Research on the Application of Blockchain Technology in Online Public Opinion Risk Management Systems: Postprint

Authors: Guo Sulin, Huang Wei, Li Ji

Date: 2023-04-01T16:15:53+00:00

Abstract

[Purpose/Significance] To explore the application value of resilience management and blockchain theory in constructing online public opinion risk management systems, overcome the technical limitations of traditional management systems, address the critical challenges and pain points in existing online public opinion risk management, and enhance management efficiency. [Method/Process] Based on online public opinion risk management and resilience management theory, this study establishes a theoretical framework for resilient risk management of online public opinion. It then proposes an online public opinion risk management system architecture using blockchain technology, and provides detailed elaboration on the intelligent ledger for risk identification and perception, risk association trees, and smart contracts. [Results/Conclusion] The constructed public opinion risk management system, blockchain data assurance system architecture, and blockchain-enabled intelligent ledger for online public opinion risk identification and perception, risk association trees, and smart contracts, make risk management data more secure and traceable while strengthening organizational resilience and adaptability. This can effectively guide relevant system development, enhance the controllability of online public opinion risk management, and improve management efficiency.

Full Text

Research on the Application of Blockchain Technology in Network Public Opinion Risk Management Systems

Guo Sulin, Huang Wei, Li Ji

School of Management, Jilin University, Changchun 130022

Abstract

[**Purpose/Significance**] This study explores the application value of resilient management and blockchain theory in constructing network public opinion risk management systems, aiming to overcome the technical limitations of traditional management systems, address existing challenges and pain points in network public opinion risk management, and improve management efficiency.

[**Method/Process**] Based on network public opinion risk management and resilient management theory, we establish a theoretical framework for resilient risk management of network public opinion. We then propose a network public opinion risk management system architecture using blockchain technology, and elaborate in detail on the intelligent ledger for risk identification and perception, risk association trees, and smart contracts.

[**Result/Conclusion**] The constructed public opinion risk management system and blockchain data guarantee architecture, along with the blockchain-based intelligent ledger for risk identification and perception, risk association trees, and smart contracts, make public opinion risk management data more secure, traceable, and organizationally adaptable. This can effectively guide relevant system development, enhance the controllability of network public opinion risk management, and improve management efficiency.

Keywords: blockchain; network public opinion; risk management

1. Introduction

Since blockchain technology was first proposed in 1991, it has taken root and flourished in numerous fields with its unique appeal. From Blockchain 1.0 represented by Bitcoin, to Blockchain 2.0 based on smart contracts such as Ethereum, and now to the more industrially valuable "Blockchain ×" applications, blockchain scenarios have gradually expanded, bringing disruptive changes and breakthrough innovation space to various industries [1]. Applying blockchain technology to network public opinion management and risk perception/identification can reconstruct the public opinion information ecosystem, increase the value density of public opinion information, eliminate false information dissemination, strengthen user privacy protection, and provide a solid foundation for effective public opinion risk response.

Therefore, based on existing blockchain and network public opinion management theories, and targeting the difficulties and pain points in network public opinion management, we propose a blockchain-based network public opinion risk management system to address three theoretical and practical issues: First, how to establish a theoretical framework for network public opinion risk perception and identification based on risk management and network public opinion management theories? This addresses key challenges such as system resilience in public opinion risk management, improvement of perception and identification

accuracy, risk analysis accuracy, sustainability of dynamic response, construction of big risk correlation databases, and immediate response during control windows. Second, how to construct a network public opinion risk management system architecture based on blockchain and network public opinion management theories? This solves functional issues including data integrity, authentication, independent third-party review, management audit and accountability, data updates, and resource adequacy, while compensating for traditional system defects like low data security, difficulty ensuring authenticity, and vulnerability to loss or damage. Third, how to design intelligent ledgers, risk association trees, and smart contracts for network public opinion risk management based on blockchain theory? This addresses data traceability and tampering, data support for risk-sharing mechanisms, risk tracking, performance design, accuracy of major risk analysis, improvement of early warning levels, and automated response capabilities.

In the converged media environment, public opinion information spreads faster, impacts wider areas, and exhibits stronger destructive power through online-offline integration. When public opinion themes involve emergencies or socially sensitive incidents, they are more likely to trigger large-scale mass incidents or even crises that threaten the construction of a harmonious society, creating unprecedented pressure and challenges for governments and regulatory agencies in effectively responding to public opinion risks. In the processes of identification, analysis, and response, accurate identification based on risk perception is particularly crucial.

2. Literature Review

2.1 Research Status of Blockchain Technology

As a technological revolution in the 21st century, blockchain's core advantages lie in decentralization and providing solutions to traditional centralized model problems—including information security, inefficient trust, and high interaction costs—through chain data structure encryption, timestamps, proof of work, and consensus mechanisms [3]. Blockchain architecture has no central server and generally includes five components: distributed networks, underlying data, distributed ledgers, consensus mechanisms, and network applications [4]. All nodes maintain a trustless peer-to-peer relationship, databases are immutable, non-forgeable, and irrevocable, and all data is traceable [5]. The underlying data stored in block form is verified based on consensus mechanisms [6], which can create new blocks and allow agents to record system states in transaction order through timestamps. In any scenario, the characteristic that block creation requires cost effectively curbs spam production, significantly enhances system security, destroys the soil for false information propagation, and mitigates intermediary conflicts to create win-win situations.

With the gradual deepening of blockchain application scenarios, blockchain research has also made considerable progress. H. W. Kim et al. [7] used blockchain

technology to enhance mobile storage device computing power and capacity, building a mobile device resource information chain based on resource authentication. M. E. Greiner [8] introduced the concept of trust-free systems and proposed solutions to trust issues in peer-to-peer systems, suggesting that traditional trust mechanisms established through costly trusted intermediaries will be replaced by cryptographic protocols based on decentralized algorithms and smart contracts. E. Dmitry et al. [9] noted that blockchain technology's use of public key encryption and peer-to-peer networks to solve trust problems will disrupt many industries. R. Beck et al. [10] applied this concept to business systems from a blockchain perspective, developing a conceptual prototype of a transaction system that operates autonomously based on consensus rules without mutual trust. However, the trust-free concept remains controversial; some scholars argue that trust is not eliminated but transferred from central authorities, or that market trust requires recognition of algorithmic authority that ultimately controls agent interactions [11]. Additionally, understanding the technical protocols and implementations of distributed ledgers and decentralized consensus systems, as well as decentralized applications, remains complex, requiring researchers and practitioners to fully explore and realize blockchain's potential.

2.2 Research Status of Network Public Opinion Risk Management

In risk management, risk identification is built upon risk perception [12]. Network public opinion risk perception refers to people's analysis and judgment of various risks that online public opinion may bring to netizens and society from a decision-support perspective. Public opinion risk identification systematically and continuously summarizes the propagation characteristics and patterns of potentially destructive public opinion events using various methods to discover key factors affecting public opinion trends, identify critical time nodes, and discover opinion leaders, thereby providing solid support for subsequent risk response.

Currently, scholars mainly analyze factors affecting individual public opinion event risk perception from the perspective of ordinary netizens. For example, Wang Lian and Jia Jianmin [13] used network search as an indicator of netizens' risk perception levels, employing keyword analysis to examine the dynamic characteristics of risk perception from spatial distribution and temporal evolution dimensions. A. Sugimoto et al. [14] took the Fukushima nuclear leak as an example, establishing a multiple regression model based on extensive qualitative material analysis from seminars and questionnaire surveys, revealing potential connections between media consumption and public risk perception. In public opinion risk evaluation, Zhang Yuliang [15] constructed a three-level evaluation index system for emergency network public opinion risk based on risk analysis, using the analytic hierarchy process for empirical research. Zeng Runxi et al. [16] proposed evaluating network social security risks from political, economic, cultural, social, and ecological perspectives. In comprehensive

public opinion risk identification, many scholars advocate interdisciplinary research combining management, information science, and life sciences [17]. Wang Wenyan et al. [18] used the "3.1 Kunming Terrorist Attack" as an example, pointing out from a practical perspective that group polarization tendencies, media guidance strength, and government credibility levels are key elements in identifying public opinion risks. Chen Peiyou [19] used grey fuzzy evaluation to construct a social network public opinion risk early warning model for the "Chongqing Bus Plunge Incident." L. Yu et al. [20] established a multi-agent simulation model from four information subjects—netizens, opinion leaders, government, and mass media—pointing out that dissemination speed, scope, and information disclosure degree affect risk identification and handling effectiveness. Zeng Runxi [21] proposed new paths for network public opinion governance from social and technical environments under a non-traditional security perspective.

2.3 Research Status of Blockchain Technology in Network Public Opinion Information Management

As mentioned earlier, few scholars have conducted research on network public opinion management systems based on blockchain theory, and even fewer have deeply studied public opinion risk perception and identification issues. Nevertheless, scholars domestically and internationally generally agree that applying blockchain technology to information management and network public opinion management can eliminate false information, increase information value density, establish trust between information producers and consumers, and enable information traceability, thereby reconstructing the network information ecosystem and improving management efficiency and information security/privacy protection. M. Arquam [22] constructed a secure and trusted network information propagation framework based on blockchain, where each node propagates information to peers based on reliability, and node credibility changes according to respective information. Information producers and consumers establish trust through two methods: local trust where same-level users share information, and global trust based on credibility check results from the model. The framework achieved 83% accuracy when analyzed using Facebook datasets. S. Ma et al. [23] emphasized that information management processes should focus on risk and information system control, requiring assessment of the possibility and severity of social impacts from network events to determine response strategies. They proposed a blockchain-based information risk and information system control framework using Merkle trees to design risk association trees that combine risk project ledgers, risk analysis ledgers, and risk response ledgers into proposed smart contracts for risk identification, analysis, response, monitoring, guidance, and reporting, and developed a system prototype. H. D. Huang et al. [24] noted that while many countries including the US, South Korea, and China have issued warnings and regulations about digital virtual currency, the risks and fraud behind blockchain virtual currency cannot be ignored, and Ethereum smart contract security has not received sufficient attention. Their team pro-

posed a machine learning method for sentiment analysis of Ethereum community comments, building an LSTM+CNN model that achieved over 0.80 accuracy in analyzing and predicting netizen emotions based on cryptocurrency comments collected from social networks.

Existing domestic research mainly focuses on the significance and practicality of blockchain technology in network public opinion management. Zhao Dan et al. [25] used Steemit platform data to analyze characteristics and patterns of blockchain-based public opinion propagation, concluding that the ecosystem is more harmonious. Bin Sheng et al. [26] built upon this work, constructing a SEIR model for network public opinion propagation in blockchain environments based on epidemic and game theories, using Steemit data for simulation to analyze how incentive mechanisms and risk-reward mechanisms affect propagation. Huang Xinhao and Zhao Bo [27] studied network opinion optimization using blockchain technology, noting its effective application in traceability, circuit-breaking mechanisms, and emotion early warning systems. Chen Hejie and Yan Qiang [28] suggested publishers should use advanced network tools to monitor public opinion events, analyzing the relationship between blockchain hot events and publishing planning/sales. Ding Xiaowei and Gao Shuping [29] studied financial risks from virtual currency public opinion, finding that blockchain-supported virtual currency public opinion is exceptionally active, requiring strengthened financial regulation and opinion guidance. Li Tai'an [30] affirmed blockchain's positive role in improving the network opinion environment, believing it can form joint forces in copyright protection, fake news combat, privacy protection, and information desensitization to highlight quality content and reconstruct the opinion environment.

3. Conceptual Framework for Network Public Opinion Risk Management System

To overcome existing bottlenecks in network public opinion risk management using blockchain technology, we design a resilient risk management system. This section builds upon relevant literature, following the research 脉络 from traditional risk management theory to resilient risk management theory, and then to the design of a network public opinion resilient risk management framework. Risk management is viewed as a continuous management behavior requiring accurate prediction of risk event impacts and striving to maximize opportunities through effective risk management and control frameworks, thereby reducing potential losses to organizational assets [31]. Traditional risk management theory can address quantifiable risks and predictable threats, but in the rapidly changing network environment, network public opinion risks have greater potential impact and higher uncertainty. It is impossible for management entities to address all risks, or the cost would be prohibitively high. Resilient risk management theory emphasizes "predicting and adapting to changes in highly uncertain environments, absorbing and recovering from a wide range of risk events, and seizing opportunities implied in risk events [32]," making it more

theoretically adaptable for public opinion risk perception and identification in converged media environments. When the network public opinion ecological environment changes, the "management resilience" that stays away from high variability and self-adaptability of public opinion equilibrium events can better empower the system to bear and manage risks.

Network public opinion risks have dual impacts on the realization of management objectives. The control objective of public opinion risk management information systems is to discover potential risks, bear them appropriately, and ensure they are reduced to acceptable levels, enabling management entities to flexibly select appropriate response strategies and action plans after risk identification and analysis. Public opinion risk reports must be regularly monitored and reported to management entities, tracking risk development trends, legitimacy, and existing problems. Meanwhile, changes in internal and external opinion environments, technological progress, and evolution of other risk elements require management entities to dynamically review risk management work, reanalyze risks, and even revise response plans. Continuous dynamic monitoring and control, construction of risk correlation databases, effective identification of risk data, and immediate response during control windows all highlight the advancement of the resilient risk management system conceptual framework, as shown in Figure 1 [Figure 1: see original paper].

4. Blockchain-Based Network Public Opinion Risk Management System

From a non-functional requirements perspective, existing risk management information systems in various fields share three common defects: First, low data security. Even in risk management cloud platforms, business data security remains problematic, with database hacking potentially causing immeasurable losses. Second, difficulty ensuring data authenticity. Electronic data can be tampered with or deleted without trace, while manual authenticity review consumes manpower and involves subjectivity. Third, vulnerability to data loss and damage. Risk stakeholders can easily lose or damage data during storage and utilization. A blockchain-based public opinion risk management system features tamper-proof, traceable, and decentralized storage data, eliminating database hacking risks, minimizing business data leakage possibilities, and leaving traceable trails even if leakage occurs. Critical data is no longer centrally stored in individual institutions but through blockchain P2P storage, reducing loss/damage possibilities and greatly improving security. Blockchain intelligent ledgers and smart contracts classify, compare, and execute electronic data and management processes (transactions), improving efficiency and reducing subjectivity. From a functional perspective, rampant false information in social networks forces institutions to invest substantial time and economic costs in authenticity verification, urgently requiring a powerful, secure, and trusted public opinion risk management system. Moreover, all stages of public opinion risk management—including perception/identification, analysis, response, and reporting—require

accountability, monitoring, timely updates, and adequate resources. Blockchain technology effectively supports the conceptual framework for public opinion risk management.

Based on this analysis, we propose a network public opinion risk management architecture comprising two cross-supporting subsystems: the public opinion risk management system and the blockchain data guarantee system, as shown in Figure 2 [Figure 2: see original paper].

4.1 Public Opinion Risk Management System

The public opinion risk management system framework follows the public opinion evolution lifecycle. System resilience optimization is the initial stage, involving setting risk appetite values, establishing zero-risk items, flexibly configuring and integrating internal/external resource elements, and building effective coordination mechanisms. The framework includes four functional modules: (1) Public opinion risk perception and identification. This module perceives, identifies, and records risks based on evolution elements, perception/identification models, and risk appetite thresholds. It identifies not only the risks themselves but also organizational risks, external dependencies, and assumptions such as management resilience, resource availability, and response timeliness. (2) Public opinion risk analysis. After risks are identified and recorded in the register, the system analyzes risk levels by examining latent, brewing, outbreak, decline, and extinction time nodes, calculating online/offline influence. The analysis must consider dependencies between management organizations and stakeholders, affected derivative opinions, and related users, sometimes even evaluating organizational credibility, control levels, possibilities of mass destructive events, and relationships between risk appetite and tolerance. (3) Public opinion risk response. The key lies in organizational resilience, timely perception/identification, accurate level assessment, and scientific response planning. This stage requires proposing effective, reasonable, and scientific decisions at appropriate time nodes with detailed implementation plans. (4) Public opinion risk reporting. Based on accurate perception, identification, monitoring, and analysis, management organizations no longer get lost in low-value-density complex data. Risk control is confined to reasonable, well-planned, and controllable contexts, where control performance indicators can greatly improve continuous monitoring efficiency and establish response archives through performance-level reports.

4.2 Blockchain Data Guarantee System

The blockchain data guarantee system uses blockchain technology to construct risk registers including risk identification, analysis, and response plans, storing risk identification, analysis, response, and reporting data in the blockchain to ensure traceability and tamper-proofing, thereby providing data support for risk-sharing mechanisms among management entities, netizens, and hardware. It dynamically tracks different risks based on association trees by risk level

and establishes intelligent public opinion risk ledgers. Smart contracts and performance tables are designed to improve accuracy in major risk analysis, enhance early warning levels, and increase automated response capabilities.

4.2.1 Blockchain-Based Intelligent Public Opinion Risk Ledger In public opinion risk smart contracts, the risk register is formed during risk identification and updated according to risk analysis and control processes. The intelligent ledger is divided into three categories (see Figure 3 [Figure 3: see original paper]): (1) Comprehensive risk project ledger with complete risk accounts from identification to response; (2) Risk analysis ledger for preserving evaluation level information of different risk event accounts; (3) Risk response ledger for preserving response program items of different risk event accounts under unique identifiers.

The blockchain-based intelligent public opinion risk ledger has ten key attributes: (1) Event ID. Unique identifiers enable managers to quickly locate specific risks, with brief thematic descriptions and performance annotations on response success/failure. (2) Event description. Supplementary information not covered by the ID. (3) Category. Classification according to standards such as emergencies, sensitive events, social, livelihood, and government affairs. (4) Trigger threshold. Thresholds that activate or terminate responses. (5) Status. Records of evolution states including latent, outbreak, decline, and extinction. (6) Risk level. Records according to the organization's "extremely high, high, moderate, low, none" scale. (7) Outbreak probability. Records based on analysis models. (8) Influence. Numerical influence values from analysis models, with actual impact recorded if events occur. (9) Response plan. Plans formulated from dimensions including positive response, verification, one-time response, dynamic response, monitoring, information analysis, responsibility division, and credibility restoration. (10) Management organization. Records of grassroots organizations, senior managers, spokespersons, and stakeholder groups.

4.2.2 Blockchain-Based Public Opinion Risk Association Tree The complete risk register includes risk analysis ledgers, risk response ledgers, and comprehensive risk ledgers. The risk association tree built upon blockchain Merkle trees establishes correspondence between ledgers through classification accounts, enabling fast, low-cost, and free location and retrieval of latest register information, as shown in Figure 4 [Figure 4: see original paper]. The transaction tree stores specific block transactions, the receipt tree stores detailed data of multiple transactions, and the risk association tree stores inclusion relationships among the three ledgers. The first two trees ensure data consistency and reduce client-side data storage levels, overcoming defects in traditional public opinion data management.

The risk association tree establishes relationships among the three ledgers that can be quickly correlated through hash values. In Figure 4 [Figure 4: see orig-

inal paper], Block 163845 writes risk analysis and response ledgers, while the comprehensive ledger is written to Block 163846. Risk events, analyses, and responses correlate based on risk hash values. Risk Event 22 obtains status data showing risk level 5 and outbreak state. During this process, each blockchain agent only needs to download corresponding block headers. For example, based on the comprehensive ledger for Event 22 in Block 163846, one can obtain hash values corresponding to risk analysis ID and response ID, then quickly locate Event 22's risk analysis and response data in Block 163845. Similarly, knowing the risk ID in the analysis ledger enables locating the comprehensive ledger on Block 163846 based on hash values.

4.2.3 Blockchain-Based Public Opinion Risk Smart Contracts The blockchain data guarantee system includes three smart contracts: (1) Smart Contract 1. Primarily responsible for key performance indicators and automatic KPI calculation; obtains event ID and type; acquires transaction ledgers, analysis ledgers, and response ledgers; obtains corresponding comprehensive ledgers; generates comprehensive ledger transaction blocks for consensus confirmation. (2) Smart Contract 2. Responsible for response level approval and dynamic adjustment; obtains event ID and type; acquires corresponding transaction ledgers and response ledgers; calculates response values; determines response level rules based on influence; for status-changed events, generates new comprehensive ledgers to terminate responses and calls Smart Contract 3 for consensus; establishes risk sets in response ledgers based on event IDs; forms systematic response plans based on changed approval levels; updates approval levels in comprehensive ledgers and submits for consensus. (3) Smart Contract 3. Responsible for status change confirmation; obtains event IDs; determines status changes in analysis or response ledgers based on blockchain transaction ledgers; acquires latest event IDs from comprehensive ledgers; judges whether to approve modifications to identification, response, and reporting statuses. If modification is not permitted, it generates pending status and reaches consensus on new comprehensive ledgers. If permitted, it submits for consensus confirmation.

5. Research Conclusions

Based on network public opinion risk management and resilient management theory, this study establishes a resilient risk management theoretical framework for network public opinion, proposes a blockchain-based risk management system architecture, and elaborates on the intelligent ledger for risk identification and perception, risk association trees, and smart contracts.

This research demonstrates innovation in both theoretical and practical aspects. Theoretically, it combines network public opinion risk management theory with resilient management theory to propose a resilient risk management framework, deepening the application of risk management theory in the network public opinion field. In constructing the system architecture, we designed public opinion

risk management and blockchain data guarantee subsystems, and detailed core blockchain applications including intelligent ledgers, risk association trees, and smart contracts. The value of resilient management and risk management theories is further excavated under blockchain support. Practically, the "management resilience" of the theoretical framework can effectively address high variability and self-adaptability in network public opinion equilibrium events, while blockchain applications overcome traditional system bottlenecks. Throughout the entire lifecycle of network public opinion risk management, the system makes management data more secure, traceable, organizationally adaptable, and efficient, effectively guiding relevant departments in developing blockchain-based systems and enhancing controllability and efficiency.

During the research process, due to the focus on applying blockchain to solve core public opinion risk management problems and space limitations, the constructed management system could not provide deeper design for the resilient risk management architecture. Future research will further develop the resilient risk management architecture design, develop a network public opinion risk management system using blockchain technology, and focus on solving the coordination of online-offline public opinion information interaction and interweaving, using typical cases to demonstrate the scientificity, advancement, and operability of the constructed system.

References

[1] LEE B H, LEE J H. Blockchain-based secure firmware update for embedded devices in an Internet of things environment[J]. Journal of supercomputing, 2017, 73(3): 1152-1167.

[2] CHAKRAVORTY A, RONG C. Ushare: user controlled social media based on blockchain[EB/OL]. [2019-09-27]. https://www.researchgate.net/publication/312211808_{{{Ushare}}{{use

[3] BUCHANAN N H. Social security is fair to all generations: demystifying the trust fund, solvency, and the promise to younger Americans[J]. Cornell journal of law & public policy, 2017, 27(2).

[4] UNDERWOOD S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11): 15-17.

[5] TAPSCOTT D, TAPSCOTT A. How blockchain will change organizations[J]. MIT sloan management review, 2017, 58(2): 10-.

[6] DORRI A, STEGER M, KANHERE S S, et al. BlockChain: a distributed solution to automotive security and privacy[J]. IEEE communications magazine, 2017, 55(12): 119-125.

[7] KIM H W, JEONG Y S. Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain[J]. Human-centric computing and information sciences, 2018, 8(1): 11-20.

[8] GREINER M E, WANG H. Trust-free systems-a new research and design direction to handle trust-issues in P2P Systems[C]//21st Americas conference on information systems, AMCIS2015. San Francisco: Curran Associates Inc, 2015: 1-16.

[9] DMITRY E, PAVEL R. The All-Pervasiveness of the blockchain technology[J]. Procedia computer science, 2018, 123(1): 116-.

[10] BECK R, CZEPLUCH J S, LOLlike N, et al. Blockchain-the gateway to trust-free cryptographic transactions[EB/OL]. [2019-09-27]. https://www.researchgate.net/publication/302589
{{{THE}}}{{GATEWAY}}}*{{{TO}}}*{{TRUST}}}-FREE_{{{CRYPTOGRAPHIC}}_{{TRANSACTIONS}}

[11] LUSTIG C, NARDI B. Algorithmic authority: the case of Bitcoin[C]//2015 48th Hawaii international conference on system sciences. New York: IEEE, 2015: 743-752.

[12] Li Huaqiang, Fan Chunmei, Jia Jianmin, et al. Public risk perception and emergency management in sudden disasters: a case study of the 5·12 Wenchuan Earthquake[J]. Management world, 2009(6): 52-60, 187-188.

[13] Wang Lian, Jia Jianmin. Dynamic characteristics of risk perception in sudden disaster events: evidence from web search[J]. Management review, 2014, 26(5): 169-176.

[14] SUGIMOTO A, NOMURA S, TSUBOKURA M, et al. The relationship between media consumption and health-related anxieties after the Fukushima Daiichi nuclear disaster[J]. PLOS ONE, 2013, 8(8): e65331.

[15] Zhang Yuliang. Risk evaluation index system for emergency network public opinion based on occurrence cycle[J]. Information science, 2012, 30(7): 1034-1037, 1043.

[16] Zeng Runxi, Luo Junjie, Zhu Meiling. Research on network social security risk evaluation index system[J]. E-government, 2019(3): 36-45.

[17] Ma Ning, Liu Yijun, Lian Ying. Literature review on public opinion risk research in emergencies[J]. Journal of intelligence, 2019, 38(6): 88-94.

[18] Wang Wenyan, Liu Zhen, Wang Qiuju. Weibo public opinion risk identification and prevention measures: a case study of the "3.1 Kunming Terrorist Attack"[J]. News world, 2014(8): 179-180.

[19] Chen Peiyou, Hou Tiantian. Social network public opinion risk early warning research based on ANP-grey fuzzy evaluation: a case study of the "Chongqing Bus Plunge Incident"[J]. Information science, 2019, 37(5): 115-120.

[20] YU L, LING L, LING T. What can mass media do to control public panic in accidents of hazardous chemical leakage into rivers? a multi-agent-based online opinion dissemination model[J]. Journal of cleaner production, 2017, 143(1): 1203-1214.

[21] Zeng Runxi, Chen Chuang. Evolution mechanism and intelligent governance of network public opinion from a non-traditional security perspective[J]. Modern intelligence, 2018, 38(11): 9-13.

[22] ARQUAM M, SINGH A, SHARMA R. A blockchain based secure and trusted framework for information propagation on online social networks[J]. Computer science, 2018, 62(4): 1157-1164.

[23] MA S, HAO W, DAI H N, et al. A blockchain-based risk and information system control framework[C]//2018 IEEE 16th intl conf on dependable, autonomic and secure computing, 16th intl conf on pervasive intelligence and computing, 4th intl conf on big data intelligence and computing and cyber science and technology congress (DASC/PiCom/DataCom/CyberSciTech). New York: IEEE, 2018: 106-113.

[24] HUANG H D, HONG P W, LEE Y T, et al. SOC: hunting the underground inside story of the ethereum Social-network Opinion and Comment[J]. Computer science, 2018, 62(3): 156-161.

[25] Zhao Dan, Wang Xiwei, Han Jieping, et al. Research on characteristics and patterns of network public opinion information propagation in blockchain environments[J]. Journal of intelligence, 2018, 37(9): 127-133, 105.

[26] Bin Sheng, Sun Gengxin, Zhou Shuang. Public opinion propagation model in social networks based on blockchain technology[J]. Journal of applied sciences, 2019, 37(2): 191-202.

[27] Huang Xinhao, Zhao Bo. Research on network opinion optimization based on blockchain technology[J]. China media technology, 2019(1): 48-51.

[28] Chen Hejie, Yan Qiang. Research on book public opinion of hot events based on big data technology[J]. Science-technology & publication, 2019(4): 83-85.

[29] Ding Xiaowei, Gao Shuping. Discussion on financial and public opinion risk management of virtual currency[J]. Modern communication (Journal of Communication University of China), 2018, 40(1): 133-139.

[30] Li Tai'an. Blockchain reconstructs the network opinion environment[J]. Media, 2017(21): 87-90.

[31] DEMEK K C, RASCHKE K L, JANVRIN D J, et al. Do organizations use a formalized risk management process to address social media risk?[J]. International journal of accounting information systems, 2017(28): 31-44.

[32] Lyu Wendong, Wang Xiaofei, Zhao Yang. Rethinking risk management from an organizational resilience perspective[J]. Management modernization, 2017, 37(4): 101-104.

Author Contributions

Guo Sulin: Paper writing and final revision, data processing and empirical analysis.
Huang Wei: Proposed research proposition and research 思路.
Li Ji: Paper revision.

Note: Figure translations are in progress. See original paper for figures.