

An IoE blockchain-based network knowledge management model for resilient disaster frameworks



Amir Javadpour^a, Farinaz Sabz AliPour^b, Arun Kumar Sangaiah^{c,*}, Weizhe Zhang^a,
Forough Ja'far^d, Ashish Singh^e

^a Department of Computer Science and Technology (Cyberspace Security), Harbin Institute of Technology, Shenzhen, China

^b Department of Engineering Managements & Systems Engineering Old Dominion University, 2101 Hampton Blvd Norfolk, VA, United States of America

^c International Graduate School of Artificial Intelligence, National Yunlin University of Science and Technology, Yunlin, Taiwan

^d Department of Computer Engineering, Sharif university of technology, Tehran, Iran

^e School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT), Bhubaneswar, India

ARTICLE INFO

Article History:

Received 17 May 2022

Accepted 14 June 2023

Available online 27 June 2023

Keywords:

Blockchain technology
Decentralized network
Disaster supply network
Internet of things
Network simulation
Resilience

ABSTRACT

The disaster area is a constantly changing environment, which can make it challenging to distribute supplies effectively. The lack of accurate information about the required goods and potential bottlenecks in the distribution process can be detrimental. The success of a response network is dependent on collaboration, coordination, sovereignty, and equal distribution of relief resources. To facilitate these interactions and improve knowledge of supply chain operations, a reliable and dynamic logistic system is essential. This study proposes the integration of blockchain technology, the Internet of Things (IoT), and the Internet of Everything (IoE) into the disaster management structure. The proposed disaster response model aims to reduce response times and ensure the secure and timely distribution of goods. The hyper-connected disaster supply network is modeled through a concrete implementation on the Network Simulation (NS2) platform. The simulation results demonstrate that the proposed method yields significant improvements in several key performance metrics. Specifically, it achieved more than a 30% improvement in the successful migration of tasks, a 17% reduction in errors, a 15% reduction in delays, and a 9% reduction in energy consumption.

© 2023 Published by Elsevier España, S.L.U. on behalf of Journal of Innovation & Knowledge. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Introduction

A disaster can have significant physical, economic, and social impacts. The location of a disaster is a critical focal point for supply chain management activities. Disaster relief supply chain management is designed to (1) manage current and future disasters, (2) coordinate with other competitive or complementary supply chains, (3) achieve desired outcomes, and (4) integrate and coordinate the activities of various parties involved (Aslam et al., 2021; Day et al., 2012; Ilbiz, 2020). Disaster supply chain management has unique characteristics, including large-scale operations, irregular demand, and unreliable transportation information (Verma, 2021). Engineering a disaster supply chain is challenging due to the dynamic nature of disasters, such as their location, type, spread, and magnitude (Balcik & Beamon, 2008). Therefore, a multidisciplinary research approach is needed to address the challenges of disaster relief networks, with a focus on shortening response times to prevent losses and uncertainties (Holguin-Veras et al., 2007; Mohammed, 2019). The lack of vital

information about available infrastructure, supplies, and demands in the initial phase of a disaster can significantly complicate this dynamic environment (Javadpour et al., 2022; Sangaiah et al., 2022b). However, time is a critical resource in disaster management, and accessing accurate information regarding the severity of the disaster and the required demands is essential. This study aims to propose a dynamic, reliable, and transparent tracking system for the aid supply chain. It combines blockchain technology and the Internet of Things (IoT), as proposed by Betti et al. (2020), with a fast and secure transaction mechanism, as proposed by Perez-Sol'a et al. (2019), to monitor demand provision, response time, and enhance disaster management efficiency. This model can help to overcome the challenges associated with the dynamic nature of disasters and improve response times.

Problem statement

In a disaster response, various parties are involved, making the process more challenging. Each party pursues distinct and, in some cases, conflicting strategic goals, contributing to the complexity of the disaster response. According to research conducted by Pour

* Corresponding author.

E-mail address: aksangaiah@ieee.org (A.K. Sangaiah).

(2021), the four main categories of challenges in a disaster supply chain are network communication, transparency, information management, and performance measurement. In some situations, an oversupply of non-essential goods may delay the logistical response. Therefore, a systematic approach is required to prioritize requirements, such as involving all parties, enabling swift trust, and providing collaboration channels. To achieve this, information technologies such as real-time risk monitoring, online dashboards, knowledge repositories, decision-making tools, interactive communication, and collaboration can be applied at every phase of a disaster (Imran et al., 2015; Sakurai & Murayama, 2019). However, Othman et al. (2017) argue that most literature uses centralized planning approaches for the emergency supply chain. In contrast, a distributed planning approach may be more suitable given the large and distributed nature of the emergency supply chain. One approach that permits immediate action is decentralization. Therefore, this study focuses on communication and collaboration among participants in a disaster response and aims to develop a decentralized network platform.

Research importance and necessity

Recent frequent disasters highlight the crucial role of a resilient disaster management network (Tomasini & Van Wassenhove, 2009; Sangaiah et al., 2022a). However, inconsistency in disaster response arises when the event evolves, but the information is not updated regularly (Glik et al., 2007), resulting in a suboptimal disaster response. Therefore, real-time information is essential to improve the quality of disaster response. Coordination among multiple organizations and agencies is also vital for an effective disaster response. Communication and collaboration of disaster aid networks are necessary to provide the right assistance to the affected population at the right time. This study proposes a synchronized combination of blockchain technology and IoT to track the response progress and optimize the allocation of tasks to the network participants. The Dynamic Voltage and Frequency Scaling (DVFS) algorithm is applied to achieve this objective.

Research objectives

Effective disaster response is often hindered by a lack of coordination in relief distribution and overlapping institutions (Holguín-Veras et al., 2007; Schipper & Pelling, 2006). To design a reliable disaster supply aid system, a comprehensive understanding of the operations, interactions, and methods involved is necessary for analyzing flows and prioritizing demands and goods (Holguín-Veras et al., 2007). This study aims to support the monitoring of supply network performance, enhance disaster response resilience, and reduce response time by developing a model that combines blockchain technology with IoT. The proposed system utilizes zero-confirmation transactions to simulate response action allocation, employs smart contract-enabled simulations, and evaluates performance in managing disaster complexity through a blockchain platform.

Examining research questions

This study aims to introduce a new approach for optimizing disaster response activities by providing a practical decision support tool. The decentralized network feature of the model enhances transparency and trust in information management, network communication, and collaboration. Additionally, the modeling and simulation capacity of the proposed method enables a more advanced understanding of the interrelated processes and functions within the system of interest. The research questions that this study seeks to answer are:

1. In what ways can a blockchain-enabled model enhance the performance of disaster aid networks?

2. How can a blockchain-enabled model improve the resilience of disaster aid management?

Research novelty and innovation

To effectively operate and monitor a disaster response network, independent data centers are required to handle hardware, infrastructure, implementation, and resource sharing. Cloud computing is a cost-effective solution that can improve service quality, and the proposed methodology allows users to submit requests to different data centers in one cloud. To enhance the network's performance, virtual machines can be used for distributed computing, networking, and services, dynamically allocating resources to each node on the server while transferring data without interruption. Load balancing techniques can also be used to optimize task distribution among various hubs and avoid overloading one host. The DVFS algorithm, proposed by Gu et al. (2014), can be applied to balance the workload and reduce energy consumption. The main contributions of this study are (1) exploring the relationship between blockchain technology and institutional interactions using smart contracts, (2) applying the DVFS algorithm to blockchain-based platforms to analyze disaster management complexities, and (3) reducing energy consumption and processing time. This study proposes a novel blockchain-based disaster management model that utilizes the DVFS algorithm to prevent hub overloading, reduce energy consumption, and improve system processing time.

Related work

There is a new research trend of applying new technologies to tackle challenges in disaster management. A wide range of solutions has been introduced, using computer modeling and artificial intelligence to leverage accurate information and support decision-making. Distributed Ledger Technology (DLT) is one of the techniques applied to address some of the challenges in disaster networks (Coppi & Fast, 2019). DLT can support updating information with consensus, share transaction databases, and record them with tamper-proof, time-stamped auditable history (Rajan, 2018). Blockchain is a form of DLT that operates as a peer-to-peer (P2P) network to overcome vulnerabilities of centralized systems while considering economic model risks (Coppi & Fast, 2019). The main characteristics of a blockchain are decentralization, immutability, disintermediation, transaction sharing, creation and movement of digital assets, and being tamper-proof. Blockchain is referred to as the "trust machine" because it does not require any entity to record and verify records (Matthew, 2016). Blockchain-based tools can have economic benefits as well as alleviate losses from disasters. Several studies have applied DLT and improved disaster management. For example, Coppi and Fast (2019) studied the application of DLT to address some of the challenges of disaster supply networks, including transparency, efficiency, scalability, and sustainability. Fitwi et al. (2019) developed a distributed agent-based framework to provide a secure and reliable information exchange technique. Rajan (2018) designed a holistic system to reduce natural disaster risks by forecasting automatically triggered responses and disbursing required funding using blockchain technologies. This study reviews the addressed challenges and proposed approaches in the literature and categorizes the results into four categories. A summary of the proposed solutions to tackle the critical challenges of disaster supply networks is described in Table 1. A smart contract is a software program that contains policies and rules for negotiating terms and actions between parties. Integrating smart contracts into DLT increases efficiency and scalability by decentralizing services (Rajan, 2018). Network participants can achieve a consensus on the outcome of the contract execution, and the transaction in the smart contract is automatically and independently executed on each node of the network, based on the data contained in

Table 1

Solutions proposed for each challenge resulted from the systematic literature review.

Category	Proposed Solution	Authors
Network Communication and Information Flow	<ul style="list-style-type: none"> Replacing credibility with swift trust Coordinating knowledge process without a shared Megastructure Coordinating the clusters to serve final recipients Achieving a better communication through a decentralized network 	Altay and Green III (2006); Haghani et al. (2009); Jahre and Jensen (2010a); Luna and Pennock (2018); Majchrzak et al. (2007); Jahre and Jensen (2010b)
Transparency	<ul style="list-style-type: none"> Digitalizing supply chains to provide swift trust, information sharing, and public/private Partnership Making funds traceable Using time stamped and digitally verified information 	Dubey et al. (2020); Papadopoulos et al. (2017); Stewart and Leinhardt (2009)
Data and Information Management	<ul style="list-style-type: none"> Creating an information repository to provide integrated information sources in detection and adoption for appropriate disaster response 	Goswami et al. (2018); Mackey and Nayyar (2017); Scholten et al. (2014)
Performance Measurement	<ul style="list-style-type: none"> Enhancing resiliency through collaboration, coordination, and trust Enhancing scalability Using interdependent systems to enhance the response abilities Simulating and evaluating of metrics to identify supply chain links and institutional roles 	Dubey et al. (2020); Scholten et al. (2014)

the triggered transaction. The incorporation of smart contracts into blockchain technology allows for the automatic verification of processes within the supply network, thereby enabling real-time evaluation and monitoring, and transparent reporting on the affected region. These features foster a more visible and trustworthy collaboration, where different parties can be tracked (Rajan, 2018).

DVFS is an effective tool for assessing the maximum level of disaster management complexity. It can identify malicious requests to network nodes and sort tasks to optimize resource management of the disaster response network. Xu et al. (2017) used DVFS to develop a robust blockchain-based decentralized resource management framework to reduce energy costs. The implementation of DVFS supports the vast input data from a disaster event and optimizes the processing costs to respond to it (Pour, 2021). Recent studies have applied DVFS to reduce energy consumption in various domains. For instance, Calheiros and Buyya (2014) proposed an energy-efficient execution of cloud models using DVFS in the field of disaster management, and Shirvani et al. (2020) have emphasized the significance of DVFS techniques and virtual machine migration in disaster-resilient fault-tolerant systems.

Research statement and proposed methods

Disaster supply chain networks are highly vulnerable and uncertain, making them more complex to manage. A deep understanding of the risks and complexities of these networks is necessary to maintain their dynamic, efficiency, and resilience. The conventional disaster decision-making process faces critical challenges, including a lack of consideration for the dynamic nature of the events, the uncertain attributes of disasters, and limited time to make irreversible decisions without reliable information (Altay & Green III, 2006). The solution to these challenges is to create a decentralized communication and collaboration platform that involves all parties in a disaster response, leading to a more resilient and efficient disaster response. Therefore, this study aims to evaluate the impact of blockchain technology and IoT on the disaster aid network's performance, response time, and complexity management.

Blockchain-Enabled disaster aid network

In this study, blockchain technology is implemented in the disaster aid network to address some of the limitations of centralized

communication systems. To enhance communication among the involved parties, a network structure based on blockchain technology is designed, where nodes represent clients and supply chain processes within the network. The disaster node, which receives a higher rate of input and has more complexity, is also included. Military, NGOs, industries, and government agencies interact with each other in a peer-to-peer (P2P) configuration, which allows real-time information and feedback to be gathered from the affected area. To prevent integrity attacks, nodes perform data encryption and hashing enabled by blockchain technology, and any abnormality is reported to the entire network. A tracking mechanism is employed to link updated information to the chain using the P2P validation process, which can increase trust within the system. This technique ensures that all valid participants of the network are aware of any changes and updates, leading to better transparency and transaction auditing. According to Hassan et al. (2019), this method can reduce the risks of fraudulent activities and enhance the accuracy of information. Matthew (2016) also suggests that blockchain technology can lead to better transparency and accountability.

DVFS algorithm integration to the proposed model

A large number of abnormal requests from one of the network's nodes, which can be a group of clients, indicates a disaster case on that node that can be detected and sorted using the DVFS algorithm. DVFS is a sorting process embedded in the server that enables the analysis of disaster management complexity. By sorting data on servers and evaluating the transaction power, the nodes on which the disaster has occurred can be identified based on the high rate of added data. The disaster response activities can be prioritized and allocated to network participants based on real-time information. Using two types of migration algorithms (i.e., local and external), the stored information can be linked to manage the network's enforced traffic load from the disaster node. Employing DVFS can alter the network that is bombarded with vast input data from the disaster zone and optimize the related costs. In token-based blocks, information will be rewritten only once. When the existing blocks on the servers located in the disaster area are rewritten, the monitoring cost would decrease to zero.

In this model, there are two main parts. The first part consists of a set of IoT nodes, representing the flow of the disaster, and is comprised of clients such as C1 and C2. A matrix is created to generate

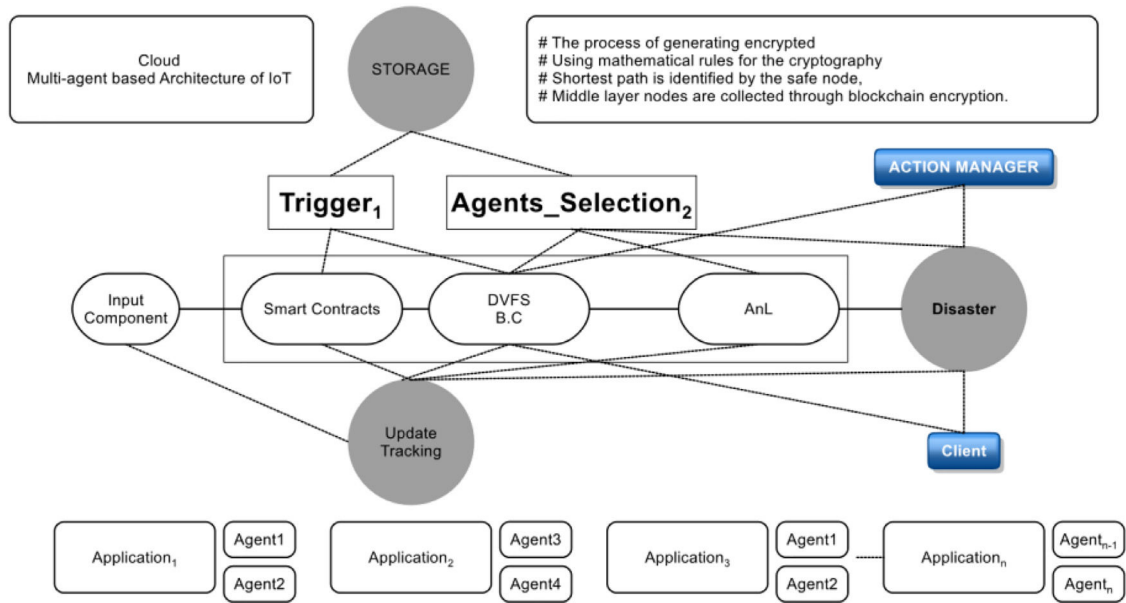


Fig. 1. The proposed model: Generating encryption for input components using smart contracts, Blockchain, DVFS, and MAS in the middle layer.

flows and simulate various disaster conditions. The second part explains the blockchain calculation mechanism applied to different chains, where DVFS is utilized to sort the queue of processes waiting for review. Physical and virtual machines are used to update the calculations within the queue, and the queuing algorithm is processed to determine the status of demands and enable their monitoring. Consequently, the entire network is transparent and can be audited by all participants.

The control stage is based on the agreements on the server, and in this phase, transactions are reviewed with DVFS, a processor is assigned to them, and a block is added to the chain. According to a study conducted by Perez-Sol'a et al. (2019), this method consists of two phases: queue development and coding and mining.

The process of generating encrypted information through cryptography is crucial. Once the secure node identifies the shortest path,

it collects the public keys of the middle layer nodes through blockchain encryption.

The conceptual model comprises three phases (as shown in Fig. 1). Numerous components are involved in generating input data for updating and tracking the network. The data are stored in the storage component, which is triggered and reviewed by the agents. Smart contracts are sorted using DVFS and then analyzed. Finally, the decision-making process is facilitated by MAS. The combination of these three steps constitutes the disaster stage, in which the entire response team can monitor the progress from different locations.

MAS application to the proposed model

The Multi-Agent System (MAS) enables the implementation of a natural metaphor for the meta-scheduling function, which is a

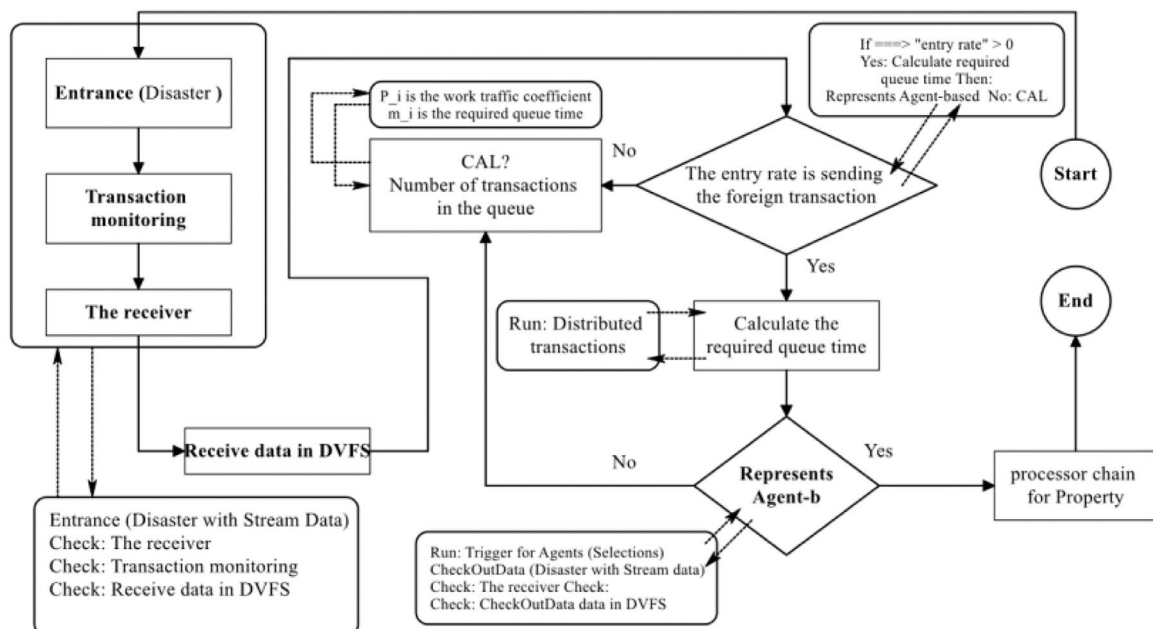


Fig. 2. The flowchart for executing the proposed model.

Table 2

Definition of indices used to develop the proposed model.

Index	Definition
e	The entrance rate of the stream to the network
e_k	The entrance rate of external transaction
Y_k	The number of requests to clients
i	The confirmation request rate (i.e., the number of confirmations)
t	Initial waiting time
C_{ai}	Square index for the external variety
C_{si}	Square index for the internal variety
P_i	Work traffic coefficient
m_i	The required queue time
W	Weight
Total W_i	Total weights applied to the network
P_{qi}	Probability of waiting in the queue
N_i	The number of transactions in the queue

practical tool to model a large number of entities with dynamic interactions between various agent teams and their collaborations (Buford et al., 2006). The main features of MAS are efficiency, flexibility, and reliability (Dorri et al., 2018). In the proposed model, data are stored in the storage component, activated with a trigger, and reviewed by intelligent agents. When MAS is activated, a binary agent-based condition considers the relationship between the updated tracking and action management. MAS also facilitates interactions between the entities within the network and exploration of the emergent behavior of the disaster. Each agent uses the system's objectives, actions' history, and interactions to make decisions to solve the allocated tasks. Finally, the developed conceptual model optimizes the receipt of all needs, periodizing and allocating tasks, monitoring response

activities, and making time transparent to the entire disaster response network. To execute the model, a flowchart is designed (Fig. 2). The intended indices in the equations are defined in Table 2, and the algorithm to execute the conceptual model is shown in Fig. 3.

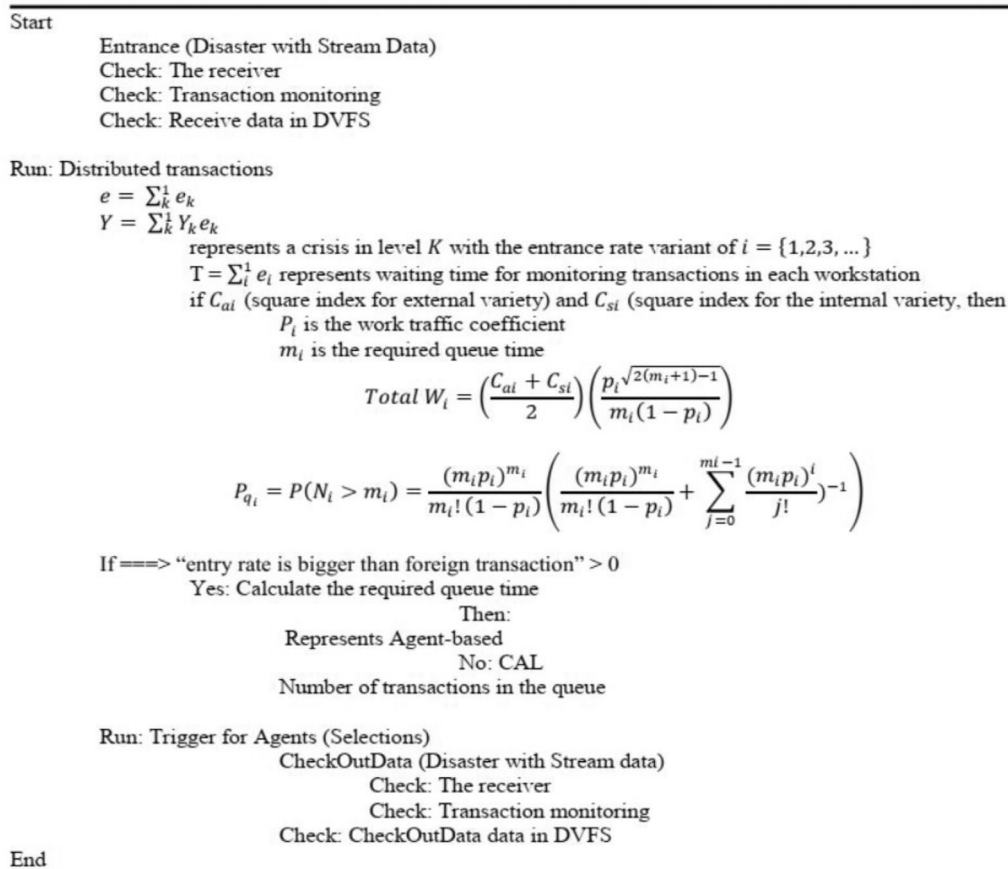
Simulation and results

In this study, two cases have been examined to evaluate the proposed model. The first case considers the proposed model using blockchain technology and the DVFS algorithm. The second case includes the multi-agent system (MAS) embedded in the proposed model. The flowchart of the model execution is depicted in Fig. 4. The study's results are compared with a published article titled "The Analysis of Resilience Strategies and Ripple Effect in Blockchain-coordinated Supply Chains (SCESHL)" (Lohmer et al., 2020) to validate the model and assess the improvements that it contributes to the existing body of knowledge.

We considered the reference model in two forms. The first form is the blockchain-coordinated supply chain model proposed by the authors, which uses the BeepBeep tool. For the second form, we combined this model with the DVFS algorithm to evaluate the differences. All the conditions executed in the simulations are shown in Table 3. To demonstrate the simulation results, we defined some metrics in Table 4 to evaluate the performance of all four scenarios, which are depicted below.

Successful migrations

Fig. 5 shows the number of successful migrations to virtual machines plotted against the number of events over time on the X

**Fig. 3.** The algorithm generated for the proposed model, including agents, triggers, and model execution steps.

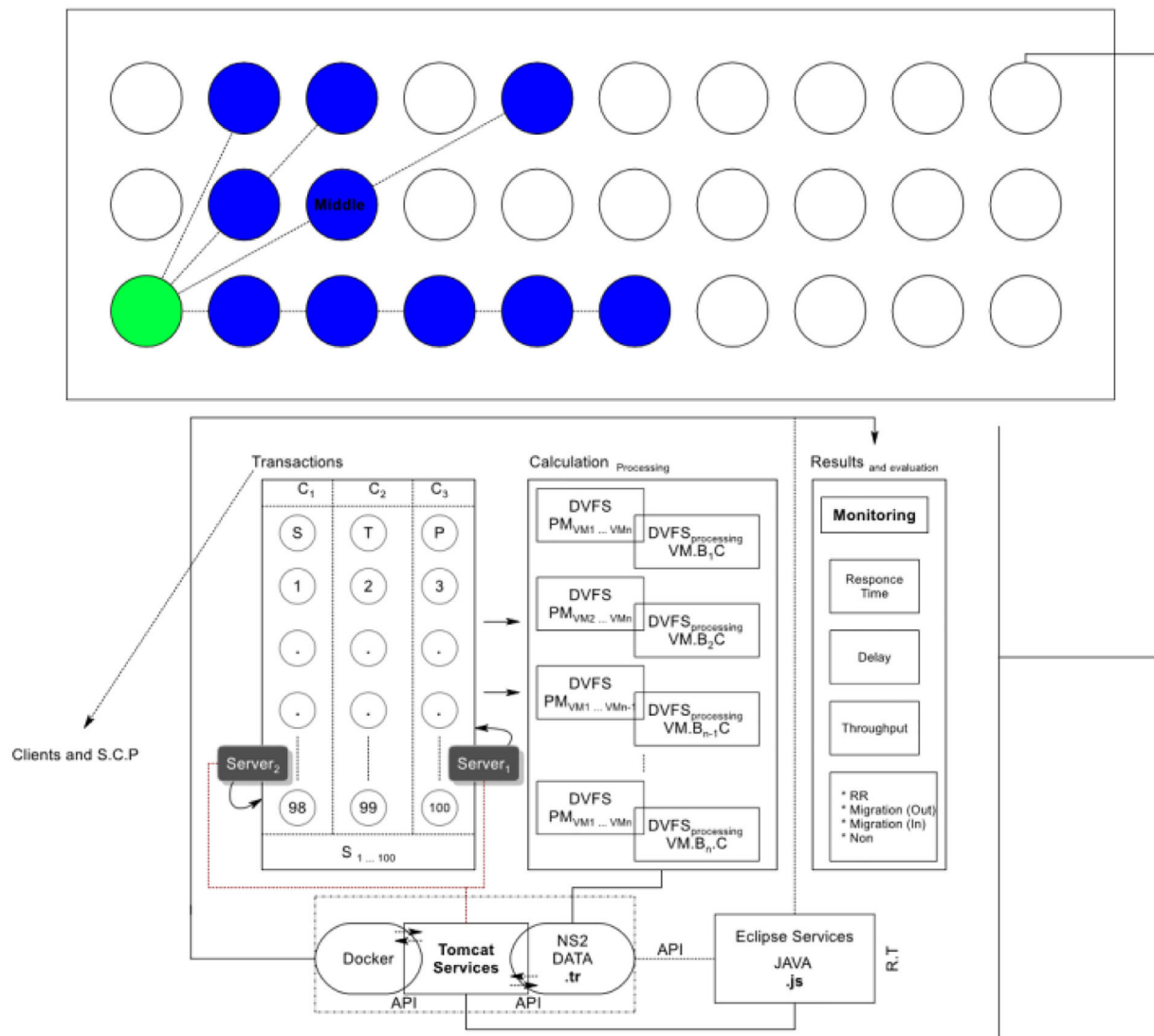


Fig. 4. Network diagram, including inputs, middle nodes, blockchain, and producing server for transactions.

Table 3

The conditions defined for the simulated scenarios.

Scenario	Condition
1	SCESHL Model
2	DVFS Algorithm embedded to the SCESHL Model
3	The Proposed Model (i.e., Blockchain-enabled DVFS-based)
4	The Proposed Model Advanced with MAS

Table 4

Performance evaluation metrics for the simulation scenarios.

Output	Description
Successful Migration	The number of transferred tasks from an overloaded node to the next block of the virtual machine with enough capacity to handle
Errors	The number of unsuccessful migrations of tasks handled by the virtual machines
Delay	Time, in minutes, required for handling the tasks in a blockchain-based method
Energy Consumption	The amount of energy, in kWh, needed to receive the requests and process them within the network

and Y-axes, respectively. Migration is the condition where actions are moved to the next block if the current block is overloaded until all virtual machines are used efficiently, especially in a heavy load of data traffic in the system. The proposed model shows more successful migrations of virtual machines compared to the reference model, indicating better performance and complexity management. As the number of events increases, the complexity of disaster management also increases. Thus, the system needs to perform more successful migrations of tasks to manage requests more effectively. One of the main differences between the two evaluated models is their input data. The reference model uses labeled agents simulated with Any-Logic, while the proposed model uses IoT nodes as the input data stream, i.e., demands from affected zones, which are then allocated as tasks to the virtual machines.

Errors

In Fig. 6, the Y-axis shows the error rate based on the number of actions and the functions producing those actions, while the X-axis represents the probability of failures of the actions. The blockchain-based processing line involves a high number of actions and complex timing. When the DVFS algorithm is applied in the second scenario, the error rate is improved by approximately 8% compared to the first

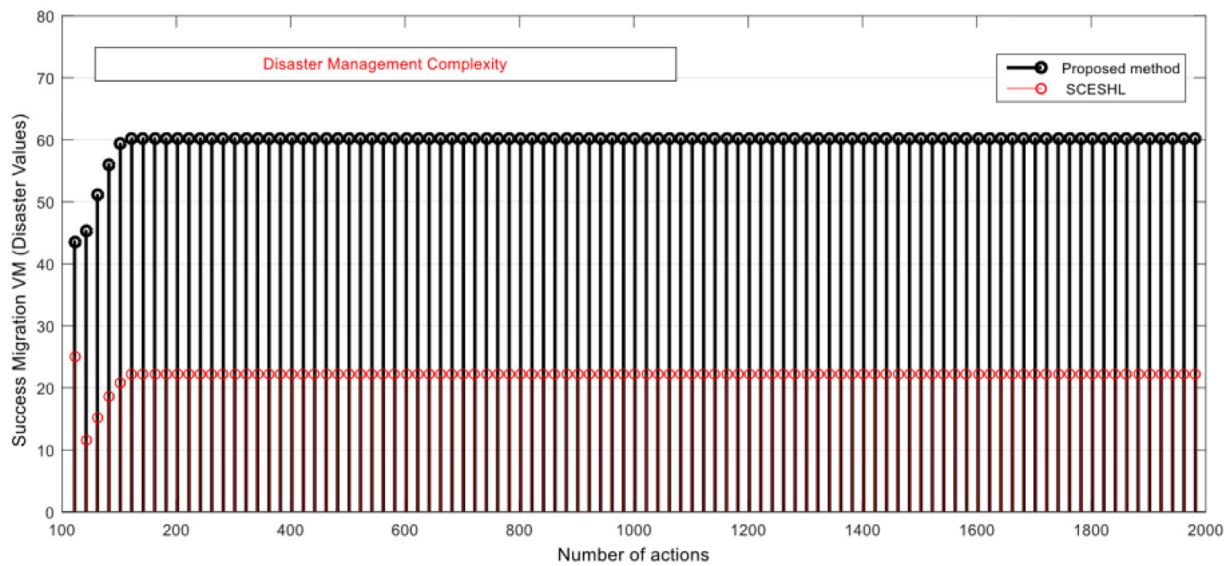


Fig. 5. Comparison of the proposed method against SCESHL regarding the number of successful migrations.

scenario. The last two scenarios have improved the error rates by 15% and 17%, respectively. The diagram shows that when the option of migration is available, the tasks (i.e., the demands requested from the affected population) can be handled more effectively, and the disaster can be managed more efficiently. As the errors in the system decrease, the delay time also decreases.

Delay

Fig. 7 shows the relationship between the number of actions/events in terms of the blockchain functions that handle the tasks (X-axis) and the delay time in minutes (Y-axis). The proposed model demonstrates less delay, which is attributed to fewer errors. The tasks entering the machines are processed at a faster pace in the third and fourth scenarios. In the fourth scenario, fewer errors and delays are indicated due to the improved management of the relationship

between the blockchain and DVFS using MAS. There is a 5% improvement in each scenario, from one to four.

Energy consumption

Fig. 8 depicts the energy consumption required to receive and process the requirement requests (i.e., actions) within the network to manage the allocated tasks. The Y-axis represents the energy consumption in kWh, and demonstrates that the proposed model follows green computing policies. The X-axis shows time in minutes, and illustrates that the proposed model is optimized around 9.12% higher compared to the referenced model. Initially, all the conditions have nearly identical results, which validate the network configurations. However, the proposed model uses a blockchain and DVFS-based algorithm that consumes less power than the referenced model. This diagram confirms that the proposed model provides more efficient results while consuming minimum energy, thereby indicating that the computation

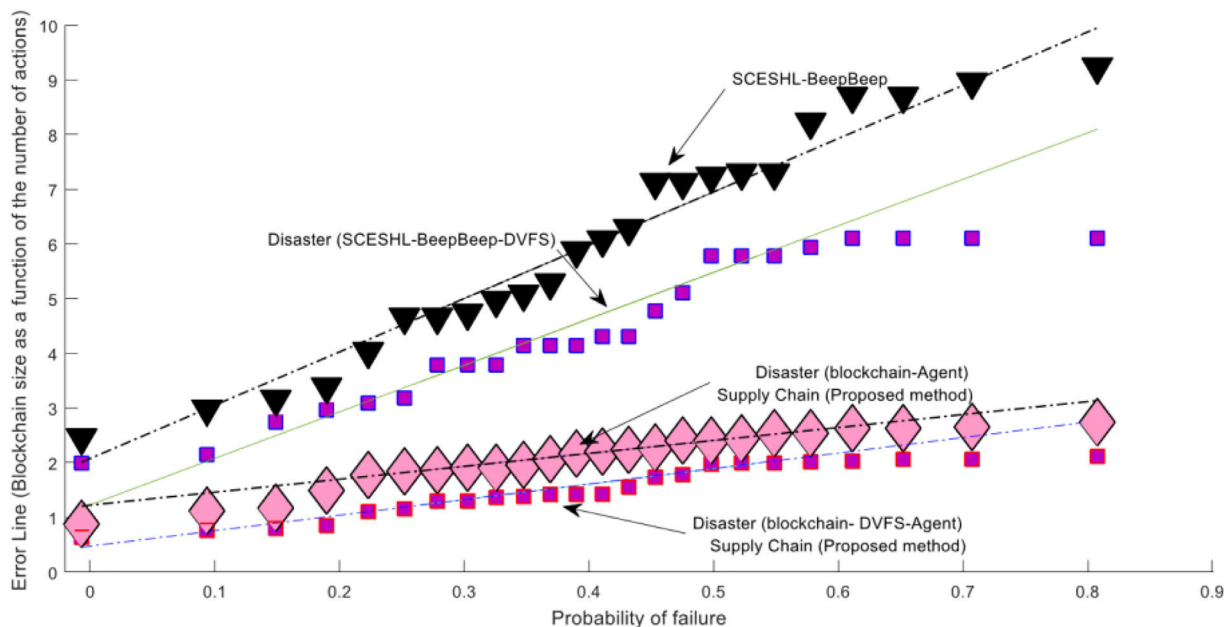


Fig. 6. Comparison of the probability of failure for events and their functions of the two models.

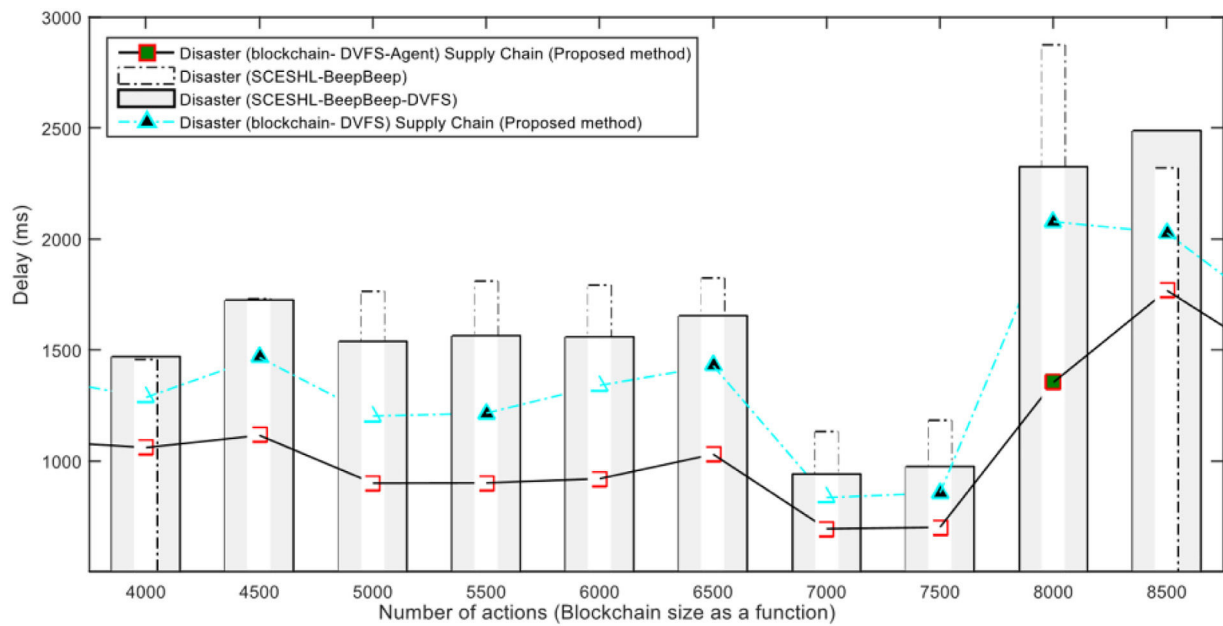


Fig. 7. The delay rate for the tasks received as the demands in all scenarios of both models.

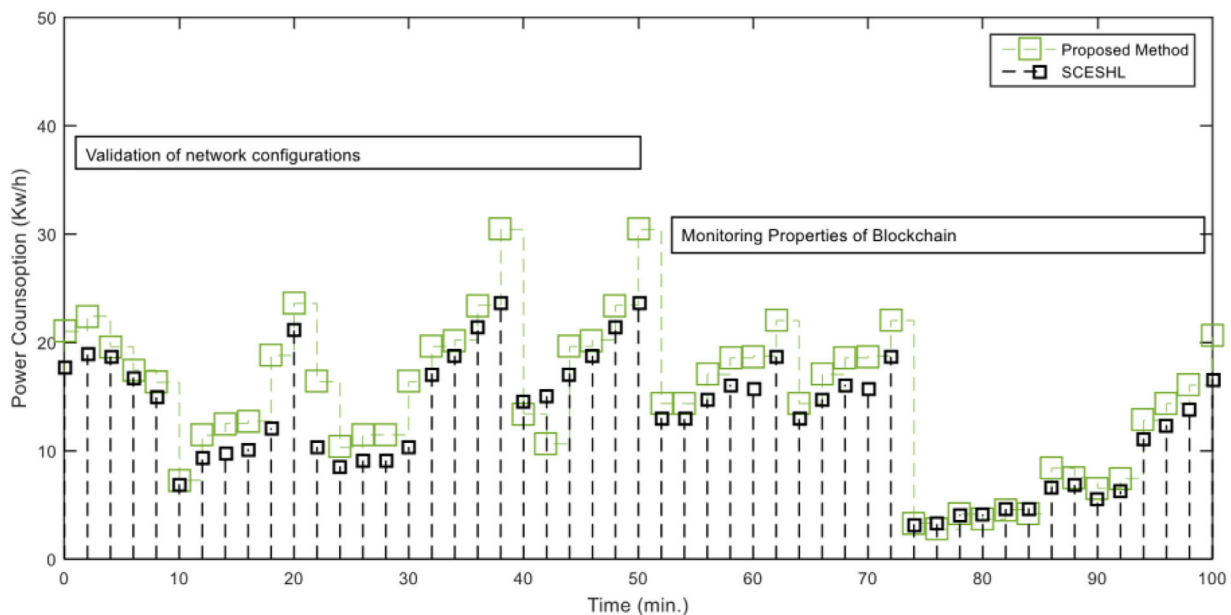


Fig. 8. The amount of energy consumption for handling the tasks in each time interval for both models.

complexity of the proposed model is lower than that of the referenced model. The simulation results validate that the proposed model is more efficient, has a lower rate of failures and delays in the entire network, and is optimized for energy consumption

Discussion and conclusion

The study's results demonstrate that implementing an integrated model that utilizes both blockchain and DVFS can improve the performance of a disaster supply network. The simulation results support the research questions by showing a positive correlation between response time, supply provisions, and a decentralized network that facilitates real-time information sharing. Additionally, the proposed method outperforms the reference model by improving successful task migrations by more than 30%, reducing errors by 17%, decreasing delays by 15%, and consuming 9% less energy.

Furthermore, the simulation results confirm a significant enhancement in the performance, monitoring, and complexity management of the disaster aid network.

Method implication

The proposed method demonstrates the potential applicability of blockchain technology in disaster aid management and supports a comprehensive analysis of its impact on disaster management resilience. The quantitative simulation experiments provide insights into the functioning mechanisms of management complexities in responding to disasters, and the model can serve as a practical tool for handling large-scale disaster data. The study's findings offer valuable insights for other researchers and disaster response teams, highlighting the significant improvements achieved in disaster aid network performance, monitoring, and complexity management.

Limitations and future work

The article proposes an IoE (Internet of Everything) blockchain-based network knowledge management model for resilient disaster frameworks. The model aims to improve disaster management by enhancing the resilience of the disaster response network through real-time information sharing, optimized resource allocation, and efficient task management. The article discusses the limitations of current disaster management systems and highlights the potential of blockchain technology to overcome these limitations. It provides an overview of the IoE concept and its integration with blockchain technology to enable real-time information sharing and efficient resource allocation. The proposed model combines blockchain technology with Dynamic Voltage and Frequency Scaling (DVFS) to optimize resource utilization and reduce energy consumption. The model uses a Multi-Agent System (MAS) to manage the relationship between the blockchain and DVFS. The article describes the simulation experiments conducted to evaluate the performance of the proposed model. The simulation results indicate significant improvements in successful task migrations, reduced errors and delays, and optimized energy consumption. The article also highlights some limitations of the proposed model, including the cost of running full nodes, latency in transaction confirmation, and slower transaction processing compared to traditional payment systems. The article suggests further research to address these limitations and explore the role of legal counsel and governance in DLT-based disaster management frameworks. Overall, the article presents a promising approach to improving disaster management through the integration of blockchain technology and IoE concepts. The proposed model has the potential to enhance the resilience of disaster response networks, optimize resource utilization, and reduce energy consumption. The current application of distributed ledger technology (DLT) in the humanitarian sector has some limitations, mainly due to the absence of robust regulatory frameworks, which can result in multiple legal frameworks. Therefore, further research is needed to explore the role of legal counsel within each phase of a disaster management project (Coppi & Fast, 2019). Additionally, there is a lack of clarity regarding the responsibilities of DLT applications in the humanitarian sector. Another challenge is the knowledge gap regarding governance and ethics related to DLTs. There are also some limitations of blockchain technology. First, the operation and maintenance costs of running full nodes can be significant. Second, there may be major latency issues with transaction confirmation processes. Third, the transaction processing speed may be slower compared to traditional payment systems. Finally, the consensus mechanism requires the entire network to perform complex algorithms for mining (Rajan, 2018).

Acknowledgements

This work was supported in part by the Joint Funds of the National Natural Science Foundation of China (Grant No. U22A2036), the Shenzhen Colleges and Universities Stable Support Program No. GXWD20220817124251002, Guangdong Provincial Key Laboratory of Novel Security Intelligence Technologies (2022B121010005).

References

Altay, N., & Green, W. G., III (2006). Or/ms research in disaster operations management. *European journal of operational research*, 175(1), 475–493.

Aslam, J., Saleem, A., Khan, N. T., & Kim, Y. B. (2021). Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *Journal of Innovation & Knowledge*, 6(2), 124–134.

Balcik, B., & Beamon, B. M. (2008). Facility location in humanitarian relief. *International Journal of logistics*, 11(2), 101–121.

Betti, Q., Montreuil, B., Khoury, R., & Halle, S. (2020). Smart contracts-enabled simulation for hyperconnected logistics. *Decentralised internet of things* (pp. 109–149). Springer pages.

Bufo, J. F., Jakobson, G., & Lewis, L. (2006). Multi-agent situation management for supporting large-scale disaster relief operations. *International Journal of Intelligent Control and Systems*, 11(4), 284–295.

Calheiros, R. N., & Buyya, R. (2014). Energy-efficient scheduling of urgent bag-of-tasks applications in clouds through dvfs. In *Proceedings of the 2014 IEEE 6th international conference on cloud computing technology and science* (pp. 342–349). IEEE pages.

Coppi, G. and Fast, L. (2019). Blockchain and distributed ledger technologies in the humanitarian sector. Technical report, HPG Commissioned Report.

Day, J. M., Melnyk, S. A., Larson, P. D., Davis, E. W., & Whybark, D. C. (2012). Humanitarian and disaster relief supply chains: A matter of life and death. *Journal of Supply Chain Management*, 48(2), 21–36.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2018). Multi-agent systems: A survey. *IEEE access : practical innovations, open solutions*, 6, 28573–28593.

Dubey, R., Gunasekaran, A., Bryde, D. J., Dwivedi, Y. K., & Papadopoulos, T. (2020). Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *International Journal of Production research*, 58(11), 3381–3398.

Fitwi, A. H., Nagothu, D., Chen, Y., & Blasch, E. (2019). A distributed agentbased framework for a constellation of drones in a military operation. In *Proceedings of the 2019 Winter Simulation Conference (WSC)* (pp. 2548–2559). IEEE pages.

Glik, D. C., et al. (2007). Risk communication for public health emergencies. *Annual review of public health*, 28, 33.

Goswami, S., Chakraborty, S., Ghosh, S., Chakraborty, A., & Chakraborty, B. (2018). A review on application of data mining techniques to combat natural disasters. *Ain Shams Engineering Journal*, 9(3), 365–378.

Gu, L., Zeng, D., Barnawi, A., Guo, S., & Stojmenovic, I. (2014). Optimal task placement with qos constraints in geo-distributed data centers using dvfs. *IEEE Transactions on Computers*, 64(7), 2049–2059.

Haghani, A., Afshar, A.M., et al. (2009). Supply chain management in disaster response.

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, 97, 512–529.

Holguín-Veras, J., Perez, N., Ukkusuri, S., Wachtendorf, T., & Brown, B. (2007). Emergency logistics issues affecting the response to katrina: A synthesis and preliminary suggestions for improvement. *Transportation research record*, 2022(1), 76–82.

Ilbiz, E. (2020). Blockchain: A new disruptive innovation for knowledge risk management. *Knowledge risk management* (pp. 119–132). Springer pages.

Imran, M., Castillo, C., Diaz, F., & Vieweg, S. (2015). Processing social media messages in mass emergency: A survey. *ACM Computing Surveys (CSUR)*, 47(4), 1–38.

Jahre, M., & Jensen, L. M. (2010a). Coordination in humanitarian logistics through clusters. *International Journal of Physical Distribution & Logistics Management*.

Jahre, M., & Jensen, L. M. (2010b). Coordination in humanitarian logistics through clusters. *International Journal of Physical Distribution & Logistics Management*, 40, 657–674.

Javadpour, A., Pinto, P., Ja'fari, F., & Zhang, W. (2022). Dmaids: A distributed multi-agent intrusion detection and prevention system for cloud iot environments. *Cluster computing* (pp. 1–18) pages.

Lohmer, J., Bugert, N., & Lasch, R. (2020). Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study. *International journal of production economics*, 228, 107882.

Luna, S., & Pennock, M. J. (2018). Social media applications and emergency management: A literature review and research agenda. *International journal of disaster risk reduction*, 28, 565–577.

Mackey, T. K., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert opinion on drug safety*, 16(5), 587–602.

Majchrzak, A., Jarvenpaa, S. L., & Hollingshead, A. B. (2007). Coordinating expertise among emergent groups responding to disasters. *Organization science*, 18(1), 147–161.

Matthew (2016). Colored coins: Bitcoin, blockchain, and land administration.

Mohammed, I. A. (2019). A systematic literature mapping on secure identity management using blockchain technology. *International Journal of Innovations in Engineering Research and Technology*, 6(5), 86–91.

Othman, S. B., Zgaya, H., Dotoli, M., & Hammadi, S. (2017). An agent-based decision support system for resources' scheduling in emergency supply chains. *Control Engineering Practice*, 59, 27–43.

Papadopoulos, T., Gunasekaran, A., Dubey, R., Altay, N., Childe, S. J., & FossoWamba, S. (2017). The role of big data in explaining disaster resilience in supply chains for sustainability. *Journal of Cleaner Production*, 142, 1108–1118.

Perez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2019). Double-spending prevention for bitcoin zero-confirmation transactions. *International Journal of Information Security*, 18(4), 451–463.

Pour, F. S. A. (2021). *Application of a blockchain enabled model in disaster aids supply network resilience*. PhD thesis, Old Dominion University.

Rajan, S. G. (2018). *Analysis and design of systems utilizing blockchain technology to accelerate the humanitarian actions in the event of natural disasters*. PhD thesis, Massachusetts Institute of Technology.

Sakurai, M., & Murayama, Y. (2019). Information technologies and disaster management—benefits and issues. *Progress in Disaster Science*, 2, 100012.

Sangaiah, A. K., Javadpour, A., Ja'fari, F., Pinto, P., Ahmadi, H., & Zhang, W. (2022a). Cmlsp: The design of a detection mechanism for sinkhole attacks in smart cities. *Microprocessors and Microsystems*, 90, 104504.

Sangaiah, A. K., Javadpour, A., Pinto, P., Ja'fari, F., & Zhang, W. (2022b). Improving quality of service in 5g resilient communication with the cellular structure of smart-phones. *ACM Transactions on Sensor Networks (TOSN)*.

- Schipper, L., & Pelling, M. (2006). Disaster risk, climate change and international development: Scope for, and challenges to, integration. *Disasters*, 30, 19–38.
- Scholten, K., Sharkey Scott, P., and Fynes, B. (2014). Mitigation processes – antecedents for building supply chain resilience capabilities. *Supply chain management*, 19.
- Shirvani, M. H., Rahmani, A. M., & Sahafi, A. (2020). A survey study on virtual machine migration and server consolidation techniques in dvfs-enabled cloud datacenter: Taxonomy and challenges. *Journal of King Saud University-Computer and Information Sciences*, 32(3), 267–286.
- Stewart, S. T., & Leinhardt, Z. M. (2009). Velocity-dependent catastrophic disruption criteria for planetesimals. *The Astrophysical Journal*, 691(2), L133.
- Tomasini, R., & Van Wassenhove, L. (2009). From preparedness to partnerships: Case study research on humanitarian logistics. *International Transactions in Operational Research*, 16, 549–559.
- Verma, M. (2021). Amalgamation of blockchain technology and knowledge management system to fetch an enhanced system in library. *International Journal of Innovative Research in Technology*, 7(11), 474–477.
- Xu, C., Wang, K., & Guo, M. (2017). *Intelligent resource management in blockchain-based cloud datacenters*: 4 (pp. 50–59). IEEE Cloud Computing.