Ingénierie des Systèmes d'Information
Vol. 29, No. 1, February, 2024, pp. 19-25
Journal homepage: http://iieta.org/journals/isi

Comparative Analysis of Blockchain Platforms for Security Enhancement in Online Social Networks

Susan Mohammed[1*], Nabeel Al-Aaraji[1], Ahmed Al-Saleh[2]

[1] Software Department, IT College, University of Babylon, Babel 51002, Iraq
[2] Information Networks Department, IT College, University of Babylon, Babel 51002, Iraq

Corresponding Author Email: susanmohammed@itnet.uobabylon.edu.iq

https://doi.org/10.18280/isi.290103

Received: 20 July 2023
Revised: 3 December 2023
Accepted: 9 January 2024
Available online: 27 February 2024

Keywords:
online social networks, security attacks, blockchain, centralized social networks, decentralized social networks, blockchain platforms, Steem, Ethereum

ABSTRACT

As people's lives become more reliant on Online Social Networks (OSN), ensuring the security and protection of their personal information has become critical. These platforms expose users to possible security flaws and privacy violations, like identity theft, even while they provide a variety of tools for communication and interest sharing. This paper is a survey paper that examines the security concerns of online social networks, such as Sybil attacks, in which phony identities threaten integrity; identity theft, which exploits personal information; and de-anonymization, which exposes user identities. Furthermore, it provides a thorough examination of Blockchain technology as a dependable solution to these security issues. Furthermore, this study finds the best secure solutions by evaluating various Blockchain platforms such as Steem, Hive, Sapien, and Ethereum. The findings reveal that Blockchain technology provides a robust and effective security framework for safeguarding online social networks, offering enhanced protection against various OSN attacks.

1. INTRODUCTION

Online social networks are the most widespread and commonly used methods of connection and communication worldwide. It now forms a crucial part of our social lives and enables us to communicate with friends, family, coworkers, and others. The way people use the Internet for both personal and professional purposes has been transformed by social network platforms like Facebook, Twitter, and WhatsApp [1]. Due to these social networks' enormous popularity and the frequent use by young people and others who disregard security and privacy, much potentially private information is being published online for public viewing [2]. The continuous increase in the number of members and the huge amount of personal information being exchanged has created new security risks that pose a threat to users [3].

Many security and privacy attacks occur on online social networks, necessitating remedies to maintain users' privacy and keep shared data safe from different attacks. Private information of persons or organizations, digital identity, financial assets, intellectual property, and organizational secrets and resources are all vulnerable to assaults in Online Social Networking [4].

Several methods for using blockchain to stop fake profiles and news and to prevent social security attacks have been proposed. Different blockchain components, platforms, and models are being used to protect and keep social network data safe from attacks and privacy violations. The focus is on reviewing studies that delve into the intersection of attacks on social networks and the utilization of secure blockchain platforms, components, and models. This paper aims to provide insights into the landscape of attacks and identify blockchain solutions that offer heightened security to safeguard social network data. The following survey reviews some of the studies that have focused on this area.

Ba et al. [2] analyzed blockchain Online Social Networks (OSN) to understand the recent trend of decentralized social applications (Dapps) and described which characteristics were important in a blockchain-based social network. Real data were analyzed by exploring one of the most famous DApp sites and comparing many blockchain platforms to decide which could apply perfectly to a real social scenario, like Facebook. The author discovered that practically all social DApps are built on the Ethereum platform. Other significant blockchains include Steem and Hive, which were built with social interaction in mind. As a result, these blockchains offer several social features that other blockchains do not. The author further reported that the most crucial factors in selecting a blockchain are scalability and transaction fees. The consensus algorithms must also be considered. The authors also evaluated the characteristics of the blockchains used in DApps, discussed how they might be enhanced to meet social needs, and clarified that no current blockchains make sense when considering social scenarios like Facebook or YouTube. However, social blockchains like Steem and Hive are preferred, and EOSIO is a good Ethereum substitute in a social setting. The author also reviewed recent developments in blockchains, including Ethereum, which can enhance the use of the technology in social contexts.

Chen and Cho [5] suggested a secure and reliable framework for social networking using a model built on a blockchain-enhanced social networking framework to create

value for user-generated content. The paper explained the application of this framework for robots and Internet of Things (IoT) devices in collocated spaces. It acknowledges the difficulties associated with integrating blockchain technology into social networking sites and introduces Blockchain-Enhanced Social Networking Sites (BEV-SNS). This framework aims to incentivize user behavior on social networking sites (SNSs) with two primary goals: providing control over data access and facilitating value creation through SNS transactions. The inherent structure of blockchains allows users to tailor sharing and reward parameters within BEV-SNS frameworks, ensuring a secure, reliable, and rewarding networking experience. This stands in contrast to the existing social networking model, which lacks sufficient provisions for privacy, security, and trust [5].

Chen et al. [6] stated that moving to decentralized OSNs has many user benefits, such as data privacy, availability, and access control. Furthermore, OSN providers can enjoy a scalability cost reduction. They employed the blockchain as a trusted server to deliver central control functions by integrating smart contracts. They also segregated the storage services to give users total control over their data and tested the efficacy of their framework using sets of real-world data in the experiment.

Farnaghi and Mansourian [7] stated that blockchain technology was used to develop OSN services to decentralize its operations. The Interplanetary File System (IPFS) can normally store a large volume of data, requiring low-security requirements to make data decentralized. A decentralized autonomous organization was created to enable users to self-manage the OSN autonomously. Their study demonstrated how blockchain technology is employed in OSNs. Users keep their security information to prevent security information leaks from centralized servers. Users do not need to worry about service outages caused by centralized entities because the social network service is decentralized.

Guidi [8] discussed many security issues with utilizing social networks. This paper stated that blockchain could secure any network, such as centralized (peer-to-peer) and distributed networks. Furthermore, blockchain can be a security system for commercial banking transactions. This study emphasized the possibilities of blockchain technology in numerous industrial areas, including supply chains, where it can effectively handle the marketing of counterfeit goods by keeping track of the complete supply chain mechanism in a timestamped and tamper-proof manner in real-time. They also discussed how blockchain could be used in the healthcare industry to store and securely share Electronic Health Records. Blockchain may also be able to address problems facing the IoT sector by managing a sizable number of devices in a distributed and peer-to-peer fashion. Blockchain technology can also help the governance sector by offering safe systems for managing and tracking assets and identities. The previous related works found that blockchain played a big role in saving and securing social networks. Previous research emphasizes the substantial impact of blockchain on enhancing the security of social networks. Notably, blockchain contributes to security by ensuring data integrity, mitigating the risks of fake profiles, and effectively countering the propagation of misinformation.

The rest of this paper is as follows: in parts two and three, we discuss an exploration of the dynamics of online social networks and an in-depth analysis of blockchain technology. Part four discusses a detailed examination of the significance of blockchain-based decentralized social networking platforms and their importance in the context of online social networks. Parts five and six delve into the distinctive features characterizing decentralized social networks and a thorough analysis of various blockchain-based social network platforms. Parts seven and eight discuss insightful discussions on security attacks targeting online social networks and comprehensive exploration of effective solutions. Finally, parts nine and ten are engaging discourse summarizing the findings and conclusions, providing a thoughtful wrap-up to the paper.

2. ONLINE SOCIAL NETWORKS (OSN)

OSNs are social media platforms that are accessible via the Internet and are used to maintain contact with friends, family, coworkers, customers, or clients. Through websites like Facebook, Twitter, LinkedIn, and Instagram, OSN can have a social purpose, a corporate purpose, or both. It is a crucial foundation for marketers who want to engage customers [7].

Existing OSNs are usually centralized, meaning OSN companies often fully own all user data and services. In the centralized model, most OSN providers offer free services to their users, and in return, they reserve the right to use the data posted by the users in any way possible. This model raised concerns about the privacy and ownership of the content, which requires great trust in the OSN providers. OSNs must also be highly scalable to include an ever-increasing number of users, which is challenging for a centralized architecture. Data availability can also become an issue concerning server downtime and service shutdowns. In addition, because of the severe lack of interoperability between different OSN sites, users wishing to share the same data on different OSN networks had to carry that data separately. The problems of centralized OSNs prompted research to shift to a decentralized OSN. Work in this field addresses issues such as privacy, access control, data availability, scalability, use of data in various administrative areas through social applications, security attacks on OSN, etc. [6].

3. BLOCKCHAIN TECHNOLOGY

Blockchain is a shared, immutable ledger for recording transactions, tracking assets, and building trust [7], as shown in Figure 1.

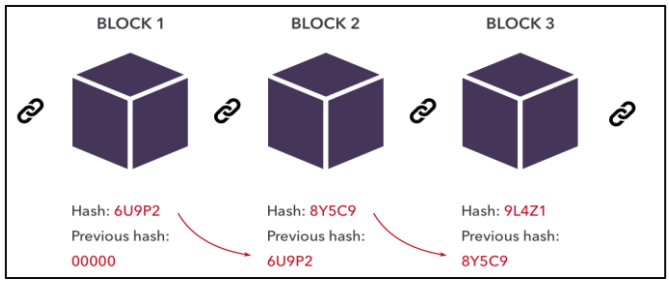

Figure 1. Architecture of blockchain blocks

A blockchain is made up of a chain of blocks, each of which is built on top of the one before it. A Blockchain stores transaction information, a timestamp, and the cryptographic hash of the preceding block. Since the ledger is distributed and open to all users, it is difficult to alter blocks once they have been added to the chain. Continuous updates and

synchronization are made to the ledger. The new transaction must be encrypted and verified by the other users in the network if we need to add it to the ledger. Here comes the role of a consensus protocol, the transaction is considered valid and added to the ledger only if there is a consensus among the majority of users. The two most important characteristics of blockchain technology are the distributed consensus protocol and the anonymity property [8].

Cryptographic hash functions are integral to the blockchain's core mechanics. When a transaction is added, these functions condense data into a unique hash, ensuring data integrity. The hash also links blocks, forming an immutable ledger. Altering any transaction not only changes its hash but affects subsequent blocks, enabling easy detection of tampering. Moreover, hash functions play a crucial role in consensus protocols, efficiently verifying transaction validity. In essence, cryptographic hash functions underpin the blockchain's security, transparency, and consensus processes [9].

There are two major categories of blockchains. The first is permission-less which allows anybody to use them. The second is private and permission, where participation in the block validation process is allowed for a designated set of authorized validator nodes (i.e., miners) [10].

The following example highlights how Steemit leverages blockchain to create a decentralized and incentivized social network, where users are directly rewarded for their contributions [11].

Steemit is a blockchain-based social network that utilizes blockchain technology to reward content creators through cryptocurrency incentives. Users on Steemit can create and curate content. Blockchain ensures transparency in content creation, and the platform rewards users with cryptocurrency based on the popularity and quality of their contributions [11].

- **Decentralization:** Content is not controlled by a central authority, fostering a decentralized and censorship-resistant social network [11].
- **Incentivized Participation:** Users are financially rewarded for their engagement, promoting quality content and active participation [11].

4. BLOCKCHAIN-BASED DECENTRALIZED SOCIAL NETWORKING PLATFORMS

DApps are blockchain-based decentralized networking platforms. These platforms are built on blockchain protocols that enable application development and smart contracts. Many blockchain protocols support DApps, such as Ethereum, Steem, Hive, and Stellar. No central proprietary authority oversees the data of DApps, and thus, blockchain social networks are decentralized. Instead, the data distribution is done across servers at each network node in a homogeneous and decentralized manner [11].

In recent years, social networking sites have sparked numerous controversies. Major platforms like Twitter, Facebook, and YouTube possess the authority to censor users and content, even against users' preferences [12]. Users can also restrict money flow on their own. Blockchain technology can solve all these issues. Social network ventures can avoid censorship by keeping user content on a blockchain’s immutable ledger [11].

Decentralized social networks differ from traditional media sites in several key aspects that attract users. Firstly, unlike a single website, decentralized social networks comprise numerous communities, each equipped with its own code copy. Secondly, users have the flexibility to determine the visibility of their instance, whether public or private. Additionally, they can connect with users from other instances and even across different platforms [13].

Like traditional social network platforms, decentralized social networks enable users to post content, add comments, utilize hashtags, and share information. The main drawback is that their user interface may be less visually appealing compared to centralized social media networks. However, what these networks lack in aesthetics, they compensate for with enhanced freedom, privacy, security, and decentralization [14].

By leveraging decentralized social networks, users can tap into unique opportunities, such as creators earning token equivalents for major cryptocurrencies. This capability extends beyond creative expression, enabling creators to monetize their content. A compelling example is Steemit, a decentralized social network where creators earn cryptocurrency tokens (Steem) commensurate with the popularity and quality of their content. This innovative approach not only empowers content creators but also opens avenues for them to sell products in exchange for crypto on select decentralized social networks [15].

5. FEATURES OF DECENTRALIZED SOCIAL NETWORKS

Platforms for social networks not governed by a single entity are known as decentralized platforms. These platforms have greater security, user control, and freedom from censorship. These platforms are excellent for usage in repressive regimes because they can be harder to shut down. Although these platforms are now less well-liked than centralized platforms, their unique qualities can entice many people to switch from centralized to decentralized social platforms. Decentralized social networks have several benefits and features, including the following [14].

5.1 No single central server

The most crucial item to consider is that decentralized social media networks often do not rely on a single central server. A single central organization controls most of the largest and most popular social networks, including Facebook, Twitter, and Instagram. This could be dangerous since it could result in massive cyberattacks, takeovers, and information leaks [12].

5.2 Hosts multiple networks within one platform

Platforms for decentralized social networks serve a different purpose than centralized ones. They favor networks that give people the freedom to choose what they want. Anyone can create a network that enables people with shared interests to collaborate. A decentralized platform enables the simultaneous hosting of numerous social networks of different types. In general, anyone using the Internet can start their community, and anyone with similar ideas or interests can use this type of social media. A separate server can power many networks inside a decentralized social network platform. Users can communicate with other networks through independently hosted decentralized networks [13].

5.3 Increased security

Contrary to conventional platforms that use a single centralized server, large decentralized social network platforms employ several separate servers. Utilizing extra servers considerably reduces the possibility of a full network failure brought on by technical issues. Using this clustered system also significantly lowers the risk of cyberattacks [14].

Decentralized social networks have made communication easier and also given people a different option for data protection. Users can create accounts on federated social networks without having to give their email addresses or phone numbers. These cloud-based social networks also use public-key cryptography to secure user accounts. Users are not required to log in using their true identities and they can choose aliases in their private accounts to increase their level of anonymity further [15].

5.4 Increased user control

For individuals who reject constraints, decentralized networks provide a way out because they give them no control over their data or what they disclose in private communications. Decentralized social networks give users total control over their data, interactions, and experiences. Decentralized networks are often used by people who want to shield themselves from invasive marketing and advertising and its associated risks [16].

6. BLOCKCHAIN-BASED SOCIAL NETWORK PLATFORMS

There are many blockchain-based social network platforms, for example, Society2, Peepeth, Sapien, Steemit, and Hive. We will explain them briefly [12].

- **Society2** is an architecture for a decentralized social network that is client-, information-, and speech-driven. Participants can exchange information and manage their relationships, conversations, and status on the site [3].
- **Peepeth** is like the Twitter decentralized social network. Accounts and "peeps" (posts) on Peepeth are stored on the blockchain. Members can accept cryptocurrency tips. One distinctive aspect is that members are only permitted one "Ens" (analogous to a "like") every day. This rule was enacted to encourage high-quality content and participation [15].
- **Sapien** is one of the platforms based on Ethereum. A proof of value consensus protocol has been used to build a completely autonomous social network environment that pays content creators and fights false information to give consumers back control over their social network experience. Sapien users are given a speech structure and encouraged to get involved in the community [12].
- **Steemit** is a social media and blogging platform based on blockchain. According to Steemit, users of social networking sites ought to fairly reap the advantages of their attention and labor. With its cryptocurrency STEEM, it rewards users for creating and curating content [10].
- **Hive** is a completely decentralized messaging platform; thus, there is no centralized target for malicious users to steal or alter data. The blockchain-based nature of the HIVE also ensures the integrity of the data. HIVE guarantees that a message sent across a network will not be altered by having three different points of data integrity verification, including the Ethereum blockchain. HIVE also ensures the confidentiality of data by encrypting all information sent across the network [2].
- **Ethereum** with the use of the blockchain platform Ethereum, users can send and receive money without the involvement of a middleman like a bank. The Ethereum blockchain is decentralized, meaning nobody controls it, just like Bitcoin. Thus, the data submitted to the blockchain cannot be altered by a single person or authority. The Ethereum blockchain system was the first to implement "smart contract" technology. A smart contract comprises only cryptographic rules when specific requirements are satisfied. These rules are protocols or small pieces of code. The blockchain is used to distribute the smart contract code [17].

Today, Ethereum is the most popular platform, mainly because along with Bitcoin, it is one of the most well-known platforms and offers the smart contracts necessary to enable DApps. Ethereum has a high level of assault resistance. It would cost billions of dollars to compromise Ethereum, and even then, success would not be guaranteed [16].

7. ONLINE SOCIAL NETWORK SECURITY ATTACKS

The daily OSN activities of billions of active web users are sharing pictures, personal information, location, tagging, and blogging making these users more vulnerable to various privacy issues. The attackers are prompted to act abusively and steal information from OSN by various factors, including secret information, professional information, financial gain, molestation, access control, etc. [13]. The following lists the most well-known OSN security attacks:

- **Fake profile attack**

The adversary can create a new account like the original user account in any social network by collecting information about the user from different OSNs. The fake profile attack is similar to Sybil or social bots attack [18]. Fake profile attacks can have detrimental effects on both users and the network. Users are vulnerable to misleading interactions, potentially causing reputational harm. The network, in turn, faces compromised credibility as fake profiles are utilized to spread misinformation, undermining the platform's trustworthiness [18].

- **De-anonymization attack**

Anonymization involves using certain techniques from unauthorized access to hide personal information. In the de-anonymization technique, the attacker tries to expose user information by tracking the network topology, user group membership, and cookies [18]. De-anonymization attacks pose risks to user privacy and network integrity. Users may suffer from privacy breaches, exposing them to identity-related crimes and potential harassment. This jeopardizes the network's reputation for user privacy, leading to a decline in trust among its user base [18].

- **Sybil attack**

In this attack, the adversary gathers the user's personal information by creating fake profiles. The main reason is to reduce the reputation values of the user on the OSN by using one online entity to manage several fake profile entities. The adversary promoted his account's popularity and reputation

through this attack by voting for it [6]. Sybil attacks impact users by manipulating social connections and eroding trust within the network. Users may find their interactions compromised and the authenticity of the network's user base in question. The network itself experiences compromised integrity, potentially leading to the spread of biased content and a less secure environment [6].

• Malware attack

Malware is malicious software expressly developed to infect or access a computer system, usually without user information. The intruder can spread malware and contaminate devices and networks in numerous ways. In social network platforms, the malware uses the OSN's structure to propagate in it, such as the number of vertices, number of edges, average shortest path, and longest path [15]. Malware attacks can severely impact both users and the network. Users face compromised security, leading to potential financial loss and unauthorized access to personal information. Simultaneously, the network's reputation is at risk due to compromised user devices spreading malware, along with potential disruptions to the platform's infrastructure [15].

• Identity theft

In this attack, the attacker uses the victim's identity, including his social security number, phone number, and address, without the victim's consent to commit the crime. Using various social engineering techniques, the attacker can easily use these facts to access a victim's friend list and demand their private information. Because he poses as a legitimate user, the attacker can use that profile in any way, which could gravely harm trustworthy clients [4]. Identity theft poses significant risks to both users and the network. Users may suffer severe personal and financial consequences, including unauthorized financial transactions and damaged credit scores. The network's reputation is substantially harmed, as it becomes perceived as a platform vulnerable to identity theft, resulting in declining user trust and engagement [4].

8. BLOCKCHAIN SOLUTIONS OF OSN'S SECURITY ATTACKS

Services on traditional social networks are entirely centralized. All information is held by network administrators, who also have complete control over user navigation and everything else on their networks. Numerous requests have been made for networks to change their service models and capabilities due to issues including serious implications for secrecy, limitations, and regulation. Many modern studies combine blockchain with social networks to fix social network problems such as privacy, security, and safety alternatives [3].

The single point of failure problem is one of the problems that central systems are criticized for because it represents one of the system's weaknesses. In contrast, decentralized systems are implemented in a distributed manner. However, this implementation suffers from a data synchronization problem called the Byzantine generals' problem. In other words, the system of decentralized ledger participants must achieve consensus, which means an agreement upon every message broadcasted to everyone in the network. Common Byzantine fault tolerance achievement can be achieved if the "loyal generals' decisions" have a majority agreement [19].

Using blockchain with social networks (decentralized social network platforms) provides solutions to several challenges in social networks, such as single point of failure, security attacks, user control, etc., which are the features of decentralized social networks. These platforms are called blockchain-based social networks [20].

Blockchain technology offers robust solutions to mitigate attacks on online social networks. By implementing decentralized identity verification, blockchain enhances user authentication and reduces the risk of fake profiles. Its cryptographic features enable pseudonymous transactions, mitigating de-anonymization threats and ensuring user privacy. Blockchain's consensus mechanisms and decentralized governance models make it economically unfeasible for attackers to conduct Sybil attacks and manipulate the network. The decentralized nature of blockchain also hinders malware attacks by eliminating single points of failure and enabling secure smart contract execution. Additionally, blockchain's immutability safeguards against identity theft, providing users with greater control over their personal information. In essence, blockchain serves as a foundational layer for building secure, transparent, and resilient online social networks [21].

The future of blockchain in social networking platforms is marked by trends such as enhanced privacy solutions, tokenization of social interactions, interoperability, decentralized content moderation, NFT integration, user governance, DeFi integration, green blockchain solutions, and the convergence of blockchain with augmented and virtual reality. These developments aim to create more user-centric, inclusive, and secure digital communities. The potential integration of sustainable blockchain technologies, adherence to regulatory frameworks, and the emergence of clearer governance models will likely shape the landscape, offering users greater control, transparency, and innovative ways to engage and transact within decentralized social ecosystems.

9. DISCUSSION

Social networks have many downsides, including fraudulent accounts, incorrect information, inadequate content screening, digital piracy, data breaches, identity fraud, and digital piracy. Social networks are also vulnerable to several security vulnerabilities. To overcome these restrictions, several studies introduced blockchain technology in social networks. Transparency, traceability, tamper-proofing, secrecy, security, information control, and supervision are a few of the many services that blockchains can offer. Tamper-proofing refers to the practice of securing a system or data in a way that makes it extremely difficult for unauthorized individuals to alter or manipulate without detection. Blockchain services can solve many social networking problems, especially the security problem, which is one of the most common problems in social networks.

In recent years, the combination of blockchain and social network platforms has generated great interest from researchers due to its rapid advancement and continued popularity. Many papers have suggested solutions for social network problems from innumerable viewpoints. This topic has become one of the most important and popular topics.

The research papers mentioned above suggest many ways to secure online social networks using the blockchain. Some papers suggested using a particular blockchain platform over another [17]. Others suggested building a model based on the blockchain to achieve high security for social networks [22].

Despite the different and diverse ways of using the blockchain, most researchers agree that its use will secure social networks optimally.

The requirements that must be met to build a strong and secure integrated decentralized application are the types and features of the platform and the type of consensus protocol used to determine the strength and speed of the network. A consensus protocol is a set of rules and mechanisms that enable distributed systems, particularly in blockchain technology, to reach an agreement on the state of a shared ledger or database. It ensures that all nodes in the network agree on the validity of transactions, maintaining consistency and preventing double-spending. The Ethereum network is the most popular and widely used because of the possibility of using smart contracts because it has high flexibility that allows for building a decentralized application that meets the user's requirements.

A blockchain model must be built with two objectives: the first is to control access to data, and the other is to create value through social networking site deals. The current (centralized) social networking model does not provide much privacy, security, and trust. Meanwhile, using a Blockchain-based social network model guarantees the user to try more reliable networks with a higher security reward system.

A blockchain-based framework for decentralized online social networks uses the smart contracts of the Ethereum platform. The blockchain was a trusted server to implement the functions to prepare traditional centralized social network servers. When comparing the traditional centralized social networks with the proposed design, it was found that the latter provides efficiency, security, and functionality characterized by privacy.

The characteristics of blockchain, such as resistance to tampering, data interconnection, and trust, have made blockchain the most secure system. Blockchain provides privacy and high security for the data published within the network. The blockchain provides strong security mechanisms for all types of networks, even for online financial exchanges, like those in banking institutions [10, 23].

In summary, the key outcomes of the mentioned research papers contribute to the existing body of knowledge by presenting diverse strategies for securing online social networks through blockchain. These insights encompass considerations such as platform selection, consensus protocols, and the specific objectives of blockchain models, offering a nuanced understanding of the potential and challenges associated with integrating blockchain technology into social networking platforms**.**

10. CONCLUSIONS

This paper finds that blockchain is a promising technology for improving the security of online social networks because it has many advantages such as the dependence of the blockchain on cryptographic algorithms to ensure data integrity, confidentiality, and reliability. Blockchain also has smart contracts for data access, making the database distributed and tamper-proof. In addition, users are given complete control over their valuable content. Thus, compared to the existing centralized OSNs, blockchain-based social media is a good alternative.

This paper explored how five researchers use blockchain technology to secure online social networks. The problems with present blockchain platforms are reviewed, and the characteristics most crucial for selecting an appropriate blockchain are identified. Some decentralized online social network platforms, like Steem, Hive, Sapien, Ethereum, etc., can be used to secure social networks because they offer several social features that other blockchain platforms do not. Ethereum is also determined to be the most secure blockchain because hacking Ethereum would be complicated for a single person or group. The hack would require expensive computer hardware worth billions of dollars.

The findings indicate blockchain's promising role in enhancing online social network security through improved data integrity and user control.

This work stands out from prior research by specifically focusing on applying blockchain technology to enhance the security of online social networks. In contrast to earlier studies that explored broader blockchain applications or specific facets of social network security, this research provides a comprehensive examination of how blockchain's cryptographic algorithms and smart contracts can ensure data integrity and user control. The study evaluates existing blockchain platforms, including Steem, Hive, Sapien, and Ethereum, for securing social networks, offering practical insights. Notably, it identifies key criteria for blockchain selection and emphasizes Ethereum's security due to its complexity and resource-intensive nature, providing valuable practical and comparative perspectives.

Future works could build a new decentralized OSN based on blockchain technology with machine learning or deep learning that protects the online social network against the attacks that traditional social networks are exposed to.

REFERENCES

[1] Ali, M.A., Bhaya, W.S. (2021). Higher Education's certificates model based on blockchain technology. In Journal of Physics: Conference Series, IOP Publishing Ltd, 1879(2): 022091. https://doi.org/10.1088/1742-6596/1879/2/022091

[2] Ba, C.T., Zignani, M., Gaito, S. (2021). Social and rewarding microscopical dynamics in blockchain-based online social networks. In Proceedings of the Conference on Information Technology for Social Good, pp. 127-132. https://doi.org/10.1145/3462203.3475913

[3] Ba, C.T., Zignani, M., Gaito, S. (2022). The role of cryptocurrency in the dynamics of blockchain-based social networks: The case of Steemit. Plos One, 17(6): 12-26. https://doi.org/10.1371/journal.pone.0267612

[4] Meligy, A.M., Ibrahim, H.M., Torky, M.F. (2017). Identity verification mechanism for detecting fake profiles in online social networks. International Journal of Computer Network and Information Security (IJCNIS), 9(1): 31-39. https://doi.org/10.5815/ijcnis.2014.01.01

[5] Chen, N., Cho, D.S.Y. (2021). A Blockchain based autonomous decentralized online social network. In 2021 IEEE International Conference on Consumer Electronics and Computer Engineering, ICCECE 2021, Guangzhou, China, pp. 186-190. https://doi.org/10.1109/ICCECE51280.2021.9342564

[6] Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. High-Confidence

Computing, 2(2): 100048. https://doi.org/10.1016/j.hcc.2021.100048
[7] Farnaghi, M., Mansourian, A. (2020). Blockchain, an enabling technology for transparent and accountable decentralized public participatory GIS. Cities, 105: 102850. https://doi.org/10.1016/j.cities.2020.102850
[8] Guidi, B. (2020). When Blockchain meets online social networks. Pervasive and Mobile Computing, 62: 101131. https://doi.org/10.1016/J.PMCJ.2020.101131
[9] Guidi, B. (2021). An overview of blockchain online social media from the technical point of view. Applied Sciences, 11(21): 9880. https://doi.org/10.3390/app11219880
[10] Hisseine, M.A., Chen, D., Yang, X. (2022). The application of blockchain in social media: A systematic literature review. Applied Sciences, 12(13): 6567. https://doi.org/10.3390/app12136567
[11] Idrees, S.M., Nowostawski, M., Jameel, R., Mourya, A.K. (2021). Security aspects of blockchain technology intended for industrial applications. Electronics, 10(8): 951. https://doi.org/10.3390/electronics10080951
[12] Jiang, L., Zhang, X. (2019). BCOSN: A blockchain-based decentralized online social network. IEEE Transactions on Computational Social Systems, 6(6): 1454-1466. https://doi.org/10.1109/TCSS.2019.2941650
[13] Khettry, A.R., Patil, K.R., Basavaraju, A.C. (2021). A detailed review on blockchain and its applications. SN Computer Science, 2(1): 30. https://doi.org/10.1007/s42979-020-00366-x
[14] Jain, A.K., Sahoo, S.R., Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. Complex & Intelligent Systems, 7(5): 2157-2177. https://doi.org/10.1007/s40747-021-00409-7
[15] Leible, S., Schlager, S., Schubotz, M., Gipp, B. (2019). A review on blockchain technology and blockchain projects fostering open science. Frontiers in Blockchain, 2: 16. https://doi.org/10.3389/FBLOC.2019.00016
[16] Mnif, E., Mouakhar, K., Jarboui, A. (2021). Blockchain technology awareness on social media: Insights from twitter analytics. The Journal of High Technology Management Research, 32(2): 100416. https://doi.org/10.1016/J.HITECH.2021.100416
[17] Murimi, R.M. (2019). A blockchain enhanced framework for social networking. Ledger, 4 Apr.(S1): 67-81. https://doi.org/10.5195/ledger.2019.178
[18] Mustafa, A.S., Al-Mashhadani, M.A., Jasim, S.A., Shantaf, A.M., Hamdi, M.M. (2022). Blockchain in fifth-generation network and beyond: A survey. Bulletin of Electrical Engineering and Informatics, 11(3): 1399-1408. https://doi.org/10.11591/eei.v11i3.3209
[19] Muraya, C., Awuor, F., Maake, B. (2021). Fake profile identification on online social networks. Journal of Language, Technology & Entrepreneurship in Africa, 12(2): 48-59.
[20] Obeis, N.T., Bhaya, W. (2016). Review of data mining techniques for malicious detetion. Research Journal of Applied Sciences, 11(10): 942-947.
[21] Poongodi, T., Sujatha, R., Sumathi, D., Suresh, P., Balamurugan, B. (2020). Blockchain in social networking. In Cryptocurrencies and Blockchain Technology Applications. John Wiley & Sons, Ltd, pp. 55-76. https://doi.org/10.1002/9781119621201.ch4
[22] Rathee, P. (2020). Introduction to blockchain and IoT. In Advanced Applications of Blockchain Technology, Springer, pp. 1-14. https://doi.org/10.1007/978-981-13-8775-3_1
[23] Rahman, M.U., Guidi, B., Baiardi, F. (2020). Blockchain-based access control management for decentralized online social networks. Journal of Parallel and Distributed Computing, 144: 41-54. https://doi.org/10.1016/J.JPDC.2020.05.011