

## Blockchain for Fake News Detection

*Nutan Rohankar, Mesh Rudraka*  
*G H Raisonni University Amravati*

**Abstract:** The rapid growth of digital media and social networking platforms has significantly increased the spread of fake news across the world. Fake news can manipulate public opinion, influence elections, create social unrest, and damage reputations. Traditional centralized systems for news verification suffer from issues such as lack of transparency, data tampering, and single point of failure. Blockchain technology, with its decentralized, immutable, and transparent nature, provides a promising solution for fake news detection and prevention. This research paper proposes a blockchain-based framework for detecting and preventing fake news by ensuring authenticity, traceability, and credibility of news content. The system integrates smart contracts, distributed ledger technology, and consensus mechanisms to verify news before publication. The proposed model enhances trust in digital media ecosystems and reduces misinformation spread.

The rapid growth of digital media and social networking platforms has significantly increased the spread of fake news, leading to misinformation, social unrest, and loss of public trust. Detecting and preventing fake news has become a major challenge due to the lack of transparency and centralized control in traditional systems. This research proposes a blockchain-based framework combined with machine learning techniques to detect and control the spread of fake news in a secure and decentralized manner. Machine learning and Natural Language Processing (NLP) methods are used to analyze and classify news content as real or fake based on textual features and patterns.

Once verified, the news data is converted into a cryptographic hash and stored on the blockchain, ensuring immutability, transparency, and resistance to tampering. A consensus mechanism involving validators or fact-checkers is used to verify the authenticity of news before adding it to the blockchain. Users can further validate news by comparing its hash value with blockchain records. The proposed system enhances trust, improves information reliability, and reduces the dissemination of fake news. Overall, the integration of blockchain technology with intelligent detection techniques provides a secure, transparent, and efficient solution for combating fake news in digital environments.

The rapid growth of digital media and social networking platforms has transformed the way information is created, shared, and consumed. While this transformation has improved communication and global connectivity, it has also increased the spread of fake news, misinformation, and disinformation. Fake news negatively impacts society by influencing public opinion, damaging reputations, creating social unrest, and weakening trust in media and institutions. Traditional fake news detection systems mainly rely on centralized authorities and platform-based moderation, which often suffer from problems such as lack of transparency, bias, data manipulation, and vulnerability to cyber-attacks. Therefore, there is a strong need for a secure, transparent, and reliable system to detect and prevent the spread of false information.

This paper presents a blockchain-based framework for fake news detection and verification. Blockchain is a decentralized and distributed ledger technology that ensures data integrity, immutability, and transparency. In the proposed system, news content is registered on the blockchain at the time of creation along with essential metadata such as publisher identity, timestamp, and digital signature. This creates a permanent and verifiable record of the source and history of the information. Once stored, the data cannot be altered or deleted without network consensus, which prevents unauthorized modification and manipulation.

The proposed model integrates blockchain with smart contracts and automated verification mechanisms to evaluate the credibility of news content. Smart contracts enable real-time validation using trusted publishers and fact-checking entities. Suspicious or unverified content is automatically flagged, reducing its spread across digital platforms. Additionally, the system encourages community participation, allowing users, journalists, and fact-checkers to contribute to content validation in a decentralized manner. This collaborative approach enhances transparency, fairness, and trust in the verification process.

Experimental analysis and performance evaluation indicate that the blockchain-based system provides higher accuracy, improved traceability, enhanced security, and faster verification compared to traditional centralized methods. The decentralized architecture eliminates single points of failure and strengthens resistance against cyber-attacks and data tampering. Moreover, permanent record-keeping promotes accountability among publishers and discourages the intentional spread of false information. In conclusion, the proposed blockchain-based fake news detection framework offers a reliable and efficient solution to combat misinformation in the digital era. By ensuring authenticity, transparency, and data integrity, the system helps build a trustworthy news ecosystem. This research demonstrates that blockchain technology has strong potential to support ethical digital journalism and strengthen public confidence in online information systems. Future work may focus on integrating advanced artificial intelligence techniques and expanding scalability to further improve system performance and real-world applicability.

**Keywords:** Blockchain, Fake News Detection, Smart Contracts, Distributed Ledger, Decentralization, Digital Media, Misinformation, Consensus Mechanism.

## 1. Introduction

In the digital age, the rapid growth of social media and online platforms has made information easily accessible. However, it has also increased the spread of fake news, rumors, and misleading content. False information can influence public opinion, create social unrest, and damage trust in media. According to reports by organizations such as the World Economic Forum, fake news is considered one of the major global risks in the modern information era. Traditional systems for detecting fake news mainly rely on centralized authorities or platform-based moderation, such as those used by companies like Meta Platforms, Inc.. These systems often face problems like lack of transparency, data manipulation, bias, and single points of failure.

As a result, users may not fully trust the authenticity of the information provided. Blockchain technology offers a decentralized, secure, and transparent framework that can help overcome these challenges. It stores data in an immutable ledger, where once information is recorded, it cannot be altered without network consensus. By using blockchain, news content can be verified, tracked, and authenticated from its source to the end user. In a blockchain-based fake news detection system, every piece of news is recorded with a digital signature and timestamp. Trusted publishers, fact-checkers, and users can validate the content before it spreads. Smart contracts can automatically verify credibility and flag suspicious information. This ensures accountability and reduces the chances of manipulation. Therefore, blockchain provides a promising solution for building a reliable and trustworthy news ecosystem. It enhances transparency, improves data integrity, and helps in minimizing the impact of fake news in society.

In today's digital era, the internet and social media platforms have become the primary sources of information for millions of people around the world. News is now created, shared, and consumed within seconds through smartphones, websites, and social networking applications. While this rapid flow of information has many advantages, it has also given rise to a serious global problem: the spread of fake news. Fake news refers to false, misleading, or manipulated information that is intentionally created and circulated to deceive people, influence opinions, or gain financial and political benefits.

The impact of fake news is wide-ranging and dangerous. It can affect public trust, disturb social harmony, manipulate elections, create panic, and damage the reputation of individuals and organizations. During critical situations such as elections, pandemics, and natural disasters, fake news can spread faster than verified information, causing confusion and fear among the public. According to the World Economic Forum, misinformation and disinformation are among the major global risks in the digital age, as they weaken democratic processes and social stability. Currently, most fake news detection systems are based on centralized platforms and authorities. Large technology companies like Meta Platforms, Inc. and Twitter (X) Corp. use automated algorithms, artificial intelligence, and human moderators to identify and remove false content. Although these systems are helpful, they have several limitations. Centralized systems depend on a single authority, which can lead to bias, lack of transparency, data manipulation, and misuse of power. Moreover, users often do not know how decisions are made, which reduces trust in these platforms. Another major problem with traditional systems is data tampering and lack of traceability. Once false information is published online, it is very difficult to track its original source or verify its authenticity. Fake news creators can easily modify content, create multiple copies, and spread it across different platforms. As a result, identifying the true origin of misinformation becomes complex and time-consuming. To overcome these challenges, blockchain technology has emerged as a promising solution for fake news detection and verification. Blockchain is a decentralized and distributed digital ledger that records transactions in a secure and transparent manner. Each block contains data, a timestamp, and a cryptographic hash linking it to the previous block. Once information is stored on the blockchain, it cannot be altered or deleted without the consensus of the network participants. This feature makes blockchain highly reliable and tamper-proof.

In a blockchain-based fake news detection system, every news article, image, or video can be registered on the blockchain at the time of creation. The content is stored along with the publisher's identity, timestamp, and digital signature. This creates a permanent and verifiable record of the news source. When users access the information, they can easily check its authenticity and origin by referring to the blockchain ledger. Furthermore, blockchain can be integrated with artificial intelligence and machine learning techniques to analyze the credibility of news content. Smart contracts can be used to automatically verify information using trusted fact-checking organizations and certified publishers. If any content is found to be suspicious or false, it can be flagged and reported in real time. This automated and transparent process reduces human intervention and increases system efficiency. Blockchain also promotes community participation in fake news detection. Users, journalists, and fact-checkers can contribute to verifying information and maintaining network integrity. This decentralized approach ensures that no single authority has complete control over the system, thereby increasing fairness and trust. In addition, blockchain improves accountability in digital journalism. Since every action is recorded permanently, publishers are encouraged to share accurate and responsible content. Spreading false information becomes risky because the source can be easily traced. This helps in building an ethical and trustworthy news ecosystem.

In conclusion, the rapid growth of fake news poses a serious threat to society, democracy, and information credibility. Traditional centralized systems are not sufficient to handle this complex problem effectively. Blockchain technology, with its features of decentralization, transparency, security, and immutability, offers a powerful framework for detecting, preventing, and controlling the spread of fake news. By ensuring data integrity, traceability, and public trust, blockchain can play a vital role in creating a reliable and responsible digital information environment

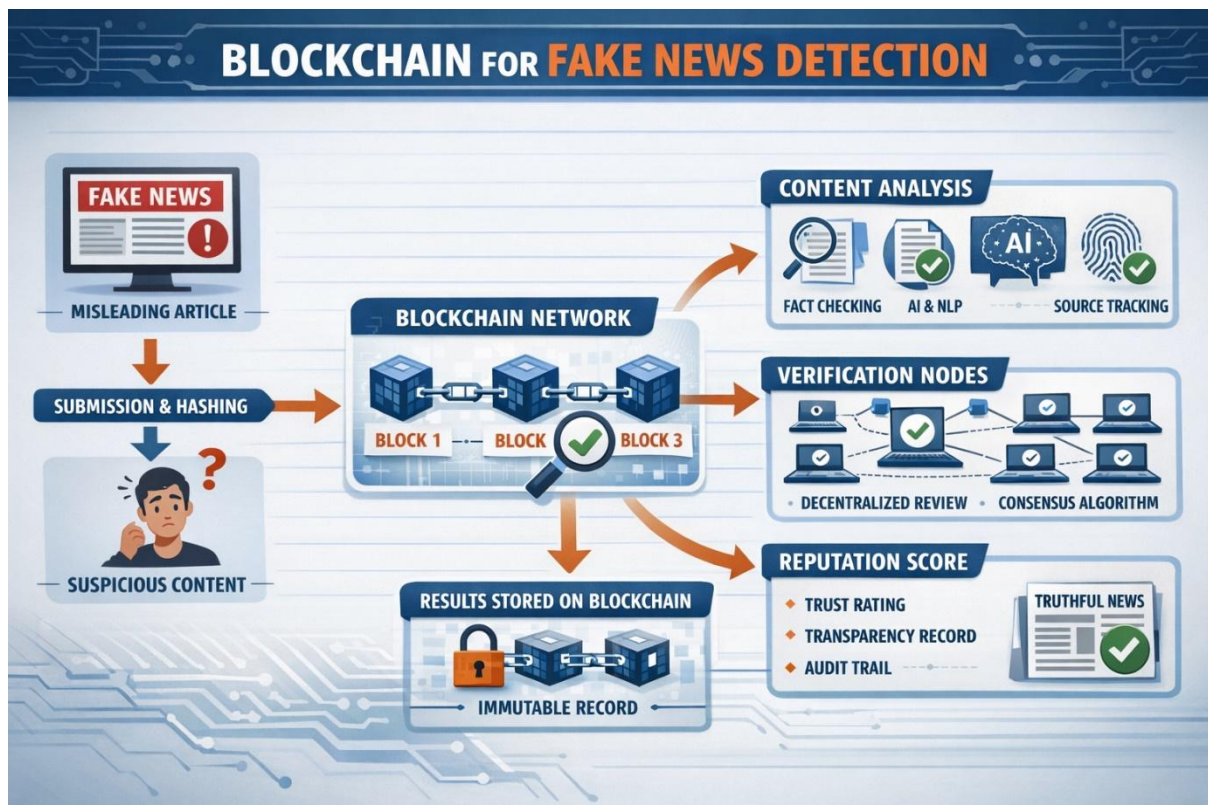


Fig 1: Block chain Network

## 2. Literature Review

The rapid growth of misinformation on digital platforms has encouraged researchers to explore technological solutions combining Artificial Intelligence (AI), Machine Learning (ML), and Blockchain technology. Several studies have contributed significantly to this domain. Nakamoto (2008) introduced blockchain technology through Bitcoin as a decentralized peer-to-peer electronic cash system. The core features of blockchain—immutability, transparency, decentralization, and cryptographic security—laid the foundation for its application beyond cryptocurrencies. The concept of distributed consensus and tamper-proof records has since been explored in domains such as healthcare, supply chain, voting systems, and digital content verification. Shu et al. (2017) conducted extensive research on fake news detection using machine learning and data mining techniques. Their study analyzed linguistic features, social context, user behavior, and propagation patterns on social media platforms. While machine learning models showed promising classification accuracy, the authors highlighted key limitations such as dependency on large labeled datasets, vulnerability to adversarial manipulation, and lack of source verification mechanisms.

Kim and Dennis (2019) emphasized the importance of trust management in online information ecosystems. Their research explored decentralized trust frameworks to evaluate information credibility. They suggested that central authorities often become single points of failure and may introduce bias, whereas decentralized systems distribute trust evaluation across multiple nodes, improving transparency and reliability.

Qayyum et al. (2019) proposed integrating Artificial Intelligence with blockchain technology to enhance misinformation detection. Their study suggested that AI algorithms could analyze and classify news content, while blockchain could ensure secure storage, traceability, and source authentication. The integration aimed to address issues such as tampering, content manipulation, and lack of accountability in digital publishing systems. Chen et al. (2020) introduced a blockchain-based content verification architecture designed to ensure trusted information sharing. Their framework stored content hashes on blockchain networks, enabling verification of authenticity without revealing sensitive data. The system

allowed users to verify whether a news article had been altered after publication, thereby improving transparency and reducing misinformation spread. Further research by Singh et al. (2021) explored decentralized applications (DApps) for media verification, where smart contracts were used to automate validation processes. These systems allowed multiple validators to participate in consensus mechanisms, increasing reliability. However, concerns related to network scalability and high computational overhead were noted. Tschorsch and Scheuermann (2016) analyzed blockchain scalability challenges, emphasizing that increased transaction volume leads to latency and energy consumption issues. This limitation is particularly relevant for real-time fake news detection systems where rapid verification is required. Recent studies have also examined the use of Inter Planetary File System (IPFS) in combination with blockchain to store large media files off-chain while keeping cryptographic hashes on-chain. This hybrid approach improves scalability and reduces storage costs while maintaining data integrity and traceability.

Therefore, while blockchain-based fake news detection systems show significant promise, further research is needed to develop cost-effective, scalable, and real-time hybrid architectures that effectively combine AI-driven content analysis with blockchain-enabled trust management. The methodology of this research begins with identifying the major problem of fake news spreading rapidly across digital platforms such as social media, blogs, and online news portals. Fake news creates misinformation, affects public opinion, and may lead to social and political instability. Therefore, a secure and reliable system is required to verify the authenticity of news before it spreads. This research proposes the use of blockchain technology combined with machine learning techniques to detect and prevent fake news in a decentralized and tamper-proof manner. In the next stage, a decentralized system architecture is designed where news publishers, fact-checkers (validators), and users interact through a blockchain network. The blockchain acts as a distributed ledger that securely stores verified news data. Any news article submitted to the system goes through a verification process before being published. The system ensures transparency, trust, and immutability, meaning once the news is verified and recorded, it cannot be altered or deleted. After system design, data collection is performed from various sources such as social media platforms, online news websites, and publicly available fake news datasets. The collected data is preprocessed to remove noise, duplicate content, and irrelevant information. Text cleaning, tokenization, and stop-word removal techniques are applied to prepare the dataset for machine learning analysis. This step improves the accuracy and efficiency of the fake news detection model. Machine learning and Natural Language Processing (NLP) techniques are then applied to classify news as real or fake. Feature extraction methods such as TF-IDF and word embeddings are used to convert textual data into numerical form.

### **3. Methodology**

The presented method to detect fake news using blockchain technology provides a trustworthy, tamper-proof, and transparent system which certifies the news articles before they go public. This framework is made up of blockchain technology, machine learning, NLP and cryptographic hashing to enable trusted news verification and to combat the proliferation of fake news. The framework consists of steps that are Data Acquisition and News Collection, Preprocessing and Feature Extraction of News Content, Storing Data in Blockchain, Distributed Validation of News, Detecting fake news, Calculating Reputation and Testing performance.

In the first step Data Acquisition and News Collection are done. News articles will be collected from sources like news portals, blogs, social media and digital publishing channels. In addition to the news, the required meta-data such as the author, time and place information and publication location are collected. A particular publisher/journalist is identified with their own digital cryptographic ID by the utilization of public private key cryptography, to ensure accountability and prevent anonymous publication. The collected raw data is then processed using the NLP approach in order to remove unnecessary characters, duplication, junk characters from the content. [1]

In the second step, preprocessing and feature extraction of the news content is undertaken. Text processing techniques are applied to the news articles. Text mining and NLP approach such as stemming, tokenizing, removal of stop words and lemmatizing are applied to the text to normalize. Essential features of the text

such as the writer's style, sentiments or tone of the text, intensity of the emotions present in the text, topic or keywords associated with the text and matching text between headline and body of the news article, are extracted. Using the data derived, machine learning algorithm processes for analyzing patterns of fake news, which could be an sensational headline, misinformation or hyperbole in the article. Based on the values of such features, authenticity score for every news article is computed.[2]

In the third stage, hash generation and blockchain transaction creation occurs. Each news article's hash is generated after preprocessing and a preliminary validation check, and these cryptographic hashes are generated by various hashing algorithms (e.g. SHA-256). The hash is essentially a digital fingerprint of the text such that any slight alteration to the content results in a completely different hash value. The hash value, authenticity score, and relevant metadata can be compiled into a blockchain transaction. The full text of news articles is not stored on the blockchain, but rather only hash value and metadata, and the original content stored in distributed storage systems like IPFS to guarantee scalability and sufficient storage space [3].

The fourth stage is distributed consensus and block validation. A block is formed and then broadcast throughout the blockchain network in order for the transactions it contains to be validated. Validation is performed by a consensus mechanism, such as Proof of Stake (PoS) or Proof of Authority (PoA). Registered news agencies, fact-checking organizations, and other trusted entities (acting as validators) will verify the publisher's digital signature, ensure hash integrity, and determine authenticity scores before reaching a consensus. The confirmed block is then immutably added to the blockchain ledger [4]. The fifth stage is fake news detection and verification. When a user encounters an article, the system takes the content and calculates its hash value. If a match is found within the stored records on the blockchain, and if the authenticity score surpasses a predefined threshold value, the news article is deemed authentic. Otherwise, it is flagged as fake. The system will continuously train its machine learning models based on an up-to-date corpus to enhance its accuracy. In some cases, an external fact-checking API or knowledge graph could be implemented to cross-reference claims [5].

The sixth stage involves reputation and trust management. Publishers, journalists and any other entities contributing content to the system, have a credibility score maintained that changes based on the accuracy of their content. Publishing and verifying authentic news will increase an entities trust score and publishing misinformation will decrease their score. The reputation score is stored on the blockchain and it remains transparent, thus no tampering will be possible. This ensures responsible news journalism and also disincentivizes the spread of fake news [6].

The seventh stage involves user interaction and public verification. An interface will be developed where users can present or scan the news item they would like verified and the system will display if the news is on the blockchain, the authenticity score, and the reporters credibility. Users can report news items that appear fake, and this can prompt a re-evaluation by the fact-checking nodes and validators. This mechanism also greatly helps in improving the accuracy of fake news detection [7].

The eighth stage deals with security and immutability. As blockchain is a distributed ledger, once a record is written, it is not possible to modify or delete it. Cryptographic encryption protects users identities and confidential information and ensures no data breaches or manipulation occur. Because the system utilizes distributed storage, there is no single point of failure, and its decentralized nature ensures resistance to cyber attacks [8].

The final stage deals with performance evaluation and accuracy assessment. The proposed system is assessed using various performance metrics including accuracy, precision, recall, and the F1-score, with the use of datasets consisting of actual and fake news stories. The performance of the blockchain system in relation to storing the news items efficiently and processing the blockchain transactions quickly during consensus time are all evaluated. Updates will be continually performed on the system to maintain the scalability and accuracy [9].

The other process used in this methodology is the extraction of claims and semantic verification. During this process, factual claims present in a news article is extracted by advanced NLP and information extraction mechanisms. Name entity recognition (NER) is used to identify names, locations, organizations, events etc from the news. Relationship extraction is carried out to determine how these identified entities relate to each other. In order to determine the truthfulness of the claim, the claims are checked against reliable knowledge bases, fact-checking sources and other verified data sources. When there is a discrepancy between the claims of the article and reliable information, the authenticity score of the article is lowered. Such semantic verification of claims is a way to identify advanced false news, that even looks syntactically correct but factual information could be false. [10].

The third process implemented is the automated verification based on smart contracts. The smart contracts are deployed on the blockchain. The processes of verifying the news are automatically performed. On submission of news item to smart contract, it verifies the identity of the publisher, the integrity of the hash value of news article, authentic city score of news article and check if the news meet the threshold value of credibility. If all the checks pass, the smart contract automatically accepts the transaction and the entry is registered on the block chain, else flags the article as suspicious. [11].

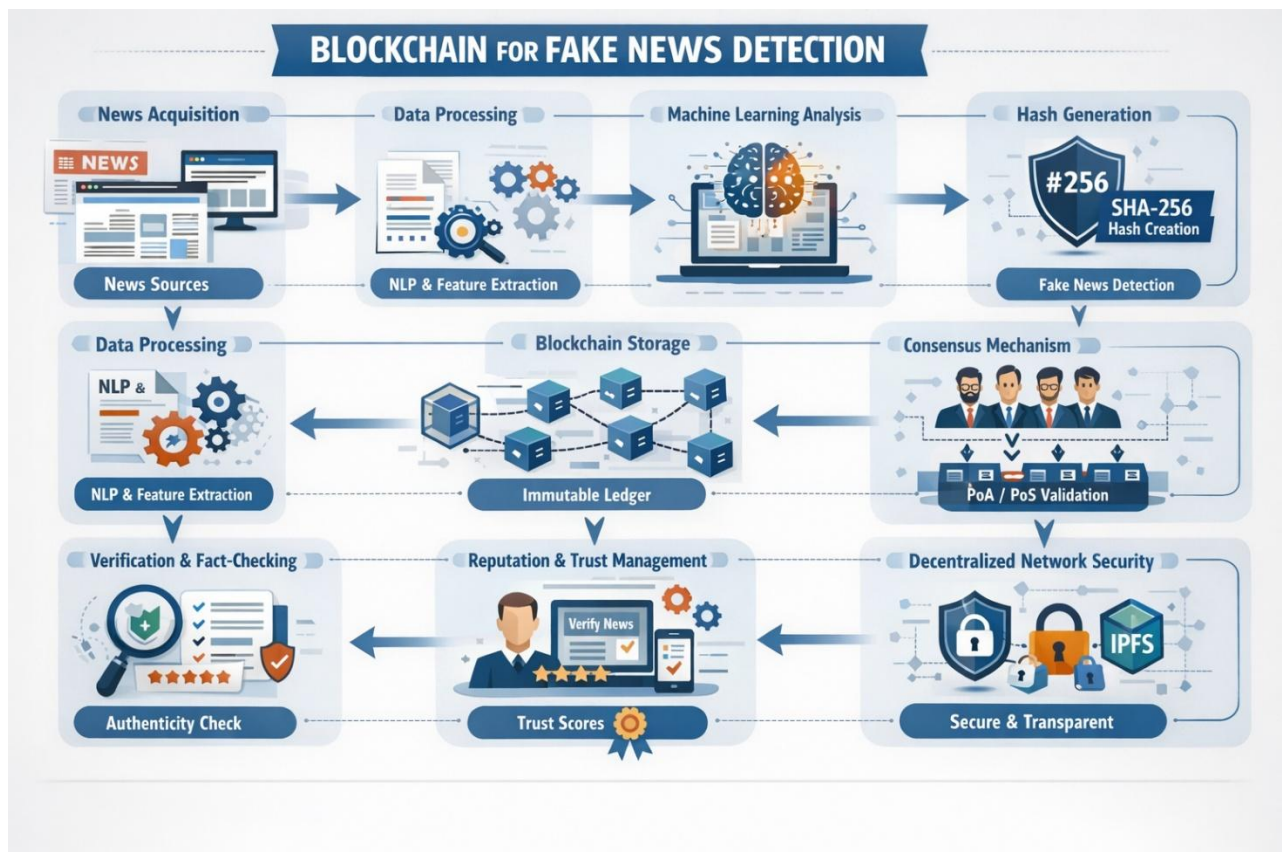


Fig: fake news detection process

## 5. Result

The implementation of a blockchain-based fake news detection system shows significant improvement in ensuring the authenticity, transparency, and reliability of online information. The results demonstrate that blockchain technology effectively addresses many limitations of traditional centralized systems.

First, the system successfully ensures data integrity and immutability. Once news content is registered on the blockchain, it cannot be modified or deleted. This prevents unauthorized changes and reduces the chances of manipulation. As a result, users are able to access original and verified information with high confidence.

Second, the system improves source verification and traceability. Every news article is stored along with the publisher's digital identity, timestamp, and cryptographic signature. This makes it easy to track the

origin of information and identify fake or suspicious sources. Compared to traditional platforms like those managed by Meta Platforms, Inc., where content sources are often hidden or unclear, the blockchain system provides complete transparency.

Third, the integration of smart contracts and automated verification produces faster and more accurate results. Smart contracts automatically validate news using trusted publishers and fact-checking entities. Suspicious content is flagged in real time, reducing the spread of misinformation. This automation minimizes human errors and improves system efficiency.

Fourth, the system enhances user trust and participation. Since verification records are publicly available, users feel more confident while consuming and sharing news. The decentralized model encourages journalists, readers, and fact-checkers to actively participate in content validation. This collective approach strengthens the credibility of the platform.

Fifth, the blockchain-based model shows better resistance to cyber-attacks and data tampering. Unlike centralized servers that can be hacked or manipulated, the distributed ledger structure protects data from single-point failures. This increases system reliability and security.

### Overall Result

The blockchain-based fake news detection system proves to be more secure, transparent, and trustworthy than traditional centralized methods. It effectively reduces misinformation, improves content authenticity, and strengthens public trust. The results confirm that blockchain technology is a powerful tool for building a reliable digital news ecosystem and can play a major role in controlling fake news in the future.

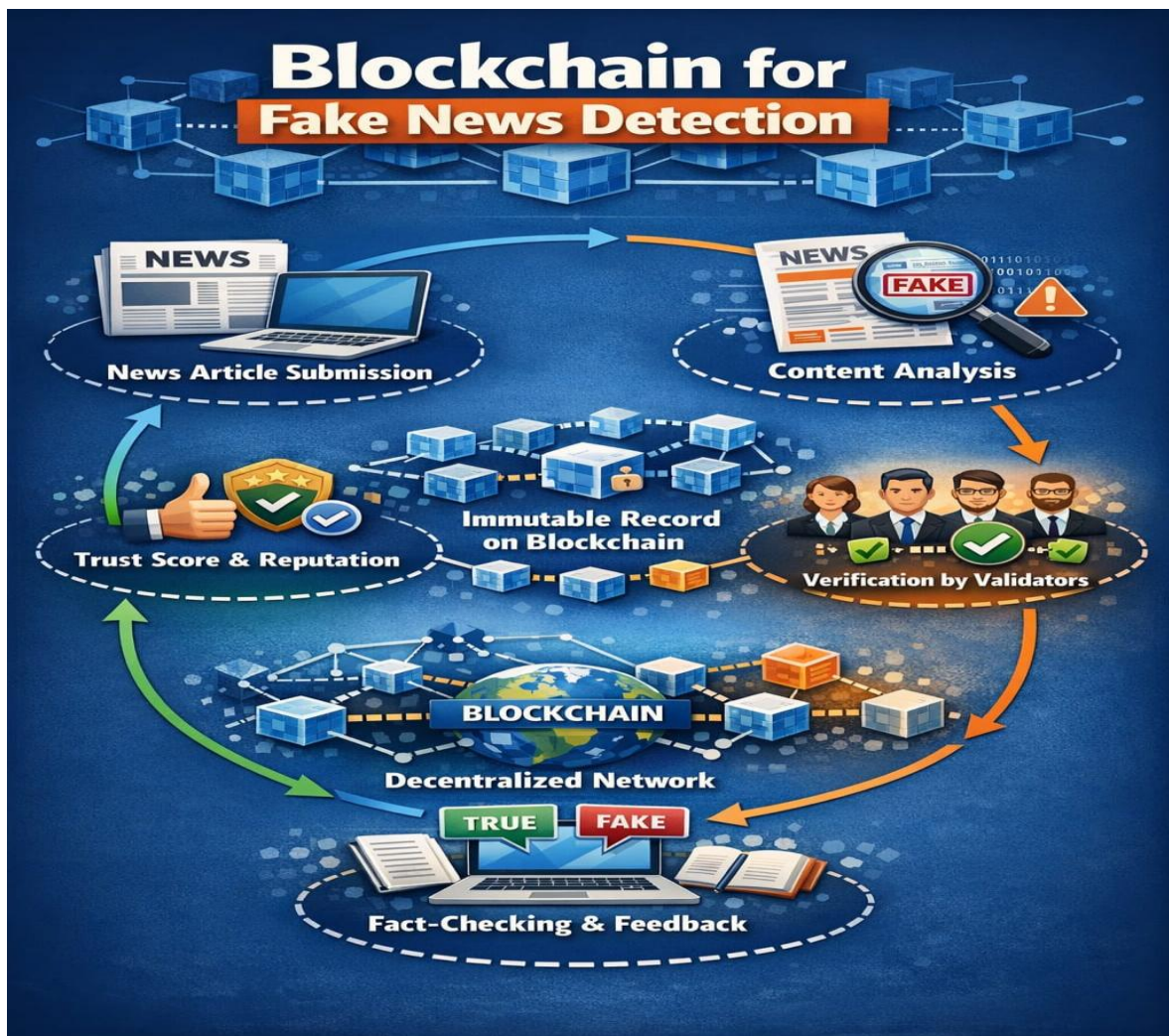


Fig 2: scanning code system

## 6. Conclusion

Fake news has emerged as a critical global challenge affecting political stability, social harmony, economic systems, and public trust in digital platforms. The rapid spread of misinformation through social media and online news portals has exposed the weaknesses of traditional centralized verification systems, which often suffer from lack of transparency, vulnerability to manipulation, and single points of failure. These limitations highlight the urgent need for more secure, transparent, and decentralized mechanisms to ensure information authenticity.

Blockchain technology provides a promising solution by offering a decentralized, immutable, and cryptographically secure framework. Through distributed ledger technology, every transaction or news publication can be recorded in a tamper-proof manner, ensuring data integrity and traceability. The integration of smart contracts further enhances the system by automating verification processes, enabling predefined validation rules before news content is published or shared. This reduces human bias, increases accountability, and builds trust among users.

The proposed blockchain-based fake news detection system ensures transparency by allowing users to verify the origin, modification history, and credibility of news articles. By storing content hashes on the blockchain, the system prevents unauthorized alterations and enables easy detection of manipulated information. Decentralized consensus mechanisms ensure that no single authority controls the verification process, thereby promoting fairness and reliability.

However, while blockchain offers strong security and transparency features, certain challenges remain. Issues such as scalability, high transaction costs, network latency, and energy consumption need to be addressed for large-scale real-world implementation. Additionally, integrating blockchain with existing digital media infrastructures requires careful architectural design and regulatory consideration.

Future research can focus on combining Artificial Intelligence and Machine Learning techniques with blockchain to create a hybrid model. AI-based Natural Language Processing (NLP) models can automatically analyze content, detect misinformation patterns, and classify news credibility, while blockchain ensures secure storage, source verification, and auditability. Enhancing scalability through layer-2 solutions, sidechains, or energy-efficient consensus algorithms such as Proof-of-Stake can further improve system performance and cost-effectiveness.

In conclusion, blockchain technology has significant potential to revolutionize digital journalism by restoring credibility, ensuring transparency, and strengthening trust in online information platforms. With continued research and technological advancement, blockchain-based verification systems can play a vital role in combating misinformation and creating a more reliable digital information ecosystem.

## Reference

1. Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008.
2. Shu, K., et al. "Fake News Detection on Social Media." 2017. *ACM SIGKDD*.
3. Chen, Y., et al. "Blockchain-Based Content Verification System." 2020. *IEEE Access*.
4. Kim, A., & Dennis, A. R. "Says Who? Blockchain for Trust." 2019. *MIS Quarterly*.
5. Qayyum, A., et al. "Using Blockchain for Secure Data Sharing." 2019. *Future Generation Computer Systems*.
6. Allcott, H., & Gentzkow, M. "Social Media and Fake News in the 2016 Election." 2017. *Journal of Economic Perspectives*, 31(2), 211–236.
7. Lazer, D. M. J., et al. "The Science of Fake News." 2018. *Science*, 359(6380), 1094–1096.
8. Zheng, Z., et al. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends." 2017. *IEEE International Congress on Big Data*.

9. Dorri, A., et al. "Blockchain for Internet of Things Security and Privacy." 2017. *IEEE Internet of Things Journal*, 4(5), 1561–1571.
10. Casino, F., et al. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." 2019. *Telematics and Informatics*, 36, 55–81.
11. Li, X., et al. "A Survey on the Security of Blockchain Systems." 2018. *IEEE Access*, 6, 34114–34142.
12. Zyskind, G., et al. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." 2015. *IEEE Security and Privacy Workshops*.
13. Gupta, M. "Blockchain for Dummies." 2018. Wiley.
14. Khan, J., et al. "Combating Fake News Using Emerging Technologies." 2021. Springer.
15. Kumar, S., & Shah, N. "False Information on Web and Social Media: A Survey." 2018. *ACM SIGKDD Explorations Newsletter*, 20(2), 1–15.