计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191200124

基于区块链的一体化应急应战机制

邵炜晖[1]　王　宁[1]　韩传峰[2]　许维胜[3]
1 同济大学教育技术与计算中心　上海 200092
2 同济大学可持续发展与新型城镇化智库　上海 200092
3 同济大学电子与信息工程学院　上海 201804

摘　要　我国应急与应战体系设置分散,信息沟通渠道缺失,协调机制不健全,导致动员效能不高,资源调度冲突,指挥协调不畅,亟须融合应急与应战体系,以提升一体化应急应战能力。针对这一现状,应用区块链技术设计以专家系统为监管决策层、P2P(Peer-to-Peer)网络为自治决策层的一体化应急应战机制。基于应急应战事件位置、事件时间和事件类别建立三维区块链模型,对不同等级、不同模式下的应急应战资源协同配置问题进行统一描述。考虑一体化应急应战场景与常规点对点交易场景的区别,设计信用证明作为区块链共识机制。最后,在以太坊开发框架下搭建有限节点参与的一体化应急应战区块链原型系统并进行仿真,仿真结果证明基于区块链的一体化应急应战机制是合理且可行的。

关键词:应急应战一体化;融合机制;资源配置;区块链
中图法分类号　TP312

Integrated Emergency-Defense System Based on Blockchain

SHAO Wei-hui[1],WANG Ning[1],HAN Chuan-feng[2] and XU Wei-sheng[3]
1 Education Technology and Computing Center,Tongji University,Shanghai 200092,China
2 Sustainable Development and New-type Urbanization Think-tank,Tongji University,Shanghai 200092,China
3 School of Electronics and Information Engineering,Tongji University,Shanghai 201804,China

Abstract　The emergency-defense system of China is decentralized,lacking information communication channels and coordination mechanisms. This condition results to low mobilization efficiency,resource scheduling conflicts and poor coordination performance,which highlights the urgency to upgrade the capacity of integrated emergency-defense system. In response to this situation,this paper studies the integrated emergency-defense mechanism with the expert system as the supervisory decision-making layer and the P2P(Peer-to-Peer) network as the autonomous decision-making layer. Based on the location,time and category of emergency response events or national defense events,a three-dimensional blockchain model is established to describe resource scheduling problems in different situations. Considering the difference between the integrated emergency-defense scenario and the conventional peer-to-peer transaction scenario,a consensus mechanism based on credit certificate is designed. Finally,an integrated emergency-defense blockchain prototype system of limited nodes to participate is built on Ethereum. Simulation results of the prototype system prove that the blockchain based integrated emergency-defense mechanism is reasonable and feasible.

Keywords　Integrated emergency-defense system,Fusion mechanism,Resource allocation,Blockchain

1　引言

构建一体化应急应战体系和能力,符合国家的发展战略,极具重要性和紧迫性。但是,当前应急处置和国防动员在一体化层面尚缺乏顶层设计,主要表现在:1)应急与应战组织体系分散设置,缺乏系统整合和有效对接,导致能力重复建设与能力不足的现象并存;2)协调和信息沟通等机制不完善,存在多头管理、指挥机构不权威、实施程序不兼容、救援力量不统用、资源浪费等问题;3)资源储备、配置不合理,未形成应急应战资源共享机制,在紧急状态下易造成人员和物资的调度冲突[1-2]。

针对上述问题,学术界对一体化应急应战体系展开研究。在一体化应急应战机制方面,Correia 提出一种基于知识管理的分布式应急管理系统架构,以实现实时决策支持[3];Dorasamy 提出基于知识管理实现应急管理系统中的信息搜索任务[4];Song 等根据 ACP 和复杂网络理论,提出一种基于代

到稿日期:2019-12-20　返修日期:2020-06-05　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:国家自然科学基金项目(61773292,71841036,61973238);上海市科学技术委员会研究项目(19DZ1209200)
This work was supported by the National Natural Science Foundation of China(61773292,71841036,61973238) and Research Project of Shanghai Science and Technology Commission(19DZ1209200).
通信作者:邵炜晖(shaoweihui@tongji.edu.cn)

理的应急管理模拟系统[5]。在一体化应急应战实践方面，Jia等[6]通过比较美日应急应战一体化的实践经验发现，美国强调政府主导，完善法律法规并优化配置相关资源；日本则重视地方应急管理机构设置、国家防灾宣传及对民众自救意识的提升；Kaneberg 研究了瑞典的一体化应急应战系统，该系统强调军民协作，构建自主应急防御网络[7]；Araghizadeh 对伊朗面对自然灾害时的军民协调问题进行了定性研究，提出应通过组织或政治支持来加强军民间的协调[8]。整体来说，现有研究主要集中于应急应战一体化的概念综述、必要性分析以及现行体系问题等方面的内容，但缺乏一体化应急应战机制体系的形式化表达及一体化应急应战系统建设技术方案等方面的研究。

现代应急与应战体系的信息化、网络化、智能化态势日益明显，在一体化应急应战体系下，信息空间、物理空间与人类社会行为将紧密耦合，从而形成一个复杂的信息物理社会融合系统(Cyber Physical Social Systems，CPSS)。对这一复杂系统进行机制设计与建模仿真具有一定的挑战性。区块链技术(Blockchain)利用块链式结构验证、存储数据，利用分布式节点共识算法生成、更新数据，利用密码学方式确保安全传输和访问数据，利用由自动化脚本组成的智能合约编程与操作数据[9]。这一全新的分布式基础架构与计算范式凭借透明性、去中心性、安全性等特点打破了传统中心化的组织、信息及管理限制，被广泛应用于经济、金融和社会系统中[10]，也为一体化应急应战机制体系的设计提供了新的思路。

本文基于区块链技术对一体化应急应战机制进行研究。第 2 节设计了以专家系统为监管决策层、P2P 网络为自治决策层的一体化应急应战机制；第 3 节建立考虑事件位置、时间和类别的三维区块链模型，设计信用证明作为区块链共识机制；第 4 节基于以太坊搭建有限节点参与的一体化应急应战区块链原型系统并进行仿真；最后总结全文并对下一步研究进行展望。

2 一体化应急应战机制设计

2.1 传统应急应战体系

如图 1 所示，传统应急体系和应战体系均可抽象为具有三层结构的复杂网络。

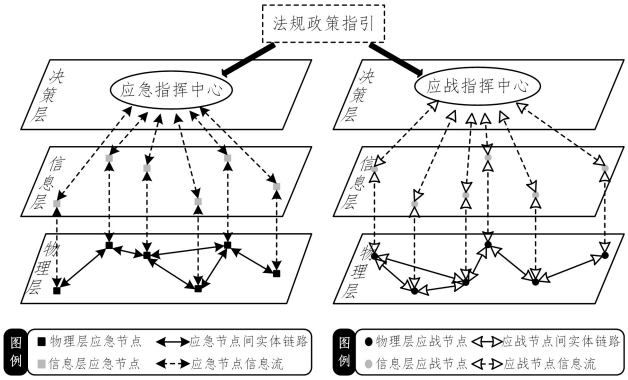


图 1 传统应急体系与应战体系

Fig. 1 Traditional emergency response system and national defense system

底层为物理层，表示应急、应战节点的资源储备与交互链路。节点资源储备广义上包括信息情报、人员配置、技术能力和物资储备等。节点间链路由于物理条件的限制，并非点对点的互联网络，而是具有一定拓扑结构的非完备网络。中间层为信息层，用于存储各节点的信息及数据。传统的应急、应战体系分立，应急、应战节点只与对应的上级应急、应战指挥中心相互通信来上报需求信息并接收调度指令。应急节点间、应战节点间、应急与应战节点间的信息不相通。顶层为决策层，应急应战指挥中心接收应急、应战节点的信息，依据国家政策法规，专家系统分析得出应急应战策略并下达调度指令。

在上述应急、应战体系下，事件处置流程自上而下，导致应急、应战节点无法第一时间对突发事件进行有效响应；应急、应战体系间缺乏系统整合和有效对接，造成应急应战能力的重复建设与无序调度。

2.2 基于区块链的一体化应急应战体系

针对传统应急、应战体系的诸多问题，本文基于区块链技术设计一体化应急应战体系，以提高我国一体化应急应战的能力。

体系结构方面，基于区块链的一体化应急应战体系设计为包含自治决策层和监管决策层的双层架构，将分离的应急体系与应战体系融合。如图 2 所示，自治决策层将各节点应急应战能力标准化，通过基于区块链的 P2P 网络提供安全的、去中心化的资源交互平台，从而打通应急与应战体系。监管决策层的应急与应战指挥中心间数据互通，该决策层对自治决策层的自发资源调度进行实时监管、及时干预。

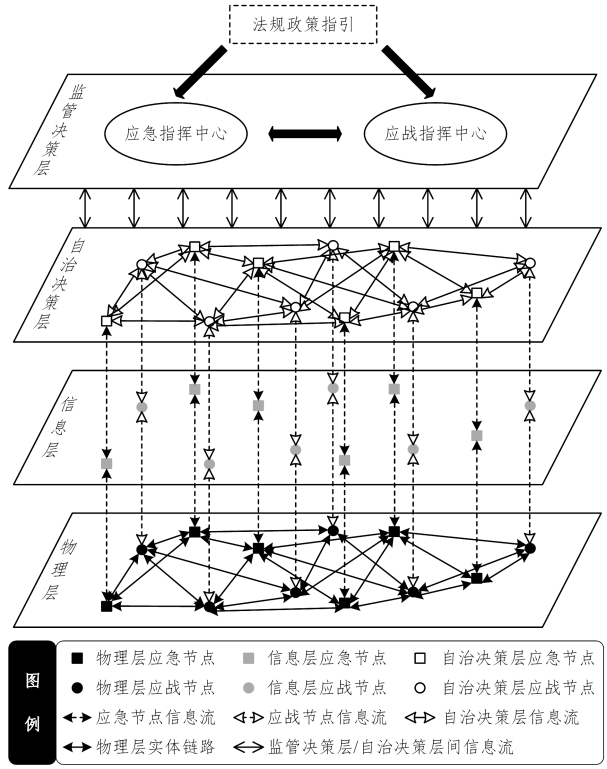


图 2 基于区块链的一体化应急应战体系

Fig. 2 Blockchain based integrated emergency-defense system

事件处置方面，基于区块链的一体化应急应战体系对突

发事件的响应流程如图 3 所示。应急应战事件发生后，应急应战需求通过广播发布至自治决策层的 P2P 网络，各应急、应战节点立即自发响应。同时，应急应战事件上报至监管决策层的应急、应战指挥中心。两中心对突发事件定性分级并咨询对应的专家系统，研究应对策略，同时对应急应战事件态势和自治决策层正在进行的资源调配进行实时监控及干预。应急应战事件结束后，监管决策层根据自治决策层区块链激励机制对应急、应战节点进行结算奖励。

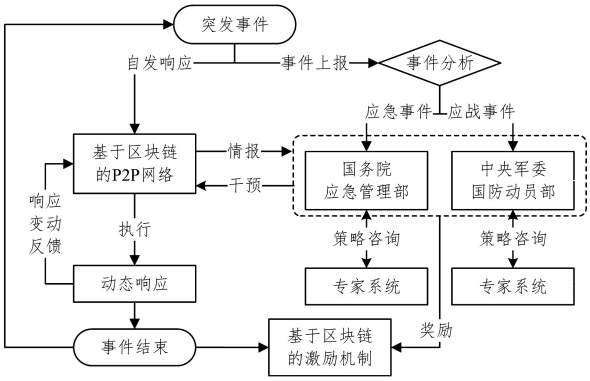


图 3 一体化应急应战体系对突发事件的响应流程

Fig. 3 Incident response process of blockchain based integrated emergency-defense system

该体系的应用场景可分为：应急或应战事件单独发生的单一场景，以及应急和应战事件同时发生的混合场景。对于单一场景，一体化应急应战机制下的应急体系与应战体系互为增强，能有效避免重复建设，补充欠缺资源，提高响应速度，较单一的应急、应战体系更具优越性；对于混合场景，一体化应急应战机制下的监管决策层可对各节点的应急应战行为进行干预，有目的地引导自治决策层进行应急应战响应。一般情况下，优先响应应战事件。

3 一体化应急应战区块链建模

3.1 区块链结构

应急事件与应战事件具有一定差异：应急事件往往是单一事件，随机发生且不可预测；应战事件既可能是单一的局部冲突，也可能是全面的大规模战争，其发生具有一定的因果性。同时，应急事件与应战事件又都具有发生时间可重叠、响应需求连续等共性。总的来说，不同类型、不同规模的应急和应战事件可能在多个地区同时发生并发展，因此本文建立一个三维区块链模型对应急应战资源一体化配置问题进行统一描述。区块链中的每个区块均包含 3 个维度信息，可表示为 $Block(l_i,t_i,c_i)$。其中，l_i 用于描述应急应战事件发生的地理位置；t_i 用于描述某时间段内应急应战事件随时间变化的需求，如信息、情报、人力、物资、技术等；c_i 用于表示事件类别。i 大于 0 表示应急事件，可分为事前预防准备、事初信息共享、事中应急处置、事后灾后重建等类别；i 小于 0 表示应战事件，可分为事前战争动员、事初情报收集、事中资源调配、事后战后恢复等类别。此外，一体化应急应战区块链区块带有时间戳，确保了形成区块链的唯一性及连续性。

如图 4 所示，一体化应急应战区块链中每个区块都代表一个应急应战需求，区块不断产生表示应急应战需求不断出现与发展。

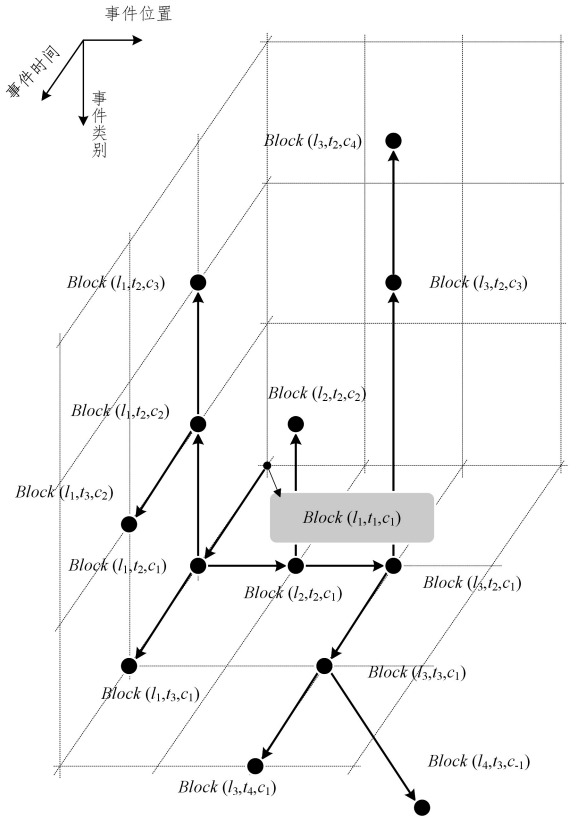


图 4 一体化应急应战区块链示例

Fig. 4 Example of integrated emergency-defense blockchain

t_1 时段内，位置 l_1 处发生事件类别为 c_1 的应急事件，各应急应战节点基于智能合约自主响应需求，具体响应情况记入区块 $Block(l_1,t_1,c_1)$ 中。

t_2 时段内，位置 l_1 处已发生的 c_1 类别事件持续，应急应战节点响应情况记入区块 $Block(l_1,t_2,c_1)$ 中。此后，位置 l_1 处事件依次发展至 c_2 和 c_3 类别，各应急应战节点自主响应情况分别记入区块 $Block(l_1,t_2,c_2)$ 和 $Block(l_1,t_2,c_3)$ 中。此外，位置 l_2 和位置 l_3 处在 t_2 时段内也发生应急事件。位置 l_2 处发生的应急事件类别为 c_1 且发展至 c_2 类别，各应急应战节点自主响应情况分别记入区块 $Block(l_2,t_2,c_1)$ 和 $Block(l_2,t_2,c_2)$ 中。位置 l_3 处发生的应急事件类别为 c_1 且发展至 c_3 和 c_4 类别，各应急应战节点自主响应情况分别记入区块 $Block(l_2,t_2,c_1)$，$Block(l_2,t_2,c_3)$ 和 $Block(l_2,t_2,c_4)$ 中。

t_3 时段内，位置 l_1 处已发生的 c_1 和 c_2 类别事件，且位置 l_3 处已发生的 c_1 类别事件持续，应急应战节点响应情况分别记入区块 $Block(l_1,t_3,c_1)$，$Block(l_1,t_3,c_2)$ 和 $Block(l_3,t_3,c_1)$ 中。同一时段内，位置 l_4 处发生事件类别 c_{-1} 的应战事件，各应急应战节点响应情况记入区块 $Block(l_4,t_3,c_{-1})$ 中。

t_4 时段内，位置 l_3 处已发生的 c_1 类别事件持续，应急应战节点响应情况记入区块 $Block(l_3,t_4,c_1)$ 中。

3.2 区块链结构

一体化应急应战区块链单个区块的物理及逻辑架构如图 5 所示。

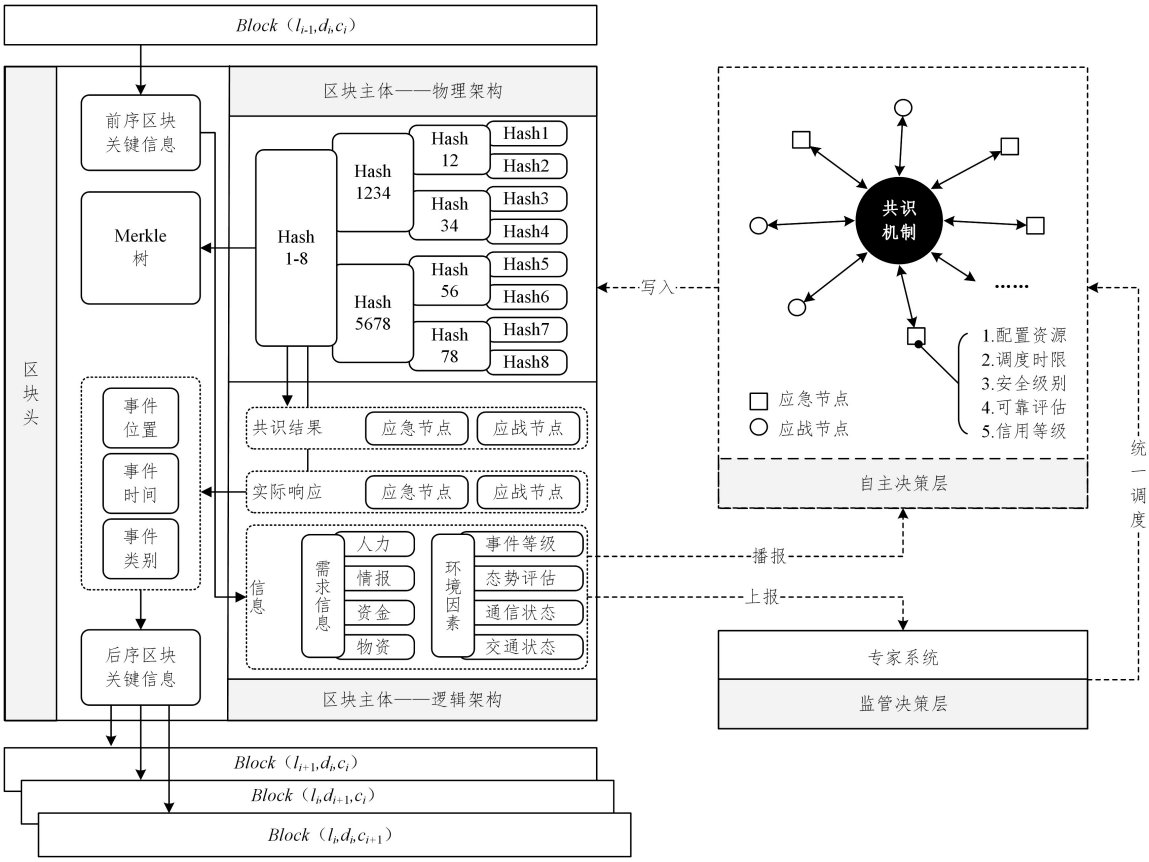


图 5 一体化应急应战区块链区块的物理及逻辑架构

Fig. 5 Physical and logical architecture of blocks in integrated emergency-defense blockchain

应急应战事件发生后，需求节点在自治决策层的区块链中发布人力、情报、物资、资金等需求信息和事件等级、态势评估、通信状态、交通状态等环境信息，同时上报监管决策层。各应急应战节点根据自身应急应战能力提供响应时间、支援能力、信用等级等信息，得到共识的应急应战方案及实际应急应战能力交互情况，由获得区块链记账权的节点记入区块中，后续作为评估应急应战节点所做贡献的依据。记账节点通过链式结构将当前区块链接到前一区块，形成最新的区块主链。在共识机制中，设计监管决策层具有最高权限，其可直接干预自治决策层共识结果并写入区块链，从而实现对应急应战节点的统一调度。

一体化应急应战区块链可借鉴比特币，采用多种技术确保数据安全，如采用时间戳技术确保每一个区块按照时序链接，采用哈希函数确保交易信息不被篡改，采用 Merkle 树数据结构记录交易信息，采用非对称加密实现身份认证等[11]。

3.3 共识机制设计

共识机制(Consensus)旨在确认去中心化系统中区块数据的有效性，是区块链的核心技术之一。最具代表性的共识机制是中本聪在早期比特币区块链中设计的工作量证明(Proof of Work，PoW)共识机制[12]。

在比特币系统中，各节点基于各自的算力相互竞争，共同解决一个求解复杂但验证容易的 SHA256 数学难题，最快解决该难题的节点将获得区块记账权和系统自动生成的比特币奖励。PoW 共识机制近乎完美地整合了比特币系统的货币发行、交易支付和验证等功能，并通过算力竞争保障了系统的安全性和去中心性；但其也存在着显著的缺陷，如算力竞争造成资源浪费，交易确认时间过长导致实时性差等。此后，研究人员针对不同的应用场景需求设计了一系列新的共识机制，如权益证明(Proof of Stake，PoS)[13]、瑞波共识机制(Ripple Consensus，RC)[14]、授权股份证明机制(Delegated Proof of Stake，DPOS)[15]等。

区块链支撑的一体化应急应战场景与常规的去中心化点对点交易场景有本质区别。普通点对点交易场景下，基于区块链的 P2P 交易平台具有去中心化特征，各节点的市场行为完全由其偏好和市场情况决定。一体化应急应战场景下，基于区块链的 P2P 网络主要实现信息情报的精准采集以及人力和物资的紧急调配，强调需求和供给能力的精准对接和快速满足，对智能合约完成后的价值转移问题不做过多强调。此外，监管决策层可直接干预各节点自发的应急、应战行为，各节点不能完全自由地进行 P2P 交易。因此，一体化应急应战区块链需要引入新的共识机制。

信用证明(Proof of Credit，PoC)是一种以应急应战节点信用为依据的共识机制。在一体化应急应战区块链(如图 6 所示)中，供给节点在区块链上发布其公钥和特征值，特征值包含供给位置、响应能力等信息；需求节点在区块链上发布其公钥和特征值，特征值包含需求位置、紧急程度、需求量等信息。为保证数据安全，两类节点的具体信息分别保存在本地数据中心；为防止需求节点上报虚假需求信息，需求节点的特

征值还须包含其信用承诺，并将其保存在区块链上的信用数据库中。

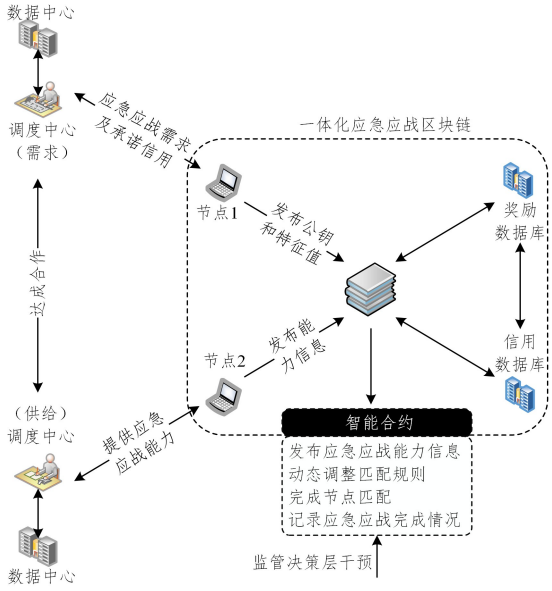


图 6 PoC 共识机制

Fig. 6 PoC consensus mechanism

3.4 智能合约设计

智能合约封装区块链系统的各类脚本代码、算法，是实现区块链系统灵活编程和操作数据的基础。例如，比特币通过非图灵完备的简单脚本代码编程实现延时支付、担保交易等交易控制功能；以太坊通过图灵完备的脚本语言构建任意复杂和精确定义的智能合约与去中心化应用[16]。

一体化应急应战区块链的智能合约将实现需求节点和供给节点间的高效匹配，具体匹配规则由自治决策层各节点决定，并受监管决策层直接干预。如图 7 所示，匹配规则是动态变化的，上述过程由于不考虑其他冗余信息，仅通过特征值的查表匹配，因此可快速、准确地实现供需匹配。

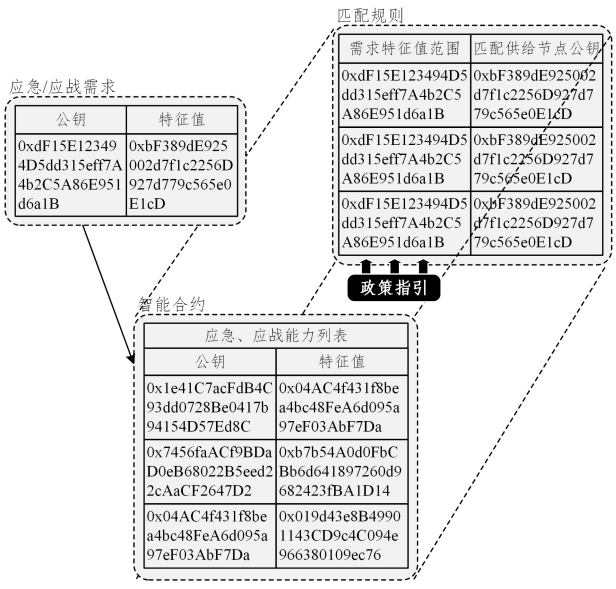


图 7 一体化应急应战区块链智能合约

Fig. 7 Smart contract of integrated emergency-defense blockchain

匹配的双方将直接进行协商，沟通应急应战的供给需求细节，达成一致后即开始进行应急应战物资和人员的调配。若在指定时间限制内需求被满足，则需求者向一体化应急应战网络发出“需求满足确认”，该次应急应战事件被认为已完成，并被记录在区块链中，同时相应参与节点的信用和奖励数据库被更新。供需匹配成功的示意图如图 8 所示。

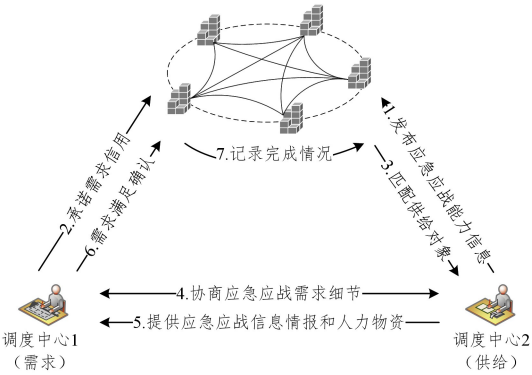


图 8 供需匹配成功示意图

Fig. 8 Successful match of demand and supply

若供给者未能在指定的时间限制内满足需求者的要求或未能达到协商要求，则需求节点向一体化应急应战网络发出“需求延误确认”，该次应急应战事件被认为尚未完成，且同样被记录在区块链中。根据实际情况，供给者的信用值和奖励值将降低，需求者的紧急程度将提升并在下一轮匹配中获得更高的优先级。供需匹配失败的示意图如图 9 所示。

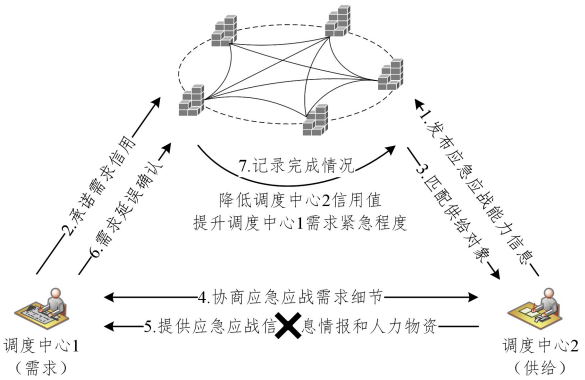


图 9 供需匹配失败示意图

Fig. 9 Failure match of demand and supply

4 一体化应急应战区块链原型系统的搭建与仿真

本文基于以太坊（Ethereum）开发框架搭建一体化应急应战区块链原型系统，以验证所提出的一体化应急应战机制的可行性。实验环境为 Ubuntu 18.04.2，通过以太坊客户端 Geth 搭建以太坊并部署相应的智能合约，应急应战节点可通过以太钱包应用（Ethereum Wallet）连接至上述私有链。

4.1 区块链搭建及基本功能验证

在 Ubuntu 环境下进入 Terminal，安装以太坊客户端，步骤如下：

>sudo add-apt-repository -y ppa:ethereum/Ethereum

>sudo apt-get update

>sudo apt-get install -y ethereum

在已安装以太坊的开发环境中搭建一体化应急应战区块链，新建目录 ethereum 用于存储私有链的数据和配置文件。

步骤 1 创建文件 integration.json 用于初始化创世区块，如图 10 所示。

```
pragma solidity ^0.4.21;
contract Token {
mapping(address=>uint) public balancesOf;
  address public owner;
constructor() public {
    owner = msg.sender;
balancesOf[msg.sender] = 500;
  }
  function transfer(address _to,uint _value) public {
    if (balancesOf[msg.sender]<_value) return;
    if (balancesOf[_to]+ _value<balancesOf[_to]) return;
balancesOf[msg.sender] -= _value;
balancesOf[_to]+=_value;
  }
  function mint(uint _amount) public {
balancesOf[owner]+= _amount;
  }
}
```

图 10 一体化应急应战区块链创世区块的初始化配置

Fig. 10 Initial configuration of integrated emergency-defense blockchain's genesis block

步骤 2 创建创世区块。

>geth--datadir ". /" init integration.json

当前目录中新增的 geth 和 keystore 文件夹分别用于保存区块链的相关数据和该链条中的用户信息。

步骤 3 创建一体化应急应战私有链。私有链创建成功的示意图如图 11 所示。

>geth--datadir ". /" console 2≫geth.log

图 11 一体化应急应战私有链创建成功示意图

Fig. 11 Schematic diagram of successfully created integrated emergency-defense blockchain

步骤 4 在区块链上创建密码为 123456 的用户 Account1、密码为 123456789 的用户 Account2 作为应急应战节点，Account1 和 Account2 分别被分配唯一的节点账户地址。当前链上所有已创建的账户可通过 eth.accounts 指令查看。

>personal.newAccount("123456")

>personal.newAccount("123456789")

步骤 5 开始挖矿。挖到的以太币(Ether)会默认保存在第一个创建的账户 Account1 中。挖矿是执行以太坊私有链智能合约的基础。

>miner.start(1)

步骤 6 将以太钱包连接至 Geth 客户端上创建的一体化应急应战私有链中。

> ethereumwallet -- rpc /home/ubuntu/ethereum/geth.ipc

图 12 所示即为 Geth 客户端上已创建的用户 Account1 和 Account2。

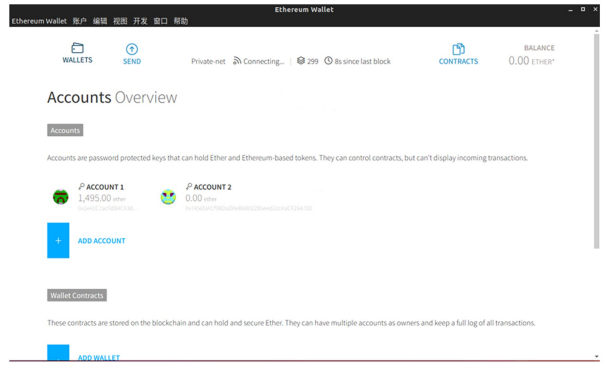


图 12 完成配置的以太钱包界面示意图

Fig. 12 Ethereum wallet interface when configurations are completed

步骤 7 在 Account1 以太钱包界面中设置交易对象 Account2 及以太币交易总数并输入密码确认，进行节点间交易功能的测试。如图 13 所示，测试结果证明所建立的区块链可用于记录节点间应急应战能力的转移情况。

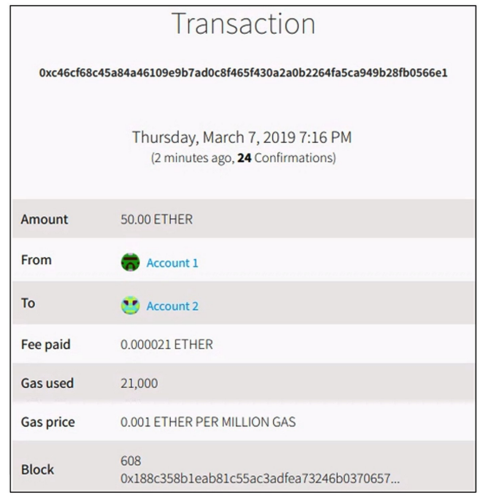


图 13 节点间应急应战能力的转移模拟

Fig. 13 Capability transfer simulation among emergency response nodes and national defense nodes

4.2 应急应战节点的配置

利用原型系统模拟某地区应急应战网络，设置中心专家系统节点 1 个，其代表应急应战体系中的监管决策层，具有最高权限；设置应急节点 8 个，其代表部署于该地区的应急处置中心；设置应战节点 7 个，其代表部署于该地区的应战准备中心。

如表 1 所列，所有节点具有唯一的身份识别地址，节点的位置、类型、人力和物资等信息保存在以太坊私有链中。节点账户中存有不同数量的以太币，用于表示不同节点响应应急应战事件的应急应战能力转移情况，即所做贡献。

表 1 应急应战节点的信息

Table 1 Information of emergency response nodes and national defense nodes

节点	节点账户地址	ETH	
监管决策层	中心专家系统	0x1e41C7acFdB4C93dd0728Be0417b94154D57Ed8C	6609
	应战节点 021	0xdF15E123494D5dd315eff7A4b2C5A86E951d6a1B	351.6
	应战节点 025	0xbF389dE925002d7f1c2256D927d779c565e0E1cD	213.4
	应战节点 0551	0xC0A26e6a7a392d8da6Bd3CA51C2ECd97FD72E169	76.9
	应战节点 0571	0xd081487376455CA7C0ad9a3cD6a9e0Cd792e107A	42.1
	应战节点 0510	0xA62113079E0133E05f8BC7BCbFDa231dcF99fCBE	68.4
	应战节点 0574	0xA7180308A4451Cc1e693b0C4A5D4897EA0906A77	23.6
	应战节点 0513	0xD8F04B38004e5d97aaC27d19DDF31c00f1AEBd41	15.8
自治决策层	应急节点 021	0x7456faACf9BDaD0eB68022B5eed22cAaCF2647D2	263.2
	应急节点 025	0x04AC4f431f8bea4bc48FeA6d095a97eF03AbF7Da	125.3
	应急节点 0551	0x04AC4f431f8bea4bc48FeA6d095a97eF03AbF7Da	56.3
	应急节点 0571	0xb7b54A0d0FbCBb6d641897260d9682423fBA1D14	36.2
	应急节点 0510	0x019d43e8B49901143CD9c4C094e966380109ec76	75.1
	应急节点 0574	0x43acC9174dFD5c6e50f5c243e9c65c74FF5a97b6	61.8
	应急节点 0513	0x23e44B920daD1C7a5aB4AC1637ef05Ee30a9fC9E	21.7
	应急节点 0553	0x6e248Fb1Def8E48893a97dBEc850C944894f5cf4	44.6

各节点配置情况在以太钱包应用中的展示如图 14 所示。

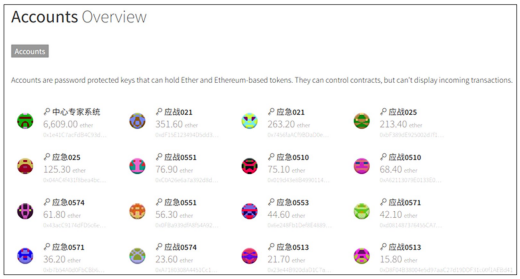


图 14 应急应战节点的配置及展示

Fig. 14 Configuration of emergency response nodes and national defense nodes in Ethereum Wallet

4.3 智能合约部署与仿真

以中心专家系统的物资分配为例，使用 Solidity 语言编写智能合约以实现应急应战事件的发布与响应，通过以太币记录节点间应急应战能力的交互情况。智能合约的伪代码如图 15 所示。

```
pragma solidity ^0.4.21;
contract Token {
mapping(address=>uint) public balancesOf;
  address public owner;
constructor() public {
    owner=msg.sender;
balancesOf[msg.sender]=500;
  }
  function transfer(address _to, uint _value) public {
    if (balancesOf[msg.sender] < _value) return;
    if (balancesOf[_to]+_value <balancesOf[_to]) return;
balancesOf[msg.sender] -= _value;
balancesOf[_to] += _value;
  }
  function mint(uint _amount) public {
balancesOf[owner] += _amount;
  }
}
```

图 15 智能合约 Token2871 伪代码

Fig. 15 Pseudo code of smart contract Token2871

部署应急应战节点交互行为的智能合约，并将其记为 Token2871。调用该智能合约执行 mint 进行挖矿。应战 021 节点响应 Token2871 完成合约，通过其账户地址(0xdF15E123494D5dd315eff7A4b2C5A86E951d6a1B)可以查看具体的响应情况，如图 16 所示。

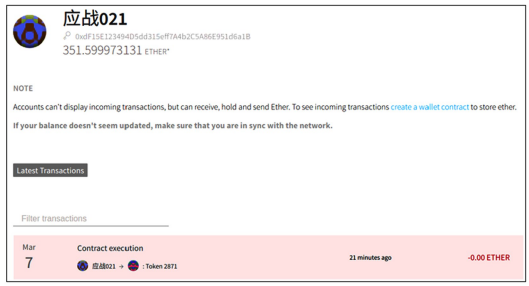


图 16 应战节点 021 响应 Token 2871

Fig. 16 National defense node 021 responses to Token 2871

上述智能合约的发布与响应过程在一体化应急应战体系中解释为：中心专家系统发布某需求并广播至一体化应急应战区块链中，所有节点均收到该需求，符合具体需求条件的节点提出响应请求。应战 021 节点与中心专家系统节点达成合约并响应该需求，该信息得到了 P2P 网络 PoC 机制的共识并被写进区块链中，代表着一次应急应战阶段性事件的完成。

类似地，在一体化应急应战区块链的 P2P 网络中，任意两节点间都可以采用直接对接需求达成智能合约的方式优先展开应急应战工作，所有应急应战事件需求与响应记录均被完整地记录于区块链中且不可篡改。中心专家节点被赋予最高权限，可根据政策变化或实际情况灵活地对应急应战节点间的行为进行干预。

结束语 本文提出一种由专家系统为监管决策层、区块链 P2P 网络为自治决策层的一体化应急应战机制。在该机制下，通过三维区块链模型对不同等级和模式下应急应战资源的配置问题进行统一描述，设计信用证明作为区块链共识机制。最后，模拟某地区的应急应战网络，搭建一体化应急应战区块链原型系统并进行仿真实验，实验结果有效证明了所提模型的合理性。

不难发现，区块链通过汇聚节点算力、权益等资源实现数

据验证和记账工作，其本质是共识节点间的任务众包过程。在一体化应急应战区块链中，应急、应战节点参与该过程的目标各不相同，须设计激励分配和行为约束机制，鼓励节点自发、有序地参与应急应战工作，避免指挥不畅，减少调度冲突，提高动员效能，进而提升一体化应急应战能力。

因此，下一步工作将从以下两方面展开。

(1)对于细化的应急应战事件类型，建立相应的区块链激励机制及监管约束规则，并依此设计共识机制及智能合约，实现所提出的一体化应急应战区块链的完备功能。

(2)设计表征响应速度、资源利用率、动员资源总量等指标的应急应战响应效果评价体系，在不同场景下对基于区块链的一体化应急应战机制进行仿真评价，验证其优越性。

参 考 文 献

[1] WEI Z Y, TANG W H, AN L. On the Construction of China's National Defense Mobilization Emergency Response Integration System from the Mobilization Practice of Major Countries in the World [J]. Technology Foundation of National Defence, 2009 (8): 59-62.

[2] MIAO Y, SU P. Construction of the Integration of Meeting an Emergency and an Enemy Attack in the USA and the Enlightenment[J]. Military Economic Research, 2010(5): 30-33.

[3] CORREIA A, SEVERINO I, NUNES I L, et al. Knowledge management in the development of an intelligent system to support emergency response[C]// International Conference on Applied Human Factors and Ergonomics. Cham: Springer, 2017: 109-120.

[4] DORASAMY M, RAMAN M, KALIANNAN M. Integrated community emergency management and awareness system: A knowledge management system for disaster support[J]. Technological Forecasting and Social Change, 2017, 121: 139-167.

[5] SONG Z C, GE Y Z, DUAN H, et al. Agent-based simulation systems for emergency management[J]. International Journal of Automation and Computing, 2016, 13(2): 89-98.

[6] JIA T T, YANG L C. Main Practices and Enlightenment of integrated emergency-defense system in American and Japanese[J]. Dual Use Technologies & Products, 2014(7): 185-186.

[7] KANEBERG E, HERTZ S, JENSEN L M. Voluntary defense networks in emergency preparedness in developed countries: the case of Sweden [J]. Revista Científica General José María Córdova, 2019, 17(26): 228-250.

[8] ARAGHIZADEH H, PEYRAVI M, SHARIFIFAR S, et al. Civil-Military Coordination in Natural Disasters: A Qualitative Study[J]. Iranian Red Crescent Medical Journal, 2020, 22(1).

[9] SWAN M. Blockchain: Blueprint for a New Ec-onomy[M]. O'Reilly Media. Inc., 2015.

[10] YUAN Y, WNG F Y. Blockchain: The State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[11] Bitcoin Sourcecode[EB/OL]. https://github.com/bitcoin/bitcoin/, 2016.

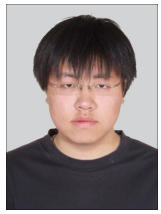
[12] Antonopoulos A M. Mastering Bitcoin: Unlocking Digital Crypto-Currencies[M]. O'Reilly Media, Inc., 2014.

[13] LARIMER D. Transactions as proof-of-stake[EB/OL]. http://7fvhfe.com1.z0.glb.clouddn.com/@/wp-content/uploads/2014/01/TransactionsAsProofOfStake10.pdf, 2013.

[14] SCHWARTZ D, YOUNGS N, BRITTO A. The ripple protocol consensus algorithm[EB/OL]. https://ripple.com/files/ripple_consensus_whitepaper.pdf, 2014.

[15] LARIMER D. Delegated proof-of-stake white paper[EB/OL]. http://www.bts.hk/dpos-baipishu.ht-ml, 2014.

[16] Ethereum White Paper. A next-generation smart contract and decentralized application platform[EB/OL]. https://github.com/ethereum/wiki/wiki/WhitePaper, 2015.



SHAO Wei-hui, born in 1988, Ph.D, Engineer. His main research interests include educational informatization, big data and blockchain.