Science, Engineering and Technology Vol. 5, No. 1, pp. 213-247
www.setjournal.com *https://doi.org/10.54327/set2025/v5.i1.222*

An Overview on Blockchain-based Social Media

Patikiri Arachchige Don Shehan Nilmantha Wijesekara[1]

[1]*Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka.*

Abstract

Social Media (SM) platforms allow users to create and share multimedia content characterized by interaction among the users through profile creation, messaging systems, communities, etc. Blockchains can improve the security and ethical aspects of SM due to their innate security characteristics. We overlook countless blockchain-based SM schemes, where we perceive 9 duties of blockchain-based SM abstraction and dissect them intensively, rooted in SM- and blockchain-linked traits in contrast to existing reviews that do not review in broad scope and lack a critical analysis to show ways to focus on practical implementation. We heaped a preparatory sample of 93 works by sieving the studies for leaching rules and delving into E-repositories by employing a mixed-method systematic review with a narrative synthesis and quality assessment approach. Built upon the scrutiny, in blockchain-based SM, blockchain can assist by providing social media platforms (G1), social DApps (G2), copyright protection (G3), harassment prevention (G4), ensuring privacy and security (G5), fake/vicious news prevention (G6), data/user behavior/event processing and analysis (G7), proper incentivization (G8), and user migration (G9). Critical analysis uncovers that from blockchain-based social media, an overall 40% harness 20% from G6 and G7 each, 82.5% harness conventional blockchain, and 22.5% harness DPoS consensus. Next, we critically analyze the strengths and weaknesses of the reviewed works, focusing on performance and characteristics. Furthermore, we identified lack of empirical validation, under-exploration of ethical concerns and biases in detection models, and non-assessment of decentralization risks as gaps in the study. Eventually, we reveal the opportunities and discomforts of the abstraction of blockchain-based SM, state the study's limitations, and then bestow solutions to resist them with future directions emphasizing practical implications.

Keywords*: security, blockchain, social media, blockchain-grounded social media, social media ethics.*

1. Introduction

In a social network, users have their own profiles containing profile pictures and personal information that remain as a virtual identity that others can view, while users can share diverse content just like text, photos, videos, links, status updates, etc. through posting [1]. In Social Media (SM) forums, users can seek advice on certain topics, share knowledge, seek the opinion of subject experts, and are mainly knowledge-based, where the social media richness is relatively lower [2]. Blogging has supported older adults to develop their identity, express themselves, and support adult values, engaging them actively after retirement and providing them with the opportunity to be in a

Corresponding author: *Patikiri Arachchige Don Shehan Nilmantha Wijesekara* (*nilmantha@eie.ruh.ac.lk)*
Received: *14 October 2024*; Revised: *14 March 2025*; Accepted: *17 March 2025*; Published: *20 March 2025*

community [3]. Messaging platforms are not limited to personal messaging and also support group and community chats where multiple people can engage in a single conversation, facilitating social interaction and collaboration [4]. The objective of professional networks is professional interaction in comparison to social interaction in social networks, while the user profiles are more aligned in the direction of professional facts like work experience, education, and career accomplishments rather than personal hobbies, desires, etc. [5]. People can contribute their ideas and skills for collaborative work openly, where users can join and collaborate irrespective of their expertise in collaborative projects [6]. A virtual world demonstrates a three-dimensional space in which users can act as avatars to interact with other avatars, like in real life, that are portrayed by an elevated level of social presence with media richness [7].

In virtual worlds, copyright infringement can occur when users create avatars and environments that are based on copyrighted content and distribute them without permission [8]. Moreover, copyright infringement is seriously observed in content communities where users may upload copyrighted music, videos, or images without a proper license, leading to legal action by the copyright holders [9]. Social media often lacks content moderation systems to remove misinformation, mainly due to the high volume of content that is shared; thus, misinformation can spread unchecked [10]. Harassment on social media can occur in various types, such as cyberbullying intended to harm others, trolling that involves offensive comments to provoke others, hate speech targeting individuals based on religion, caste, etc., and sharing someone's sensitive images or videos without his/her consent to take revenge [11]. Algorithms in social media attempt to maximize user engagement, which can be negatively affected by the creation of echo chambers and exploiting users' attention for financial gain [12]. The survey in [13] shows that there has been significant privacy exposure on social networks, and the level of exposure differs based on the specific networking platform, gender, age, etc., and the personal data collected can sometimes be misused for financial attacks on users. In this study, we discuss how blockchain has been leveraged to overcome these drawbacks of social media.

Blockchain is a segregated ledger framework that securely reserves transactions through a communication network [14]. In conventional blockchain, there exists a straight progression of blocks in which every block carries a bunch of transactions, and at the same time, any block is connected to a prior one utilizing a secure hash, creating a chain [15]. The mesh blockchain differs from the conventional blockchain in that entries are not bunched into blocks, in contrast, independently connected to several prior transactions [16]. E-signature, which is implemented utilizing key-pair cryptography, is utilized to guarantee the genuineness of operations by utilizing a secret key for registering the operations and a publicized key to validate the signs [17]. Self-executing contracts are utilized to implement accords without third parties, removing the requirement for brokers, decreasing the dangers of hoaxing and exploitation, and additionally fortified by the risen status of assurance owing to blockchain's unalterable attributes [18].

In this work, we perceive 9 duties of blockchain-based SM abstraction. First, there are BSM networks like Steemit, ARTICONF, UShare, etc. that have a specific blockchain-driven systematic implementation of social media [19]. Next, there exist social DApps, like in the case of the Ethereum blockchain, to cater to specific requirements of social media, such as storage of user privacy settings [20]. After that, BSM can facilitate copyright protection for user-generated content, preventing copyright infringement, and incentivize content creators accordingly [21]. Moreover, BSM can facilitate harassment prevention, ensure privacy and security, and prevent fake/vicious news from spreading by making use of the tamper-proof nature of blockchain along with harassment/fake news detection techniques [22]. Additionally, blockchain can facilitate verifying trustworthiness while events/user behavior/data are analyzed by conventional techniques like machine learning or natural language processing [23]. Finally, in BSM, user migrations can occur as a

result of blockchain fork events, and such migrations can be modeled to understand user migrations [24].

We investigated 2 existing surveys related to the concept of how blockchain is utilized in social media. In [25], the authors do a systematic literature review on blockchain in social media, while the reviewed literature has mostly focused on fake news blocking and data privacy protection. Similarly, the literary analysis in [26] focuses on blockchain-based social media platforms, discussing their main features and drawbacks. However, to our best feeling, we are the ones to review blockchain-based SM in a broad scope, considering blockchain-based SM platforms, blockchain social media DApps, copyright infringement prevention, content moderation, reducing misinformation, reducing harassment, fair monetization and payments, and prevention of privacy exposures. Thus, this review is unique compared to existing reviews, considering the broad scope of the investigation and corresponding findings.

The significance of this research is that it can demonstrate methods for the researchers to draw conclusions about the ongoing developments and uniqueness of blockchain-based social media to foster in future studies that concentrate on practical application and empirical verification. Additionally, we highlight the dangers of centralization, which may encourage legislators to create just governance frameworks. By using this research, the researchers can gain insight to create successful engagement tactics like tokenized incentives by comprehending issues with user incentive systems.

Figure 1 renders the matter sketch of this examination. As shown in Figure 1, in the first part of the paper, we relegated and briefly interrogated social media conceptions in section 3, where various types of platforms are described and evaluated based on criteria such as media richness and self-presentation. This is followed by a conspectus about the blockchain scheme revealed in section 4, and an overview of active blockchain-based social media schemes in section 5, which is then analyzed intensively on the overviewed blockchain-based social media schemes in section 6. The discussion continues with the opportunities and discomforts of blockchain-based SM in section 7, and ultimately, section 8 serves as the conclusion by synthesizing the findings, mentioning limitations, proposing solutions, and outlining future research directions.

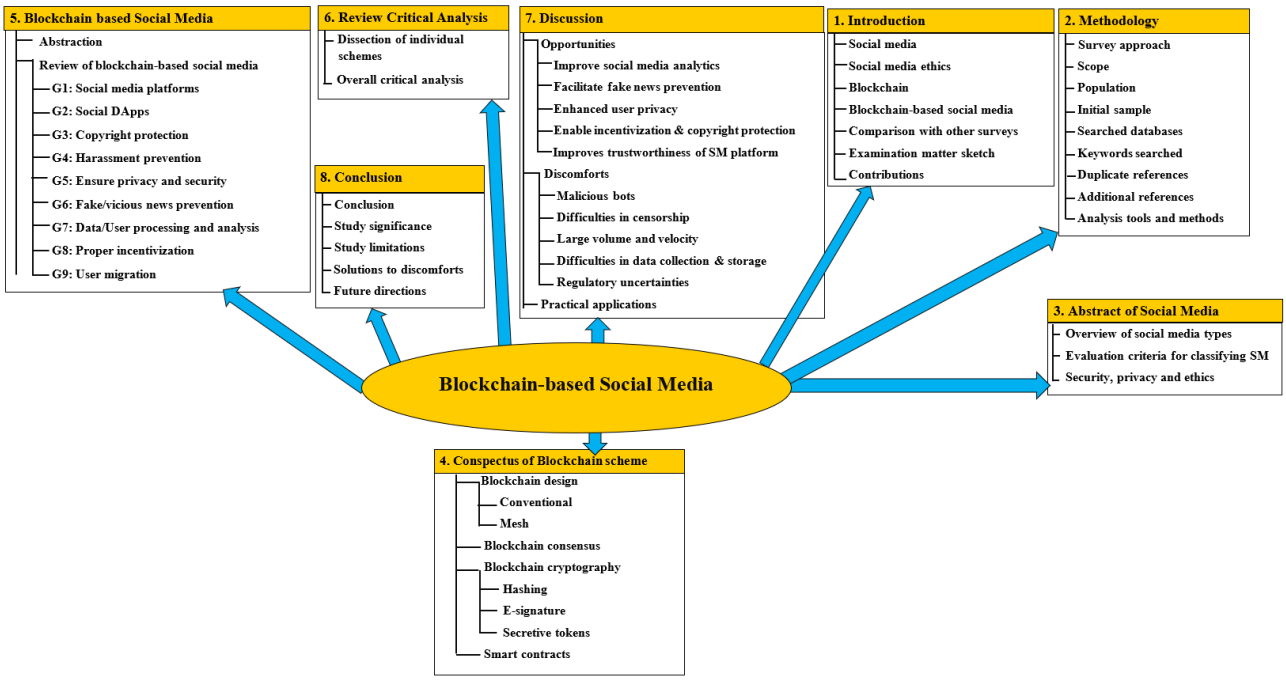


Figure 1. Matter sketch of blockchain-based social media examination.

2. Methodology

The methodology employed in this survey is a systematic literature review, where we find answers to two research questions: R1 ("What are the existing blockchain-based social media frameworks?") and R2 ("What are the trends, gaps, and challenges in deploying blockchain for social media?"). In order to answer the above research questions, it follows a mixed-method systematic review with a narrative synthesis and quality assessment approach as we qualitatively review the literature with conceptual grouping with a percentage-based quality assessment. Since the included studies provide descriptive and conceptual insights rather than numerical meta-analysis data, a narrative synthesis approach was employed to group and interpret findings effectively.

This scrutiny overviews the new research inspections on blockchain-based social media communicated as online papers over the ages, employing a mixed quality assessment approach [27]. Concretely, it counts several of the basics of social media and blockchain. In consequence, all novel research findings and online material published on SM, blockchain-based SM, and blockchain portray the group of possibilities for review within the boundaries of this scrutiny. However, works in the possibility group are rigorous to probe in this work. Because of that, employing the matching surveying word combinations and leaching rules, we heaped 95 works from novel research findings and online material.

We delved into Google Scholar article search engine, ScienceDirect journal repository, ACM digital database, Wiley publishing platform, MDPI academic database, and IEEE Xplore research database. The handpicked surveying word combinations were "Social media" OR "Blockchain-based SM" OR "Blockchain-based social networks" OR "Blockchain-rooted forums" OR "Blockchain-rooted blogs" OR "Blockchain-rooted messaging" OR "blockchain-based professional networks" OR "blockchain-based content communities" OR "Blockchain-rooted virtual worlds" OR "Blockchain-based SM copyright infringement" OR "Blockchain-based SM harassment" OR "Blockchain-based SM misinformation" OR "Blockchain-rooted SM monetary exploitation" OR "Blockchain and SM privacy" OR "Blockchain-based SM analytics" OR "Blockchain".

A set of predefined criteria governed the selection of studies, referred to as leaching rules. First, the mentioned writing commands English composition, and latterly, it commands notably resemblance to the surveying word combination. Next, for establishing the truthfulness of the scrutiny conducted, serialized journals were delegated primacy over forum reports and pre-print reports. We didn't favor novel research findings in a chosen publication manager fulfilling the leaching rules; contrariwise, we conceived all publication managers with similar treatment. The concluding leaching rule reveals that a chosen novel research finding commands dispersal inside the time gap of 2015 and 2024.

The preparatory sample was condensed to 93 works, since it was discovered that 2 works were excesses. We sourced diverse techniques and concepts related to the review, utilizing 45 other works. To connect this scrutiny with preexisting scrutinies, we furthermore blended 2 review documents with the collection of studies, attaining the collective numeral of works to 140.

As the number of studies was small, we used manual forms to record the study's details (methods, results, limitations if they exist, time, etc.) in order to extract useful data from them by manually reading the articles. Moreover, we didn't employ PRISMA as it demands extensive documentation, systematic tracking, multiple reviewers, and does not align well with the proposed review with qualitative synthesis that does not involve any meta-analysis.

To scan the gathered blockchain-based social media, we utilized the grid schema for the scrutiny analysis. We drew perceptions related to the reviewed frameworks, leveraging a workbook application to disinterestedly analyze scrutiny data coexisting with social media- and blockchain-rooted characteristics [28].

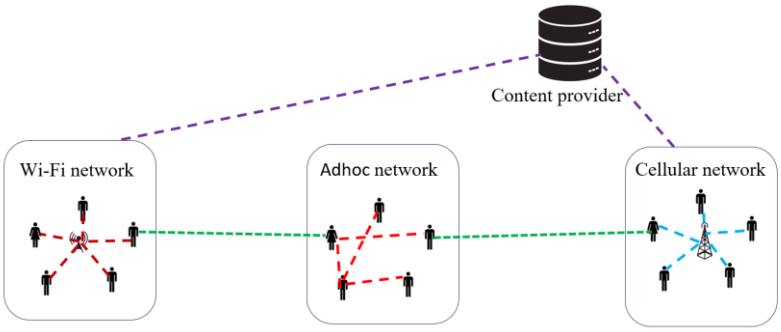


Figure 2. Architecture of a hybrid mobile social network.

3. An Abstract of Social Media

In this section, we provide an overview of social media types and classify social media based on some criteria, then move on to discussing security, privacy, and ethics in SM and SM analytics.

3.1. Overview of social media types

3.1.1. Social networks

Social networking refers to the practice of connecting with other people and forming relationships with them using online platforms [29]. In a social network, users have their own profiles containing profile pictures and personal information that remain as a virtual identity that others can view. In these networks, users can distribute diverse items, just like text, photos, videos, links, status updates, etc., through posting. In these posts, users can express themselves, show their talents, and tell experiences. Users can further interact with one another by commenting on posts, liking them (reacting to posts), and appreciating or providing feedback on others content. Research has shown that celebrities' posts and contextual interactions have a favorable impact on spontaneous purchasing in social marketplaces, based on a fuzzy set analysis done on social network data collected from Pakistani respondents [30]. Network data analytics can be leveraged to analyze trends in social media networks through data collection [31].

One of the key features of social networking is the maintenance of relationships by allowing users to connect with others of their desire. Moreover, it facilitates social circles to create a community of people having similar interests, hobbies, ambitions, etc. who can communicate with each other to achieve the objectives of the social circle. Social circles can be effectively used for scientific studies. A study of whether perceived norms regarding descriptive and liking norms related to the Facebook circle's eating habits predicted the participants' food consumption body mass index, has shown a positive relationship among them using linear regression [32].

Figure 2 renders the architecture of a hybrid mobile social network. As shown in Figure 2, a hybrid mobile social network can consist of a collection of interconnected networks such as ad hoc networks, Wi-Fi networks, and cellular networks. In these networks, content providers will provide content to the social media users available in the network.

3.1.2. Forums

Forums are cyber conversation media in which users can publish messages, inquire about queries, and participate in discussions on diverse subjects. On these platforms, users can seek advice on certain topics, share knowledge, and seek the opinion of subject experts. These platforms are mainly knowledge-based, where the social media richness is relatively lower since the main intention is knowledge exchange [33]. The speed at which instructors post and initiate forums has been known to show an influence on the student posting rate and engagement in the forums, according to a study with 200 participants [34]. Forums are generally arranged as threads, with each thread centered around a

specific discussion. Users can create new threads or provide reply to an existing thread. Forums exist to have community engagement, allowing users to share experiences and provide support to one another. Research shows that online discussion threads have features of face-to-face group work, even though interaction is limited compared to social networks, and they can be visualized as group discussions [35]. The thread ownership of a forum is typically distributed among the participants.

3.1.3. Blogs

Blogs are more like personal publishing platforms, where individuals post content in the form of articles, essays, etc. Blogs also allow comments and discussion; however, the post is centered more around the content creator's perspective than the participant's opinions. Blogging has supported older adults to develop their identity, express themselves, and support adult values, engaging them actively after retirement and providing them with the opportunity to be in a community. Other participants often engage in the role of readers and are allowed to ask questions related to the blog [3]. Blogs are structured as chronological entries, with each post covering a specific theme. The ownership of content in blogs belongs to either the content creator or the organization that publishes the content. However, many blogs do not specify who authored them, such as travel blogs created by web hosts who produce narratives about particular destinations without specifying who created them [36].

3.1.4. Messaging

Messaging platforms allow the exchanging of messages (texts), media files (audio and video), and engaging in real-time communication. The instant nature of these platforms allows communication with a low latency in real-time in comparison to social networks that typically engage in non-real-time mode [37]. Google Firebase is a database that provides real-time service by updating in real-time and keeping track of transferred data, allowing communication with minimum delay across the internet [38]. These are not limited to personal messaging and also support group and community chats where multiple people can engage in a single conversation, facilitating social interaction and collaboration. A study done regarding group communication on the WhatsApp messaging platform found that the subject of discussion is mostly education or business compared to personal issues and events, while females have a higher probability of sharing personal issues and engaging in gossip [39]. Messaging platforms are also utilized by businesses to address inquiries of the customers and engage in conversation in order to improve customer satisfaction. On these platforms, users expect a high level of privacy, such that conversations are typically end-to-end encrypted, making conversations private. More security features, such as content deletion, chat deletion, and privacy settings, exist on these platforms. A study that analyzed the user status sharing feature of WhatsApp proved that content privacy concerns have had an effect on the type of theme selected for sharing, which includes a particular type of feeling [40].

3.1.5. Professional networks

Professional networks allow individuals to connect, interact, and collaborate in a professional context. Due to the prevalence of these, industries can build relationships, share professional knowledge, and seek career opportunities. Studies have shown that professional networking is identity-congruent and tends to expand the network, while self-interest can be used to predict networking intentions [41]. The objective of these networks is professional interaction in comparison to social interaction in social networks. The user profiles are more aligned in the direction of professional facts like work experience, education, and career accomplishments rather than personal hobbies, desires, etc. Ontologies have been shown to represent user profiles in these networks that have classification hierarchies, and matching frameworks can be built to consider profiles and assign weights [42]. Similar to social networks, professional networks build connections among colleagues, industry peers, and recruiters, and they can interact through messaging and group discussions. These networks also support

educational resources, webinars, and online courses for individuals to engage in learning activities. They also provide the opportunity for job seekers to connect with recruiters, making the overall recruitment process efficient and fast. Work in [43] uses a graph neural network to include professional connections to support missing user information with contextual information of professional connections having a job-specific attention technique to tally with the person's job-fit model. They can circulate industry-related news among the professionals such that they are aware of the latest events and trends in the industry.

3.1.6. Collaborative projects

Collaborative projects permit concurrent synthesis of work by numerous users to work towards a shared goal. Global collaborative projects have increased the motivation of students to take actions as digital citizens to overcome barriers to digital citizenship and use them for collaboration in learning [44]. People can contribute their ideas and skills for the collaborative work openly, where users can join and collaborate irrespective of their expertise. In these, projects can be developed effectively, as feedback from peers is received in real-time and work can be adjusted iteratively considering comments. Due to collaboration, work achieves a higher level of success than if the project were done by a single individual. In [45], authors show that collaborative projects are essential for online presence to communicate with stakeholders and employees and further show that negative facts posted can pose a threat to firms. The best real-world example of a collaborative project is Wikipedia, the free encyclopedia. Graduate courses have introduced Wikipedia projects where students need to write high-quality articles for Wikipedia collaboratively by applying course work content learned in the classrooms [46].

3.1.7. Multimedia sharing (content communities)

Content communities are online spaces where users can create, share, and engage with multimedia content like videos, audios, and images. They promote user-generated content, allowing people to produce and disseminate content. According to a survey done based on YouTube, the quantity of posts and reviews has a favorable influence on the sensed reliability and value of the user generated content [47]. In contrast to traditional media sharing, where there is minimum interaction between the content creators and fans, in content communities, the creators and audience are actively engaged by viewers liking and commenting on the content shared and subscribing to the channels of the creators, while the creators can respond to comments. Studies show that medium to long length videos uploaded during office hours on weekdays with lesser active events tend to attract a higher level of community engagement than others [48]. Creators can monetize their content by using advertisement revenues, sponsorships, merchandise sales, etc. These platforms have content recommendation systems to recommend content to users based on user interests and search histories, with the objective of engaging the users more time on the platform. Content communities also support live streaming and short-form videos. The multimedia content community authorities can collect data from a central location, analyze it, and make decisions according to the outcomes to provide a good service to the clients [49].

3.1.8. Virtual worlds

A virtual world demonstrates a three-dimensional space in which users can act as avatars to interact with other avatars like in real life. These are featured by a raised degree of social presence with media richness and differ from virtual reality in this perspective, as the user experiences being with many others in a virtual space [50].

Figure 3 renders the design of a web-driven virtual world. As shown in Figure 3, a virtual world client in a local site communicates with a virtual world server, while scripts in the local site communicate with a database using a communication channel. The server processes client requests, ensuring data exchange between the virtual world and the database, enabling real-time updates and interactions within the virtual environment.

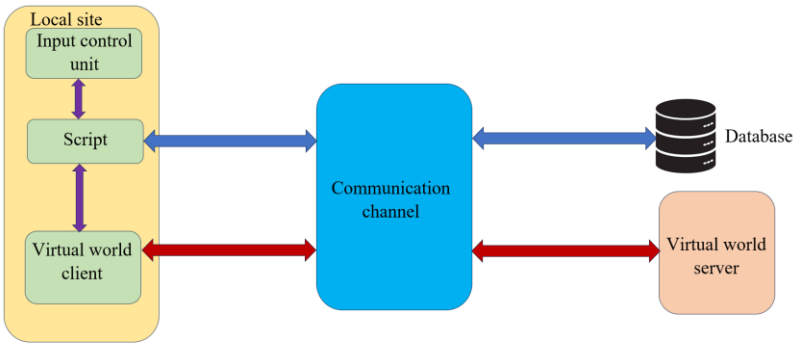


Figure 3. Design of a web-driven virtual world.

Virtual social worlds (VSW) – Virtual social worlds resemble real-life environments like cities and fantasy realms where users can socialize, explore, create content, participate in events, engage in commerce, etc. In these social worlds, users can connect with each other from various areas of the world, creating communities with shared interests. These worlds lack game mechanics, in contrast to virtual game worlds, and they can include fun elements through business interaction, learning activities, and socialization [51]. Moreover, users have the freedom to express themselves creatively through avatar customization, virtual property development, and content creation. Further, they provide an opportunity for the users to escape from the real world and embed them in fantasy environments. Research done in the "Second Life" virtual world shows that racial minority people exposed to cues from white dominant avatars begin to think of the virtual world as identity-threatening, which has resulted in being psychologically disconnected from the world [52].

Virtual game worlds (VGW) – These are virtual environments primary designed for the gaming experience rather than social interactions and have characteristic gameplay mechanics, challenges, and progression systems. Even though some degree of social interaction exists in virtual games also, the primary focus is on the gaming experience, such as winning battles, solving puzzles, participating in competitions, etc. An analytical study shows that these virtual worlds are dominated by avatars in the form of white men, while female minorities are least observed [53]. Furthermore, the multiplayer option allows for collaboration and competition with each other. In comparison to virtual social worlds, these can improve the skills of the players, like issue resolving, strategic thinking, and communication, as these skills may be required to win the game. Further, in these environments, players can buy and sell virtual assets either using in-game earned rewards or using virtual/real currencies. In a study regarding the massive multiplayer game RuneScape, researchers found that game economics partially depicts practical economics, and these virtual worlds can be utilized to understand real economics [54]. In another study regarding the virtual game world "World of Warcraft", it was proved that motivations related to teamwork and competition have resulted in speedy progression inside the game, and virtual involvement in the game does not negatively affect day-to-day activities [55].

3.2. Evaluation criteria for classifying social media

3.2.1. Based on social presence/media richness

Social media richness is the amount of interactivity and depth of communication on a given SM platform. It can be indicated by individual or combined effects of textual richness, visual richness, interactivity, and personalization. Studies suggest that there exists a favorable correlation among media fullness and the usage of SM for learning in the organizations evaluated using media richness theory [56]. Blogs that allow longer-form textual content have a high degree of textual richness, allowing users to engage in deeper discussions. Content communities are rich in visual richness, as users can share multimedia content such as

music, videos, photos, etc. Social networking sites often provide a higher level of interactivity through live streaming that provides users to interact with each other using comments, likes, shares, etc. Media richness has shown an influence on the adoption of social media by microbusinesses, as explained by media richness theory and quality theory [57]. Personalization is giving an opportunity for user preferences. In content communities, personalization is high, as there exist personalized content recommendations that match personal interests. Research has shown that trait-based personality matching leads to a higher possibility of engagement with social media and has identified the best personality traits and user characteristics suitable for this purpose [58]. Interactivity, visual richness, and personalization are even much higher in virtual worlds, where players are either cooperative or compete with each other virtually. Generally, SM fullness is little in blogs and cooperative projects, moderate in social networks and digital communities, and large in virtual worlds. In social media networks having high communication richness, a high quality of service is required entirely because of the load of communication that needs to be transmitted per unit of time and the quality expected in them [59]. Thus, in order to satisfy such high-end quality of service requirements, routing techniques that adhere to these service constraints need to be used on these platforms [60].

3.2.2. Based on self-presentation

Self-presentation is the intentional formation of an individual's identity using profile information, photos, interactions, etc. The degree of self-presentation can be diverse based on the social networking platform used and the individual's preferences. For instance, blogs can contain writings that reflect the writers' interests and personality traits. By analyzing 124 blogs, work in [61] has shown that blogs written by young adults pay attention to daily activities, friends, and relationships rather than self-presentation. In social networks, the user profile containing the profile picture, bio, and personal information depicts a high degree of self-presentation. Moreover, on social networking sites, users can create narratives about themselves by storytelling in posts and comments. A study involving Finnish young adults using the Facebook platform proves that social norms are major factors in driving towards content sharing and self-presentation in both automated and manual sharing techniques [62]. In virtual social worlds, users have customization options for avatars, environments, and virtual possessions since users can design the avatar to reflect their desired appearance and style. Moreover, virtual social worlds allow role-playing and fantasy scenarios, allowing users to embody alternate identities and experiment with them. However, role playing and fantasy scenarios have shown a high prevalence of attachment disorganization within the players with considerable dissociative features and further state that players can use dissociation to protect from abuse in attachments [63]. Furthermore, virtual social worlds provide a high degree of social interaction to maintain connections among the users, allowing for self-expression and self-disclosure. Virtual worlds have pseudo-anonymous features that allow users to conceal their identities such that they can express themselves freely due to their concealed identities. It has been found that being completely self-expressive or non-self-expressive has been driven by motivations of relationship formation and reputation maintenance, according to a study done on participants in the virtual world game Second Life [64]. Thus, generally, self-portrayal is large in blogs, social networks, and VSWs, while it is low in cooperative projects, digital communities, and VGWs.

3.3. Security, privacy, and ethics in social media

3.3.1. Copyright infringement

Copyright infringement occurs when someone uses or shares a copyrighted work without permission from the copyright holder. In virtual worlds, this can occur when users create avatars and environments that are based on copyrighted content and distribute them without permission. Moreover, avatars created by players should be considered the joint work of the game creator and player and copyrighted accordingly, according to incentive theory and natural rights theory [8]. This is seriously observed in content communities where users may upload copyrighted music, videos, or

images without a proper license, leading to legal action by the copyright holders. For instance, for prank videos on YouTube, the prank video creators have been heavily harmed morally and economically due to copyright infringement, and government regulations have not been strong enough to take satisfactory action against violators [65].

3.3.2. Misinformation

Misinformation is the spreading of incorrect or false information through social media. Due to the high speed at which they operate, misinformation can be spread fast before the post creator can identify and correct it. If false information gets a high attention, it can be amplified by algorithms that prioritize it based on attention factors, such as the number of likes and shares. Confirmation of this misinformation by several users can reinforce this misinformation. Specifically, health misinformation related to smoking, vaccines, diets, and eating disorders has been higher on social media, according to a systematic review [66]. Social media often lacks content moderation systems to remove misinformation, mainly due to the high volume of contents that are shared; thus, misinformation can spread unchecked. Moreover, social media has been criticized for unfair use of content moderation considering ethnicity, communities, and minorities, and content moderation policies are driven by business priorities, government regulations, and outside pressure [67]. On these platforms, there can be malicious users who create fake accounts and spread misinformation intentionally for financial or political gain. If decisions are taken based on misinformation, they can have a negative impact on society, as the effects of decisions are less effective due to incorrect information.

3.3.3. Harassment

Harassment is a serious issue on social media having significant social, legal, and psychological implications. Harassment can occur in various types, such as cyberbullying intended to harm others, trolling that involves offensive comments to provoke others, hate speech targeting individuals based on religion, caste, etc., and sharing someone's sensitive images or videos without his/her consent to take revenge. Research has shown that there has been sexual abuse of social media users by analyzing stories released by people who were abused [68]. Due to harassment, individuals can become mentally ill, leading to anxiety and depression. It can also affect professional life, sometimes causing individuals to lose job opportunities. As from a study done in a student campus, it has been revealed that one quarter of students have been harassed by sending angry or threatening messages, and this has affected negatively towards the wellbeing of the students [69]. Due to the anonymity of social media, it can be challenging to hold individuals accountable. Moreover, it can be challenging to take legal action against harassment, since social media networks often work globally. As social media networks also promote freedom of speech, it is difficult to compromise when they are misused for verbal harassment. However, there are international regulations and legal protection laws for serious harassment, such as by women who have undergone sexual harassment on social media [70].

3.3.4. Monetary exploitation

Social media can provide the opportunity for scams and fraudulent schemes like phishing, pyramid schemes, and false investment opportunities. A systematic literature review suggests that women having lower technical knowledge on security at lower middle age are more vulnerable to phishing attacks on social media [71]. Since social media often provides monetization for content creators through features like ad revenue sharing and subscriptions, it can incentivize platforms such as clickbait to generate more views and engagement. However, researchers have proposed machine learning-based tools [72] to detect clickbait in social media with high accuracy without using meta-features [73]. Algorithms in social media attempt to maximize user engagement, which can be negatively affected by the creation of echo chambers and exploiting users' attention for financial gain. In [74], authors show that echo chambers and filter bubbles have an influence on SM variation of information

sources, and the diversity changes with the social media platform that users have chosen. Influencers who have a large number of social media followers may advertise content solely for monetary gain without considering the interests of the followers. Social media may monetize content that has been uploaded for free by content creators through targeted advertising, which can be considered monetary exploitation in cases where a proper percentage of revenue is not provided back to the content creators.

3.3.5. Privacy

Social media platforms collect private data like browsing habits, locations, interactions, personal preferences, etc. in order to target advertisements on them. Nevertheless, this can spawn privacy problems when data is collected lacking the user's explicit permission. The survey in [13] shows that there has been significant privacy exposure on social networks, and the level of exposure differs based on the specific networking platform, gender, age, etc. The personal data collected can sometimes be misused for financial attacks on users. Specifically, cybercriminals can make use of this private data to extract passwords, email addresses, etc. to launch cyber-attacks on the users. For instance, in [75], authors show how social ties among Facebook users and voter registration records can be used to get an idea about users who live within the city and to create detailed profiles from the inferences. Even though these platforms have configurable privacy settings, these settings are complex and can expose the privacy of users more than they anticipate. Social media has also been criticized for sharing user private data with government organizations for surveillance purposes. Privacy and security have arisen as an important part of a social community, as there exist evidence to mention that some people have even committed suicide due to undesirable privacy exposure from social networks, despite the fact that they have also been used for suicide prevention [76]. Thus, users must take precautions to set safe privacy settings and manage their personal profiles carefully.

3.4. Social media analytics

In social media analytics, data is collected, analyzed, and interpreted to gain an idea about user behavior, sentiment, trends, and opinions. Data analytics tools that attempt to analyze the data and find a desired relationship can be utilized for this purpose [77].

3.4.1. Scraping

Scraping uses automated tools and application programming interfaces to extract data. It can collect data varying from individual posts to entire user timelines. In [78], a socially smart platform is implemented for web crawling or web scraping along with an application programming interface to retrieve top posts from diverse social media sites once the resource locator is given. Similarly, another research implements web scraping in social media by using an application programming interface supplied by Facebook and Twitter along with Regex for matching text using patterns [79].

3.4.2. Sentiment analysis

Sentiment analysis aims to determine whether the sentiment is positive, negative, or neutral. Natural Language Processing (NLP) can be leveraged to analyze text data and classify it based on sentiment. Using both visual and textual features, a sentiment analysis method for images has been feasible using supervised and unsupervised approaches formulated as an optimization technique for finding the local optimum solution [80]. Moreover, SMARTSA is a lexicon-driven sentiment classification scheme for genres of social media that extracts contextual perspective using local and global context [81].

3.4.3. Text analytics

In text analytics, meaningful insights are derived by analyzing texts. They can use techniques like named entity recognition, topic modeling, and keyword extraction to identify important entities, topics, and keywords, giving insights into emerging trends and user

interests. In [82], text mining is used to analyze patient stories on a care opinion platform to explore medical experiences, where topic modeling and sentiment analysis are specifically used for analysis to get an insight from them. In [83], word clouds, which are a method of cleaning text using the most frequently used words, are utilized for text analysis of tweets in order to get an idea about the sentiment.

3.4.4. Opinion mining

Opinion mining attempts to extract user opinion, attitudes, and preferences that go beyond sentiment analysis by analyzing the reasons behind opinions. Aspect-based sentiment analysis is leveraged using latent Dirichlet allocation for topic modeling and mentioning the main component of the user address, where word dependencies are extracted to identify the user's comment's polarity [84]. Ortony-Clore-Collins and a convolutional neural network are jointly used in [85] for opinion summarization in microblogging schemes, which is tested using sentiment classification performance.

3.4.5. News analytics

News analytics focus on analyzing news items shared on social media platforms. Specifically, it identifies trending news topics, analyzes news sentiment, and tracks the spreading of news articles. It can be used to identify the impact of news events on public opinion and behavior. In [86], authors show how news analytics can aid in tracking changes brought by social media news distribution in order to develop a scheme to monitor digital news. Moreover, MAQSA is a scheme that has been proposed for news analytics in social media by providing a topic-based dashboard to summarize news articles, helping editors understand user involvement and audience sentiment change over time [87].

Table 1 renders active literature on social media conceptions, inspected in terms of the SM conception, prevailing literature for those conceptions, the procedure followed in literature, and corresponding results.

Table 1. An abstract of active literature on social media conceptions.

Social media conception	Active literature	Procedure	Findings/Results
Social networks	Impulse buying [30]	Fuzzy set analysis	Celebrities' posts and contextual interactions have a positive effect on impulse buying
	SM eating habits [32]	Linear regression	Facebook circle's eating habits predicted the participants food consumption body mass index
Forums	Online discussion forums [34]	A 200-participant astronomy program	Instructors posting speed and initiate forums have shown an influence on the student posting rate
	Interaction on online forums [35]	Interviews and content analysis	Online discussion threads have features of face-to-face group work
Blogs	Online content creation [3]	Older adults interviewing	Providing older adults with the opportunity of being in a community
	Blog ownership [36]	Examine features of travel blogs	Web hosts who produce narratives about particular destinations
Messaging	Google Firebase [38]	Realtime communication application to send text messages	Keep track of transferred data allowing communication with minimum delay
	WhatsApp group communication [39]	A questionnaire survey	Subject of discussion is mostly education or business
	WhatsApp user state sharing [40].	Status data collected using telephone interviews have been analyzed	Content privacy concerns have had an effect on the type of theme selected for sharing

Table 1 continued

Table 1 (continued). An abstract of active literature on social media conceptions.

Social media conception	Active literature	Procedure	Findings/Results
Professional networks	Identity and professional networking [41]	4 studies done to identify relationships	Professional networking is identity congruent and tends to expand the network
	Profiles [42]	Use ontologies to represent profiles	Discuss on profile similarity and compatibility
	Person job-fit [43]	Graph neural network to include professional connections, attention mechanism	Effective for a use case demonstrated using LinkedIn
Collaborative projects	Global collaborative projects [44]	Qualitative case study using interviews and Wiki data analysis	Increased the motivation of students while taking actions to overcome barriers in digital citizenship
	Wikipedia [45]	Supply an inner view regarding collaborative projects	Negative facts posted can cause a threat for firms
	Wikipedia projects [46]	Observations from instructors and post-project reflection survey	For less computer literacy students, effort has been used to learn the tool more than course content application
Content communities	UGC on YouTube [47]	Assess sensed reliability and value of produced items in YouTube	Quantity of posts and reviews have a favorable influence on sensed reliability and value of the user produced items
	YouTube video content features [48]	Analysis of videos from digital influencers to identify factors	Long length videos uploaded in weekday office hours tend to attract a high community engagement
Virtual social worlds	Learning fun in SVW [51]	Model fun and investigate how it is related to learning experience	Identify fun activities in social virtual worlds and identify play and socialization
	Second Life [52]	Experiments where participants read fictitious profiles of second life avatars	Identity threatening for racial minor people
Virtual game worlds	White man's MMOG [53]	Content analysis for gender and race	Dominated by avatars in the form of white men
	RuneScape [54]	Analyze texts, observations, self-reports, etc.	Game economics partially depicts the real-world economics
	World of warcraft [55]	Investigate connections among self-reported motives and real game behaviors	Motivations related to teamwork and competition have resulted in speedy progression inside the game
Media richness	SM usage for learning [56]	Media richness theory, SECI scheme	Positive relationship among media richness and usage of SM for learning inside the organizations
	MRT for SM adoption [57]	Canonical action research method, media richness theory	Media richness have shown an influence for adoption of social media by microbusinesses
	Trait based personalization [58]	An experiment to investigate effectiveness of trait-based personalization of messages	Trait-based personality matching leads to higher possibility of engagement with the social media
Self-presentation	Blogs [61]	Analyzing entries in public hosting websites	Blogs written by young adults pay attention to daily activities, friends, relationships rather than self-presentation
	Social networks [62]	Study of Finnish young adults using Facebook platform	Social norms are major factors in driving towards content sharing and self-presentation
	Virtual worlds [63]	Internet-driven survey utilizing internet addiction test	Role playing and fantasy scenarios have shown a high prevalence of attachment disorganization
	Virtual game worlds [64]	Interview data discussed in terms of different theories	Completely self-expressive or non-self-expressive has been driven by motivations of relationship formation
Copyright infringement	Avatar copyright [8]	Incentive theory and natural right theory	Avatars created by players should be considered as joint work of the game creator and player and copyrighted accordingly
	Prank videos in YouTube [65]	Using data samples of viral prank videos, Intellectual property rights	Video creators have been heavily harmed morally and economically

Table 1 continued

Table 1 (continued). An abstract of active literature on social media conceptions.

Social media conception	Active literature	Procedure	Findings/Results
Misinformation	Health misinformation [66]	Systematic review of literature	Health misinformation is high in social media
	Double standard content moderation [67]	Provide and discuss content moderation policies	Unfair use of content moderation considering ethnicity, communities, and minorities
Harassment	Sexual harassment [68]	Analyzing stories released by people who got abused using social media language model	Evidence of sexual abuse to social media users
	Cyber-aggression [69]	An internet-based survey, individual interviews	One quarter of students have been harassed
	Cyber-porn [70]	Analyze legal defense for women who were preys of social media sexual harassment	Point out legal protection
Monetary exploitation	Phishing attacks [71]	A systematic literature review	Women having a lower technical knowledge on security at lower middle age are more vulnerable to phishing attacks
	Clickbait [73]	Machine learning-based tools	Detect clickbait in social media with a high accuracy
	Echo chambers and filter bubbles [74]	Analyzing 4 years of web browsing history	Echo chambers and filter bubbles have an influence on SM variation of information sources
Privacy issues	Privacy settings & information disclosure [13]	A social experiment on response for profile access request by a stranger, survey	Significant privacy exposure in social networks
	The city privacy attack [75]	Create detailed profiles from the inferences using social ties and voter registration records	Demonstrated the attack for Facebook
	Suicide prevention [76]	A systematic review	Users have used social media sites for suicide prevention
SM scraping	Socially smart aggregation system [78]	Web scraping along with API	Retrieve top posts from diverse social media sites
	Web scraping [79]	Web scraping, API by Facebook and twitter, matching text using patterns	Overload information stored in database, could adjust information relevancy
SM sentiment analysis	Image sentiment analysis [80]	Supervised and unsupervised approaches formulated as an optimization technique	Better performance than state-of-the-art
	SMARTSA [81]	Lexicon-driven sentiment classification scheme	Improve sentiment classification
Text analytics	Patient story analysis [82]	Topic modeling and sentiment analysis	Clear sentiment in 99% stories
	SM analytics [83]	Word clouds and sentiment analysis	Can use to explain text analysis task and assess it
Opinion mining	Aspect based sentiment analysis [84]	Sentiment analysis using latent Dirichlet allocation for topic modeling	Ensemble system can accurately analyze user generated content and identify user opinion
	Opinion summarization [85]	Ortony-Clore-Collins and a convolutional neural network	Analyze micro-blog data set
News analytics	SM news analytics [86]	Critically analyzes the impact of news analytics	News analytics can aid to track changes brought by social media news distribution
	MAQSA [87]	Topic-based dashboard to summarize news articles	Provide chance for participants to define and explore own topics, dynamically specify topics and dates

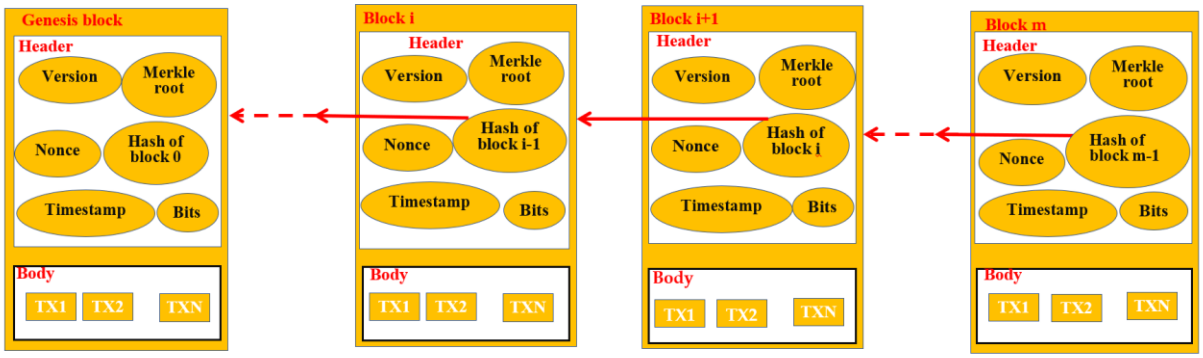
4. Conspectus on Blockchain Scheme

In this section, we provide an overview of the design, consensus, cryptography, and smart contract concepts in the blockchain framework.

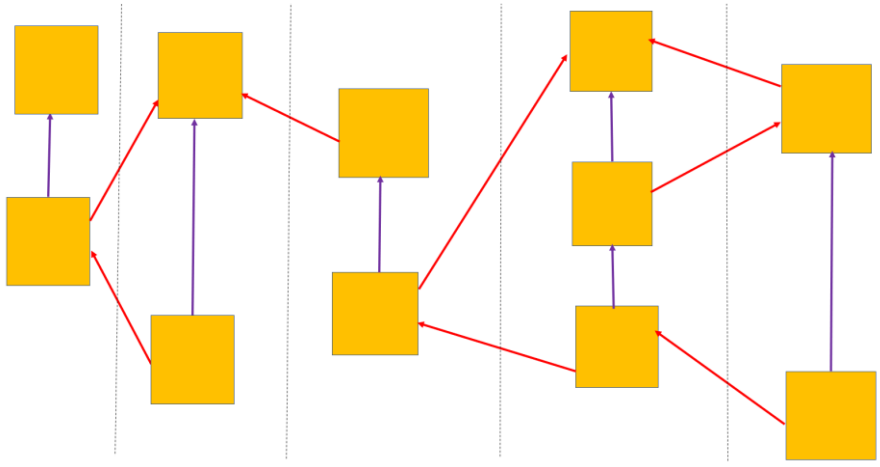
Blockchain is a segregated ledger framework that securely reserves transactions through a communication network [88]. The transactions are unalterable, resulting in them not being viable to change or remove without the agreement of the peers, further resulting in the blockchain being authentic [89].

4.1. Design

In conventional blockchain, there exists a straight progression of blocks in which every block carries a bunch of transactions, and at the same time, any block is connected to a prior one utilizing a secure hash, creating a chain [90], as shown in Figure 4(a). The mesh blockchain differs from the conventional blockchain, having entries that are not bunched into blocks, but in contrast, are independently connected to several prior transactions [91], as shown in Figure 4(b). This architecture enhances their flexibility and results in increased bandwidth as operations are able to be functioned simultaneously. There are also fused frameworks that fuse the characteristics of conventional and mesh blockchains [92]. Figure 4 renders the blockchain designs discussed.



(a)



(b)

Figure 4. Blockchain designs (a) Conventional (b) Mesh (Hash graph).

4.2. Consensus

It is the approach utilized by blockchain to achieve unanimity regarding the believability of the operations for the purpose of conserving their truthfulness [93]. In conventional consensus strategies, miners battle to figure out a complicated task, and the foremost one to figure it out receives the chance to append the coming block [94]. Distinctive consensus techniques involve relying upon the quantity of coins preserved and the capability to stake, the preservation of raised honor and sovereignty, the capability to reserve disk allocation, etc. [95].

4.3. Cryptography

Cryptographic strategies are worked to sustain the safe and unalterable features of operations, in contrast to data fusion [96]. In hashing, supplied data creates a certain size output, which is utilized to guarantee data truthfulness and invoke unequaled recognizers for blocks [97]. E-signature, which is implemented utilizing key-pair cryptography, is utilized to guarantee the genuineness of operations by utilizing a secret key for registering the operations and a publicized key to validate the signs [98]. Secretive tokens are utilized to denote the possessions, proprietorship, and proprietorship movement in segregated applications [99].

4.4. Smart contracts

In self-executing contracts, expressions of accord are explicitly recorded within the source code that can be implemented themselves after predetermined requirements are confronted [100]. Therefore, these are utilized to implement accords without third parties, removing the requirement for brokers, decreasing the dangers of hoaxing and exploitation, and additionally fortifying the status of assurance owing to blockchain's unalterable attributes [101].

5. Blockchain-based social media

In this section, which is the core of this study, first categorizes the abstraction into 9 categories, and then extensively reviews the abstraction.

5.1. Abstraction

Established on this exploration, the blockchain-based social media abstraction can be organized into the immediate 9 duties.

- Social media platforms (G1)
- Social DApps (G2)
- Copyright protection (G3)
- Harassment prevention (G4)
- Ensuring privacy and security (G5)
- Fake/vicious news prevention (G6)
- Data/User behavior/Event processing and analysis (G7)
- Proper incentivization (G8)
- User migration (G9)

Figure 5 pictorializes the abstraction of blockchain-based social media. As shown in Figure 5(a), in G1, rewards are obtained from the blockchain, and results are transmitted to the blockchain from the social media network that performs different operations like voting, posting, transferring, and following, etc. Figure 5(b) shows a generic scenario where a DApp communicates with the blockchain, social network, and smart contracts for setting privacy, verifying users, and registering users, while the online social network can comply with privacy and register OSN. In the G3 concept given in Figure 5(c), a copyright protection scenario is depicted by using blockchain for access control, incorporating encryption with IPFS for content delivery. In Figure 5(d), a harassment prevention scenario is depicted where data from a database is retrieved to the blockchain and provided to an AI model for classification and correction results are provided to the social network by the blockchain. In G5, shown in Figure 5(e), privacy is ensured by storing the data index in the blockchain, and the querier is authorized by the publisher while the data is encrypted in the SN. In G6, as shown in Figure 5(f), news organizations registered in the blockchain submit news that are validated by the

AI models along with blockchain-driven authentication to update the credibility scores. In G7, as shown in Figure 5(g), social media event data are passed through an inference and reasoning module with semantic analysis, and its output is stored in the blockchain. Figure 5(h) demonstrates a typical scenario of G8, where there exists a content sharing marketplace, where publisher and client information can be stored in storage servers with interactions with the blockchain. Figure 5(i) shows a user migration (G9) scenario using a fork operation.

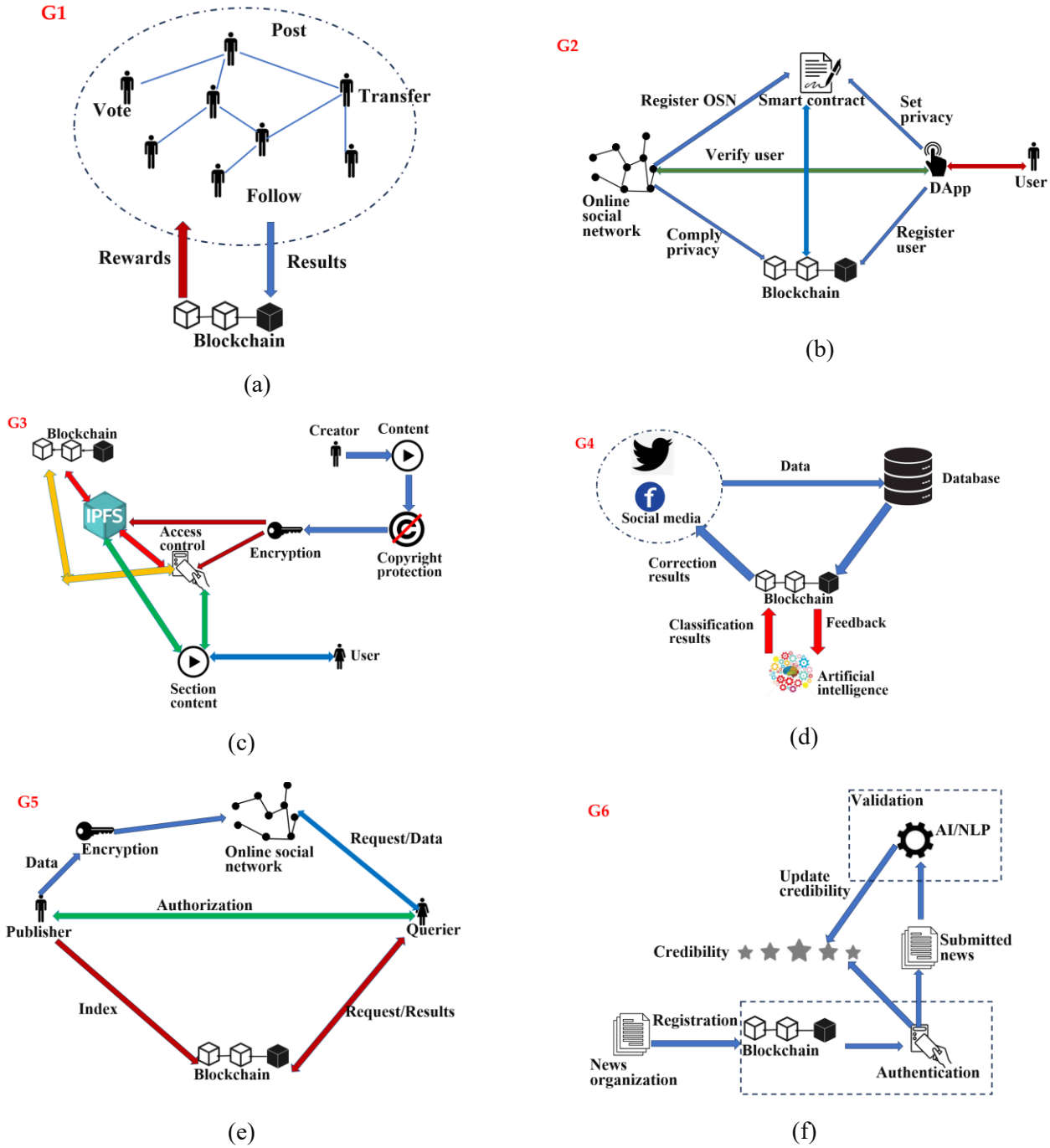


Figure 5. Abstraction of blockchain-based social media: (a) G1; (b) G2; (c) G3; (d) G4; (e) G5; (f) G6.

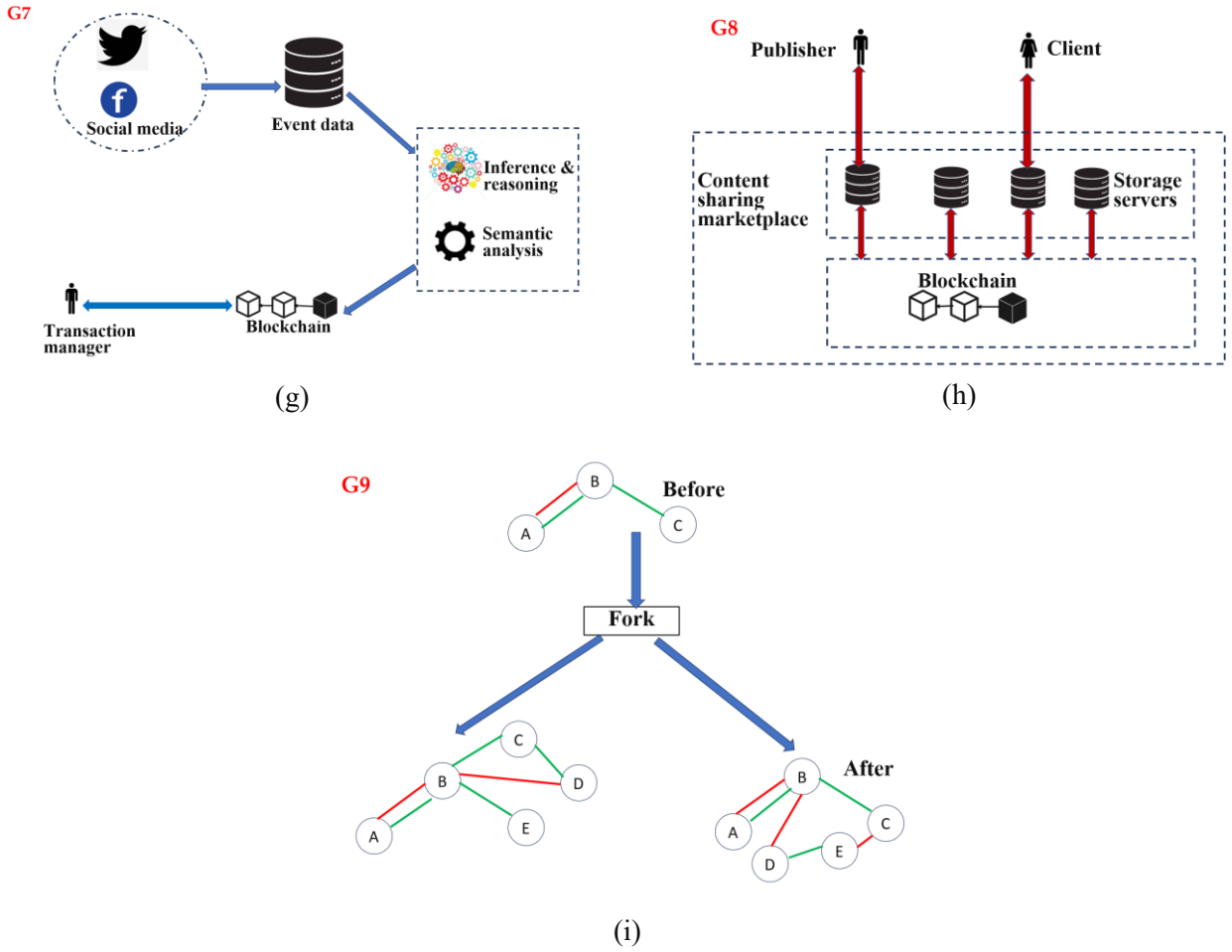


Figure 5 (continued). Abstraction of blockchain-based social media: (g) G7; (h) G8; (i) G9.

5.2. Review on blockchain-based social media

5.2.1. Blockchain-based social media platforms

Steemit is a blockchain-driven incentivized SM platform running on the Steem blockchain that leverages the delegated proof-of-stake consensus approach where users create posts and get selected rooted upon votes from other participants while providing cryptocurrency rewards to creators and curators [102]. However, in Steemit, the level of decentralization is lower than ideal, and it estimates that 16% of cryptocurrency transfers are sent to bots.

In [103], a decentralized social networking application is built on the Ethereum blockchain by leveraging self-executing contracts and IPFS, reducing server-side hardware costs and increasing availability. It has been demonstrated as a proof-of-concept using a test use case.

"SoChainDB" is a framework to obtain data from Hive, which is one of the largest blockchain-driven social media schemes, and discuss applications based on it. This framework is adaptable to other blockchain-driven social media schemes as well, with minimum modifications [104]. This framework supports all traditional social network functionalities like posting, commenting, voting, etc.

ARTICONF is an agile and open social media platform that has high trust by employing a 2-stage permissioned blockchain that uses graph anonymization methods to autonomously detect interest communities, elastic social media applications, and privileged monetary inclusion [19]. In ARTICONF, it

detects communities using graph anonymization in an industrial pilot use case.

"Ushare" is a user-driven blockchain-centric social network that facilitates users being able to manage, track, and claim proprietorship for the content shared thanks to the distributed approach in blockchain. It further has an encrypted hash table, a method to control the number of shares, and a certificate authority to administer users' circles [105]. However, it has been presented as a concept, and its performance has not been evaluated.

Other platforms – In [26], after reviewing existing blockchain social media frameworks driven by the role of content as the center, they suggest a system of blockchain-based cyber-social networks centered on the role of users. Alternatively, some have proposed a theoretical framework for blockchain-driven social media to demonstrate good business strategies by designing its governance, operation, mechanism, and organization structure [106]. However, these platforms still remain conceptual.

5.2.2. Blockchain social DApps

In [20], an Ethereum-based DApp is created to store the privacy settings of users on the social network in a decentralized manner, where a privacy setting change should be validated by a self-executing contract to make sure that they are compatible with the user's desired settings. It utilizes a graph-based model and deploys proof-of-work consensus to implement the DApp.

5.2.3. Copyright protection

In blockchain-based decentralized social media frameworks, in order to prevent copyright infringement of images, videos, audios, etc. and to protect the authenticity and originality of content, IPFS is utilized for distributed social media content storage, while smart contracts with a secret sharing technique are utilized for copyright protection [21]. A decentralized video streaming service leverages access control using IPFS and self-executing Ethereum contracts; encryption and copyright protection are realized to prevent illegal access and distribute legitimate video content with proper payments to the content creators [107]. These frameworks also remain theoretical; however, their concept is theoretically justified by studying strengths and weaknesses.

5.2.4. Prevent harassment

Blockchain has been utilized along with machine learning and NLP to identify cyberbullying on social media by using a fog architecture for detection, reducing the server load [108]. In this study, the highest accuracy has been reported by random forest and J48 classifiers when detecting cyber-bullying using a blockchain-based approach. Similarly, in another work, blockchain and federated learning are applied in a way to provide a decentralized solution for cyberbullying by establishing relations among features and running relation tests on blockchain blocks [109]. In this scheme (BFL-CS), it has resulted in the lowest computational time and has reached an accuracy of 98.2% using the blockchain-based federated learning approach.

5.2.5. Ensure privacy and security

In social media 3.0, which integrates social media networks with IoT, a privacy-aware, explainable blockchain-based social media scheme is presented in [110], where devices can contribute data to a privacy-preserving model and local updates will be evaluated by miners and rewarded using federated learning. It has been experimentally validated using real-world data sets like SM 3.0 and MNIST, and results show high privacy and satisfactory utility levels under privacy preservation restrictions. Further, it has been shown to mitigate the malicious users poisoned updates. An access control scheme that is auditable has been proposed for blockchain-driven cyber-social networks where the resource owners use public keys and access control lists to create access control policies while a private key is maintained in the Ethereum blockchain to decrypt data after validating permissions [111]. The researchers have used the Rinkeby Ethereum testnet in this framework, and experimental results show that it performs better than attribute-driven access control in

terms of gas consumption. A trusted information dissemination system in blockchain-based social media has been implemented by creating a chain combining blocks where each node propagates data considering its credibility with other nodes, where credibility can change based on the available information and trust is calculated both locally and globally [112]. In this scheme, misinformation can be detected along with the source with high accuracy using real-world and synthetic datasets. BPP is a blockchain-driven privacy safeguarding scheme for social networks that leverages public key cryptography for data sharing, retrieval, and accessing fairly without privacy issues, along with a keyword search algorithm to cater to user queries [113]. BPP's simulation results show higher security and low time cost. For secure social media marketing with enhanced transparency and reliability, blockchain has been put forward by the combined use of CryptoNight mining with the YAC consensus approach, preventing falsified data attacks [114]. In this scheme, a keyword search algorithm and public key cryptography are included and have resulted in a higher CPU efficiency and have achieved a high dimensionality in identifying attacks in SM marketing. A scheme for secure social networking by effectively attaching user IDs with user-generated content to give them value has been realized with blockchain, and a use case has been discussed for a framework of robots and IoT devices [115]. This scheme has a query/algorithm tracker and archival features. Some have proposed blockchain to adhere to general data protection regulations in social networks for consent management for personal data processing [116]. In this scheme, Facebook has been taken as a case study for the consent management mechanism.

5.2.6. Fake/Vicious news prevention

In order to reduce false news and fabricated images, a tamper-proof blockchain has been put forward as a resolution to notarize online user activity, where there is a systematic way to verify data for notarizing by authentically archiving it, which has been validated using an instant messaging system as a proof-of-concept [22]. A hybrid proactive and reactive approach to preventing fake/vicious news on social media messaging platforms leverages blockchain and keyed-watermarking for integrity protection of the content while also maintaining accountability for the user of the content, such that fake/vicious news can be immediately stopped by forward/backward tracking [117]. In study [117], bloXroute servers and Raft consensus are proposed to improve the scalability and throughput. Some propose data mining as a blockchain consensus approach to validate the knowledge disseminated on social sites for preventing fake news by identifying it, alerting readers, punishing such fake news creators, and rewarding true news creators, known as "Fakechain" [118]. Simulation results in Fakechain show that it has high trustworthiness, shows gas cost increase with source quantity, and satisfactory precision. Similarly, another blockchain-based social media news validation system has been enforced, making use of Ethereum self-executing contracts along with IPFS and MetaMask to provide credibility indicators during news dissemination to limit fake news spreading [119]. In this scheme, NetLogo is used for agent-based modeling, and it has been able to improve the social media content quality, as simulations suggest that NCI (number of reports and participants who received news) decreases under high fake news scenarios while it increases at low fake news scenarios. Alternatively, some have used non-fungible token content ratings for detecting rumors and bogus news in peer-to-peer blockchain-based social media networks in order to ensure appropriate news is disseminated, known as "authentic facts" [120]. Basically, in this system, if the rating percentage accuracy is greater than 70%, it is considered an authentic news. Moreover, a gamification segment and blockchain consensus approach of proof-of-authority with a dedicated weighted ranking algorithm working as a reward method in gamification have been effective in determining the integrity of false news on the internet of fake media things [121]. Similar to the previous study [120], this study [121] also uses a voting system to evaluate the credibility of the social media news. In blockchain-based social media networks, blockchain has been proposed to store the digital identity of people by creating social accounts that users have to verify with the database while the hashed identity is shared in

the database, preventing the creation of multiple fake accounts by a given person and reducing the probability of the generation of fake news [122]. Alternatively, some have used reinforcement learning with natural language processing to detect fake news, fake accounts, and fake posts where blockchain is utilized to provide authority proof for the digital content [123]. In this study, using data collected from social media such as Facebook, Twitter, etc., the simulation results show that the mean absolute error of the proposed method is the least of 173 compared to other machine learning approaches.

5.2.7. Data/User behavior/event processing and analysis

"SteemOps" is a large dataset created by dividing data collected from the blockchain-driven social media framework Steemit into 3 schemas for social network operating, witness-election operation, and value-transfer operation that can be readily used to generate insights [23]. In SteemOps, 900 million operations of Steemit are categorized into 3 groups. Similarly, in [124], authors discuss how data can be collected in a Steemit blockchain-driven SM system using APIs and how blockchain-structured data can be analyzed using large-scale graph libraries. In another research study, bot accounts that post automatically to get rewards from Steemit, discouraging human rewards, were detected by extracting a set of custom features without limiting the number of characteristics by using clustering distance among blog entries or feedback [125]. This study shows that features of the Clustering Distance among Frequent words and articles (CDFA) result in better accuracy, precision, recall, etc., in almost all the machine learning techniques considered. Similarly, in [126], using user activity as a feature and other public features in the use case of the Steemit platform, the social behaviors of users are analyzed to distinguish bots from human users by using bot detection techniques. This study has utilized 29 million blocks from the Steem blockchain and analyzed the transfer, follow, post, and comment operations to better distinguish bots from humans. In cryptocurrency social media forums, strategies like sentiment analysis and topic modeling are utilized to diagnose trends and themes, and blockchain technology is utilized for data authentication and verification, which has been very useful in visualizing cryptocurrency market phase shifts [127]. For instance, the sentiment analysis using machine learning algorithms predicts that Bitcoin sentiment has changed to negative in 2021. In another scheme, machine learning and NLP are jointly utilized to identify events and get insights on real-time events in social media frameworks through text analysis, while blockchain is engaged to verify the trustworthiness of the detected events, removing the single authority in conventional systems [128]. The results show that this scheme has a high success rate of false events under a higher number of attackers, the success rate of events decreases with the threshold value, and the F1-score improves with data enrichment. Moreover, some have used community detection algorithms on the Steemit platform to understand the interactions between users on a community basis, where modeling has been done by community detection algorithms on graphs and evaluated against community structure measures [129]. The evaluations reveal that they have been able to detect a significant amount of block producers in the monetary graph, and communities can be quite large. Temporal characteristics of the Steemit blockchain-driven social media scheme have been investigated by analyzing link creation dynamics and the reward-claiming process, where blockchain data is developed as a time-directed network to analyze inter-event time distribution and bursty nature [130]. The analysis reveals that processes depict bursty traits such as those observed in human dynamics; however, 2 aspects regarding behavior and bursty nature time scale show some deviations.

5.2.8. Proper incentivization

Sociala is a blockchain-based social media scheme for writers that is incentivized with minimized nefarious node choice by using a modified delegated proof of stake consensus, which avoids centralization pitfalls and rewards the writers for their novel contributions [131]. Sociala has shown high randomness, diversity, and stability. Alternatively, in work [132], a user-managed data wallet is proposed by implementing it using blockchain-driven smart contracts to mutually

transfer data among multiple parties with the consent of data producers, providing a well-deserved incentive for them. In this study [132], a data exchange scenario using the DXT data exchange token is discussed using a paper-driven feasibility evaluation. LBRY is an online decentralized marketplace driven by blockchain, allowing users to publish and download content by paying appropriate payments, while blockchain is utilized to maintain digital currency and synchronize namespaces and metadata's index [133]. Evaluation in LBRY shows that Claimtrie memory size increases with block height, and throughput varies with time. Furthermore, it creates a good incentive for better distribution. Similarly, in [134], a decentralized platform for content sharing in a fault-tolerant approach involves participating blockchain peers to engage it to administrate content listings and as a transaction processor to fairly pay money for the content generators leveraging smart contracts. This decentralized content-sharing platform has shown good scalability due to lower overhead.

5.2.9. User migration

A user transition model in blockchain-driven cyber-SM, as a result of a fork event, is realized, representing evolutions of fork-driven migrations, growth characteristics, and user behaviors like whether to remain in the original blockchain or not, etc. [24]. In this study, the Steem-Hive fork event is considered, and results show the importance of taking into account socio-economic data in user migration. Due to the hard forks in blockchain-driven SM networks, research has found that it is probable for marginal groups to leave and densely connected groups are highly probable to retain, while user transitions diversely impact the social network socially and financially [135]. Specifically, they have found correlations in social and monetary layers using entropy and density values by constructing a graph from the Steem blockchain created in 2016 up to a fork event that occurred later and by obtaining socio-economic operations.

6. Review Critical Analysis

6.1. Dissection of individual schemes

Table 2 communicates the intensive dissection of blockchain-based social media schemes about social media traits (extra capabilities, performance), blockchain traits (fabric, consensus, and smart contracts), and disclosed time.

Table 2. Dissection of blockchain-based social media schemes.

Abstraction	Project	Blockchain fabric	Blockchain consensus	Smart contracts	Extra capabilities	Performance	Time
Social media platforms (G1)	Steemit [102]	Conventional	DPoS	No	Voting, cryptocurrency rewards	Level of decentralization is lower than ideal	2019
	Decentralized social network [103]	Conventional	PoW	Yes	IPFS, DApp	The system has been demonstrated as a test use case	2018
	Hive [104]	Conventional	DPoS	Yes	Voting, hive user base, comments, posts, token transactions	Supports all traditional social network functionalities	2022
	ARTICONF [19]	Conventional	BFT	Yes	Graph anonymization, open and agile social media	Several pilot use cases presented	2019
	UShare [105]	Conventional	PoS	Yes	User control, claim, ownership control, hash table, Turing complete relationship	No performance analysis presented	2017
	BCE social media [106]	Generic	Generic	Yes	Incentive mechanism, organizational structure	No performance evaluation	2023

Table 2 continued.

Table 2 (continued). Dissection of blockchain-based social media schemes.

Abstraction	Project	Blockchain fabric	Blockchain consensus	Smart contracts	Extra capabilities	Performance	Time
Social DApps (G2)	Match privacy settings [20]	Conventional	PoW	Yes	Graph based model, DApp	DApp has been implemented and tested	2021
Copyright protection (G3)	Social media DRM [21]	Conventional	Generic	Yes	IPFS, manage copyright, Hashing, Rest API	No performance evaluation	2021
	Video streaming [107]	Conventional	PoW	Yes	IPFS, cryptography, copyright protection	Feasible implementation	2020
Harassment prevention (G4)	Cyberbullying prevention [108]	Conventional	PoS	Yes	Machine learning, natural language processing	Higher accuracy with most ML when deployed with blockchain	2021
	Cyberbullying with recommendations [109]	Conventional	PoW/PoS	Yes	Federated learning, formal modeling, LSTM	Good detection performance metrics	2024
Ensuring privacy and security (G5)	DP-BFL [110]	Generic	Generic	No	Federated learning, social media 3.0	High utility, enhanced privacy, and elevated efficiency	2021
	Access control management [111]	Conventional	PoW/PoS	Yes	Cryptography, access control	61,648 gases required to evaluate ACL rules	2020
	OSN information propagation [112]	Conventional	Generic	Yes	Credibility and trust driven	83% accuracy	2021
	BPP [113].	Conventional	PoW/PoS	Yes	Keyword search algorithm, public key cryptography	Higher security and efficacy demonstrated	2021
	BCDSMM-CNYAC [114]	Conventional	YAC	Yes	CryptoNight mining algorithm	Prevent falsified data attack	2022
	Social networking [115]	Conventional	Generic	No	Archive, query/algorithm tracker	Use case discussed for a robots and IoT device framework	2019
	Data protection in OSNs [116]	Generic	Generic	No	Consent management model	Discuss GDPR compliance of the proposed method	2020
Fake/vicious news prevention (G6)	Notarization [22]	Generic	Generic	No	Authentic archiving	Showed an instant messaging scenario	2019
	Reducing fake news [117]	Generic	Generic	No	Keyed watermarking, maintain accountability	Feasible framework for curtailment of fake news	2021
	FakeChain [118]	Conventional	PoS	Yes	Truth finder algorithm	Proof of concept shows efficient fake news detection	2019
	SM news verification system [119]	Conventional	Custom	Yes	IPFS, MetaMask, Web3.js	Limit user behavior in spreading fake news	2021
	Authentic facts [120].	Generic	Generic	No	NFT	Satisfactory performance and efficiency	2021
	Internet of fake media things [121]	Conventional	PoAuthority	Yes	Gamification, weighted ranking algorithm	Proof of concept providing a mechanism of trust for news is presented	2020
	Digital identity verification [122]	Generic	Generic	No	Hash identity, social accounts	No performance analysis exists	2020
	Fake media detection [123]	Conventional	PBFT, RAFT	Yes	Reinforcement learning, natural language processing	Performance of machine learning technique and blockchain are evaluated	2021

Table 2 continued.

Table 2 (continued). Dissection of blockchain-based social media schemes.

Abstraction	Project	Blockchain fabric	Blockchain consensus	Smart contracts	Extra capabilities	Performance	Time
Data/User behavior/Event processing and analysis (G7)	Steemops [23]	Conventional	DPoS	No	Dataset schema	Organizes 900 M operations of Steemit into 3 groups.	2021
	Social media decentralization [124]	Conventional	DPoS	No	APIs, graph libraries	No performance evaluation	2021
	Posting bot detection [125]	Conventional	PoB	No	Clustering distance, custom features, machine learning	Better F1 scores and classification performance	2021
	User and bot behavior analysis [126]	Conventional	DPoS	No	User activity features, bot detection techniques	Bots are more active than humans and can be detected by public features	2020
	BB E-analysis [127]	Conventional	PoW/PoS	Yes	Emotion analysis, subject modeling, authentication	Analysis can be employed to predict cryptocurrency price swings	2023
	BB event detection [128]	Conventional	PoAuthority	Yes	Machine learning, natural language processing	High success rate of false events under higher number of attackers	2021
	Interaction communities [129]	Conventional	DPoS	No	Community detection algorithms, community message structures	Communities are usually large and exist large number of block producers	2021
	Social and rewarding dynamics [130]	Conventional	DPoS	No	link creation dynamics and reward claiming process	Processes depict bursty traits typical of human dynamics	2021
Proper incentivization (G8)	Sociala [131]	Conventional	mDPoS	No	Incentivization, minimized nefarious node choosing	High randomness, diversity, and stability	2023
	Data exchange wallet [132]	Conventional	PoW	Yes	User control, fair data exchange	An example of simple exchange of data for DXT is shown	2018
	LBRY [133]	Conventional	PoW	No	Digital currency, namespace and metadata index	Evaluated throughput and Claimtrie memory size	2020
	Decentralized marketplace [134]	Conventional	BFT	Yes	Content sharing, content listing, transaction processing	Result in lower overhead	2020
User migration (G9)	Fork-driven user migration [24]	Conventional	DPoS	No	Fork-driven migrations, user behavior	Consider a case-study on Steem-Hive fork event	2022
	Groups in user migration [135]	Conventional	DPoS	No	User migration analysis	Marginal groups leave and densely connected groups are more probable to stay	2022

6.2. Overall critical analysis

Figure 6 pictorializes the tendencies of blockchain-based social media schemes about social media traits, blockchain traits, and disclosed time.

As pictorialized in Figure 6a, G6 and G7 are the highest fraction (20%) of BC-based social media abstraction, after G5 (17.5%), G1 (15%), G8 (10%), G3 (5%), G4 (5%), G9 (5%), and G2 (2.5%). After that, in BC-based social media, 82.5% of works make use of a conventional blockchain, while the leftover 17.5% make use of a general fabric, as pictorialized in Figure 6b. Additionally, as pictorialized in Figure 6c, a large quantity of works (25%) has been put forwarded to make use of non-specific consensus, coming after DPoS (22.5%), PoW (12.5%), PoW/PoS (10%), and the like. At the end, when scanning the oscillation of works

linked with BC-based social media, as pictorialized in Figure 6d, it is straightforward that the abstraction has been instigated by 2018, intensified until 2021, and constricted after that.

Now, let us critically analyze the strengths and weaknesses of the reviewed literature in terms of their performance parameters/features, as depicted in Table 3.

Table 3. Strengths and weaknesses of blockchain-based social media schemes.

Performance metric/feature	Strength	Weakness/Limitation
Decentralization	High [109, 124, 131]	Low [102]
Support for traditional social network functions	High [104]	
Anonymous trusted participation	High [19]	
Privacy setting management	High [20]	
Node coordination		Difficult [107]
Time consumption and latency		High [107]
Accuracy	High [108, 112], >90% [109], satisfactory [120, 24]	
Computational complexity	Low [114]	High [109]
Privacy	High [110]	
Efficiency	High [110, 113]	
Gas cost	Low [111]	
Scalability	High [111, 117, 134]	
Security and transparency	High [113, 114, 128, 132]	Low attack resistance [131]
Malicious software bot detection	Good [125, 126]	Difficult [115]
GDPR compliant consent management	High [116]	
Limit fake news spreading	High [117, 119, 121, 123]	
Validator credentials		Limited [119]
Authentication	Good [127]	
Success rate	High [128]	
Bursty traits	High [130]	
Throughput	Good [133]	

As evident from Table 3, we can identify support for traditional social network functions, anonymous trusted participation, privacy setting management, satisfactory accuracy, high privacy, efficiency, low gas cost, high GDPR-compliant consent management, fake news limiting, good authentication, high success and bursty traits, and good throughput as strengths of the reviewed frameworks. Clearly, difficulties in node coordination, high time consumption and latency, and limited validator credentials can be identified as limitations of blockchain-based social media frameworks. However, there exists some contradictory evidence of performance for some features. For instance, security of most frameworks has been reported high; however, the attack resistance is lower in [131] due to the utilization of modified DPoS. Similarly, decentralization is high in most of the frameworks, except for the study that uses DPoS [102]. Moreover, there is contradictory evidence on computational complexity, as the study [114] reports a lower computational complexity due to the use of YAC consensus with a mining algorithm, whereas the study [109] demands a higher computational complexity due to interconnection with cutting-edge technologies. Furthermore, scalability of some [111, 117, 134] blockchain-based social media frameworks has been reported as high due to the use of efficient consensus techniques such as RAFT; due to low payload-consuming mechanisms, etc., even though it is generally understood that blockchain solutions are less scalable. Not only that, one study [131] suggests that it has a lower attack resistance due to the utilization of modified DPoS, although many solutions report that they are secure and transparent.

Most studies remain in prototype or theoretical stages except for case studies: Steemit [102], SoChainDB [104], ARTICONF [19], robots [115], Steemit bot detection [125], and fork-driven user migration [24]. Thus, one of the main gaps of the reviewed frameworks is that most of them are validated in simulation environments and list out practical real-world implementations as future work. Thus, most of them lack empirical validation; thus, it is less known about the practical implementation issues. Furthermore, ethical concerns and biases in detection models are under-explored, and decentralization risks are not assessed, and contradictory performance needs further investigation. Moreover, the present studies on blockchain-based social media lack security analysis under modern computer attacks like quantum computing attacks.

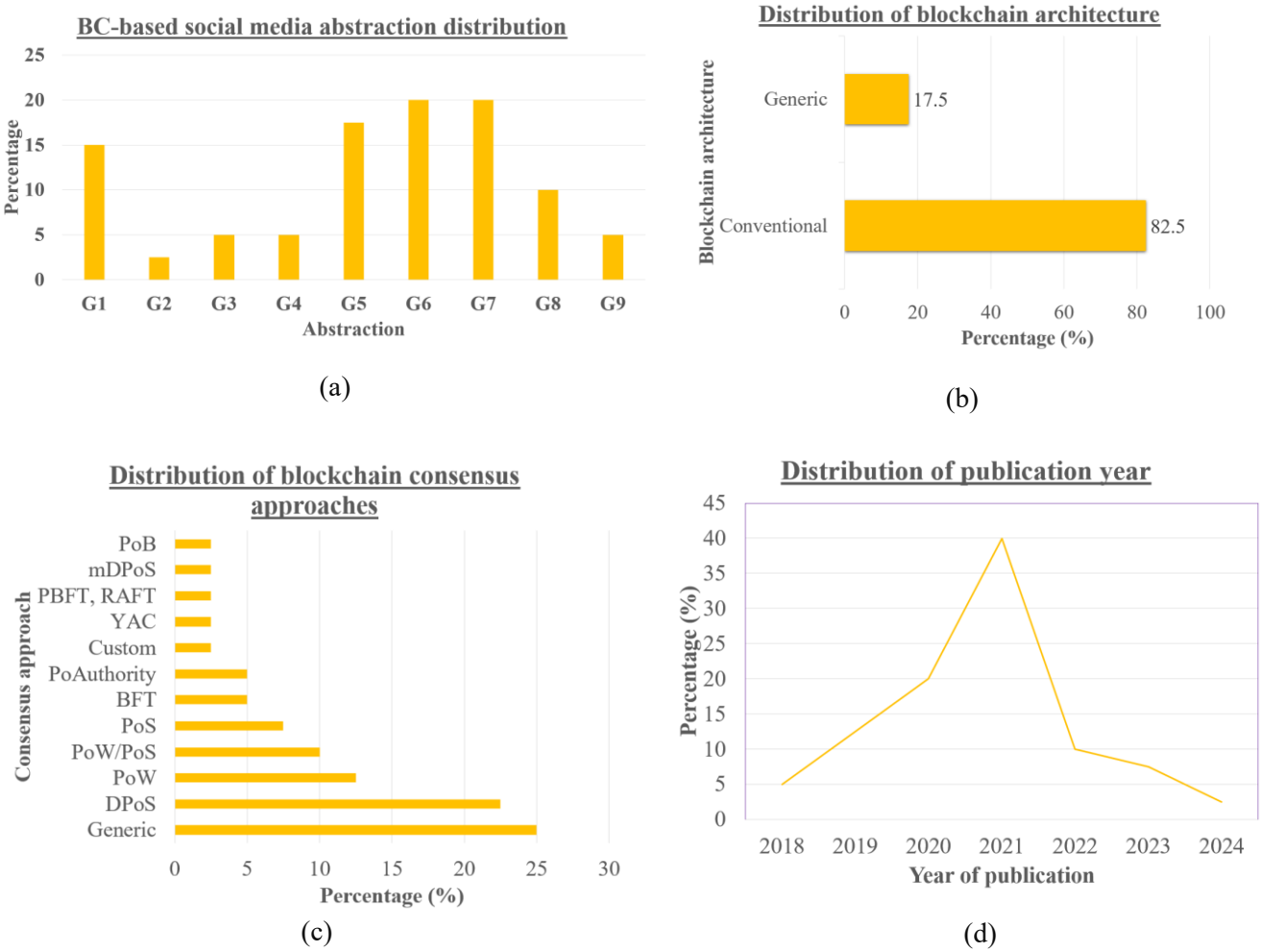


Figure 6. Overall dissection (a)BC-based social media abstraction (b) BC fabric (c) BC consensus (d) Transmission time

7. Discussion

7.1. Opportunities

7.1.1. Improve social media analytics

According to a study conducted on blockchain-based social media's impact on analytics, it has been found that this platform indeed improves areas like demand forecasting, recommendations, promotions, advertisements, etc. [136]. Specifically, blockchain can be utilized for authentication and verification of users in the process of a particular analysis task, making the analysis more trustworthy and effective. Analysis techniques may include sentiment analysis, feature extraction, detection algorithms, machine learning, etc. For example, if emotion analysis and subject modeling are leveraged to understand trends in a social network, blockchain can aid in data authentication and verification, making the analysis more legitimate and effective than traditional analysis techniques utilized alone.

7.1.2. Facilitate fake news prevention

Blockchains facilitate authentic archiving of data with integrity protection thanks to their immutable features. These features of blockchain, along with secondary protection measures like keyed watermarking, fingerprinting, etc., can be leveraged to prevent the spreading of fake news. Moreover, blockchain consensus algorithms can be utilized to come to an agreement regarding the validity of news, punish fake news creators, and alert readers. Moreover, smart contracts can be utilized to provide credibility indicators for news spread

on social media, allowing users to identify the legitimacy of news easily. Not only that, blockchain can act as an effective way to prevent the creation of fake accounts by storing the digital identities of users, reducing the chance of generating fake news. Finally, blockchain can also provide authenticity in detecting fake news/posts using another technique like machine learning or natural language processing.

7.1.3. Enhanced user privacy

Federated learning has been put forward as a privacy safeguarding method that can be successfully amalgamated with blockchain mining to exchange data in social networks in a privacy-preserving manner, protecting the user's sensitive private data from being shared. Access control can be implemented based on blockchain, where the content creators can define access control policies controlling access to the content shared on social media. Moreover, these systems can adapt additional cryptographic techniques like public key cryptography or other encryption techniques to further reinforce the privacy of data on top of the pseudo-anonymous privacy provided by blockchain. Most importantly, blockchains protect data ownership, allowing users to have control over their personal data by storing it in a decentralized approach using blockchain without risking privacy leakages of data controlled by centralized authorities in traditional social media networks.

7.1.4. Enable incentivization and copyright protection

On conventional social media platforms, there exist only a limited number of measures for protecting the copyright of the content creators. Thus, copyright infringement can occur easily in those networks when unauthorized users redistribute copyrighted work or recreate work by plagiarizing content and sharing it on social media without permission. In blockchain-based social media, copyright infringement can be minimized by using distributed file systems and the power of smart contracts to detect copyright issues and automatically send payments to the content creators, thus not only preventing copyright infringement, but also enabling fair incentivization. These smart contracts can further implement access control and get the support of encryption for further protection of copyrighted content.

7.1.5. Improves the trustworthiness of SM platform

In the process of analyzing users and events in SM, blockchain can be utilized to improve the trustworthiness of those users and events by implementing verification measures and removing the requirement for centralized authorities, who can be untrusted in some scenarios. Moreover, blockchain-driven social platforms may disseminate data by coming into collective agreement by using the nodes trust scores calculated based on their reputation, behavior, information held, etc., making the overall data transmission more trustworthy. This kind of credibility score can also be used to further penalize malicious users and reward good users, and it may also be utilized to reduce vicious media from being circulated in the social media framework. In cases where high trust is required, these platforms may use a permissioned blockchain, like in the case of ARTICONF, while detecting interest communities.

7.2. Discomforts

7.2.1. Malicious bots

A study done on the Steemit blockchain-driven social media platform reveals that 16% of cryptocurrency shares are sent to suspected bots [102]. Even though bots' detection techniques can be utilized to detect them, it can be challenging to extract features and distinguish them from human users due to the high variety of data generated in social media networks. Bots can pose a threat to social media networks by manipulating algorithms to artificially inflate engagement metrics and scrape personal data from users to target advertising. They can further create fake accounts and target individuals to harass them by sending spam messages. Even though blockchains can be used to prevent the creation of fake accounts in SM systems, it can be challenging to reduce harassment messages sent by bots, as there need to have additional security measures to counter attack them, like data analytics and natural language processing.

7.2.2. Difficulties in censorship

It is challenging to implement both the right to free speech and censorship simultaneously on social media, as they can bring interfering conditions among each other. Due to the decentralization of blockchain, it is difficult for a single entity to do censorship and remove unwanted/unsuitable content from the platform [137]. Moreover, the immutability of blockchain can bring in difficulties in removing contents once they are approved and published in the SM framework. In blockchain-driven SM platforms, users' ownership of content can act as a barrier to censorship, since users have control over their own content while a third party, like an auditing agent, does not have control over them, in contrast to traditional social media.

7.2.3. Large volume and velocity of social media content

It has been found that SM networks generate large volumes of data at very high speeds [138]. Thus, this large bulk of data produced within a short amount of time demands high throughput in blockchain-based social media systems. However, it is well known that traditional linear blockchain strives to satisfy throughput requirements when presented with a large bulk of data at high speed, as consensus techniques like proof-of-work consume resources and take time for completion. Therefore, BSM systems can strive to satisfy the throughput requirements, which may result in a degraded quality of service for end users, especially in real-time scenarios such as video streaming, post responses, etc.

7.2.4. Difficulties in data collection and storage

Storage of social media data directly on blockchain can definitely introduce scalability issues since new data is generated each second with high velocity and variety, and traditional blockchain systems are well known for scalability issues in terms of data storage [139]. Moreover, blockchain systems cost fees in terms of gas fees to store content in them, thus incurring high costs for storing large amounts of data in them. Moreover, social media data has a high degree of variety, meaning that it can occur in text, audio, video, documents, etc., making it difficult to store it in a single blockchain with a specific block structure.

7.2.5. Regulatory uncertainties

Blockchain-driven social media is still a pre-matured area of investigation that lacks regulations regarding the use of cryptocurrencies and blockchain technology itself. Due to a lack of clear regulations, it is difficult to impose legal obligations regarding user data privacy and content moderation. In that case, user privacy and content rights can be violated, and they can be harassed without proper legal action against those activities. As blockchains typically operate globally, it can introduce issues as regulations may vary from one geographical location to another [140]. Moreover, ambiguous regulations can prevent entrepreneurs and investors from engaging in social media projects, which can discourage innovative ideas from entering social media.

7.3. Practical applications

In [102], an empirical analysis of Steemit is discussed that evaluates the DPoS consensus to evaluate millions of social media operations performed by users in the period of 2016 to 2018. This study shows that decentralization introduced by blockchain has resulted in detection of bots more difficult. SoChainDB [104] is a decentralized blockchain-based solution that implements crawling and publishing data in the Hive platform and has been demonstrated for practical applications like NFT markets, games, etc. It shows a method to integrate blockchain-based SM platforms with traditional SM with minimum effort. In ARTICONF [19], an industrial pilot use case is used to demonstrate its effectiveness in creating an agile social media system leveraging permissioned blockchain and to detect communities utilizing graph anonymization. Moreover, in [115], a blockchain-driven SM framework that aims to partially or fully detach user information from content has been demonstrated for an application scenario of a collocated environment of robots. It shows blockchain limitations and malicious bots as challenges for implementing the framework practically. In a Steemit bot detection [125] framework, bot detection has been feasible for the cases of Facebook and Twitter using a clustering technique. Alternatively, fork-driven user

migration [24] has been feasible in the Steem-Hive fork event use case to consider the value of social and economic data and to study the trends in fork-driven user migrations. This study suggests that blockchain fork events can trigger user migration in a practical scenario, while socio-economic data can be used to analyze the trends even though further investigation on this is required.

8. Conclusion

In this exploration, we explored social media categories like social networks and content communities, the classification of SM considering media fullness and self-portrayal, and concepts of ethics, privacy, and security in social media**.** After a conspectus of the blockchain scheme, we explored blockchain-based social media schemes. Established on this exploration, we grasped blockchain-based social media abstraction under 9 duties**:** providing social media platforms (G1), social DApps (G2), copyright protection (G3), harassment prevention (G4), ensuring privacy and security (G5), fake/vicious news prevention (G6), data/user behavior/event processing and analysis (G7), proper incentivization (G8), and user migration (G9). Additionally, we intensively dissected the explored documents under the 9 duties of abstraction, SM-, and blockchain-linked traits. Then, we critically analyzed the literature by identifying strengths and weaknesses of the studies and identified gaps. According to the review analysis, it is clear that fake/vicious news prevention (G6) and data/user behavior/event processing and analysis (G7) are the most frequently utilized blockchain-based social media abstractions, while conventional blockchain with DPoS consensus is the most preferable choice in terms of blockchain. Finally, we revealed the opportunities and discomforts of the abstraction of blockchain-based SM and proposed future directions in the following section to overcome the discomforts, emphasizing practical applications. This work contributes a useful review study to the existing literature that critically analyzes the blockchain-based social media in the broad scope without being restricted to a specific SM platform or a particular use case, unlike other studies.

8.1. Study significance

This scrutiny ameliorates the active literature by provisioning efficacious knowledge affiliated with blockchain-based social media**.** The study highlights that most blockchain-based social media frameworks remain at the prototype or theoretical level. This can show strategies for the examiners to conclude the active advancements and distinctness of blockchain-based social media to cultivate in imminent research focusing on real-world implementation and empirical validation. We also reported centralization risks that can motivate policy makers to design fair governance structures. By understanding challenges in user incentivization mechanisms, effective engagement strategies like tokenized rewards can be developed by the researchers.

8.2. Study limitations

Since narrative synthesis is based on descriptive summaries, instead of statistical meta-analysis, the interpretations can be subjective. Moreover, we didn't evaluate the strength of the studies, as we treated them equally; the assessment of the frameworks may be harder to maintain consistency. Moreover, some categories of the qualitative assessments have very low prevalence percentages, implying that the significance of those classes' qualitative assessments is insignificant.

8.3. Solutions to discomforts

Established on the discomforts understood, coming solutions can be delivered to resist them.

- As demonstrated in previous works, bot detection techniques can be utilized to distinguish malicious bots from human users. Moreover, BSM platforms should extract features from data that resemble bot behavior in order to detect them successfully.
- To overcome censorship difficulties, BSM can implement mechanisms for users to vote on content moderation, subsequently contributing to enforcing them in a decentralized manner. Moreover, content moderation algorithms like machine learning and NLP can be incorporated into BSM systems to flag harmful items residing on social media. Furthermore, rewarding systems

can be introduced to provide rewards like tokens that encourage users to act responsibly.

- The large volume and velocity of social media content cannot be prevented. Thus, blockchain systems should adapt to these circumstances. For that, a mesh blockchain can be utilized, which is known for its parallel processing capability and high throughput compared to the traditional blockchain. Moreover, energy- and time-efficient consensus approaches like proof-of-authority/stake can be replaced with traditional time-consuming consensus approaches like proof-of-work to improve transaction efficiency.
- To overcome the difficulty of storing social media data directly on the blockchain due to its storage limitations, one can use off-chain storage for storing a large bulk of social media data while only storing references to them, such as their cryptographic hash, on the blockchain. IPFS is the most abundantly used decentralized off-chain data storage associated with blockchain to store social media data.
- To tackle regulatory uncertainties, blockchain-based social media platforms must have globally accepted laws and regulations that can be utilized to take action against individuals or organizations that violate them. Such social media platforms should also have clearly defined policies regarding the use of cryptocurrencies utilized in blockchains for transactions to maintain the characteristics of integrity and authenticity provided by the blockchain.

8.4. Future directions

As oncoming tracks in BSM, authorities may work together to strengthen the regulations related to BSM in order to provide a globally accepted framework to act in case of misconduct. Moreover, academicians may conduct research to find effective methods to reduce performance bottlenecks present in current blockchains so that they can adhere to big data situations that arise in SM. As SM platforms also evolve over time, blockchain solutions should also be changed accordingly to cater to new requirements arising due to change. Moreover, future work should concentrate on large-scale pilot studies of blockchain-based social media platforms in real-world settings and further evaluate the economic feasibility of them, as this study identified a scarcity in empirical validations. Furthermore, robust mechanisms for decentralization of content moderation for fair regulation without bias should be more studied, as present studies do not address them. Since blockchain-based social media lack attack analysis and robust security measures under quantum computer attacks, future work should analyze the attack scenarios and provide robust solutions to resist the attacks. Not only that, in the future, explainable AI models may be required to reduce bias and inaccuracies in tasks like fake news detection, as present solutions lack model accountability. Finally, user-friendly interfaces and interoperable solutions are required in practical implementations to interact with traditional platforms, as currently, most of the studies remain theoretical. Thus, future case studies should evaluate the empirical performance in an explainable manner to realize the reasons for performance tradeoffs to better implement blockchain-based SM platforms in a practical scenario.

Conflict of interest

Authors declare no conflict of interest.

Data availability statement

No data or additional materials were utilized for the research described in the article.

Acknowledgment

The authors would like to acknowledge the help of reviewers who provided valuable comments to improve the quality of the article.

Declaration of generative AI-assisted tools

No AI tools were used for this research. All papers were reviewed manually, text was completely written, and all images were manually drawn without any AI involvement by the authors.

References

[1] J. Penni, "The future of online social networks (OSN): A measurement analysis using social media tools and application," *Telemat. Inform.*, vol. 34, no. 5, pp. 498–517, 2017.

[2] C. G. Berdanier, C. Whitehair, A. Kirn, and D. Satterfield, "Analysis of social media forums to elicit narratives of graduate engineering student attrition," *J. Eng. Educ.*, vol. 109, no. 1, pp. 125–147, 2020.

[3] R. Brewer and A. M. Piper, ""Tell It Like It Really Is": A case of online content creation and sharing among older adult bloggers," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2016, pp. 5529–5542.

[4] K. Oseni, K. Dingley, and P. Hart, "Instant messaging and social networks: The advantages in online research methodology," *Int. J. Inf. Educ. Technol.*, vol. 8, no. 1, pp. 56–62, 2018.

[5] S. Brenner, S. Aksin Sivrikaya, and J. Schwalbach, "Who is on LinkedIn? Self-selection into professional online networks," *Appl. Econ.*, vol. 52, no. 1, pp. 52–67, 2020.

[6] B. S. Solomon, D. Duce, and R. Harrison, "Methodologies for using social media collaborative work systems," in *Proc. 1st Int. Workshop Requirements Eng. Soc. Comput.*, 2011, pp. 6–9.

[7] P. R. Messinger *et al.*, "Virtual worlds—past, present, and future: New directions in social computing," *Decis. Support Syst.*, vol. 47, no. 3, pp. 204–228, 2009.

[8] T. T. Ochoa, "Who owns an avatar-copyright, creativity, and virtual worlds," *Vand. J. Ent. & Tech. L.*, vol. 14, p. 959, 2011.

[9] S. Agrawal and A. Sureka, "Copyright infringement detection of music videos on YouTube by mining video and uploader meta-data," in *Big Data Analytics: 2nd Int. Conf. BDA 2013*, 2013, pp. 48–67.

[10] H. Allcott, M. Gentzkow, and C. Yu, "Trends in the diffusion of misinformation on social media," *Res. Politics*, vol. 6, no. 2, p. 2053168019848554, 2019.

[11] J. A. Pater, M. K. Kim, E. D. Mynatt, and C. Fiesler, "Characterizations of online harassment: Comparing policies across social media platforms," in *Proc. ACM Int. Conf. Support. Group Work*, 2016, pp. 369–374.

[12] M. Cinelli, G. D. F. Morales, A. Galeazzi, W. Quattrociocchi, and M. Starnini, "The echo chamber effect on social media," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 118, no. 9, p. e2023301118, 2021.

[13] M. Aljohani, A. Nisbet, and K. Blincoe, "A survey of social media users' privacy settings & information disclosure," in *Proc. 14th Aust. Inf. Secur. Manag. Conf.*, 2016, pp. 67–75.

[14] P. A. D. S. N. Wijesekara, "Ethical knowledge sharing leveraging blockchain: An overview," *Sci. Eng. Technol.*, vol. 4, no. 1, pp. 112–136, 2024.

[15] J. Liu, H. Zhang, and L. Zhen, "Blockchain technology in maritime supply chains: Applications, architecture, and challenges," *Int. J. Prod. Res.*, vol. 61, no. 11, pp. 3547–3563, 2023.

[16] P. A. D. S. N. Wijesekara, "A literature review on access control in networking employing blockchain," *Indones. J. Comput. Sci.*, vol. 13, no. 1, pp. 734–768, 2024.

[17] L. Li, D. Huang, and C. Zhang, "An efficient DAG blockchain architecture for IoT," *IEEE Internet Things J.*, vol. 10, no. 2, pp. 1286–1296, 2022.

[18] A. Roushan, A. Das, A. Dutta, and U. K. Bera, "A multi-objective supply chain model for disaster relief optimization using neutrosophic programming and blockchain-based smart contracts," *Supply Chain Analyt.*, p. 100107, 2025.

[19] R. Prodan *et al.*, "ARTICONF: Towards a smart social media ecosystem in a blockchain federated environment," in *Proc. Eur. Conf. Parallel Process.*, 2019, pp. 417–428.

[20] G. Lax, A. Russo, and L. S. Fascì, "A blockchain-based approach for matching desired and real privacy settings of social network users," *Inf. Sci.*, vol. 557, pp. 220–235, 2021.

[21] M. Kripa, A. N. Mahesh, R. Ramaguru, and P. P. Amritha, "Blockchain framework for social media DRM based on secret sharing," in *Proc. ICTIS 2020: Inf. Commun. Technol. Intell. Syst.*, vol. 1, pp. 451–458, 2021.

[22] G. Song, S. Kim, H. Hwang, and K. Lee, "Blockchain-based notarization for social media," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, 2019, pp. 1–2.

[23] C. Li, B. Palanisamy, R. Xu, J. Xu, and J. Wang, "Steemops: Extracting and analyzing key operations in Steemit blockchain-based social media platform," in *Proc. 11th ACM Conf. Data Appl. Secur. Privacy*, 2021, pp. 113–118.

[24] C. T. Ba *et al.*, "Fork-based user migration in blockchain online social media," in *Proc. 14th ACM Web Sci. Conf.*, 2022, pp. 174–184.

[25] M. A. Hisseine, D. Chen, and X. Yang, "The application of blockchain in social media: A systematic literature review," *Appl. Sci.*, vol. 12, no. 13, p. 6567, 2022.

[26] B. Guidi, "When blockchain meets online social networks," *Pervasive Mobile Comput.*, vol. 62, p. 101131, 2020.

[27] P. A. D. S. N. Wijesekara, "A study in University of Ruhuna for investigating prevalence, risk factors, and remedies for psychiatric illnesses among students," *Sci. Rep.*, vol. 12, no. 1, p. 12763, 2022.

[28] P. A. D. S. N. Wijesekara and Y. K. Wang, "A mathematical epidemiological model (SEQIJRDS) to recommend public health interventions related to COVID-19 in Sri Lanka," *COVID*, vol. 2, no. 6, pp. 793–826, 2022.

[29] X. Lei *et al.*, "The relationship between social media use and psychosocial outcomes in older adults: A systematic review," *Int. Psychogeriatr.*, pp. 1–33, 2024.

[30] A. U. Zafar *et al.*, "The impact of social media celebrities' posts and contextual interactions on impulse buying in social commerce," *Comput. Hum. Behav.*, vol. 115, p. 106178, 2021.

[31] P. A. D. S. N. Wijesekara *et al.*, "Data gathering optimization in hybrid software-defined vehicular networks," in *Proc. 20th Acad. Sessions*, 2023, p. 59.

[32] L. K. Hawkins, C. Farrow, and J. M. Thomas, "Do perceived norms of social media users' eating habits and preferences predict our own food consumption and BMI?," *Appetite*, vol. 149, p. 104611, 2020.

[33] P. A. D. S. N. Wijesekara and S. Gunawardena, "A comprehensive survey on knowledge-defined networking," *Telecom*, vol. 4, no. 3, pp. 477–596, 2023.

[34] M. Mazzolini and S. Maddison, "Sage, guide or ghost? The effect of instructor intervention on student participation in online discussion forums," *Comput. Educ.*, vol. 40, no. 3, pp. 237–253, 2003.

[35] V. Gritsenko, "Interaction on online forums and group communication: A case study of an IT support community," *Procedia-Soc. Behav. Sci.*, vol. 236, pp. 14–24, 2016.

[36] D. Azariah, "Whose blog is it anyway? Seeking the author in the formal features of travel blogs," in *Proc. 11th Humanit. Grad. Res. Conf.*, 2010, pp. 1–18.

[37] P. A. D. S. N. Wijesekara, W. M. A. K. Sangeeth, H. S. C. Perera, and N. D. Jayasundere, "Underwater acoustic digital communication channel for an UROV," in *Proc. 5th Annu. Res. Symp. (ARS2018)*, 2018, p. E17.

[38] N. Chatterjee, S. Chakraborty, A. Decosta, and A. Nath, "Real-time communication application based on Android using Google Firebase," *Int. J. Adv. Res. Comput. Sci. Manag. Stud.*, vol. 6, no. 4, pp. 74–79, 2018.

[39] A. Koçak and Ö. Y. Vergiveren, "Group-based communication: Contents and practices of WhatsApp group use by generations and genders," *Online J. Commun. Media Technol.*, vol. 9, no. 4, p. e201922, 2019.

[40] R. Malekhosseini, M. Hosseinzadeh, and K. Navi, "Evaluation of users' privacy concerns by checking of their WhatsApp status," *Softw. Pract. Exp.*, vol. 48, no. 5, pp. 1143–1164, 2018.

[41] M. Raj, N. J. Fast, and O. Fisher, "Identity and professional networking," *Pers. Soc. Psychol. Bull.*, vol. 43, no. 6, pp. 772–784, 2017.

[42] J. Pokorný, "Profiles in professional social networks," in *Proc. 2012 Int. Conf. Inf. Syst. Dev.*, 2013, pp. 387–399.

[43] H. Chen *et al.*, "Professional network matters: Connections empower person-job fit," in *Proc. 17th ACM Int. Conf. Web Search Data Min.*, 2024, pp. 96–105.

[44] S. E. Snyder, "Teachers' perceptions of digital citizenship development in middle school students using social media and global collaborative projects," Ph.D. dissertation, Walden Univ., 2016.

[45] A. Kaplan and M. Haenlein, "Collaborative projects (social media application): About Wikipedia, the free encyclopedia," *Bus. Horiz.*, vol. 57, no. 5, pp. 617–626, 2014.

[46] A. J. Kenny, J. D. Wolt, and H. S. Hurd, "Collaborative Wikipedia projects in the virtual classroom," *Nat. Sci. Educ.*, vol. 42, no. 1, pp. 85–90, 2013.

[47] I. A. Mir and K. Ur Rehman, "Factors affecting consumer attitudes and intentions toward user-generated product content on YouTube," *Manag. Mark.*, vol. 8, no. 4, p. 637, 2013.

[48] A. C. Munaro *et al.*, "To engage or not engage? The features of video content on YouTube affecting digital consumer engagement," *J. Consum. Behav.*, vol. 20, no. 5, pp. 1336–1352, 2021.

[49] P. A. D. S. N. Wijesekara *et al.*, "An optimization framework for data collection in software-defined vehicular networks," *Sensors*, vol. 23, no. 3, p. 1600, 2023.

[50] R. Schroeder, "Defining virtual worlds and virtual environments," *J. Virtual Worlds Res.*, vol. 1, no. 1, pp. 1–3, 2008.

[51] M. W. Bell, S. Smith-Robbins, and G. Withnail, "This is not a game–social virtual worlds, fun, and learning," in *Researching Learning in Virtual Worlds*, 2010, pp. 177–191.

[52] J. E. R. Lee and S. G. Park, "Whose second life is this? How avatar-based racial cues shape ethno-racial minorities' perception of virtual worlds," *Cyberpsychol. Behav. Soc. Netw.*, vol. 14, no. 11, pp. 637–642, 2011.

[53] T. F. Waddell, J. D. Ivory, R. Conde, C. Long, and R. McDonnell, "White man's virtual world: A systematic content analysis of gender and race in massively multiplayer online games," *J. Virtual Worlds Res.*, vol. 7, no. 2, p. 1, 2014.

[54] T. E. Bilir, "Real economics in virtual worlds: A massively multiplayer online game case study: Runescape," *SSRN 1655084*, 2009, pp. 1–183.

[55] J. Billieux *et al.*, "Why do you play World of Warcraft? An in-depth exploration of self-reported motivations to play online and in-game behaviours in the virtual world of Azeroth," *Comput. Hum. Behav.*, vol. 29, no. 1, pp. 103–109, 2013.

[56] A. Gyamfi, "Media richness perspective of social media usage for learning: Perception of cocoa researchers in Ghana," in *Evaluating Media Richness in Organizational Learning*, 2018, pp. 1–15.

[57] D. Mandal and R. J. McQueen, "Extending media richness theory to explain social media adoption by microbusinesses," *Te Kura Kete Aronui*, vol. 5, pp. 1–28, 2013.

[58] S. Winter, E. Maslowska, and A. L. Vos, "The effects of trait-based personalization in social media advertising," *Comput. Hum. Behav.*, vol. 114, p. 106525, 2021.

[59] P. A. D. S. N. Wijesekara and S. Gunawardena, "A machine learning-aided network contention-aware link lifetime- and delay-based hybrid routing framework for software-defined vehicular networks," *Telecom*, vol. 4, no. 3, pp. 393–458, 2023.

[60] P. A. D. S. N. Wijesekara, K. L. K. Sudheera, G. G. N. Sandamali, and P. H. J. Chong, "Machine learning based link stability prediction for routing in software-defined vehicular networks," in *Proc. 20th Acad. Sessions*, 2023, p. 60.

[61] E. Mazur and L. Kozarian, "Self-presentation and interaction in blogs of adolescents and young emerging adults," *J. Adolesc. Res.*, vol. 25, no. 1, pp. 124–144, 2010.

[62] S. Uski and A. Lampinen, "Social norms and self-presentation on social network sites: Profile work in action," *New Media Soc.*, vol. 18, no. 3, pp. 447–464, 2016.

[63] A. Schimmenti, F. Guglielmucci, C. P. Barbasio, and A. Granieri, "Attachment disorganization and dissociation in virtual worlds: A study on problematic Internet use among players of online role-playing games," *Clin. Neuropsychiatry*, vol. 9, no. 5, pp. 195–202, 2012.

[64] P. L. McLeod and G. Leshed, "As long as they don't know where I live: Information disclosure strategies for managing identity in Second Life™," in *Reinventing Ourselves: Contemporary Concepts of Identity in Virtual Worlds*, 2011, pp. 191–211.

[65] N. H. Sharfina, H. Paserangi, F. P. Rasyid, and M. I. N. Fuady, "Copyright issues on the prank video on YouTube," in *Proc. Int. Conf. Environ. Energy Policy (ICEEP 2021)*, 2021, pp. 90–97.

[66] V. Suarez-Lledo and J. Alvarez-Galvez, "Prevalence of health misinformation on social media: Systematic review," *J. Med. Internet Res.*, vol. 23, no. 1, p. e17187, 2021.

[67] Á. Díaz and L. Hecht-Felella, "Double standards in social media content moderation," *Brennan Center Justice N.Y. Univ. Sch. Law*, pp. 1–40, 2021.

[68] A. G. Chowdhury, R. Sawhney, R. Shah, and D. Mahata, "#YouToo? Detection of personal recollections of sexual harassment on social media," in *Proc. 57th Annu. Meet. Assoc. Comput. Linguist.*, 2019, pp. 2527–2537.

[69] F. Mishna *et al.*, "Social media, cyber-aggression and student mental health on a university campus," *J. Ment. Health*, vol. 27, no. 3, pp. 222–229, 2018.

[70] S. Choirunnisa, "Legal protection against women victims of sexual harassment through social media (cyberporn)," *Indones. J. Int. Clin. Legal Educ.*, vol. 3, no. 3, pp. 367–380, 2021.

[71] H. J. Parker and S. V. Flowerday, "Contributing factors to increased susceptibility to social media phishing attacks," *S. Afr. J. Inf. Manag.*, vol. 22, no. 1, pp. 1–10, 2020.

[72] P. A. D. S. N. Wijesekara, "Deep 3D dynamic object detection towards successful and safe navigation for full autonomous driving," *Open Transp. J.*, vol. 16, no. 1, p. e187444782208191, 2022.

[73] M. Jain, P. Mowar, R. Goel, and D. K. Vishwakarma, "Clickbait in social media: Detection and analysis of the bait," in *Proc. 55th Annu. Conf. Inf. Sci. Syst. (CISS)*, 2021, pp. 1–6.

[74] B. Kitchens, S. L. Johnson, and P. Gray, "Understanding echo chambers and filter bubbles: The impact of social media on diversification and partisan shifts in news consumption," *MIS Q.*, vol. 44, no. 4, pp. 1619–1649, 2020.

[75] T. Minkus, Y. Ding, R. Dey, and K. W. Ross, "The city privacy attack: Combining social media and public records for detailed profiles of adults and children," in *Proc. 2015 ACM Conf. Online Soc. Netw.*, 2015, pp. 71–81.

[76] J. Robinson *et al.*, "Social media and suicide prevention: A systematic review," *Early Interv. Psychiatry*, vol. 10, no. 2, pp. 103–121, 2016.

[77] H. M. D. P. M. Herath *et al.*, "Automatic assessment of aphasic speech sensed by audio sensors for classification into aphasia severity levels to recommend speech therapies," *Sensors*, vol. 22, no. 18, p. 6966, 2022.

[78] N. Srikanth, C. H. V. Tejaswini, and D. P. Kumar, "Socially smart: An aggregation system for social media using web scraping," *Displays*, vol. 6, no. 4, pp. 749–752, 2019.

[79] L. C. Dewi and A. Chandra, "Social media web scraping using social media developers API and regex," *Procedia Comput. Sci.*, vol. 157, pp. 444–449, 2019.

[80] Y. Wang and B. Li, "Sentiment analysis for social media images," in *Proc. IEEE Int. Conf. Data Min. Workshop (ICDMW)*, 2015, pp. 1584–1591.

[81] A. Muhammad, N. Wiratunga, and R. Lothian, "Contextual sentiment analysis for social media genres," *Knowl.-Based Syst.*, vol. 108, pp. 92–101, 2016.

[82] M. A. Zakkar and D. J. Lizotte, "Analyzing patient stories on social media using text analytics," *J. Healthc. Inform. Res.*, vol. 5, no. 4, pp. 382–400, 2021.

[83] A. I. Kabir, R. Karim, S. Newaz, and M. I. Hossain, "The power of social media analytics: Text analytics based on sentiment analysis and word clouds on R," *Inform. Econ.*, vol. 22, no. 1, pp. 25–38, 2018.

[84] I. Perikos and I. Hatzilygeroudis, "Aspect-based sentiment analysis in social media with classifier ensembles," in *Proc. IEEE/ACIS 16th Int. Conf. Comput. Inf. Sci. (ICIS)*, 2017, pp. 273–278.

[85] P. Wu, X. Li, S. Shen, and D. He, "Social media opinion summarization using emotion cognition and convolutional neural networks," *Int. J. Inf. Manag.*, vol. 51, p. 101978, 2020.

[86] T. Dwyer and F. Martin, "Sharing news online: Social media news analytics and their implications for media

pluralism policies," *Digit. Journal.*, vol. 5, no. 8, pp. 1080–1100, 2017.

[87] S. Amer-Yahia *et al.*, "Maqsa: A system for social analytics on news," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, 2012, pp. 653–656.

[88] P. A. D. S. N. Wijesekara, "Intrusion detection using blockchain in software-defined networking: A literature review," *J. Eng. Sci. Technol. Rev.*, vol. 18, no. 1, pp. 57–79, 2025.

[89] B. Appasani *et al.*, "Blockchain-enabled smart grid applications: Architecture, challenges, and solutions," *Sustainability*, vol. 14, no. 14, p. 8801, 2022.

[90] P. A. D. S. N. Wijesekara, "A review of blockchain-rooted energy administration in networking," *Indones. J. Comput. Sci.*, vol. 13, no. 2, pp. 1607–1642, 2024.

[91] Q. Wang, J. Yu, S. Chen, and Y. Xiang, "SoK: DAG-based blockchain systems," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–38, 2023.

[92] P. A. D. S. N. Wijesekara, "Network virtualization utilizing blockchain: A review," *J. Appl. Res. Electr. Eng.*, vol. 3, no. 2, pp. 136–158, 2024.

[93] S. Zhou *et al.*, "A systematic review of consensus mechanisms in blockchain," *Mathematics*, vol. 11, no. 10, p. 2248, 2023.

[94] P. A. D. S. N. Wijesekara and S. Gunawardena, "A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges," *Netw.*, vol. 3, no. 3, pp. 343–421, 2023.

[95] P. A. D. S. N. Wijesekara, "Blockchain and artificial intelligence for big data analytics in networking: Leading-edge frameworks," *J. Eng. Sci. Technol. Rev.*, vol. 17, no. 3, pp. 125–143, 2024.

[96] C. Seneviratne, P. A. D. S. N. Wijesekara, and H. Leung, "Performance analysis of distributed estimation for data fusion using a statistical approach in smart grid noisy wireless sensor networks," *Sensors*, vol. 20, no. 2, p. 567, 2020.

[97] P. A. D. S. N. Wijesekara, "A review on deploying blockchain technology for network mobility management," *Int. Trans. Electr. Eng. Comput. Sci.*, vol. 3, no. 1, pp. 1–33, 2024.

[98] S. Bhatnagar *et al.*, "Block-hash signature (BHS) for transaction validation in smart contracts for security and privacy using blockchain," *J. Mobile Multimedia*, pp. 935–962, 2023.

[99] P. A. D. S. N. Wijesekara, "Load balancing in blockchain networks: A survey," *Int. J. Electr. Electron. Eng. Telecommun.*, vol. 13, no. 4, pp. 260–276, 2024.

[100] H. Halaburda, M. Sarvary, and G. Haeringer, "Smart contracts and blockchain," in *Beyond Bitcoin: Economics of Digital Currencies and Blockchain Technologies*, 2022, pp. 135–178.

[101] X. Guo, Y. Zuo, and D. Li, "When auditing meets blockchain: A study on applying blockchain smart contracts in auditing," *Int. J. Account. Inf. Syst.*, vol. 56, p. 100730, 2025.

[102] C. Li and B. Palanisamy, "Incentivized blockchain-based social media platforms: A case study of Steemit," in *Proc. 10th ACM Conf. Web Sci.*, 2019, pp. 145–154.

[103] Q. Xu, Z. Song, R. S. M. Goh, and Y. Li, "Building an Ethereum and IPFS-based decentralized social network system," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, 2018, pp. 1–6.

[104] H. H. Nguyen *et al.*, "SoChainDB: A database for storing and retrieving blockchain-powered social network data," in *Proc. 45th Int. ACM SIGIR Conf. Res. Dev. Inf. Retr.*, 2022, pp. 3036–3045.

[105] A. Chakravorty and C. Rong, "Ushare: User-controlled social media based on blockchain," in *Proc. 11th Int. Conf. Ubiquitous Inf. Manag. Commun.*, 2017, pp. 1–6.

[106] Y. Zhan, Y. Xiong, and X. Xing, "A conceptual model and case study of blockchain-enabled social media platform," *Technovation*, vol. 119, p. 102610, 2023.

[107] S. Barua and D. Talukder, "A blockchain-based decentralized video streaming platform with content protection system," in *Proc. 23rd Int. Conf. Comput. Inf. Technol. (ICCIT)*, 2020, pp. 1–6.

[108] M. A. H. Wadud and M. A. Uddin, "Blockchain-leveraged cyberbullying preventing framework," *Preprint Res. Square rs.3.rs-21075/v2*, 2021, pp. 1–11.

[109] A. M. Alabdali and A. Mashat, "A novel approach toward cyberbullying with intelligent recommendations using deep learning-based blockchain solution," *Front. Med.*, vol. 11, p. 1379211, 2024.

[110] S. Salim, B. Turnbull, and N. Moustafa, "A blockchain-enabled explainable federated learning for securing internet-of-things-based social media 3.0 networks," *IEEE Trans. Comput. Soc. Syst.*, pp. 1–17, 2021.

[111] M. U. Rahman, B. Guidi, and F. Baiardi, "Blockchain-based access control management for decentralized online social networks," *J. Parallel Distrib. Comput.*, vol. 144, pp. 41–54, 2020.

[112] M. Arquam, A. Singh, and R. Sharma, "A blockchain-based secured and trusted framework for information propagation on online social networks," *Soc. Netw. Anal. Min.*, vol. 11, no. 1, p. 49, 2021.

[113] S. Zhang *et al.*, "A novel blockchain-based privacy-preserving framework for online social networks," *Connect. Sci.*, vol. 33, no. 3, pp. 555–575, 2021.

[114] A. M. Hil *et al.*, "Cryptonight mining algorithm with YAC consensus for social media marketing using blockchain," *Comput. Mater. Continua*, vol. 71, no. 2, pp. 3921–3936, 2022.

[115] R. M. Murimi, "A blockchain-enhanced framework for social networking," *Ledger*, vol. 4, no. s1, pp. 67–81, 2019.

[116] J. Ahmed *et al.*, "GDPR compliant consent-driven data protection in online social networks: A blockchain-based

approach," in *Proc. 3rd Int. Conf. Inf. Comput. Technol. (ICICT)*, 2020, pp. 307–312.

[117] S. Dhall *et al.*, "Blockchain-based framework for reducing fake or vicious news spread on social media/messaging platforms," *Trans. Asian Low-Resour. Lang. Inf. Process.*, vol. 21, no. 1, pp. 1–33, 2021.

[118] I. S. Ochoa *et al.*, "Fakechain: A blockchain architecture to ensure trust in social media networks," in *Proc. 12th Int. Conf. Qual. Inf. Commun. Technol. (QUATIC)*, 2019, pp. 105–118.

[119] R. F. Sari, A. S. Ilmananda, and D. M. Romano, "Social trust-based blockchain-enabled social media news verification system," *J. Universal Comput. Sci.*, vol. 27, no. 9, pp. 979–998, 2021.

[120] I. U. Shahid *et al.*, "Authentic facts: A blockchain-based solution for reducing fake news in social media," in *Proc. 4th Int. Conf. Blockchain Technol. Appl.*, 2021, pp. 121–127.

[121] Q. Chen, G. Srivastava, R. M. Parizi, M. Aloqaily, and I. Al Ridhawi, "An incentive-aware blockchain-based solution for internet of fake media things," *Inf. Process. Manag.*, vol. 57, no. 6, p. 102370, 2020.

[122] N. Balasubramaniam, "Blockchain-based digital identity verification for social media," *Euroasia J. Math. Eng. Nat. Med. Sci.*, vol. 7, no. 8, pp. 202–209, 2020.

[123] Z. Shahbazi and Y. C. Byun, "Fake media detection based on natural language processing and blockchain approaches," *IEEE Access*, vol. 9, pp. 128442–128453, 2021.

[124] B. Guidi and A. Michienzi, "The decentralization of social media through the blockchain technology," in *Companion Publ. 13th ACM Web Sci. Conf.*, 2021, pp. 138–139.

[125] T. Kim, H. Shin, H. J. Hwang, and S. Jeong, "Posting bot detection on blockchain-based social media platform using machine learning techniques," in *Proc. Int. AAAI Conf. Web Soc. Media*, vol. 15, 2021, pp. 303–314.

[126] B. Guidi and A. Michienzi, "Users and bots behaviour analysis in blockchain social media," in *Proc. 7th Int. Conf. Soc. Netw. Anal. Manag. Secur. (SNAMS)*, 2020, pp. 1–8.

[127] S. Kumari *et al.*, "Blockchain-based E-analysis of social media forums for cryptocurrency phase shifts," in *Proc. 5th Int. Conf. Invent. Res. Comput. Appl. (ICIRCA)*, 2023, pp. 1222–1225.

[128] Z. Shahbazi and Y. C. Byun, "Blockchain-based event detection and trust verification using natural language processing and machine learning," *IEEE Access*, vol. 10, pp. 5790–5800, 2021.

[129] B. Guidi and A. Michienzi, "Interaction communities in blockchain online social media," in *Proc. 3rd Int. Conf. Blockchain Comput. Appl. (BCCA)*, 2021, pp. 89–96.

[130] C. T. Ba, M. Zignani, and S. Gaito, "Social and rewarding microscopical dynamics in blockchain-based online social networks," in *Proc. Conf. Inf. Technol. Soc. Good*, 2021, pp. 127–132.

[131] S. Hasan, M. A. Habib, A. Roy, and A. T. M. Shifat, "Sociala: An incentivized decentralized social media for writers based on blockchain using modified delegated proof of stake," in *Proc. 10th Int. Conf. Netw. Syst. Secur.*, 2023, pp. 87–96.

[132] A. Norta, D. Hawthorne, and S. L. Engel, "A privacy-protecting data-exchange wallet with ownership-and monetization capabilities," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, 2018, pp. 1–8.

[133] J. Li *et al.*, "LBRY: A blockchain-based decentralized digital content marketplace," in *Proc. IEEE Int. Conf. Decentral. Appl. Infrastruct. (DAPPS)*, 2020, pp. 42–51.

[134] P. Banerjee *et al.*, "Reliable, fair and decentralized marketplace for content sharing using blockchain," in *Proc. IEEE Int. Conf. Blockchain*, 2020, pp. 365–370.

[135] C. T. Ba, M. Zignani, and S. Gaito, "The role of groups in a user migration across blockchain-based online social media," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2022, pp. 291–296.

[136] T. M. Choi, S. Guo, and S. Luo, "When blockchain meets social-media: Will the result benefit social media analytics for supply chain operations management?," *Transp. Res. Part E: Logist. Transp. Rev.*, vol. 135, p. 101860, 2020.

[137] Z. Wang, X. Xiong, and W. J. Knottenbelt, "Blockchain transaction censorship: (In)secure and (in)efficient?," in *Proc. Int. Conf. Math. Res. Blockchain Economy*, 2023, pp. 78–94.

[138] M. H. Tsou, "Research challenges and opportunities in mapping social media and big data," *Cartogr. Geogr. Inf. Sci.*, vol. 42, no. Suppl. 1, pp. 70–74, 2015.

[139] A. Chauhan *et al.*, "Blockchain and scalability," in *Proc. IEEE Int. Conf. Softw. Qual. Rel. Secur. Companion (QRS-C)*, 2018, pp. 122–128.

[140] G. Hileman and M. Rauchs, "Global blockchain benchmarking study," *Soc. Sci. Res. Netw. (SSRN)*, Rochester, NY, 2017.