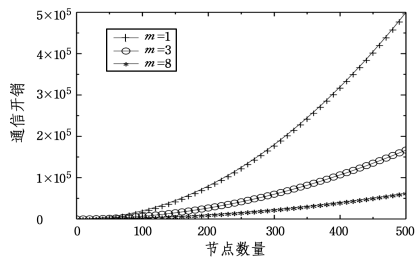


图 6 不同分组下的通信开销对比

Fig. 6 Comparison of communication overhead under different groups

3.2.2 容错能力分析

本节将分以下两种情况讨论 GPBFT 的容错能力。

1)小组主节点中没有恶意节点的情况下，存在两种可能。

①恶意节点均匀分布在每个小组中，且每组运行的恶意节点数量不超过节点总数的 1/3。此时，小组内的共识结果正确，对系统输出结果无影响，系统的容错能力为：

$$f=m\times\frac{\frac{n}{m}-1}{3} \tag{1}$$

②恶意节点集中在某几个小组中。这些恶意节点在运行 PBFT 后，根据少数服从多数的原则产生错误输出。若超过 1/3 的小组出现恶意行为，系统崩溃。此时，系统的容错能力为：

$$f=\frac{\frac{n}{m}-1}{3}\times\frac{m}{3} \tag{2}$$

2)小组主节点是恶意节点

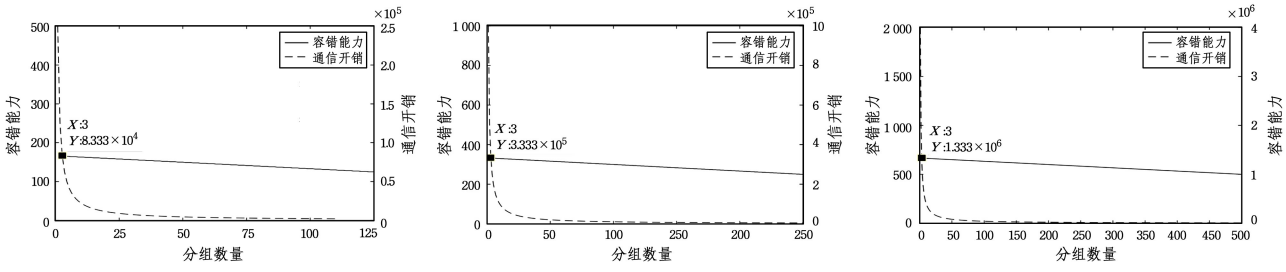
在这种情况下，恶意主节点将影响该小组中的所有节点，导致投票结果不正确。如果 1/3 以上的小组主节点出现恶意行为，则系统崩溃。系统的容错能力为：

$$f=\frac{m-1}{3} \tag{3}$$

综上，若恶意节点均匀分布，则系统容错性能不变；若恶意节点是小组主节点，则系统容错性能降低。当分组数量 m 值增大时，系统容错能力降低。为了保障系统安全性和容错性，本文提出在每一轮共识后更改小组主节点；同时，将黑名单机制添加到系统中，即一旦发现恶意节点，就将其列入黑名单中，并阻止其参与系统共识。黑名单机制可以有效地防止恶意节点的出现。

在 GPBFT 共识机制中，分组数 m 值越大，通信开销越小，系统容错能力也随之降低。因此，确定最佳 m 值尤为重要。我们将通过容错能力和通信开销来确定其最佳值。

假设恶意节点均匀分布，我们将共识节点 n 的值分别设为 500，1000，2000。图 7 给出不同节点数下，容错能力与通信开销的关系。由图 7 可见，当分组数量 $m<3$ 时，系统通信开销较大，容错能力稍强；当分组数量 $m>3$ 时，系统通信开销较小，容错能力稍弱。综上，GPBFT 共识机制分组数的最佳值为 3。



(a)共识节点 $n=500$ (b)共识节点 $n=1000$ (c)共识节点 $n=2000$

图 7 容错能力与通信开销的关系

Fig. 7 Relationship of fault tolerance and communication overhead

3.2.3 共识方案对比

此外，利用 GPBFT 共识机制可以实现区块链的一致性，且规避了 PoW 共识机制浪费资源、PoS 需要持币投票的弊端。通过参考文献[18-19]，表 1 从可扩展性、节点准入机制、电力消耗、容错率、分叉可能和吞吐量方面比较了 PoW，PoS 和 GPBFT 共识机制。

表 1 PoW，PoS 和 GPBFT 的对比

Table 1 Comparision of PoW，PoS and GPBFT

特性	PoW	PoS	GPBFT
可扩展性	好	好	良好
节点准入机制	自由进出	自由进出	授权加入
电力消耗	高	高	无
容错率/%	49	49	33
分叉可能	有	有	无
吞吐量/TPS	7(Bitcoin)	超过 300	超过 1000

4 案例分析

本节以 PM2.5 监测为例，研究环境监测区块链系统架构在 PM2.5 数据传输中的具体应用。首先，环境监测组织可借助开源联盟区块链平台，或利用 python，go 等编程语言自行建立联盟区块链。这意味着只有授权的节点才能读取区块、执行智能合同、验证新区块，这些授权节点仅包括数据采集终端、环境质量数据展示和预警平台及监管机构。在联盟区块链管理中，预先认可的节点通过分组后可参与 GPBFT 共识并验证新区块。

在每个 PM2.5 监测设备部署前，需由环境监测组织认证其身份信息。认证通过后，系统给每个设备生成一对 BLS 密钥，然后 PM2.5 监测设备方可在环境监测区块链系统上进行注册登记。PM2.5 监测设备的各个阶段(如启用、上传数据、故障、恢复上线和报废回收等)均可安全记录于区块链，随时可验。PM2.5 设备完成监测后，将待上传的监测数据(如设备类型、监测内容、监测数据、监测时间等)进行封装，随后对这些数据进行 BLS 签名。PM2.5 监测设备将签名后的数据发送至设备所在的数据采集终端。数据采集终端验证签名后再将数据上传至环境监测区块链。

PM2.5 监测设备所在的数据采集终端根据其所管辖的设备创建智能合约，智能合约通过阈值分析 PM2.5 监测数据，然后根据分析的结果发布环境状况等级，并将该等级和监测数据一起发送至环境质量数据展示和预警平台。因此，环境质量数据展示和预警平台可以为人们提供当前和历史的 PM2.5 空气质量指数及等级。

结束语 为了实现物联网环境监测系统中数据的安全传

输和记录，本文提出基于区块链的环境监测数据安全传输方案。该方案利用授权的联盟管理区块链执行智能合约，根据定义的阈值评估环境监测物联网设备收集的信息。这些智能合约将根据分析触发当前环境状况等级，并在区块链上记录有关环境监测事件响应的交易细节。本文还提出了一种基于分组的 PBFT 共识算法，减少共识达成过程中的交互次数，从而降低通信开销。因此，GPBFT 共识机制可应用于更大规模的环境监测区块链系统。文中以 PM2.5 监测为例，探讨环境监测区块链系统架构在 PM2.5 数据传输中的应用。区块链的引入大大提高了环境监测系统中数据的安全性、真实性，从而与为环境相关的科学研究、决策部署提供更可靠的信息。

参 考 文 献

[1] LI J Z, GAO H. Survey on Sensor Network Research [J]. Journal of Computer Research and Development, 2008, 45(1): 1-15.

[2] HARJITO B. Kolmogorov watermarking technique for secure the data of Wireless Sensor Networks[C]// 2017 Second International Conference on Informatics and Computing (ICIC). IEEE, 2017: 1-6.

[3] MUNSYI M, SUDARSONO A, RASYID M U H A. Secure data sensor access using attribute-based encryption for environmental monitoring[C]// 2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC). IEEE, 2017: 59-64.

[4] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org//bitcoin.pdf.

[5] JUN, MYUNGSAN. Blockchain government—a next form of infrastructure for the twenty-first century[J]. Journal of Open Innovation: Technology, Market, and Complexity, 2018, 4(1): 7.

[6] HOLBL, MARKO, KOMPARAM, et al. A Systematic Review of the Use of Blockchain in Healthcare[J]. Symmetry, 2018, 10(10): 470.

[7] ZHANG Z, ZHAO L. A Design of Digital Rights Management Mechanism Based on Blockchain Technology[C]// International Conference on Blockchain. Cham: Springer, 2018: 32-46.

[8] REYNAA, MARTIN, CRISTIAN, et al. On blockchain and its integration with IoT. Challenges and opportunities[J]. Future Generation Computer Systems, 2018, 88: 173-190.

[9] BINY, JAROD W, SURYA N, et al. IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain [J]. IEEE Cloud Computing, 2018, 5(4): 12-23.

[10] YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[11] AZARIA A, EKBLAW A, VIEIRA T, et al. Medrec: Using blockchain for medical data access and permission management [C]// 2016 2nd International Conference on Open and Big Data (OBD). Los Alamitos, CA, USA, IEEE, 2016: 25-30.

[12] TOYODA K, MATHIOPOULOS P T, SASASE I, et al. A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in The Post Supply Chain[J]. IEEE Access, 2017, 5: 17465-17477.

[13] GAO J, ASAMOAH K O, SIFAH E B, et al. GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid [J]. IEEE Access, 2018, 6(99): 9917-9925.

[14] MAO D, HAO Z, WANG F, et al. Novel Automatic Food Trading System Using Consortium Blockchain [J]. Arabian Journal for Science and Engineering, 2019, 44(4): 3439-3455.

[15] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]// International Conference on the Theory and Application of Cryptology and Information Security. New York: Springer-Verlag, 2001: 514-532.

[16] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems (TOCS), 2002, 20(4): 398-461.

[17] ZHANG F, SAFAVINAINI R, SUSILO W. An Efficient Signature Scheme from Bilinear Pairings and Its Applications[J]. Lecture Notes in Computer Science, 2004, 2947(39): 277-290.

[18] CHEN Z, CHEN S, XU H, et al. A security authentication scheme of 5G ultra-dense network based on block chain[J]. IEEE Access, 2018, 6: 55372-55379.

[19] WANG Y, CAI S, LIN C, et al. Study of Blockchains's Consensus Mechanism Based on Credit[J]. IEEE Access, 2019, 7: 10224-10231.

ZHOU Wan-kai, born in 1994, postgraduate. His main research interests include blockchain.

LONG Min, born in 1977, Ph.D, professor. Her main research interests include chaos theory and application, wireless communication and security.