1.Leveraging blockchain for industry funding: A social media analysis

**Abstract**

This study explores the impact of blockchain technology on industry funding, particularly through Initial Coin Offerings (ICOs) and Security Token Offerings (STOs). Utilizing social media analytics, specifically from X (formerly Twitter), the research analyzes 59,453 tweets using natural language processing (NLP) to assess sentiments and emerging trends surrounding blockchain funding mechanisms. The findings reveal significant insights into user opinions, the influence of sentiment on market dynamics, and the potential of blockchain to enhance funding accessibility while addressing information asymmetry among investors.

**Introduction**

The introduction discusses the digitalization of corporations and the emerging role of blockchain as a transformative technology in finance. It highlights the significance of social media in disseminating information about blockchain-based funding mechanisms and sets the stage for investigating the intersection of blockchain, ICOs, STOs, and social media analytics.

**Literature Review**

| **Topic** | **Key Findings** |
| --- | --- |
| Blockchain and FinTech | Blockchain technology enhances transparency and security in financial transactions [[2]]. |
| ICOs and STOs | ICOs provide innovative funding solutions for startups but come with challenges related to regulatory compliance [[3]]. |
| User-Generated Content | Social media serves as a valuable source for public sentiment analysis, impacting market behavior [[4]]. |

**Methodology**

**Data Collection**

We collected data from X (formerly Twitter) using the Academic API, focusing on tweets in English related to "initial coin offering," "industrial blockchain," and "security token offering" from January 1, 2020, to December 31, 2022. A total of 59,453 tweets were analyzed.

**Data Analysis Techniques**

* **Natural Language Processing (NLP)**: Employed for sentiment analysis and topic modeling using BERTopic, which captures the primary themes present in the tweets.
* **Sentiment Analysis**: Utilized RoBERTa model to classify tweets as positive, negative, or neutral.
* **Entity Network Analysis**: Conducted using Named-Entity Recognition (NER) to identify key entities within the tweets, followed by co-occurrence network analysis.

**Results**

The results indicate a significant relationship between user sentiment on X and interest in blockchain technology. A majority of the tweets analyzed expressed positive sentiment, highlighting optimism towards blockchain's transformative potential in various industries. The topic modeling identified key themes related to ICOs, STOs, investment security, and corporate challenges.

**Discussion**

The discussion interprets the findings, emphasizing the role of social media in shaping perceptions of blockchain technology and its funding mechanisms. It addresses the implications of user sentiment on market dynamics and the necessity for improved information dissemination to mitigate information asymmetry.

**Conclusion**

This research underscores the critical intersection of blockchain technology, social media, and funding mechanisms. The findings point to the necessity for stakeholders to harness user-generated content to enhance understanding and facilitate informed decision-making in blockchain investments.

**References**

1. C. Blanco-González-Tejero, E. Cano-Marin, K. Ulrich, and S. Giralt-Escobar, "Leveraging blockchain for industry funding: A social media analysis," *Sustainable Technology and Entrepreneurship*, vol. 3, no. 100071, 2024. doi: 10.1016/j.stae.2024.100071.
2. W. F. Wang, Z. Yan, Y. Luan, and H. Zhang, "Blockchain adoption and security management of large scale industrial renewable-based systems: Knowledge-based approach," *Journal of Innovation & Knowledge*, vol. 8, no. 1, 2023.
3. P. Fisch, "Initial coin offerings (ICOs) to finance new ventures," *Journal of Business Venturing*, vol. 34, no. 1, pp. 1-22, 2019.
4. O. Kraaijeveld and J. De Smedt, "The predictive power of public Twitter sentiment for forecasting cryptocurrency prices," *Journal of International Financial Markets, Institutions and Money*, vol. 65, 2020, Article 101188

2.A multi-layer trust framework for Self Sovereign Identity on blockchain:

**Abstract**

The paper presents a multi-layer trust framework for Self Sovereign Identity (SSI) on blockchain, addressing the trust issues between verifiers and issuers of verifiable credentials. The proposed framework integrates trust relationships among users for specific contexts and utilizes blockchain technology to maintain the integrity and verifiability of these relationships.

**Introduction**

The introduction discusses the growing interest in decentralized systems and the shift towards Self Sovereign Identity (SSI) paradigms, emphasizing the need for a reliable trust management system to facilitate interactions among users without a central authority.

**Literature Review**

The literature review explores existing trust management frameworks and their limitations in the context of SSI. It identifies gaps in current research and positions the proposed framework as a solution to enhance trust relationships in decentralized identity systems.

| **Author(s)** | **Year** | **Title** | **Key Findings** |
| --- | --- | --- | --- |
| Zimmermann | 1995 | The Official PGP User’s Guide | Introduced the Web of Trust concept. |
| Di Francesco Maesa et al. | 2023 | A multi-layer trust framework for Self Sovereign Identity on blockchain | Proposed a new multi-layer trust framework. |
| Lazer et al. | 2018 | The science of fake news | Highlighted challenges in trust and credibility in online information. |
| Wilson & Ateniese | 2015 | Enhancing PGP using bitcoin and the blockchain | Discussed the integration of blockchain with trust frameworks. |

**Methodology**

**3.1 Framework Design**

The design of the multi-layer trust framework is discussed, detailing each layer's purpose: issuers layer, contexts layer, and entrypoints layer.

**3.2 Implementation**

An overview of the implementation process using Solidity smart contracts on Ethereum blockchain is provided.

**3.3 Data Collection**

Description of the dataset used for evaluation, including the Extended Epinions dataset.

**Results**

The results section presents findings from the experimental evaluation of the proposed framework, detailing performance metrics such as gas usage, transaction execution times, and trust evaluation results on both public and private blockchains.

**Discussion**

This section discusses the implications of the results, addressing the strengths and weaknesses of the proposed framework and its potential impact on real-world applications regarding trust in SSI.

**Conclusion**

The conclusion summarizes the key contributions of the paper, reiterating the importance of trust management in SSI and the effectiveness of the proposed framework in enhancing user interactions.

**References**

1. D. Di Francesco Maesa, P. Mori, "A multi-layer trust framework for Self Sovereign Identity on blockchain," *Online Social Networks and Media*, vol. 37-38, pp. 100265, 2023.
2. P.R. Zimmermann, *The Official PGP User’s Guide*, MIT Press, 1995.
3. D.M. Lazer et al., "The science of fake news," *Science*, vol. 359, no. 6380, pp. 1094-1096, 2018.
4. G. Ateniese, D. Wilson, "From pretty good to great: Enhancing PGP using bitcoin and the blockchain," in *Network and System Security: 9th International Conference*, NY, USA, 2015, pp. 368-375.

3.Content privacy enforcement models in decentralized online social networks:

**Abstract**

In recent years, Decentralized Online Social Networks (DOSNs) have gained popularity due to their ability to reduce risks associated with censorship and surveillance. This paper investigates various content privacy enforcement models utilized in DOSNs, analyzing their effectiveness and limitations. We classify these models into three main types: encryption-based, LKH-based, and allocation-based. Through experimental evaluations, we assess the performance of these models in typical operations such as content publication, user joining, and user leaving. Our findings provide insights for improving privacy mechanisms in DOSNs and highlight future research directions.

**1. Introduction**

The introduction highlights the need for privacy in social networks and the unique challenges posed by DOSNs compared to traditional centralized networks. It outlines the objectives of the paper and the significance of the study in the context of digital privacy.

**2. Literature Review**

**Table 1: Summary of Privacy Enforcement Models in DOSNs**

| **Survey/Reference** | **Privacy Enforcement Model** | **Theoretical Model** | **Experimental Evaluation** | **Details** |
| --- | --- | --- | --- | --- |
| [17] | N/A | N/A | N/A | Study the architecture to implement a general purpose DOSN |
| [20] | ✓ | ✓ | N/A | Analysis of design choices |
| [29] | ✓ | ✓ | ✓ | Evaluation of the privacy management mechanisms |
| This paper | ✓ | ✓ | ✓ | Evaluation of group privacy management mechanisms |

**3. Methodology**

The methodology section describes how the research was conducted, including the design of experiments to evaluate different privacy enforcement models.

**3.1 Experimental Setup**

* Description of simulation environments and parameters used in the experiments.
* Overview of the evaluation criteria for assessing performance.

**3.2 Data Collection**

* Explanation of how data was collected and analyzed across different models.

**4. Results**

This section presents the findings from the experiments conducted on the different privacy enforcement models. It includes graphical representations of performance metrics, such as execution time and resource utilization for group join, leave, and content publishing operations.

**5. Discussion**

In this section, the implications of the results are discussed in relation to existing literature, focusing on the strengths and weaknesses of each privacy enforcement model. The discussion also includes recommendations for practitioners and future research avenues.

**6. Conclusion**

The conclusion summarizes the key findings of the study, emphasizing the importance of selecting appropriate privacy enforcement models based on group types and activities. It reiterates the need for ongoing research in the area of privacy in DOSNs.

**7. References**

The references will be formatted in IEEE style as follows:

1. C.A. Yeung et al., "Decentralization: The future of online social networking," in *W3C Workshop on the Future of Social Networking Position Papers*, vol. 2, pp. 2–7, 2009.
2. A.K. Jain et al., "Online social networks security and privacy: comprehensive review and analysis," *Complex Intell. Syst.*, vol. 7, pp. 2157–2177, 2021.
3. A. Bielenberg et al., "The growth of diaspora-a decentralized online social network in the wild," in *Computer Communications Workshops*, 2012 IEEE Conference on, pp. 13–18.
4. A. De Salve et al., "Content privacy enforcement models in decentralized online social networks: State of play, solutions, limitations, and future directions," *Computer Communications*, vol. 203, pp. 199–225, 2023.