IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

# A Literature Survey on Digital Identity Verification Based on Blockchain for Social Media

**Sanjay B[1], Sharath V[2], Assistant Prof. Indushree M[3]**
Department of Information Science and Engineering[1,2,3]
Global Academy of Technology, Bengaluru, India

**Abstract:** *This review delves into the dynamic realms of digital identity and blockchain technology, thoroughly investigating recent advancements and inventive applications where these domains intersect. The examined literature covers a broad spectrum, encompassing diverse subjects like user authentication, decentralized identity management, secure access control frameworks, and accreditation systems. Through a meticulous analysis, the review unveils a variety of methodologies employed to enhance digital identity verification, capitalizing on blockchain's inherent attributes, including decentralization, immutability, and transparency.*

**Keywords:** Blockchain-based Identity Verification, Social Media, Digital Identity Management, Smart Contracts, Machine Learning Algorithms

## I. INTRODUCTION

In the swiftly evolving landscape of social media platforms, there is an escalating demand for robust mechanisms to authenticate digital identities. The surge in online interactions, data sharing, and digital transactions underscores the need for secure and reliable means of confirming user identities. Traditional identity verification methods often prove inadequate in addressing the challenges posed by the dynamic and interconnected nature of the digital realm. In response to these challenges, blockchain technology has emerged as a promising solution, providing decentralized and tamper-resistant systems for identity verification.

This literature survey delves into the confluence of digital identity verification and blockchain technology, with a particular emphasis on its application within the realm of social media. As the digital world experiences unprecedented growth, concerns such as identity theft, data breaches, and privacy violations have become pervasive. Blockchain technology, initially designed to underpin cryptocurrencies like Bitcoin, has evolved into a versatile solution with applications across various industries, notably in the realm of identity verification. The DIVBased on Blockchain for Social Media as shown in fig 1

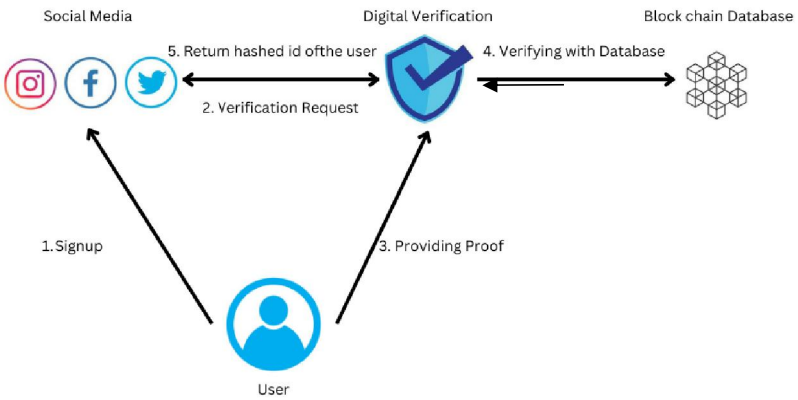


**Fig 1 :** DIV Based on Blockchain for Social Media

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

## II. LITERATURE SURVEY

Ruiguo Yu et Al., [1] as proposed, in order to improve user information security in social network calculations, the paper suggests a novel approach that combines text encryption with an authentication blockchain method. Sensitive data is not compromised by the Authentication with Blockchain algorithm, which guarantees user identity verification. For each user, this entails creating a pair of private and public keys, with the public keys being safely stored on a blockchain. Concurrently, a text encryption protocol strengthens data protection during content suggestion by preventing unwanted access by leveraging the RSA algorithm and numerous hash methods. The method protects user relationship attributes from inquisitive users by using hash functions for relationship encryption. Although all of these methods improve security, there are some clear benefits and drawbacks. Positively, the strategy uses blockchain technology to protect user data and guarantees strong user authentication. Furthermore Eranga Bandara et Al., [2] as proposed innovative answer to the problems with centralized identity systems is the "Casper" digital identity platform. It presents an Android/iOS mobile identity wallet application that acts as a blockchain and self-sovereign identity-based system. Users keep their true identities in this wallet application, and the proof of these identities is safely stored in a decentralized blockchain storage system. Notable characteristics encompass decentralized data storage, an identity verification process based on Zero Knowledge Proof, and the capacity to safely exchange identity information among diverse sectors like government agencies, banks, and healthcare. Casper uses a Zero-Knowledge evidence (ZKP) mechanism for identity verification, a blockchain-based decentralized storage system for identity evidence, a self-sovereign identity (SSI) approach, and the storage of real identity data on users' physical mobile phones in order to address privacy issues.

Peter Mell et Al., [3] as proposed the use of smart contracts on a blockchain for federated identity management, highlighting the advantages for privacy include preserving secrecy in communications between users and reliant parties (RPs) and doing away with the need for outside authentication services. Operating on the Ethereum network, the smart contract only charges for the creation and modification of user accounts, making it economically viable. The structured document includes an example, fundamental functions, contract and attribute field design, and implementation details. The smart contract protects user privacy by using methods including hashing attributes, encrypting data with the user's public key, and referencing external safe databases. Users' self-sovereignty is enhanced by hierarchical administration, which makes attribute providers more effectively validated. Improved privacy, financial savings, and hierarchical administration for sizable organizations are benefits. Furthermore Arshad Jama et Al., [4] as proposed blockchain-based identity verification system is purposefully made to take advantage of blockchain's security properties in order to store individual personal records. Three primary user kinds are introduced by this novel system: third-party requesters, users, and authorities. While third-party requesters can request access to user data, users retain control over their data access and can keep an eye on requester activities. Authorities can upload personal information and check companies. Continuous verification is ensured by using a decentralized database and blockchain technology, which improves data security, strong access control, transparency, and the veracity of confirmed identities. The system's user-centric design aims to reduce identity theft and data breaches by empowering people to take control of their personal data. The usage of user authentication, smart contracts for access, and decentralized storage by the system are covered in the document.

Guy Zyskind et Al., [5] as proposed the growing privacy concerns related to centralized data collecting and suggests using blockchain to create a decentralized personal data management system. Using a technology that turns the blockchain into an automated access-control manager, this novel solution promotes user ownership and control over personal data. Users can meet the desire for more privacy by storing, querying, and sharing data without depending on a third party. Users are given more control and privacy using a combination of techniques like policy management, fine-grained access control, compound identities, blockchain memory, ownership recognition of data, transparency, and more. The benefits include handling privacy issues, guaranteeing auditability, transparency, and fine-grained access control in addition to possible legal compliance. Nevertheless, there are issues with key management, blockchain integrity presumptions, and Proof-of-Work algorithm energy usage.

Hoang Giang Do et Al., [6] as proposed, BlockDS, a blockchain-based system intended to address issues with conventional cloud storage and provide private keyword search and safe data storage. To guarantee data security, integrity, and availability, BlockDS uses client-side encryption and a proof-of-retrievability mechanism that is enforced by blockchain technology. Users can identify certain encrypted data without downloading the complete dataset thanks

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

to the system's support for private keyword search over encrypted datasets. The danger of data loss is reduced by using distributed data storage across cloud nodes. Benefits include distributed storage that is safe and secure, private keyword search capabilities, and a permissioned blockchain model that improves security and performance. The drawbacks are as follows: dependency on cloud service providers, restricted capabilities regarding boolean keyword search and credential revocation, and implementation complexity.Kai Fan et Al., [7] as proposed,the plan combines blockchain technology with ciphertext-policy attribute-based encryption (CP-ABE) to address security issues in vehicular social networks (VSNs). Using CP-ABE for encryption and access control, it guarantees safe one-to-many data transfer while keeping track of access restrictions on blockchain for user self-certification. Resilient against collusion and cloud service provider attacks, the method allows data revocation, integrates a policy concealment mechanism, and goes through security analysis. User self-certification, policy concealing for improved security, and effective data sharing are notable benefits. Potential drawbacks, however, include the reliance on computer power and the requirement for a shorter consensus time in the blockchain component. Scalability issues and practical implementation difficulties in large-scale VSNs are examples of research gapsand alsoZheng Zhao and Yuan Liu [8] as proposed, explores a decentralized identity management system that makes use of blockchain smart contracts—most notably, Ethereum. With a focus on asset protection and user empowerment, the system uses smart contracts to create customized information sharing rules based on identity attributes and securely saves identity data on the blockchain. An attribute-based reputation model, which guarantees a reliable identity management environment, is essential to the system. Because it is user-centric, it gives people authority over their identity data and permits access by third parties. Although providing decentralization and data security, the system's complexity makes adoption and governance difficult, and security issues with smart contract vulnerabilities continue to be a worry. Research gaps include attribute-based reputation models and overcoming brush reputation problems. In its conclusion, the paper suggests an attribute-based identity management system based on blockchain technology, featuring decentralized functionalities and attribute control.

May Htet et Al., [9] as proposed, A decentralized system linking all passport offices to avoid unlawful duplication is one of the many benefits of using blockchain technology for passport issue in Myanmar. The system uses cryptographic methods to guarantee data integrity and stop changes after they are added to the blockchain. Enhancing security is the process of authenticating and verifying passports after issuing permission for overseas travel. However, there may be difficulties managing massive numbers of passport data due to scalability issues, and more study is required in the areas of privacy, system compatibility, and regulatory frameworks. Subsequent research endeavors may involve broadening the system's scope to incorporate diverse digital identities, evaluating the user experience, and investigating global cooperation and standardization concerning identity management utilizing blockchain technology. Furthermore, Antorweep Chakravorty and Chunming Rong [10] as proposed, this paper examines Ushare, a social media platform that would be built on blockchain technology and prioritize user control, content ownership, and traceability. Ushare, which prioritizes decentralization, security, anonymity, and traceability, is made up of a local personal certificate authority for user circles and encryption keys, a relationship system that manages shares, an encrypted content hash table, and a blockchain. It promotes user-controlled, anonymous, and secure content exchange within predetermined boundaries. Sharing content is protected by off-site encryption, and consistency and traceability are guaranteed by using a permissioned blockchain. By limiting shares, the Turing complete relationship system gives users authority over interactions. An additional degree of security is provided by a local personal certificate authority. Benefits like traceability, anonymity, decentralization, and resistance to censorship are all promised by Ushare. However, potential downsides include issues with key management and data security in a decentralized setting.

Samer Shorman and Mohammad Allaymoun [11] as proposed, the study highlights how blockchain technology could completely transform social networking's use of electronic authentication. It discusses the drawbacks of traditional verification techniques and offers a blueprint for a smooth integration of blockchain technology with social media networks. The concept entails building blockchain blocks with personal data associated with users' social media profiles, providing a reliable point of reference for authentication. The resultant hash code and logo on individual accounts enable followers to confirm legitimacy, which minimizes the number of phony profiles and increases the legitimacy of social networking sites. Technical complexity, privacy issues, and adoption barriers are significant problems despite the emphasis on improved security and less phony accounts. The study's findings demonstrate how

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

blockchain technology can be used to provide a reliable and safe social networking environmentand alsoLe Jiang and Xinglin Zhang [12] as proposed, in order to handle data privacy, integrity, user identity verification, newsfeed notifications, and friend recommendations in social networks, the paper presents the Blockchain-based Decentralized OSN (BCOSN) framework. Through the combination of the best features of decentralized and traditional central server OSNs, BCOSN uses smart contracts to simulate central server functionality, which is difficult to do in current decentralized OSNs. The four parts of the framework—registration, friend adding, post, and comment—use attribute-based fine-grained encryption for different friend permissions and blockchain technology for secure user registration. Notifications for actions are made possible via interfaces such as ConfirmInform and PostInform. Even with multiple concurrent users, BCOSN's message notification performance is tolerable. By integrating blockchain technology with Attribute-Based Encryption (ABE), more specifically timely ciphertext-policy ABE (CP-ABE), the system improves access control. Although BCOSN guarantees user control, data privacy, and integrity, there are still issues with decentralized functionalities that are inefficient.

Gunit Malik et Al., [13] as proposed, he necessity of improving document verification's effectiveness and security in India and suggests blockchain technology as a game-changing remedy. Direct access to documents across government databases is made possible by the blockchain system, guaranteeing a quick, dependable, and secure path. The paper presents a novel government use case and describes the architecture and structure of the blockchain-based document verification system. Recognizing challenges like the cellular nature of issuing authority, IPFS and hash values are used for global file system sharing. Although there are known restrictions when it comes to storing big files on the blockchain, asymmetric encryption guarantees safe document sharing. The benefits of blockchain technology for government include improved efficiency, increased security, and immutability, as well as a smooth user experience.

Michail Tsikerdekis and Sherali Zeadally [14] as proposed, In order to detect identity deception in social media—specifically, sockpuppetry—the paper examines nonverbal user behaviors including modifications and distribution among namespaces. The study identified deceivers with 71.3% accuracy by using machine learning methods such as Support Vector Machine, Random Forest, and Adaptive Boosting. These algorithms have the ability to handle complicated datasets and discover patterns, although their efficacy varies depending on the situation. Finding the best variables for effective detection and turning nonverbal behaviors into measurable variables are two areas of unmet research needs. The paper highlights the suggested method's computational efficiency, which makes it a useful tool for resource-constrained real-time identity deception detection in social media. Furthermore Biwen Chen et Al., [15] as proposed, the cloud-assisted vehicle social networks (VSN) provide security and privacy concerns that are addressed by the blockchain-based searchable public-key encryption system with forward and backward privacy (BSPEFB). By utilizing smart contracts to provide decentralized reliability, BSPEFB improves the integrity of keyword searches by guaranteeing accurate and unchangeable search results. It provides protection from file-injection attacks and information leaks by providing both forward and reverse privacy. The technique introduces a small amount of computational overhead but also brings decentralization and practical efficiency. Benefits include decentralization, privacy protection, and usefulness; drawbacks include possible complexity and security issues. Research gaps include inadequate privacy protection, vulnerability to leakage-abuse assaults, ineffectiveness of current systems, and centralized search servers. By addressing these problems and placing a strong emphasis on decentralization, anonymity, and search efficiency in VSN, the BSPEFB scheme helps.

## III. TOOLS USED

The offered research report makes no mention of the instruments that were employed in the investigations. It does, however, go into great detail into several blockchain-related technologies and approaches, as well as decentralized identity management, smart contracts, and machine learning algorithms including Support Vector Machine, Random Forest, and Adaptive Boosting.

The study by Peter Mell. [3] cites Ethereum, a well-known blockchain network, in the context of blockchain. It emphasizes the application of Ethereum's smart contracts to federated identity management. The study also covers cryptographic techniques and algorithms, such as hash functions and RSA, that are used to protect the integrity, security, and privacy of data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

The paper discusses machine learning in relation to Michail Tsikerdekis and Sherali Zeadally's study on identifying identity deception in social media, specifically mentioning Support Vector Machine, Random Forest, and Adaptive Boosting [14]. These algorithms are used to create models that use nonverbal user actions to identify deceivers.
The study stresses the integration of technologies and algorithms to address difficulties in digital identity verification and security across many domains, while specific tools are not mentioned directly.

## IV. RESEARCH GAP AND FUTURE DIRECTIONS

Create a robust system leveraging blockchain technology for user authentication across social media platforms. This innovative approach enhances security by mitigating the vulnerability of centralized database breaches. The implementation of smart contracts facilitates efficient management of user authentication, offering users increased control over their login credentials. This decentralized authentication system empowers users to maintain a higher level of authority over their login details, consequently diminishing reliance on centralized entities for security measures.

### FUTURE DIRECTIONS

**Enhancement of Blockchain-Powered Identity Frameworks:** The study emphasizes the necessity of more investigation to determine the best combination of factors for effective identity deception detection. A critical research gap is investigating computing efficiency in the context of social media platforms while guaranteeing robust identity verification techniques.

**Translation of Non-Verbal Behaviors into Measurable factors:**To detect identity fraud, there is a research gap in the translation of non-verbal behaviors into quantifiable factors. Subsequent research endeavors may concentrate on devising techniques for precisely recognizing and measuring nonverbal cues, hence augmenting the precision of predictive models.

**Scalability Problems with Blockchain-Based Systems:** Particularly when handling enormous volumes of passport data, research should be done on scalability issues pertaining to blockchain-based passport issuance systems. For the suggested system to be implemented practically, it must be optimized to manage higher transaction volumes.

**Improved Privacy Protection in Searchable Encryption Systems:** More research is needed to address possible security risks and improve privacy protection in blockchain-based searchable public-key encryption systems, especially in cloud-assisted car social networks. Subsequent research endeavors may concentrate on enhancing these systems to guarantee strong defense against possible weaknesses.

**Examining Regulatory Frameworks:** The study refers to the need for more study on the frameworks governing the use of blockchain technology in passport issue. Successful adoption and implementation will require careful consideration of data protection, legal ramifications, and compliance with current legislation.

## V. CONCLUSION

This thorough analysis examines how blockchain technology and digital identity interact, with a particular emphasis on social media applications. In response to the growing need for reliable digital identity verification in the ever-changing world of online interactions, this article explores various approaches that make use of blockchain's characteristics, such as decentralization, immutability, and transparency. Numerous strategies are examined through a thorough review of the literature, including blockchain-based identity platforms, smart contracts for federated identity management, creative ways to deal with privacy issues, and social media identity deception detection. According to the research, blockchain has the power to completely transform digital identity management by offering safe, open, and user-friendly solutions. But obstacles including technological complexity, privacy concerns, and acceptance hurdles highlight the need for more research in this developing subject.

## REFERENCES

**[1].** Yu, Ruiguo, et al. "Authentication with block-chain algorithm and text encryption protocol in calculation of social network." *IEEE Access* 5 (2017): 24944-24951.

**[2].** Bandara, Eranga, et al. "A blockchain and self-sovereign identity empowered digital identity platform." *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2021.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

**[3].** Mell, P., J. Dray, and J. Shook. "Smart contract federated identity management without third party authentication services. arXiv 2019." *arXiv preprint arXiv:1906.11057*.

**[4].** Jamal, Arshad, et al. "Blockchain-based identity verification system." *2019 IEEE 9th international conference on system engineering and technology (ICSET)*. IEEE, 2019.

**[5].** Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." *2015 IEEE security and privacy workshops*. IEEE, 2015.

**[6].** Do, Hoang Giang, and Wee Keong Ng. "Blockchain-based system for secure data storage with private keyword search." *2017 IEEE World Congress on Services (SERVICES)*. IEEE, 2017.

**[7].** Fan, Kai, et al. "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks." *IEEE Transactions on Vehicular Technology* 69.6 (2020): 5826-5835.

**[8].** Zhao, Zheng, and Yuan Liu. "A blockchain based identity management system considering reputation." *2019 2nd International Conference on Information Systems and Computer Aided Education (ICISCAE)*. IEEE, 2019.

**[9].** Htet, May, Phyo Thet Yee, and Jay R. Rajasekera. "Blockchain based digital identity management system: A case study of Myanmar." *2020 International Conference on Advanced Information Technologies (ICAIT)*. IEEE, 2020.

**[10].** Chakravorty, Antorweep, and Chunming Rong. "Ushare: user controlled social media based on blockchain." *Proceedings of the 11th international conference on ubiquitous information management and communication*. 2017.

**[11].** Shorman, Samer, and Mohammad Allaymoun. "Authentication and verification of social networking accounts using blockchain technology." *AIRCC's International Journal of Computer Science and Information Technology* (2019): 1-11.

**[12].** Jiang, Le, and Xinglin Zhang. "BCOSN: A blockchain-based decentralized online social network." *IEEE Transactions on Computational Social Systems* 6.6 (2019): 1454-1466.

**[13].** Malik, Gunit, et al. "Blockchain based identity verification model." *2019 international conference on vision towards emerging trends in communication and networking (ViTECoN)*. IEEE, 2019.

**[14].** Tsikerdekis, Michail, and Sherali Zeadally. "Multiple account identity deception detection in social media using nonverbal behavior." *IEEE Transactions on Information Forensics and Security* 9.8 (2014): 1311-1321.

**[15].** Chen, Biwen, et al. "A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks." *IEEE Transactions on Vehicular Technology* 69.6 (2019): 5813-5825.