Journal of Computers Vol. 37 No. 5, October 2026, pp. 427-442
https://doi.org/10.63367/19911599202610370502 6

Secure Sharing Governance of User-Generated Content in Blockchain-enabled Virtual Communities

Jian-Chun Sun, Ying Yue*, and Ai-Jing Xiao

Tangshan Vocational & Technical College,
Tangshan City 063017, Hebei province, China
sjcsjc945@126.com, yueyingbj@cuc.edu.cn, xiaoaijing_job@163.com

Received 10 July 2026; Revised 22 September 2026; Accepted 19 October 2026

Abstract. User Generated Content (UGC) is an important repository of knowledge in virtual communities but there are risks to it being widely available and replica. These risks include loss of privacy, unauthorized reuse, experience of misinformation, the infringements of rights, and maliciously distributed knowledge. Current governance on platforms concentrates on the ability to access the knowledge freely but also on reviewing and removing that data once the user generates it and subsequently posts it. Current governance structures cannot sufficiently balance the goals of knowledge sharing, user autonomy, accountability of the platform for the actions of the user, and the security of the user's generated content. This paper presents a framework for governing UGC using a decentralized governance approach utilizing a blockchain. The technical approach to governance of blockchain was used in developing programmable trust infrastructure. This includes the use of decentralized identity, traceability of UGC content, a chain of evidence prohibiting modification of evidence, the use of smart contracts for providing consent, the ability to provide privacy for access, and providing both the incentive to share and accountability for why that incentive is used. The governance mechanisms will create user autonomy, enterprise accountability, and make use of both on-chain and off-chain collaborative governance mechanisms.

Keywords: blockchain governance, virtual community, evolutionary game theory, technical governancePump selection, Improved Whale Optimization Algorithm (IWOA)

1 Introduction

Digital communities have become considerable places for social engagement and for obtaining knowledge and working together to solve problems across the Internet [1]. Users are adding to the body of knowledge that is present in these online communities by producing new posts, comments, videos, images, reviews, code and tutorials, along with experiential knowledge on question and answer (Q&A), social media, fan, open-source, and other platforms [2]. UGC is much more than just a fragment of conversation, it represents reusable assets that can support community learning, build trust, establish reputation, create value, and develop the platform. The very characteristics that provide value to UGC also render it difficult to govern. UGC can be copied, remixed, forwarded, stored, indexed, and recombined [3]. In many cases, UGC may contain both explicit or implicit private information about the user and so once that content is made publically available, the user has lost control over how that content will be accessed, interpreted, monetized or weaponized due to it's ease of distribution including the malicious exploitation of digital dissemination by distributing false knowledge, infringing content, screengrabs that violate the user's privacy rights, defamatory information, falsified media or phishing links that contains the user's personal information. Due to these characteristics of UGC, there are multiple security issues that relate to UGC such as: data security, privacy security, knowledge authenticity, authorization security, control of dissemination, accountability and governance legitimacy. Currently, the governing of virtual communities is almost entirely centralized. Governance is accomplished through the design of the platform enterprise; establishing rules; providing a recommendation system; collecting user records; moderating the content; determining what content should have visibility; and what content should be removed, down-rated, monetized or retained. The current structure of the current content platform-based UGC business model has a number of structural limitations, even though there are some operational advantages to this structure [4]. First, typically,

* Corresponding Author

users do not have substantial autonomy or control over the lifecycle of their own UGC. A user may upload a piece of content for one purpose or into one community or forum, and then other users, or the platform itself, may use that same UGC for various other purposes in other community or forum contexts. Second, the platforms that host UGC have more information and authority to make rules related to UGC than do the users who produce UGC, which leads to an opaque content moderation process; thus, users do not know how decisions made by the platform about moderation, algorithmic amplification of UGC, data processing, or the distribution of benefits from UGC are made. Third, by the time UGC content is moderated, it may already have been distributed in a manner that makes the harm that the content can cause irreversible. Fourth, there is a good chance that platform-based UGC enterprises will underinvest in security governance if the costs of implementing security governance measures are high and the likelihood of being punished for failing to comply with appropriate governance measures is low. Fifth, regulatory intervention is often delayed or based on insufficient evidence as to content provenance, appropriate authorization, or channels of dissemination of UGC. The governance of UGC security has the potential to be transformed through the use of blockchain technology [5]. The key technical capabilities of blockchain include the following: distributed ledgers; the ability to cryptographically authenticate content; records of UGC that are tamper-evident and contain metadata; mechanisms that establish consensus to validate the authenticity of UGC; smart contracts that can be implemented to establish the conditions of use, rules of access and revocation of access, and penalties for failing to comply with the terms of the smart contract; token incentive systems that reward UGC users; decentralized identity systems that support the ability to participate in a pseudonymous but an accountable manner; and systems that enable the tracing of the provenance of UGC. Users who provide high-quality knowledge to others will be rewarded through incentive mechanisms as a result of their contributions, suspiciously evaluated content of all kinds will be evaluated and reported as a malicious distribution of information and communities will be able to engage in community decision-making regarding how they want to govern themselves. In this way, blockchain may not be perceived as a complete governance solution; blockchain can record and prove the existence of knowledge, but blockchain cannot automatically determine if the knowledge represented is defamatory, misrepresentation, an invasion of privacy, or harmful in a context. Smart contracts execute rules that are pre-determined, however, badly drafted rules may take on the same character of being unfair or may be difficult to change once they are put in place [6]. Public ledgers can increase the level of transparency; however, the increased level of transparency in public ledgers may conflict with privacy rights. Token incentive schemes can motivate individuals to participate; however, they will also create speculation and collusion among users in a community as well as its members and produce low-quality content [7]. As such, understanding blockchain requires that it be viewed as technical-governance infrastructure requiring institutional rules and regulations, platform responsibilities, sector oversight, and community involvement. The purpose of this research is to answer the following question: How do blockchain-based governance systems improve the secure exchange of UGC in virtual communities while protecting user privacy and limiting malicious behaviour in the exchange of information? The method of approaching this research question is through constructing an integrated theoretical model of blockchain-based governance systems from the perspective of technical governance; blockchain governance mechanisms; evolutionary game theory [8]; and system dynamics. This work will establish four objectives for this study: (1) describe how blockchain can be used to create a secure means of sharing UGC through the use of technical governance mechanisms, including provenance; identity; access control; smart contract consent; and privacy-preserving accountability; (2) identify the governance priorities of blockchain-enabled virtual communities from the perspectives of user autonomy; the responsibilities of virtual-community enterprises; and the paths to implementation; (3) create an evolutionary game model of user, virtual-community enterprise and regulatory interactions that will be used to examine the strategic choices and stable governance conditions of all involved; and (4) construct a system dynamics model of the propagation of malicious UGC and utilize MATLAB simulations to evaluate propagation thresholds, evolutionary trends and governance factor sensitivity [9]. There are three primary contributions of this research. Theoretically, the study will add to the knowledge base on the sharing of UGC by considering the secure sharing of UGC as a socio-technical governance issue as opposed to just a technical, legal and/or managerial issue [10]. Methodologically, the integration of evolutionary game theory and system dynamics will enhance the study of both the strategic interaction and the dynamics of propagation within this area [11]. Practically, the research will propose actionable countermeasures for the governance of blockchain-enabled virtual communities, including the use of privacy-preserving architecture; smart contract-based consent; traceability as a means of accountability; moderating activities that are compatible with incentives; enterprise responsibility; regulatory audits; and threshold-based warning systems.

2 Literature Review

2.1 User-generated Content and Knowledge Sharing in Virtual Communities

The primary source of knowledge production in online communities is user-generated content (UGC). UGC is produced by everyday users rather than professionally produced content, and it becomes valuable through interaction, feedback, recommendation, interpretation, and reuse of the content. Knowledge-sharing communities benefit from UGC in many ways; UGC reduces the cost of searching for information, promotes peer-to-peer learning, allows for collective intelligence, and creates a greater network value for the platform. The volume and quality of UGC is an important factor in determining the long-term viability of online communities [12]. However, sharing UGC brings with it inherent tensions among the various parties involved in the process. Users are typically encouraged to share their experiences and knowledge, but can also inadvertently share sensitive information with their UGC [13]. While platforms want to optimize the circulation of content, excessive circulation may result in violations of user consent and promote harmful content. Communities want to encourage openness, but the ability to share information openly also creates opportunities for misuse by nefarious actors. Regulators want to ensure that platforms are accountable for UGC, but excessively regulating UGC may stifle participation by users. Thus, UGC sharing requires a balance between the above mentioned tensions, namely: openness and control, anonymity and accountability, autonomy and responsibility, incentives and sanctions, and platform efficiency and user rights [14]. Currently, there are several governance mechanisms for UGC that exist within online communities: The governance mechanisms for UGC include: community rules; content moderation; reporting systems; reputation systems; copyright notices; recommendation systems; identity verification; and compliance with applicable laws and regulations. While existing governance mechanisms are certainly still needed, they are often centralized and reactive. The platform itself is responsible for maintaining records of the creation, authorization, moderation, and dissemination of UGC. Therefore, it is often difficult for users and regulators to confirm that the platform is appropriately processing UGC [15]. Therefore, in order to achieve secure UGC sharing, governance mechanisms used to govern UGC must be transparent, auditable, and incentive-compatible.

2.2 Blockchain as Technical Governance Infrastructure

Understanding blockchain involves recognizing it as an inherently distributed record-keeping system that is resistant to tampering and other unauthorized modifications. However, when using blockchain technology in UGC or user generated content governance, it is essential that we do not attempt to store all of the raw UGC on the blockchain itself [16]. Rather, it is more beneficial to utilize blockchain technology as an optional layer of evidentiary proof regarding the provenance, authorization, accountability, and incentives of UGC. In a UGC system supported by blockchain, we may typically expect the raw UGC to be stored off-chain, while the relevant evidence would exist on-chain. Blockchain supports the governance of UGC from a technical perspective in a number of ways [17]. First, it supports governance of proof of provenance by utilizing hashes and timestamps of the UGC on the blockchain to verify if/when a UGC was modified and the originating point of the UGC registration and/or authorization. Second, it supports programmable consent, which allows smart contracts to identify what parties get access to the UGC, for what purposes, for what durations, and under what conditions. Third, it supports governability accountability that is traceable, which enables the tracing of dissemination pathways and identifying actors who have maliciously or incorrectly disseminated UGC through recorded transactions. Fourth, it supports incentives-based governance by providing tokens, reputations, staking, and/or credit mechanisms to reward responsible shares and sanction irresponsible acts. Fifth, it supports an environment of trust among multiple stakeholders by providing evidence of all transactions via the shared framework of the blockchain instead of relying on internally maintained databases of the respective platforms. However, there are also risks associated with blockchain. If/when personal information and raw UGC is stored directly on-chain, the ability to delete or modify any such information will be much more difficult [18]. Furthermore, if the transparency of the UGC is absolute, then the individual users privacy begins to deteriorate. In addition, if a smart contract is poorly written, there is the potential for the users to be bound by the smart contract under unfair authorization terms. If the governance token is the predominant means of participation in the community, the community governance may be influenced by well-capitalized or otherwise organized actors. Therefore, any governance relying on blockchain technology must ensure that user privacy is preserved; that institutions create

checks and balances on their authorities and authorities; and that the technologies supporting governance can adapt to meet both existing and future needs.

2.3 User Autonomy and Platform Responsibility

The concept of user autonomy is critical to successful UGC sharing [19]. Most users of traditional virtual communities simply accept broad terms of service without any real control over the future use of their content. In order for sharing to be safe, users must have meaningful authority over content authorization, level of access, purpose of reuse, ability to revoke, share benefits, and the ability to dispute content usage. With the use of blockchain technologies, autonomy can be enhanced by enabling user-controlled identity management, consent via smart contracts, selectively disclosing information, and creating auditable records of authorization [20]. However, user autonomy does not eliminate the responsibilities of the provider of the platform. Companies that are virtual-community enterprises are still responsible for design of interface, operation of recommendation algorithms, moderation of content, data architecture management, and defining rules of the community. Therefore, even if blockchain technology is implemented, it is still the responsibility of the company to determine how the blockchain technology will function and be used by the users [21]. Consequently, decentralization cannot be an excuse for avoiding responsibility. A virtual-community enterprise with blockchain technology should provide the following: transparency in rules; usable consent mechanisms; privacy-preserving infrastructures; timely content moderation; reasonable explanation of risks; and auditable governance records.

2.4 Malicious UGC Propagation and Privacy Information

Malicious user-generated content (UGC) propagation involves spreading content that hurts someone, whether due to its false information, invasion of privacy, infringement upon someone's rights, harassment, defamatory statements, or unauthorized reuse. If the malicious UGC involved violating someone's privacy, it is necessary to highlight that it does not simply go away once the original UGC post is removed. For example, if an individual were to create a screenshot that contains someone else's personally identifiable information (PII), malicious individuals may republish that screenshot identifying the PII and continue uploading that screenshot over time to many locations, including search engine index files. As such, even if the original UGC post containing the correct PII, unauthorized reposting or republishing of that post may inhibit the original UGC poster's privacy and contribute to their reputational and/or psychological harm. Malicious UGC propagation is both a process of diffusion and one of strategy. The process of diffusion relates to the evolution of exhibits, forwards, corrections, and resistance over the passage of time. The process of strategy relates to the decision-making of users, platforms, and regulators in determining their actions based upon expected costs and benefits. Users will determine whether or not to forward any UGC they suspect contains false information, whether to verify the authenticity of the UGC, report the UGC, or simply ignore the UGC. Enterprises will determine whether to invest in traceability, moderate their users, and/or protect the privacy of their users. Regulators will determine whether to enact strict regulation over users or to only intervene after the fact following substantial incidents. Therefore, a complete model of malicious UGC propagation should connect strategic decision-making with the evolution of the process of diffusion [22].

2.5 Evolutionary Game Theory and System Dynamics

Evolutionary game theory is well-suited for the study of boundedly rational players who develop their strategies via imitation, experience, adaptation, and comparison of payoffs. For players in virtual communities, players cannot possibly have complete information about the risks associated with sharing their private content. They may also lack the knowledge to assess the future costs associated with failure to govern such content [23]. The intensity of the regulatory oversight that is provided by regulators will depend on both public risk and the regulation performance of those in compliance. Consequently, the application of evolutionary game theory can be used to model the process by which secure sharing, passive governance, malicious propagation, and strict regulation can evolve as either stable or unstable over time [24]. System dynamics is a useful approach for capturing the stock-flow structure, feedback loops, delays, and nonlinear nature of a process. Individuals propagating malicious UGC work within a feedback loop between the degree of exposure, how they forward,

how they correct, whether they report, and the level of trust or regulation. The integration of evolutionary game theory and system dynamics provides an understanding of not only who chooses which strategies but also how those choices create the degree and pace at which malicious propagation occurs.

3 Framework and Research Propositions

3.1 Framework with 3 Layers

The proposed framework is composed of 3 Layers. 1st Layer: Technical Governance The 1st layer is termed as Technical Governance; this layer is concerned with the technology that creates the infrastructure to allow for the secure sharing of data, such as use of decentralized identity, cryptographic methods for verification of data's origin/creator, content hashing, authorization through the use of smart contracts, the storage of content off-chain, the selective disclosure of shared content, access control, recording of reputation and preserving evidence through the use of blockchain technologies [25]. 2nd Layer: Governance Mechanism Design The 2nd layer is termed as Governance Mechanism Design [26]; this design focuses on the institutional arrangements between users and enterprises, between enterprises and their regulators, and the institutional arrangements among community moderators, 3rd party auditors, and other interested parties concerning user generated content (UGC). Some mechanisms include maintaining user autonomy while ensuring enterprise accountability; providing regulatory oversight; encouraging community involvement; providing users with incentives to behave; providing users who do not behave with an opportunity for punishment; avenues for resolving disputes; maintaining an on-chain/off-chain coordination approach. 3rd Layer [27]: Dynamic Risk Control The 3rd layer is termed as Dynamic Risk Control; this layer focuses on controlling the spread of malicious UGC in an environment in which privacy and information security requirements exist. Core mechanisms include monitoring the use of an UGC; evolving our strategies to account for new data; using simulation-based analyses to assess risk relative to the distribution of competitive advantage; providing warnings about the potential risk associated with malicious UGC; determining optimal governance parameters. The Main Logic The main logic is that new forms of technological sharing that result from the application of blockchain technology will result in increased investments in governance; as more governance will be beneficial to the enterprises that have incorporated blockchain into their businesses by providing benefits related to a company's reputation, meeting compliance regulations, and reducing the risk of exploitation through good governance. The credibility of regulators and verifiability of the evidence that a company is subject to regulation will lead to more stable governance practices for blockchain-based businesses. The overall network structure diagram is shown in Fig. 1.

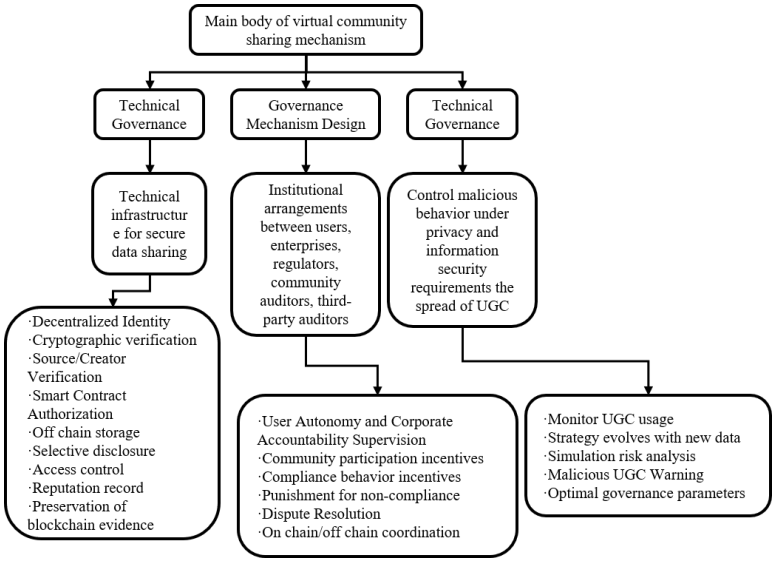


Fig. 1. Schematic diagram of the three-layer structure of the virtual community sharing mechanism

3.2 Research Propositions

Proposition 1: By providing blockchain traceability this will increase the anticipated costs of malicious UGC propagation while at the same time reducing the likelihood that a user will opt to use a malicious (or other unsafe) method of sharing.

Proposition 2: User autonomy will enhance secure sharing of information when authorization, access control and consent revocation can be enforced through technical or legal/ institutional means.

Proposition 3: The more invested in blockchain governance to a corporation, the greater degree of certainty that those entities can detect, correct and hold accountable a malicious UGC propagation.

Proposition 4: Incentives can be an effective means of promoting secure sharing of information when the rewards for verification, reporting and authorized dissemination will exceed any short term gains gained from malicious use.

Proposition 5: Privacy-protective mechanisms may help reduce a user's reluctance against traceability through improving accountability while preventing unnecessary exposure of sensitive information.

Proposition 6: The ability to contain the spread of malicious UGC will only occur if the threshold for effective propagation is lower than the capacity of the governance mechanisms for correction and deterrent action.

4 Evolutionary Game Model

4.1 Participants and Strategies

This framework has a total of three primary parties involved: users, vedlles and regulators. Users may choose to utilize either the safe or unsafe sharing methods. The safe method requires compliance with specified rules regarding sharing user-generated content (UGC) and assessing possibly false or questionable content; while still maintaining the right to keep others' proprietary information private (i.e. by not disclosing). Report (to vedlle) malicious acts of sharing when user knows about it. Unsafe sharing is when a user shares content that he or she has not obtained permission for, gives someone access to information that they could otherwise have protected themselves from someone that may share it; forwards informal or non-public content to someone else, when he/ she is aware this is untrue; forwards informal or non-public content to someone else; fails to verify if they are true or false before forwarding them; amplifies content with the intent to harm another. Vedlle uses one of two governance strategies (active/passed) in order to manage the collective community. Active governance includes investing in smart contracts, auditing records of ownership via trace data, developing privacy rules, so that users have clarity as to their rights to share their information, and establishing awards and punishments to drive compliance. Passive governance involves little or no investment (of time/effort) towards compliance, and mostly uses traditional post-moderation processes. Regulators primarily use either a strict rule-making or enforcement mechanism to govern their members. Regulators with a strict rule-making mechanism enforce their members' rights using audits and impose penalties for failure to comply [28]. Regulators who have a loose rule-making mechanism provide their members limited oversight; have significant lag times between regulators' responses to non-compliant or failed members; and are not confident about their ability to enforce regulations on their members.

$$x, y, z \in [0, 1] \tag{1}$$

Where x denotes the proportion of users choosing secure sharing, y denotes the proportion of enterprises choosing active blockchain governance, and z denotes the proportion of regulators choosing strict supervision.

4.2 Detection Probability and Privacy-loss Function

Blockchain traceability, enterprise investment, and regulatory supervision jointly affect the probability that malicious dissemination is detected.

$$q = q_0 + \alpha_1 T + \alpha_2 y + \alpha_3 z \tag{2}$$

Where q_0 is the baseline detection probability, T is the blockchain traceability level, and α_1, α_2, and α_3 are positive coefficients. In simulation, q should be limited to the interval [0, 1].

Privacy protection reduces privacy-loss cost.

$$L_p = L_{p0}(1 - P) \tag{3}$$

Where L_p is the potential privacy-loss cost without protection and P is the privacy-protection level [29].

4.3 User Payoff and Evolutionary Equation

The user-side payoff structure compares secure sharing with malicious or unsafe sharing.

$$\pi_S = R_s + I_u y + \theta P - C_s \tag{4}$$

$$\pi_M = R_m - C_m - qF_u - L_p(1 - y) \tag{5}$$

Where π_S is the payoff of secure sharing. The replicator dynamic equation for users is:

$$\frac{dx}{dt} = x(1 - x)(\pi_S - \pi_M) \tag{6}$$

Equation (6) means that the proportion of users choosing secure sharing increases when the payoff of secure sharing is higher than that of malicious or unsafe sharing [30].

4.4 Enterprise Payoff and Evolutionary Equation

The enterprise-side payoff structure compares active blockchain governance with passive governance.

$$\pi_B = B_e + I_e z + \eta x - C_b - (1 - x)(1 - q)L_e \tag{7}$$

$$\pi_N = B_e - C_n - (1 - x)L_e - zF_e \tag{8}$$

Where π_B is the payoff of active blockchain governance and π_N is the payoff of passive governance. The replicator dynamic equation for enterprises is:

$$\frac{dy}{dt} = y(1 - y)(\pi_B - \pi_N) \tag{8}$$

Equation (9) means that enterprises are more likely to adopt active blockchain governance when its expected return exceeds that of passive governance [31].

5 System Dynamics Model of Malicious UGC Propagation

The spread and evolution of malicious UGC do not follow the idealized assumption of instant propagation, and the time delay characteristics exhibit obvious universality and complexity throughout the entire propagation

process. After being exposed to malicious UGC information, non disseminators usually need to go through psychological stages such as information identification, attitude hesitation, and decision consideration before they can transform into potential disseminators with the intention of spreading. At the same time, some disseminators may experience re dissemination after stopping their dissemination behavior due to new information stimuli, secondary triggers on social networks, or changes in personal attitudes. There are significant individual differences and scenario dependencies in the time interval from stopping propagation to re propagation. The spread of malicious UGC is a dynamic process, and there is a time delay between individuals coming into contact with malicious UGC and starting to spread it, known as instant lag. In recent years, with the gradual improvement of differential equation dynamics theory, some scholars have considered time delay factors and established propagation models with time delay. They have found that time delay can cause the system to lose stability and thus generate branches. Therefore, it is particularly important to study the impact of time delay on the propagation model of malicious UGC.

1) Consider the delay effect of converting non communicators into potential communicators, as well as the interaction delay between non communicators and communicators, and establish a system of differential equations with time delay.

2) Analyze the impact of time delay on system stability and explore the Hopf bifurcation phenomenon and its critical conditions.

3) Using the Pontryagin maximum principle, solve for the optimal control strategy and verify its effectiveness through numerical simulation.

The schematic diagram of malicious UGC broadcast partition is shown in Fig. 2.

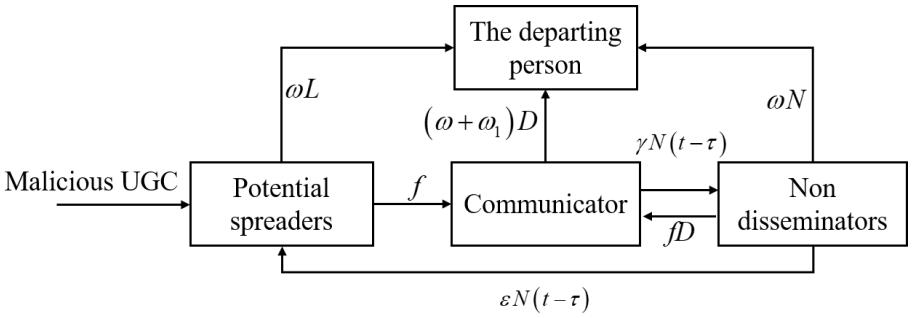


Fig. 2. Schematic diagram of propagation model

5.1 Model Structure

The evolutionary game model explains strategic interaction, while system dynamics explains how malicious UGC spreads and is controlled over time. The population of a virtual community is divided into four state variables: $S(t)$, susceptible users who have not encountered malicious UGC; $E(t)$, exposed users who have encountered malicious UGC but have not forwarded it; $M(t)$, malicious propagators who forward, reuse, or amplify malicious UGC; and $C(t)$, corrected or resistant users who verify, reject, report, or correct malicious UGC [32].

$$N = S(t) + E(t) + M(t) + C(t) \tag{10}$$

5.2 Propagation Equations

The malicious UGC propagation process is represented by the following stock-flow system.

$$\frac{dS(t)}{dt} = -\beta eff\frac{S(t)M(t)}{N} + \rho C(t) \tag{11}$$

$$\frac{dE(t)}{dt} = \beta eff\frac{S(t)M(t)}{N} - \sigma E(t) - \kappa E(t) \tag{12}$$

$$\frac{dM(t)}{dt} = \sigma E(t) - \gamma_{eff} M(t) \tag{13}$$

$$\frac{dC(t)}{dt} = \kappa E(t) + \gamma_{eff} M(t) - \rho C(t) \tag{14}$$

Where βeff is the effective exposure or propagation rate, σ is the probability that exposed users become malicious propagators, κ is the probability that exposed users become resistant, γ_{eff} is the effective correction or removal rate, and ρ is the rate at which corrected users become susceptible again. The evolutionary trajectory is described by a set of differential equations, expressed as follows:

$$\frac{dL(t)}{dt} = In_{UGC} - \frac{\beta L(t)D(t)}{1+\alpha D(t)} - \omega L(t) + \varepsilon N(t-\tau) \tag{15}$$

$$\frac{dD(t)}{dt} = \frac{\beta L(t)D(t)}{1+\alpha D(t)} + \gamma N(t-\tau) - (k+\omega+\omega_1)D(t) \tag{16}$$

$$\frac{dN(t)}{dt} = k \cdot D(t) - \omega N(t) - \left[(\gamma+\varepsilon)\cdot N(t-\tau)\right] \tag{17}$$

$$\frac{dC(t)}{dt} = \omega\left(L(t)+N(t)\right) + (\omega+\omega_1)D(t) \tag{18}$$

Among them, γ is the reproduction rate of public opinion, k is the cessation rate of public opinion dissemination, ε is the dissemination rate from non disseminator $N(t)$ to latent disseminator $L(t)$, and τ is the propagation delay.

The constructed model indicates that variables $L(t)$, $D(t)$, and $N(t)$ are all independent of $C(t)$. For the convenience of analysis, analyze independently of $C(t)$. All system parameters remain positive based on their biological significance in population modeling.

Adding time delay variables in the propagation process to characterize the time delay effect in the transformation of non propagators into complex propagation, while incorporating the quadratic conversion rate from non propagators to potential propagators, further improves the behavior law of crowd propagation and reveals the propagation law of dynamic behavior that is more complex than ordinary differential equations.

6 Simulation Design and Expected Results

The simulation is designed to illustrate how blockchain governance affects secure-sharing strategy evolution and malicious UGC propagation. The simulation does not claim to estimate a specific real platform unless calibrated with empirical data. Instead, it demonstrates the logic of the model and identifies parameter-sensitive governance conditions.

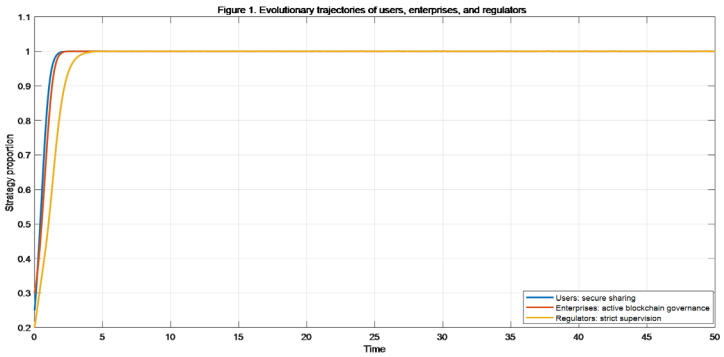


Fig. 3. Evolutionary trajectories of users, enterprises, and regulators

In Fig. 3, we display the changes over time in the three main groups that help govern user-generated content (UGC) on the blockchain: users, enterprises (or firms), and regulators. The *x*-axis represents the passage of time in the simulation, while the *y*-axis shows the percentage of users and enterprises using the good governance strategy. In particular, *x* indicates the percentage of users using secure sharing, *y* indicates the percentage of enterprises using active blockchain governance, and z indicates the percentage of regulators using strict oversight. Fig. 3 illustrates how, through the payoffs established in the evolutionary game model, the proportion of each of the three groups using the good governance strategy will evolve over time. If the curves ultimately approach one, that means that secure sharing, active governance, and strict oversight are likely to become dominant strategies. This means that the expected value of securely participating, of investing in blockchain governance by enterprises, and of being supervised by regulators exceeds the costs of all three options. The conceptual value of Fig. 3 is that it demonstrates the co-evolutionary nature of UGC governance. Users do not make use of platforms and regulators as separate and distinct from one another. When enterprises provide traceability of blockchain records for secure sharing, users incur larger expected costs from malicious dissemination and greater expected benefits from legitimate sharing. Consequently, as more users choose secure sharing, enterprises experience lower overall levels of reputational risk and lower expected costs associated with malicious dissemination, which makes them more willing to invest in blockchain governance. Also, regulators observe the overall results of the governance system when determining their own regulatory strategy and their ability to supervise enterprises based on enterprise compliance and user behavior. If the governance system produces visible social benefits and reduces malicious dissemination, then strict regulatory oversight of enterprises will be considered a more rational and stable strategy. Thus, as demonstrated in Fig. 1, there is an evidence of strategic coupling between users, enterprises, and regulators. The pattern of convergence supports the primary argument of the paper that blockchain technology will not allow for the improvement of the security of UGC by itself because it is a stand-alone technology. It works when it aligns the payoffs of all key participants and creates a stable governance equilibrium in which users share securely, enterprises actively govern, and regulators provide credible supervision.

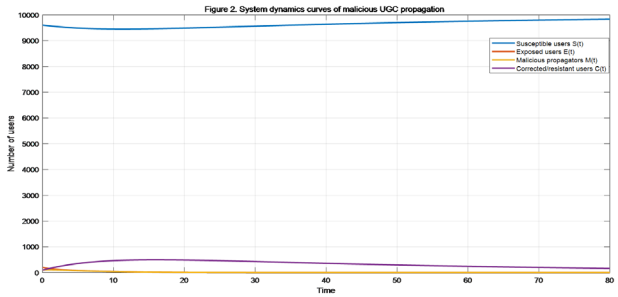


Fig. 4. System dynamics curves of susceptible, exposed, malicious-propagating, and corrected users

Fig. 4 shows how the system dynamics change for the four types of users in a malicious content UGC distribution system over time as they pass through four uneven stages: susceptible, malicious propagators, and corrected/resistant users. This transition from the dissemination of malicious UGC to a stock-flow transition can be seen in the number of users who move from being susceptible to seeing malicious content to having received some version of malicious content but not yet decided what to do with it, to actively forwarding, reusing or amplifying an even more maliciously edited version of that content and finally rejecting, correcting, reporting or being resistant to future dissemination of malicious UGC. The purpose of this figure is to show how UGC security governance alters the malicious UGC propagation system. In the early stages of the system, there is likely to be an increase in both exposed users and malicious propagators due to the diminutive numbers of malicious propagators who can and will continue to disseminate damaging content to susceptible users. However, as the traceability mechanism, correction mechanisms, reporting mechanisms, and regulatory interventions take effect, the quantity of malicious propagators should decrease. At the same time, the number of corrected/resistant users should rise which indicates an increasing capacity of each user to identify and reject or report on malicious UGC. If the curve for $M(t)$ declines while concurrently the curve for $C(t)$ is increasing, this should indicate that the governance of the users is successful in transitioning users from propagating malicious UGC to resisting its dissemination. The flow of users through these four states is significant as it establishes the dynamic nature of malicious UGC control. In fact, the UGC sharing process starts with the detection of malicious UGC, and the ultimate goal of UGC security governance is to continuously transition exposed users into resistant users and continuously decrease the numbers of active malicious propagators. This is facilitated through the use of the properties of blockchain that promote correct traceability of original copies of UGC, secure evidence collection, authorised verification of the publisher of UGC, and to hold the UGC downloader accountable for their actions. The implications of this figure also suggest that the rate at which corrections can be made to the dissemination of UGC has to be immediate. If the rate at which corrections can be made is not sufficient, then malicious propagators may begin to assemble faster than can be corrected, potentially with irreversible privacy or reputational damages. Thus, the central thesis of this manuscript is that secure UGC sharing requires an interactive, proactive, and threshold governance approach to reducing all users of malicious propagators rather than just a method of removing malicious UGC after dissemination.

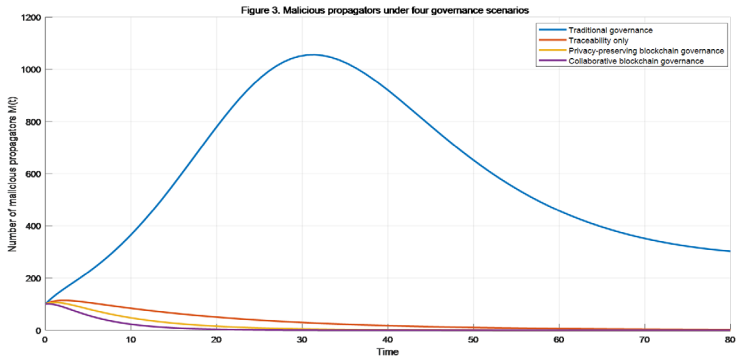


Fig. 5. Comparison of malicious propagators under four governance scenarios

In Fig. 5, there is a comparison between the level of users involved in propagating malicious-UCG under different governance structures, namely traditional governance with a lack of traceability and privacy, governance with only traceability or blockchain records for malicious UCG, privacy-preserving blockchain governance, and collaboration in blockchain governance, in relation to time and the users' continued participation in propagating malicious UCG. In the scenario of traditional centralized governance, the lack of sufficient privacy or user autonomy and the weakness of blockchain-based evidence, combined with using content moderation, user reports, and an after-the-fact deletion approach, contribute to an increase in the number of malicious UCG propagators. Furthermore, malicious propagators could sustain this high level of participation for an extended period. In the scenario using only traceability as a governance mechanism, while blockchain provides a greater ability to trace the unauthorized/dishonest dissemination of UCG, the absence of sufficient privacy protection

creates an environment of distrust and low user involvement in using this governance structure. While the level of malicious UCG propagation may be somewhat reduced using only traceability to deal with this issue, the overall impact will be diminished as users are more likely to think in terms of using traceability as a means of surveillance as opposed to empowering themselves. In the scenario of privacy-preserving blockchain governance, the governance structure is likely to have a greater deterrent effect because it combines traceability and sufficient privacy protection through off-chain storage, selective disclosure, smart-contract created consent, and privacy-preserving authorizations. Users are more likely to share in a secure manner and be willing to report UCG used against them when they can do so without significantly exposing their personal information. Finally, the collaborative blockchain governance scenario will likely produce an even greater suppression of UCG propaganda and thus the level of malicious UCG propagators. The collaborative blockchain governance model would create an environment in which individuals, enterprises, regulatory authorities, and community moderators can actively participate in governance efforts related to the good use of UGC, including traceability, sufficient privacy protections, regulatory audits, rewards/penalties, and emergency response. This means that blockchain technology and blockchain governance cannot be viewed as a single binary choice. Rather, the effectiveness of governance providers depends on the combinations of how various types of governance are used to establish good governance. Traceability alone is far less effective than traceability and privacy protections, user autonomy, enterprise accountability, regulatory supervision, or multi-stakeholder collaboration. This last point serves to support the author's position that the security of UGC provided by blockchain technology is fundamentally a socio-technical governance system as opposed to simply a technical processing solution to facilitate trust in UGC.

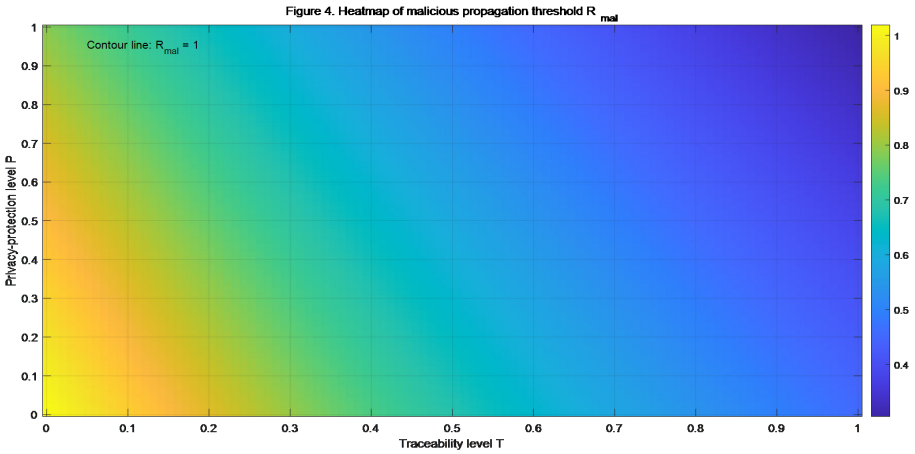


Fig. 6. Heatmap of malicious propagation threshold

This heatmap (Fig. 6) shows the malicious propagation threshold with respect to blockchain traceability (T) and privacy protection (P). The horizontal axis reflects the level of traceability, while the vertical axis reflects the level of privacy protection. The heatmap's colour intensity indicates $R_{mal}{}'$ value. The threshold R_{mal} helps assess whether UGC that is malicious typically spreads or decays. This figure exemplifies how traceability and privacy protection collectively affect R_{mal}. Malicious actors are less likely to propagate malicious UGC when T increases due to increased likelihood of being identified, audited or punished for such activity, and consequently reduces the effective propensity for malicious UGC propagation. When P increases, users can share, certify, report and distribute UGC securely, thus encouraging them to participate. Privacy protection also limits the exposure of sensitive information, thereby limiting subsequent harmful consequences. Therefore, the combined improvement of T and P decreases R_{mal} and moves the total system from a diffusion region to a suppression region. Fig. 6 contributes theoretically to isualizing the logic of threshold governance for UGC as governed via blockchain. It provides a visual aid demonstrating that traceability and privacy protection are not mutually exclusive methods of control. A common error made in digital governance is the assumption that increased traceability results in decreased privacy, whereas it is suggested in this model that both accountable traceability and privacy sensitive

design are complimentary. Accountable traceability contributes to accountability by providing traceability, whereas privacy protection enhances user trust and participation. If both dimensions are increased, a governance system will achieve sustainable suppression of malicious propagation.

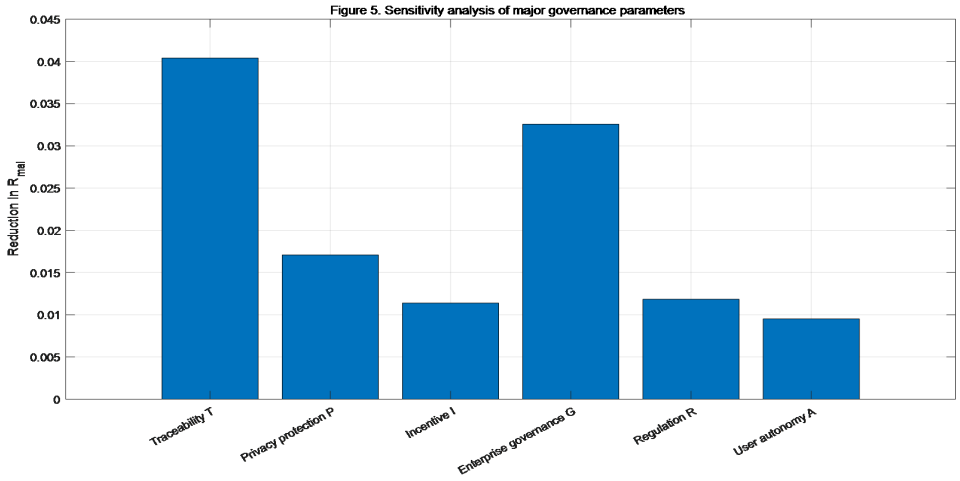


Fig. 7. Sensitivity analysis of major governance parameters

The Sensitivity Analysis of Important Governance Factors Influencing the Malicious Propagation Threshold R_{mal} is illustrated in Fig. 5. The variables that comprise this analysis include Traceability T; Privacy Protection P; Incentive Strength I; Enterprise Governance Investment G; Regulatory Oversight R; and User Autonomy A. The reduction in R_{mal} on the vertical axis indicates the degree to which a marginal increase of each variable will decrease R_{mal} . The larger the bar for that given governance variable, the more significant the suppression effect of that variable on the malicious propagation of UGC. The primary objective of Fig. 7 is to assist in identifying which governance variables have the most marginal influence under the default parameter conditions. A significant effect associated with Traceability indicates that improving the provenance of content, dissemination records, authority logs, and preservation of evidence is very influential in reducing malicious propagation. A strong effect associated with Privacy Protection indicates that the willingness of users to engage in secure sharing and reporting largely depends on whether the platform is protective of sensitive information. The existence of a strong Enterprise Governance Investment effect implies that having effective governance at the platform level depends significantly on investing in infrastructure, moderation capacity, and the implementation of smart contracts. A strong Regulatory Oversight effect means that having standards, penalties, audits and compliance pressure will be critical to prevent platforms from underinvesting in the security aspect of governance. Fig. 7 also provides practical insight for policy makers as it indicates that because of the limited resources for governance, there will be a limit to the investment made by both the platform and regulators across each variable. Therefore, the Sensitivity Analysis provides guidance for identifying priority items. For example, if the model indicates that Enterprise Governance Investment and Traceability are the two variables with the strongest marginal effect, the platform should focus first on investing in blockchain provenance systems, smart contract authorizations, and real-time risk detection. If the model indicates that Privacy Protection has an equal impact, the platform should focus on developing privacy-protection governance through the utilization of off-chain data storage, encryption methods, selective disclosure of data, and maintaining anonymity when holding others accountable for the content. of traceability and punishment, users can continue to choose to share maliciously or share in an unsafe manner, because short-term benefits outweigh the long-term expected costs of those types of sharing. Second, the level of uncertainty associated with adopting or implementing active governance by a company will decrease and the level of evidence supporting that decision will increase as the level of blockchain governance increases; therefore, the willingness of enterprises to adopt active governance increases, provided the cost of doing so is reasonable. Third, when enterprises impose stricter levels of supervision and penalties and standards, the level of stability of enterprise governance will also increase. Fourth, the level of willingness to share securely by users will increase due to the absence of excessive exposure as a consequence of adding privacy protection to

the process of traceability. Fifth, when traceability, privacy protection, enterprise investment, and regulation are combined, the threshold of severity of malicious propagation will decrease significantly.

7 Conclusion

The research described in this article created a framework for managing secure sharing of User Generated Content by using blockchain technology in the virtual community space. UGC security, as described in the study, is a socio-technical governance issue that has implications for user autonomy, platform accountability, regulatory oversight, privacy safeguarding, malicious distribution of content, and the efficiency of knowledge-sharing. Technology offered by blockchain includes provenance, smart contract capability, decentralized identity systems, tamper-evident records, incentive mechanisms, and traceable accountability. However, for blockchain to be effective, it must be integrated into governance rules and enterprise commitments, user-rights mechanisms, and regulatory standards. Using the evolutionary game model, the study demonstrates that users, enterprises, and regulators adjust their strategies and behaviors based on the payoff each derives from his/her actions. Once the benefits of legitimate sharing, privacy protection, incentive compatibility, and anticipated penalties for malicious distribution of UGC are greater than the short-term benefits derived from the latter, secure sharing will become stable. Enterprises use active governance mechanisms using blockchain technology when the anticipated reductions in risk, regulated incentives provided by the government, enhancement of the company's reputation, and trust established with the user community exceed the costs incurred to implement the blockchain solution. Regulators maintain strict oversight of the governance process when the governance benefits resulting from their oversight and the pressure for accountability exceed the costs of providing oversight. The study also used a system dynamics model to demonstrate that the deployment of blockchain technology as a governance mechanism can be used to manipulate the malicious distribution threshold for UGC. Malicious UGC will fall under the control of the governance system when the effective malicious distribution rate is less than the correction and deterrent capabilities available within the governance system. This process establishes the potential for using a threshold-based early warning system and provides the foundation for optimizing governance by utilizing a simulation approach. Future research could take a number of different directions to extend this article. First, by developing empirical research studies, it will be possible to collect platform data that could then be used to calibrate the parameters of the models described in this paper. Second, through comparative research, it should be possible to investigate the differences between the various blockchain architectures. Finally, through the use of both experimental research and survey research, it will be possible to investigate how users perceive the use of smart contract-based consent, traceability, privacy protection, and incentive structures in real virtual community settings.

8 Acknowledgement

This study was Supported by the Ministry of Education (MOE) Youth Foundation Program for Humanities and Social Sciences Research (Project No. 25YJC860028).

References

[1] Y. Tausczik, X.-Y. Huang, Knowledge generation and sharing in online communities: current trends and future directions, Current Opinion in Psychology 36(2020) 60-64. https://doi.org/10.1016/j.copsyc.2020.04.009

[2] Y.A. Ahmed, M.N. Ahmad, N. Ahmad, N.H. Zakaria, Social media for knowledge-sharing: a systematic literature review, Telematics and Informatics 37(2019) 72-112. https://doi.org/10.1016/j.tele.2018.01.015

[3] N. Schröder, C.-D. Schultz, F. Paetz, A. Grzadziel, M. Clegg, Unraveling the Influence: Exploring the Role of User Generated Content Along the Customer Journey and Understanding Its Relevance for Research and Practice, Schmalenbach Journal of Business Research 77(3)(2025) 457-496. https://doi.org/10.1007/S41471-025-00214-9

[4] S. Kostić, J. Spajić, Đ. Alavuk, I. Šiđanin, B. Laličić, S. Bunčić, The Role of User-Generated Content in Social

Commerce: A Systematic Review, Sustainability 18(3)(2026) 1601.1-1601.20.
https://doi.org/10.3390/SU18031601
[5] B. Dziundziuk, V. Dziundziuk, Methodology for integrating blockchain into digital governance systems: analysis of challenges, benefits, and opportunities for society, Science and Public Policy 52(6)(2025) 815-825.
https://doi.org/10.1093/SCIPOL/SCAF022
[6] H. Taherdoost, Smart Contracts in Blockchain Technology: A Critical Review, Information 14(2)(2023) 117.1-117.19.
https://doi.org/10.3390/INFO14020117
[7] K. Chen, Y.-F. Fan, S.-S. Liao, Token Incentives in a Volatile Crypto Market: The Effects of Token Price Volatility on User Contribution, Journal of Management Information Systems 40(2)(2023) 683-711.
https://doi.org/10.1080/07421222.2023.2196772
[8] X.-M. Xie, S. Xu, Y.-M. Wu, Research of Virtual Community Expectation Gap and User Silence Behavior, China Soft Science (S2)(2024) 338-346.
[9] X.-L. Wang, J. Zhang, L.-J. Zhao, Z.-J. Xia, Research on Microblog Public Opinion Derived Topic Communication based on Improved SEIR Model, Journal of Information Resources Management 12(4)(2022) 95-104+120.
https://doi.org/10.13365/j.jirm.2022.04.095
[10] L. Zhang, N.-X. Sang, Research on Social Network Structure of Virtual Learning Community, Adult Education 44(10)(2024) 56-60.
https://doi.org/10.3969/j.issn.1001-8794.2024.10.009
[11] Z. Fan, W. Zhang, Meta Analysis of the Influencing Factors of User Sharing Behavior in Knowledge-based Virtual Communities—Induction Based on Role Theory, Journal of Modern Information 44(8)(2024) 69-78.
https://doi.org/10.3969/j.issn.1008-0821.2024.08.007
[12] J.-Y. Fang, Y. Ni, J. Zhang, Value assessment of UGC short videos through element mining and data analysis, Applied Sciences 13(16)(2023) 9418.1-9418.22.
https://doi.org/10.3390/APP13169418
[13] J.-H. Tao, W. Dong, Y.-L. Tian, Research on Differences of Group Clustering and Knowledge Sharing of Behavior Characteristics of Integrating Learners—Taking Zhihu Programming Topics as Examples, Adult Education 45(3)(2025) 10-17.
https://doi.org/10.3969/j.issn.1001-8794.2025.03.002
[14] Z.-B. Shen, M. Wang, The Influence of Virtual Brand Community Governance Mechanism on the Innovation Behavior of Different User Groups, Chinese Journal of Management 23(2)(2026) 302-311.
https://doi.org/10.3969/j.issn.1672-884x.2026.02.011
[15] M. Chi, X.-H. Bi, Y.-S. Xu, Research on Effect of Mobile Academic Virtual Community Governance Mechanism on Knowledge Sharing Behavior —Trust as a Mediating Variable, Management Review 33(2)(2021) 164-175.
https://doi.org/10.14120/j.cnki.cn11-5057/f.2021.02.015
[16] F. Yang, M.Z. Abedin, Y.-N. Qiao, L.-Y. Ye, Toward Trustworthy Governance of AI-Generated Content (AIGC): A Blockchain-Driven Regulatory Framework for Secure Digital Ecosystems, IEEE Transactions on Engineering Management 71(2024) 14945-14962.
https://doi.org/10.1109/TEM.2024.3472292
[17] F. Cengiz, Blockchain governance and governance via blockchain: decentralized utopia or centralized dystopia?, Policy Design and Practice 6(4)(2023) 446-464.
https://doi.org/10.1080/25741292.2023.2247203
[18] M.H. Ziegler, M. Nowostawski, B. Katt, A Systematic Literature Review of Information Privacy in Blockchain Systems, Journal of Cybersecurity and Privacy 5(3)(2025) 65.1-65.21.
https://doi.org/10.3390/jcp5030065
[19] H.-C. Song, J. Wei, Q.-L. Jiang, What Influences Users' Intention to Share Works in Designer-Driven User-Generated Content Communities? A Study Based on Self-Determination Theory, Systems 11(11)(2023) 540.1-540.19.
https://doi.org/10.3390/systems11110540
[20] M.S. Al Jasem, T. De Clark, A.K. Shrestha, Toward Decentralized Intelligence: A Systematic Literature Review of Blockchain-Enabled AI Systems, Information 16(9)(2025) 765.1-765.26.
https://doi.org/10.3390/info16090765
[21] K. Guerra, V. Prybutok, Blockchain technology: an analysis of economic, technical, and legal implications, International Review of Law, Computers & Technology 40(1)(2026) 156-176.
https://doi.org/10.1080/13600869.2025.2497632
[22] A. Jain, J. Dhar, Optimum control model of malicious news spread on social networks having hidden accounts, Results in Control and Optimization 17(2024) 100468.1-100468.14.
https://doi.org/10.1016/J.RICO.2024.100468
[23] D. Hariyani, P. Hariyani, S. Mishra, M.K. Sharma, Causes of organizational failure: A literature review, Social Sciences & Humanities Open 10(2024) 101153.1-101153.22.
https://doi.org/10.1016/j.ssaho.2024.101153
[24] C. Hilbe, M. Kleshnina, K. Staňková, Evolutionary Games and Applications: Fifty Years of 'The Logic of Animal Conflict', Dynamic Games and Applications 13(4)(2023) 1035-1048.
https://doi.org/10.1007/S13235-023-00545-4

[25] Y. Long, Information Security Construction of Twin Space in Virtual Community of University Library, Journal of Fujian Computer 38(2)(2022) 70-72.
https://doi.org/10.16707/j.cnki.fjpc.2022.02.015
[26] Z.-H. Li, Y. Yu, X.-Y. Xu, G.-H. Qiao, Study on the Impact of Users' Knowledge Structure on the Effectiveness of Incentive Mechanisms in Blockchain-based Virtual Knowledge Community, Science and Technology Management Research (21)(2023) 142-154.
https://doi.org/10.3969/j.issn.1000-7695.2023.21.017
[27] F.-G. Hu, X.-Q. Wang, An Ethical Review of the Educational Virtual Community Empowered by Metaverse, Modern Educational Technology 32(11)(2022) 5-14.
https://doi.org/10.3969/j.issn.1009-8097.2022.11.001
[28] F. Chen, K. Zhou, J.-M. Zhu, H.-Y. Jiang, J.-X. Yang, Evolutionary game analysis of data elements in a blockchain-based trusted data space, Journal on Communications 46(10)(2025) 100-117.
https://doi.org/10.11959/j.issn.1000-436x.2025185
[29] H.-Y. Gao, C.-J. Cao, X. Xu, Q.-Q. Pei, X. Lu, H. Lei, Survey on blockchain ecosystem common security risk analysis, Chinese Journal of Network and Information Security 11(2)(2025) 1-25.
https://doi.org/10.11959/j.issn.2096-109x.2025015
[30] Aorigele, L.-X. Li, J.-Z. Du, Survey of Blockchain Based Data Sharing Incentive Mechanism, Journal of Computer Engineering and Applications 61(18)(2025) 78-98.
https://doi.org/10.3778/j.issn.1002-8331.2501-0262
[31] Q. Zhong, G.-Y. Zhang, Research on tripartite evolutionary Game of cloud manufacturing service platform trading from the perspective of blockchain empowerment, Journal of Science and Technology Management 26(5)(2024) 1-13.
https://doi.org/10.16315/j.stm.2024.05.001
[32] C. Liu, S.-W. Huang, H.-Y. Yang, Q. Cao, X.-Y. Liu, Network negative energy propagation dynamics model and simulation, Journal of Computer Applications 39(10)(2019) 2966-2972.
https://doi.org/10.11772/j.issn.1001-9081.2019040664