applied sciences

MDPI

Review

The Application of Blockchain in Social Media: A Systematic Literature Review

Mahamat Ali Hisseine , Deji Chen * and Xiao Yang

College of Electronic and Information Engineering, Tongji University, Shanghai 201804, China; mahamat@tongji.edu.cn (M.A.H.); xiaoyang@tongji.edu.cn (X.Y.)
* Correspondence: dejichen@tongji.edu.cn; Tel.: +86-185-0172-4250

Abstract: Social media has transformed the mode of communication globally by providing an extensive system for exchanging ideas, initiating business contracts, and proposing new professional ideas. However, there are many limitations to the use of social media, such as misinformation, lack of effective content moderation, digital piracy, data breaches, identity fraud, and fake news. In order to address these limitations, several studies have introduced the application of Blockchain technology in social media. Blockchains can provides transparency, traceability, tamper-proofing, confidentiality, security, information control, and supervision. This paper is a systematic literature review of papers covering the application of Blockchain technology in social media. To the best of our knowledge, this is the first systematic literature review that elucidates the combination of Blockchain and social media. Using several electronic databases, 42 related papers were reviewed. Our findings show that previous studies on the applications of Blockchain in social media are focused mainly on blocking fake news and enhancing data privacy. Research in this domain began in 2017. This review additionally discusses several challenges in applying Blockchain technologies in social media contexts, and proposes alternative ideas for future implementation and research.

Keywords: blockchain; social media; online network sites; application of blockchain

Citation: Hisseine, M.A.; Chen, D.; Yang, X. The Application of Blockchain in Social Media: A Systematic Literature Review. *Appl. Sci.* **2022**, *12*, 6567. https://doi.org/10.3390/app12136567

Academic Editor: Federico Divina

Received: 30 May 2022
Accepted: 27 June 2022
Published: 28 June 2022

1. Introduction

Social media invoke digital platforms reachable by the internet and permit users to form and interact in virtual groups. People can easily share information, which greatly strengthens communication and contact. They can find old classmates and acquaintances, connect with novel groups, or find persons with similar attractions across political, financial, and geographic boundaries. Thus, social media enable millions of internet users around the world to exchange information. They deliver access to a massive data source on an incredible ratio [1–3]. However, there are certain limitations to social media. Academics, officials, and users have recognized several crucial problems, including massive control by limited firms, the publication of false content, discussions around restricted or unrestricted dialog, compromised confidentiality, and political restrictions [4]. Using private details on social media increases apprehension with respect to confidentiality and involves security issues. Netizens face considerable exposure to several kinds of attacks in light of the variety and particularity of the private materials exchanged on different sites [5]. Netizens can be exposed to a loss of privacy and control over their personal information. It is inexpensive to deliver news over a network, and quicker and simpler to distribute it via social media; large amounts of bogus content with deliberately incorrect articles form online for a variety of reasons, including to obtain economic and political advantage [6]. Researchers have discovered that fake articles are disseminated more quickly on Twitter than factual content by a considerable margin, that fallacious content is 70% more likely to be retweeted on Twitter than trustworthy content, and that it influences the first 1500 users six times as quickly [7]. These societal issues pose a substantial challenge in contemporary times. Many

researchers have been working in this area in order to resolve these issues. Text analysis, labeling, artificial intelligence, and machine learning methods can be used to detect fake articles. However, recognizing the source of such news for liability purposes remains a major challenge for which no concrete method exists today. Several specialists have already started working on ways of responding to this problem by deploying Blockchain technologies in connection with social media. As an outcome, diverse entities have collaborated on developing prominent inventions towards obtaining a blockchain deployed on social media.

In recent years, the decentralization of social services has been considered an opportunity to overcome the main privacy issues in social media, fake news, and censorship. Blockchain technology represents the most well-known decentralized technique today, and has been considered in developing the new generation of decentralized social platforms [8]. In the beginning, Blockchain was used only for Bitcoin; nowadays, however, it is being implemented on many other platforms and used for several different objectives [9]. The application of Blockchain in social media brings several benefits, including improved user privacy, bypassing of restrictions, and the possibility for participants to engage in cryptocurrency transactions through social media platforms [10]. Privacy protection is a very complex concept, usually referring to the protection of data that entities such as individuals or groups do not want to be known by outsiders. In a blockchain, a decentralized data repository is generated where critical information is secured, making it very difficult for anyone to crack the data [11]. For those in repressive regimes or where censorship is an issue, blockchains deployed in a social networking context offer the benefits of secure authentication while ensuring anonymity [12]. A transparent autonomous process can be implemented that allows connections to be verified by different participants [13]. Blockchains make it very easy for an entity to be tokenized and exchanged on the Blockchain. This means that any content, whether pictures, music, or video, can be tokenized and traded on the Blockchain [14]. Blockchains can guarantee the origin, credibility, and traceability of data by offering a transparent, immutable, and certifiable operation registry while producing a safe peer-to-peer environment for keeping and exchanging material [15]. Another utility is combating disinformation by tracing and checking the provenance of potentially perilous data. Another application is the creation of a registry of uploaded photos containing data such as geographical positions, contratual agreements, copyright possession, and other metadata that are certifiable by everyone [16]. As we will discuss, several current issues with social media can be addressed by Blockchain technology, and much research has been carried out in this area, making a summary of all the proposed solutions necessary.

This systematic review elucidates research trends and ways in which Blockchain can be used in social media. It identifies research gaps and proposes future research directions. The research questions underlining this systematic review are as follows. (1) What are the different methods and techniques proposed by past studies to leverage blockchain technology in social media? (2) What are the existing challenges and limitations of blockchain application in social media? (3) What are the knowledge gaps future research can address?

The remainder of this study is organized as follows. Section 2 briefly introduces Blockchain, its main characteristics, and its components. Section 3 provides an overview of social media, and introduces the most popular platforms that combine the two technologies. Section 4 presents the methodology, used in this review, and Section 5 provides an overview of selected papers. Section 6 discusses the main applications of Blockchain in social media and answers the research questions posed above, while Section 7 presents the conclusion together with future research areas.

2. Overview of Blockchain

A blockchain is a growing distributed ledger that keeps a permanent record of all transactions that have taken place in a secure, chronological, and immutable way. It was conceptualized and first used in 2008 by an unknown person or group named Satoshi

Nakamoto to create the Bitcoin cryptocurrency. The primary aim is to use a cryptosystem to encrypt the sequence of bits in electronic files so as not to be anteceded or tampered with [17,18]. When evaluating a blockchain, the notable characteristics to consider include audibility, privacy, confidentiality, consistency, decentralization, and integrity [19,20]. Blockchain technologies can be categorized into three types: Public Blockchains (anyone can join the network), Private Blockchains (the members are chosen based on conditions), and Consortium Blockchains (semiprivate blockchains limited to a group) [21]. All three types can additionally be classified as Permissionless (public Blockchain), permissioned (private Blockchain), or both (Consortium blockchain). A Blockchain network comprises several components and attributes, such as a distributed and immutable ledger, Peer-to-Peer (P2P) networks, a consensus mechanism, and smart contracts.

2.1. Cryptography Hash Function

A hash function is a cryptographic algorithm that is widely used in blockchain technology. A hash function returns any kind of input as a string of bytes with a fixed length and structure. The output formed is named a hash value. A hash value formed from data using an explicit hashing algorithm is always the same length and one-way, that is, it cannot be reversed. The SHA-256 is the most illustrious of all cryptographic hash functions, and is used widely in blockchain technology.

2.2. Immutable Ledger

Blockchain is recognized for its ability to be immutable. When people talk about Blockchain's "immutability", they are referring to the impossibility of adjusting the data after it is recorded and stored. This is an essential attribute when dealing with blockchains. Figure 1 shows how the blocks are linked and how each block contains the previous block's hash value.

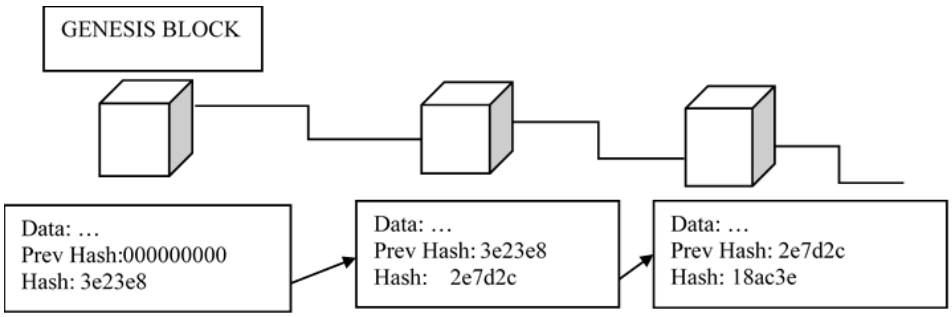

Figure 1. Illustration of block links.

The first block does not have previous blocks, and is named the genesis block. As can be seen, immutability emphasizes the fact that a blockchain is very secure and well designed. When the hash varies and no longer equals the previous hash in the ledger, the blockchain rejects that hash, making it invalid, similar to a bad check. A hacker would need to completely modify the next block, the block after that, and indeed the whole blockchain.

2.3. Distributed Peer-to-Peer Networks

By using a blockchain, interaction between two parties through a peer-to-peer model can be easily accomplished without any third-party requirement. Blockchain uses P2P protocols, which permits all network members to hold an identical copy of contacts, allowing agreement over a consensus mechanism.

2.4. Distributed Application

To preserve an effective digital transaction platform, the blockchains used by most cryptocurrencies utilizes Distributed Applications (ĐApps). Dapps are software applications which are usually maintained and implemented on cloud services and can work on

various systems at the same time. Many DApps have been built and deployed on a model based on Blockchain, although DApps can run on a cloud environment or other network systems as well [22].

2.5. Consensus Protocol

A consensus protocol is an agreement between nodes in a blockchain network that submits transactional information, and is one of the most critical blockchain technology components. A blockchain network is restructured through the arrayed consensus protocol in order to certify that contacts and blocks are organized correctly, to guarantee the distributed ledger's integrity and consistency, and ultimately to enhance trust between nodes. There are several consensus mechanisms used in various blockchain networks. Proof of Work (PoW) was the first consensus mechanism used in Blockchain. In this mechanism, the miners, who are the nodes, resolve cryptographic or mathematical problems using their machines [23]. Proof of Stake (PoS) represents an alternative to PoW, as it is more energy efficient; it utilizes a collection method that is pseudorandom in order to choose the validator of the following block from among the current nodes [24]. In addition, to these, there are other popular mechanisms, including consensus proofs such as Delegated Proof-of-Stake (DPoS), Byzantine Fault Tolerance (BFT), and Proof of Elapsed Time (PoET). In addition to the conventional blockchain consensus protocols, other alternative protocols have been proposed in recent years for specific applications, such as Proof of Familiarity (PoF), Proof of Benefit (PoB), Proof of Participation and Fees (PoPF), Proof of Vote (PoV), CHB, and CHBD; others for more general-purpose use include Proof of Reputation (PoR), Proof of Reputation X (PoRX), Proof of Phone (PoP), Proof of Learning (PoL), Proof of Search (PoSe), Proof of Sincerity (PoSn), Proof of Adjourn (PoAj), Proof of Evolution (PoE), Proof of Experience (PoEx), and Proof of Accuracy (PoA) [25].

2.6. Smart Contracts

Smart contracts refer to computer programs that obey a succession of previously established instructions stored on a blockchain [26]. Today, smart contracts remain popular in the cryptocurrency industry, primarily for exchanging currencies. However, they are not limited to this context, and many insurance and property companies are adopting smart contracts for better scalability at cheaper rates. In a nutshell, smart contracts are an essential component for many platforms. The advantages of smart contracts are multiple. A smart contract allows anyone to protect an arrangement, automate payment, and eliminate the risk of scams while at the same time reducing intermediary fees. Unfortunately, accurate implementation of a smart contract's code cannot ensure its complete safety. An examination of existing smart contracts illustrates that a substantial portion of them are undeniably exposed [27]. A study found that while developers care a great deal about code security, there are no effective ways to prove the correctness, reliability, and security of code [28]. In 2021, digital assets built on a smart contracts with a value equivalent to USD 680 million were cracked or stolen due to safety weaknesses [29]. The importance of smart contract security cannot be exaggerated, particularly now that smart contracts are acquiring more attention. One study used pure methods to implement a smart contract design pattern which increased the security of the source code to allow for the continuous delivery and deployment of selected classes while updating verification rule classes at runtime [30]. Continuous integration, continuous delivery, and continuous deployment are the software development industry practices that allow organizations to regularly and constantly issue new features and products [31]. Research suggests that use of the continuous deployment framework in generating distributed applications for blockchain nodes can raise the design level of smart contracts and deployment arrangements, encompassing security algorithms for registering new nodes in the blockchain network while achieving automation of the deployment of reconfigurable blockchain networks with updatable and extensible smart contracts at runtime [32].

3. Social Media Basics

Social media can be defined as a website or mobile application that allows users to build a network of friends, relations, or subscribers and that promotes social interactions between individuals, groups of individuals, or organizations. It is a relatively new concept, only emerging in recent years. The principle is to find people the user knows, which in turn allows the user to contact other people. Progressively, such a network can quickly become very considerable. In the virtual world, a social network is an internet site that allows users, whether professionals or individuals, to share information. Social network development is changing with each passing day in light of the extension of the internet, and has progressed from personal usage to corporate media communication and collaboration [33]. People can create specific profiles and communicate more efficiently through these sites, which emphasize interaction and camaraderie. These sites allow registered members to submit data such as birthday information, interests, education background, career, songs, pictures, media files, and hyperlinks, and to share them with others.

3.1. The Different Types of Social Media

There are different types of social media, all with their own unique characteristics.

3.1.1. Social Networking Sites

Social networking sites are used to allow individuals associate with one another online [34]. These sites allow users to create profiles with photos and connect with other users who share their interests, for example, Facebook, Twitter, and Instagram [35].

3.1.2. Social Media for Sharing Photos, Videos, and Music

Video hosting platforms provide independent filmmakers, journalists, and other creators with a way to connect with their audiences and to stream videos quickly and easily [36]. Apart from the sharing function, such media allow the creation of a profile and permit commenting, thus placing them in the category of social platforms. The most famous are YouTube, Tiktok, Snapchat, Vimeo, Instagram, Flickr, Pinterest, and Dailymotion.

3.1.3. Professional Networks

Professional social networks play an essential role in the recruitment process, and have become a natural support system for people to develop their professional careers. While LinkedIn may be the world's largest professional networking site, there are several others options as well, such as Meetup, Reddit, and Jobcase [37]

3.1.4. Social Media Messaging

Generally free, messaging platforms allow billions of users to exchange information across the world. The most notorious are Messenger, WhatsApp, Skype, WeChat, and QQ.

3.1.5. Forums

Forums are the oldest social platforms. They are timeless and remain popular with Internet users today. Users can interact, create discussions, ask questions, and respond to multiple topics.

3.2. The Most Popular Social Media Sites Today

Nowadays, the most popular social media sites based on the number of monthly active users are Facebook (2.9 billion), YouTube (2.2 billion), WhatsApp (2 billion), Instagram (2 billion), WeChat (1.26 billion), TikTok (1 billion), and Sina Weibo (573 million) [38].

Figure 2 shows the top twenty most-used social media rankings according to the number of monthly active users in April 2022.

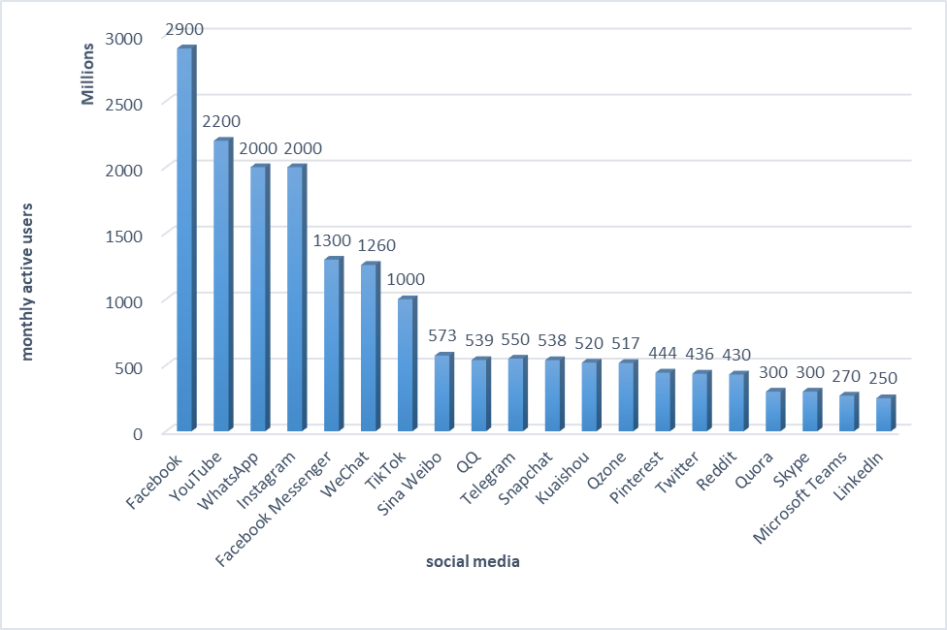

Figure 2. Top The twenty most-used social media platforms based on the number of monthly active users in April 2022. Source: Buffer Library.

3.3. Existing Blockchain-Based Social Media Platforms

Apart directly using blockchains in existing popular social media, there are already blockchain-based social media platforms such as Society2, Peepeth, Sapien, and Steemit [39].

- Society2 is a social media architecture that is decentralized according to the client, management of information, and speech. Members have options such as exchanging information, and the platform handles their status, conversation, and contacts [40].
- Peepeth consists of Ethereum and IPFS from the database and the Peepeth frontend. Peepeth's posting, liking, following, and other behaviors need to pay gas fees to be packaged on the blockchain. With no company controlling the data, anyone can build a frontend that reads and writes smart contracts, saving the content to the blockchain [41].
- Sapien is another platform based on Ethereum; it has the goal of using a proof of value consensus protocol to return control of the social media experience to users by creating a truly autonomous social network environment that compensates content creators and combats bogus information. It provides users with a speech structure and promotes community enthusiasm and participation [42].
- Steemit is a decentralized social media structure that promises to develop groups and improve social interactions by awarding members with cryptocurrency for their content based on the number of positive reviews they receive. The platform provides users with structured news and analysis, appropriate replies to personalized inquiries, and a stable cryptocurrency pegged to the US dollar, among other things [43].

4. Methodology

The detailed methodology of any systematic review should be fully reported in order to facilitate better understanding of the authenticity and availability of the review's results. In order to assist in the complete and transparent reporting of systematic reviews, researchers have developed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) to explain the methods and terms in system reviews of the latest research progress [44]. We follow the PRISMA methodology in this study. A systematic literature review aims to synthesize scientific research on an explicit subject through accurate analysis of past and present studies. This systematic literature review includes the standard steps: abstract, introduction, methods, results, and discussion.

This study covers all the characteristics of a usual systematic review: a clear title and clear purpose; a comprehensive retrieval strategy; clear inclusion and exclusion criteria; a list of all selected studies; evaluation of the characteristics of each selected study and the quality the research methodology; systematic reporting of research results; and assessment of the possibility of any publication bias.

4.1. Eligibility Criteria

Below, we lay out the inclusion and exclusion conditions used for this review and how studies were gathered for synthesis.

4.1.1. Inclusion Criteria

Blockchain and social media are recent fields of inquiry, and studies have only emerged in recent years; hence, publication date was not used as an eligibility criterion. However, papers were included in this SLR if they satisfied the criteria below:

- Papers published in journals or conference proceedings, as these are much better indexed in scholarly databases and are easier to find;
- Papers written in English;
- Papers containing the following keywords: ("Blockchain" OR "Blockchain platform" OR "Blockchain application") AND ("Social media" OR "Social network" OR "Social platform" OR "Online community" OR "media platform");
- Papers must have proposed methods to resolve an issue in social media by applying blockchain to improve privacy and security or have proposed a model using one of the characteristics or components of blockchain.

4.1.2. Exclusion Criteria

The review excluded:

- Reviews, reports, case reports, abstract-only papers, patents, magazines, and editorials, as well as books, dissertations, and theses, all of which are hard to find and infrequently available online;
- Papers for which the full text was not available online;
- Papers with a title and abstract not explicitly related to both blockchain and social media.

4.2. Information Sourcing

The next step in our research approach was to determine the online databases and internet materials to be used data collection. We chose eight highly relevant sources by researchers in computer technology-related fields. A final search was carried out on 5 April 2022. The databases we used were

1. Scopus
2. Web of Science
3. IEEE Xplore
4. ACM digital library
5. ScienceDirect
6. Wiley Online Library
7. EBSCO
8. ProQuest

4.3. Search Strategy

The search methodology is fundamental for any systematic review. The determination of search terms is the second phase. We first defined a search term relating to our study topic; second, we described alternatives for the terms and similar theories. One of the keywords we used was "blockchain", along with the associated terms "blockchain platform" and "blockchain application". The other key term was "social media", along with the associated terms "social network", "social platform", "online community", and "media platform".

The search strings were built by combining the keyword with the connectors "AND" and "OR." Each database uses its own search syntax; thus, different query and search strings were constructed, as illustrated in Table 1.

Table 1. Query Strings.

Database	Query Strings
Scopus	TITLE-ABS-KEY ((("Blockchain" OR "Blockchain platform" OR "Blockchain application") AND ("Social media" OR "Social network" OR "Social platform" OR "Online community" OR "media platform")))
Web of Science	TS = ((("Blockchain" OR "Blockchain platform" OR "Blockchain application") AND ("Social media" OR "Social network" OR "Social platform" OR "Online community" OR "media platform")))
IEEE Xplore	("All Metadata": blockchain OR "All Metadata": blockchain platform OR "All Metadata": blockchain application) AND ("All Metadata": social media OR "All Metadata": social network OR "All Metadata": social platform OR "All Metadata": online community OR "All Metadata": media platform)
ACM digital library	[[All: "blockchain"] OR [All: "blockchain platform"] OR [All: "blockchain application"]] AND [[All: "social media"] OR [All: "social network"] OR [All: "social platform"] OR [All: "online community"] OR [All: "media platform"]] AND [[All: "blockchain"] OR [All: "blockchain platform"] OR [All: "blockchain application"]] AND [[All: "social media"] OR [All: "social network"] OR [All: "social platform"] OR [All: "online community"] OR [All: "media platform"]]
ScienceDirect	(("blockchain" OR "blockchain platform" OR "blockchain application") AND ("social media" OR "social network" OR "social platform" OR "Online community" OR "media platform"))
Wiley Online Library	"(blockchain OR blockchain platform OR blockchain application) AND (social media OR social network OR social platform OR online community OR media platform)" anywhere
EBSCO	("blockchain" OR "blockchain platform" OR "blockchain application") AND ("social media" OR "social network" OR "social platform" OR "online community" OR "media platform")
ProQuest	ti((("blockchain" OR "blockchain platform" OR "blockchain application") AND ("social media" OR "social network" OR "social platform" OR "online community" OR "media platform"))) OR ab((("blockchain" OR "blockchain platform" OR "blockchain application") AND ("social media" OR "social network" OR "social platform" OR "online community" OR "media platform")))

4.4. Data Selection Process

Initially, we recovered 6762 articles from eight databases. The returned results from the most to least were as follows: Science Direct, 2211 items; Wiley Online Library, 1097; Scopus, 721; IEEE Xplore, 708; EBSCO, 583; Web of Science, 517; ProQuest, 463; and ACM digital library, 453. All references found during the search were collected. Duplicate items were subsequently removed using the Endnote reference manager.

The screening procedure and ultimate choice of whether to include a study were shared between two people. While a single screening can use time and resources more effectively, there is a higher risk of missing the relevant research content. A double screening may vary from repeated examination of all records (examined independently by two investigators) to merely inspecting the result. Any divergence of opinion about a paper's qualification was handled after deliberation with the third author, who aided with the choice phase. This helped to keep any risk of bias within reasonable limits. This method can filter irrelevant records while auditing subsequent steps to improve audit efficiency. Subsequently, after the duplicates were removed, two authors directed the eligibility conditions by checking the title, abstract, and keywords in light of the research questions and debated which studies should be used for the next filtering. When a decision about inclusion or exclusion was not straightforward, the whole document was thoroughly analyzed in order to make a final inclusion decision with reference to the eligibility criteria. After the initial screening phase, 846 papers were left, of which 804 were subsequently excluded. As a result, 42 items qualified for inclusion. The process used for screening and selection is shown in Figure 3.

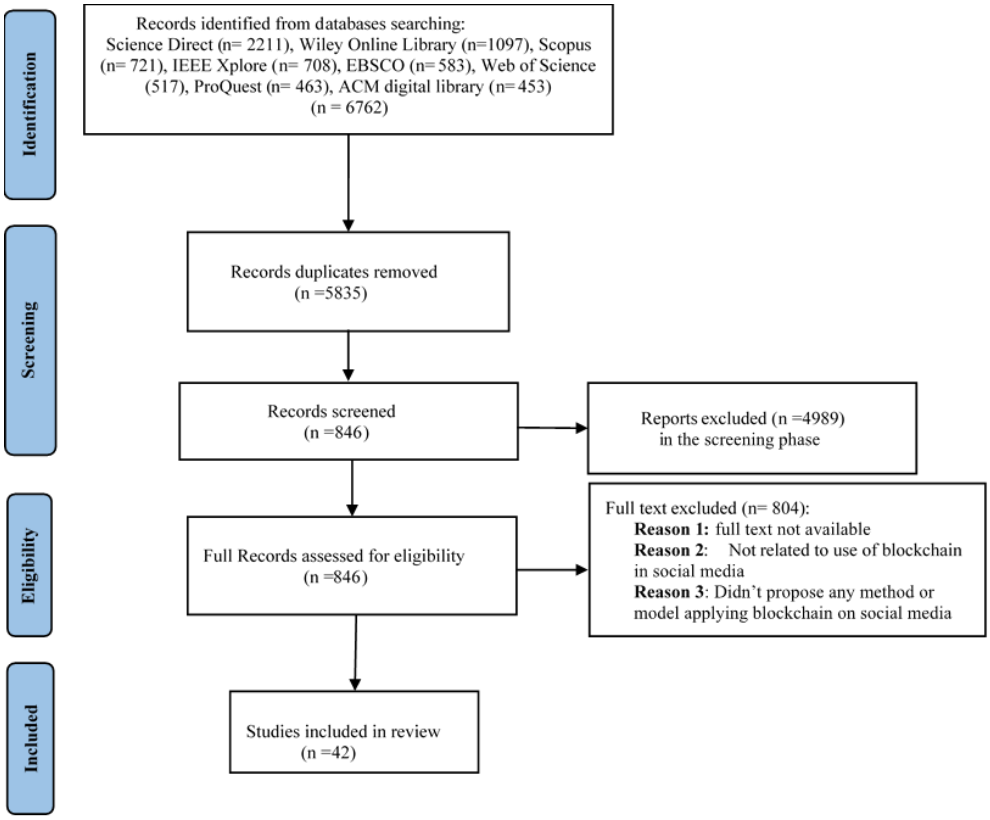

Figure 3. PRISMA Flow Diagram for the Data Collection Process.

5. Results

We retrieved 6762 records from eleven electronic databases, of which 927 were excluded as duplicates and an additional 4989 were removed during screening. The full text of the remaining 846 articles was retrieved for comprehensive review. Of these, 42 met the eligibility criteria, and are included in this systematic review. Table 2 shows a list of the selected papers sorted by the year, country, references, publication type, and the application area of the research paper based on the context.

Table 2. Contours of Selected Studies.

Reference	Year	Country	Type	Subject Area	Cited
[45]	2022	China	Journal	Computer Science	-
[46]	2022	Denmark India Taiwan	Journal	Computer Science	3
[47]	2022	India	Conference	Computer Science Engineering	-
[48]	2022	Australia Bangladesh United States	Conference	Computer Science Mathematics	-
[49]	2021	Bangladesh	Conference	Computer Science	-
[50]	2021	Ireland	Journal	Computer Science Engineering Social Sciences	-

Table 2. *Cont.*

Reference	Year	Country	Type	Subject Area	Cited
[51]	2021	Estonia India	Journal	Computer Science Engineering Social Sciences	1
[52]	2021	India	Journal	Computer Science Engineering	-
[53]	2021	Italy	Journal	Computer Science Decision Sciences Engineering Mathematics	3
[54]	2021	Malaysia	Conference	Computer Science Mathematics	1
[55]	2021	China	Conference	Computer Science Engineering Physics and Astronomy	1
[56]	2021	Singapore	Conference	Computer Science Decision Science Engineering	-
[57]	2021	Saudi Arabia Spain	Journal	Computer Science	-
[58]	2021	Indonesia United Kingdom	Journal	Computer Science Mathematics	-
[59]	2021	China	Journal	Computer Science Mathematics	-
[60]	2021	China Taiwan	Journal	Computer Science	16
[61]	2020	Canada Denmark India	Conference	Computer Science Decision Sciences Engineering	4
[62]	2020	Italy	Journal	Computer Science Mathematics	9
[63]	2020	United Kingdom	Conference	Computer Science Social Sciences	3
[64]	2020	Cameroon France	Journal	Computer Science	3
[65]	2020	China Saudi Arabia	Journal	Computer Science Engineering Materials Science	2
[66]	2020	Germany United States	Conference	Business Computer Science Decision Sciences Engineering	2
[67]	2020	India Viet Nam	Journal	Agricultural and Biological Sciences Business Engineering	-
[68]	2019	China	Journal	Computer Science Mathematics Social Sciences	24
[69]	2019	Italy	Conference	Computer Science	1

Table 2. *Cont.*

Reference	Year	Country	Type	Subject Area	Cited
[70]	2019	China	Conference	Business Computer Science Decision Sciences	-
[71]	2019	China	Journal	Computer Science Decision Sciences Engineering Mathematics	41
[72]	2019	Bangladesh	Conference	Computer Science Engineering	18
[73]	2019	South Korea	Conference	Engineering	17
[74]	2019	Egypt Saudi Arabia	Journal	Computer Science	5
[75]	2019	China Ireland	Journal	Computer Science Engineering Materials Science Mathematics	29
[76]	2019	China Macao	Journal	Computer Science Engineering Materials Science	7
[77]	2019	Brazil Portugal	Conference	Computer Science Mathematics	11
[78]	2019	United States	Conference	Computer Science Decision Sciences Engineering	13
[79]	2019	Germany	Journal	Computer Science	29
[80]	2019	United States	Journal	Computer Science	5
[81]	2019	Austria	Conference	Business Computer Science Decision Sciences Engineering Mathematics	2
[82]	2019	China Singapore	Conference	Computer Science	4
[83]	2018	China	Conference	Computer Science	8
[84]	2017	China United States	Conference	Computer Science	27
[85]	2017	United Kingdom	Journal	Computer Science Decision Sciences	29
[86]	2017	Norway	Conference	Computer Science	43

5.1. Selected Documents by Year

The distribution of the selected documents per year is shown in Figure 4. There was no time limitation for selecting research papers; however, it was essential to find the latest research conducted on the use of blockchain on social media. All of the included items were published within the last five years, as shown in the figure. Globally, a sharp rise in the number of publications can be noticed. Only one article was published in 2018, followed by fifteen items in 2019, which decreased to seven in 2020 and then increased to twelve the following year. An additional four documents were published before the end of March 2022, when data collection for this review was completed (March 30).

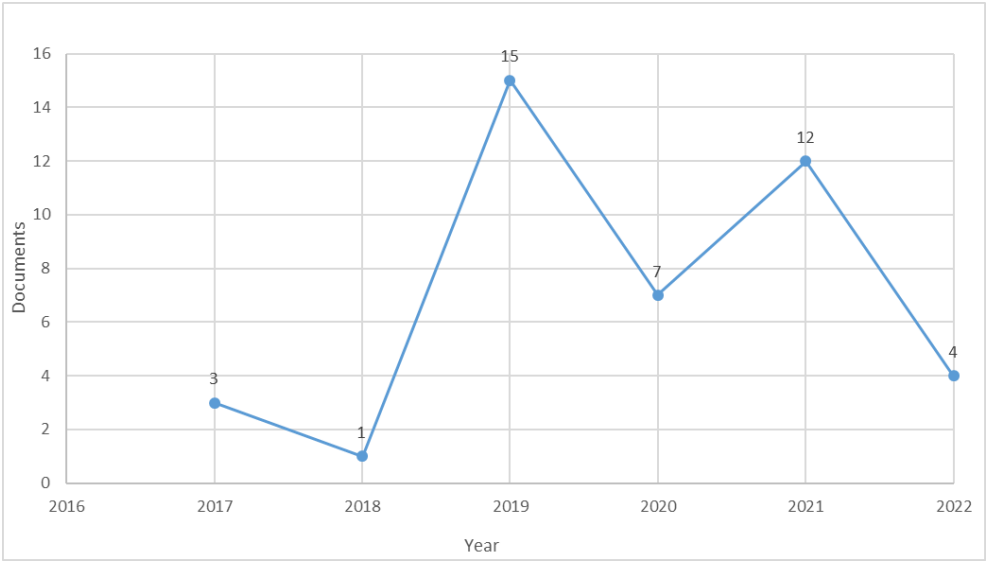

Figure 4. Documents by year.

5.2. Included Studies by Country

The records illustrate a relatively extensive spread across many countries, comprising authors from research organizations in 27 different countries. China leads research on this subject (13 documents), followed by India, the United States, Italy, and Bangladesh. Figure 5 compares the ten countries with the most publications.

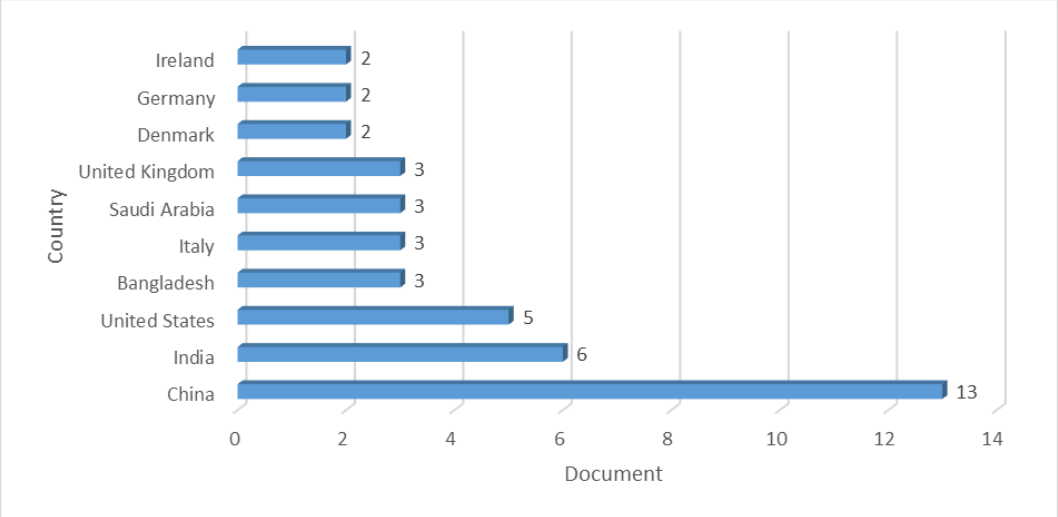

Figure 5. Documents by Country.

5.3. Publication Type

The publication type can be defined as the medium in which the paper is published, such as a journal, conference, or another type. The Figure 6 shows the distribution of documents by type. There were 22 journal papers (52%) and 20 conference papers (48%).

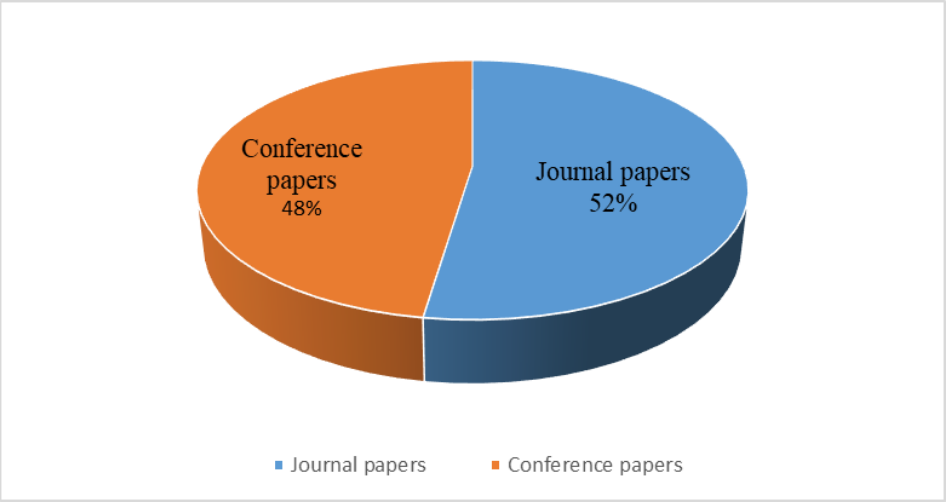

Figure 6. Publication types.

5.4. Publication by Subject Area

Figure 7 shows the papers by subject area. Several records involved two to as many as four different research areas; see Table 2. Most of the records include Computer Science as their research area (40 papers), while 18 documents cited their topic as Engineering (20%).

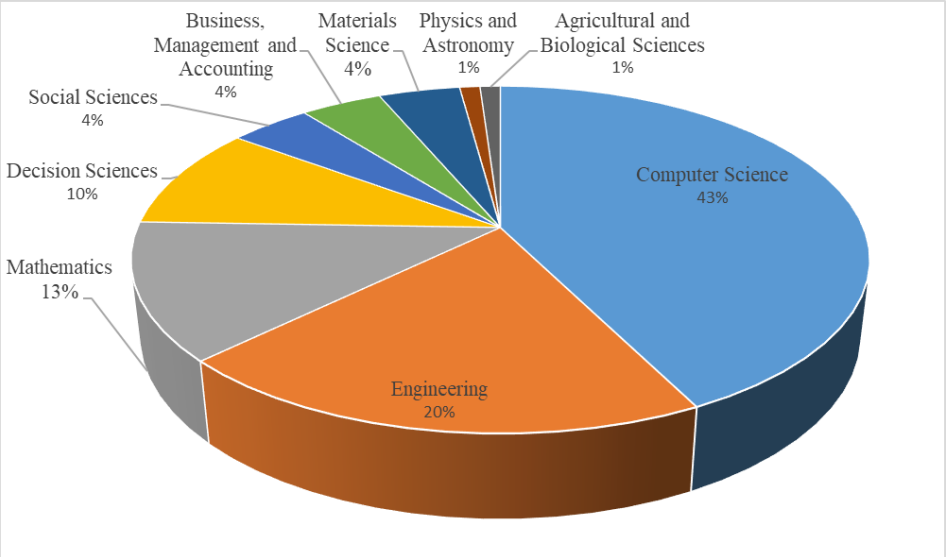

Figure 7. Publications by subject area.

5.5. Classification of Selected Papers

We found that the papers were mostly related to two domains, i.e., "data privacy and security issues" and "solutions for fake content problems". Table 3 shows the classifications with the different references. Among these papers, one addresses the issues of both data privacy and fake content.

Table 3. Classification of Selected Studies.

Category	References
Data privacy and security	[45,53,55,59,60,62,65,68,70,71,76,80–84,86]
Fake content	[46–52,56–58,61,63,64,66,67,69,72–75,77–79,85]
Data privacy and Fake content	[54]

AS shown in the table, the fake news issue received the attention of many researchers; 25 studies were about this topic, while 17 other papers were about privacy and security issues (see Figure 8).

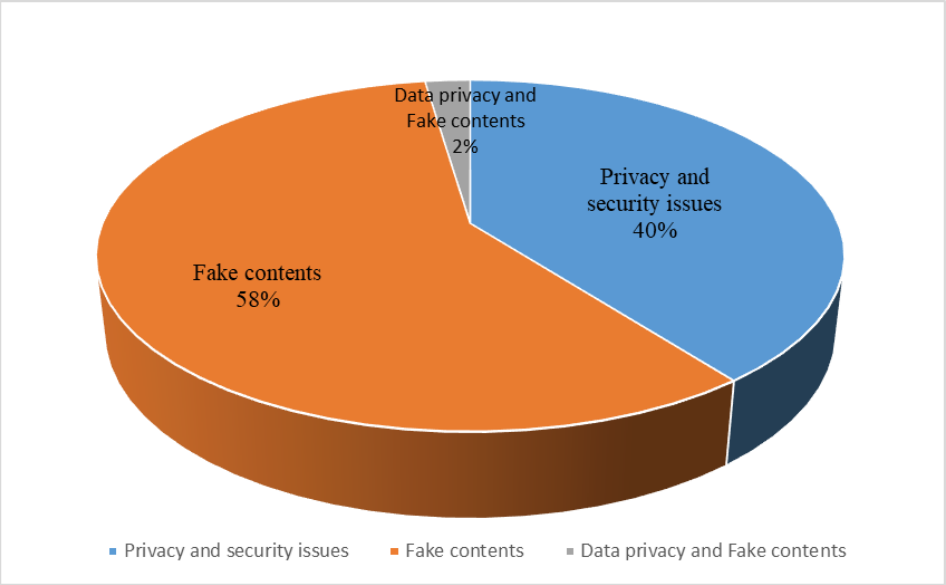

Figure 8. Classification of selected studies.

6. Discussion

6.1. Research Question Answers

6.1.1. The Different Methods and Techniques Proposed by Past Studies to Leverage Blockchain Technology in Social Media

Due to its fast progress and consistent popularity, the combination of blockchain and social media platforms is a topic that has engendered substantial consideration by researchers in recent years. Many papers have scrutinized popular social media sites from innumerable viewpoints in suggesting solutions to existing issues.

(a) Resolving Fake Content Problems

The evolution of social media has modified how we observe and manage data. Social media is nowadays the principal way to get information for many people. Never has it been as simple to access and exchange content as it is today. Everyone can register one or more profiles in minutes, often while remaining anonymous. Social media sites incentivize people to interact with a simple push of a button, and activities are generally twisted in the process of incentivization. Humans might not continuously regulate data flow in certain situations, and bots (computers that autonomously broadcast and circulate content) are able to administer social media profiles. Fake articles have been augmented through social media groups such as WhatsApp, Facebook, YouTube, etc., and are published in the system more quickly than can be envisaged. There have been varied uses of fake news in different news reporting. Several blockchain systems have been proposed to stop this phenomenon (see Table 4). The studies cited here used different Blockchain components to build a model, with smart contracta being one of the most used elements. Wahid Sadique Koly et al. [48] presented a location-aware blockchain-based news validation system. Their goal was to differentiate fake and fallacious data from authentic data. Authenticated archives are saved in a distributed blockchain, with a smart contract then developed using solidity language to build a simulated Ethereum network locally. The structure is joined with social media, and authenticated users approve the accuracy of content. In addition, all users are unidentified, allowing them to confirm any evidence without external pressure. After an assessment, the system contains two pointers to prove whether the article is real or fake. Imran Ush Shahid et al. [49] exploited the advantage of peer-to-peer networks to remove fictitious content on social media. The proposed system is based on the Ethereum

Blockchain and its smart contract functionality. It employs a rating system to check the credibility of the data. Verification has two phases, i.e., first finding the date and position engendering the NFT, then rating. Riri Fitri Sari et al. [58] presented a social media scheme to diffuse news. It is adjusted via an epidemic approach and a scale-free network. They applied a message authentication structure to detect the constancy of content and its origins based on a blockchain implemented using Ethereum-based smart contracts. The efficacy of this system was examined by an operating agent-based display with NetLogo software. Franklin Tchakounté et al. [64] produced a system to anticipate fake content based on a smart contract. The authors utilize a smart contract to calculate a trust index based on the message and group structures such as chart density, rank, group grade, and adequacy. Following the rating based on the trust index, the message is either accepted or rejected. S. Phani Praveen et al. [67] introduced a scheme called PoT (proof of trustworthiness protocol) for distinguishing and blocking fake items and disinformation. An immutable list of the identified report that is cryptographically protected is apportioned as a distributed ledger among the peers. The chain code of protocol in charge of discovering fake items is distributed to all peers in the system. A smart contract is deployed to stock items in the blockchain. Sara Migliorini et al. [69] used Blockchain to design a technique to avoid fake check-ins in LBNSs (Location-Based Social Networks). The system initially employs Smart Contract to create a unique localization system. Paul et al. [72] applied an Ethereum smart contract and employed the BFS algorithm to count the closeness of a user. Adnan Qayyum et al. [79] presented Proof of Truthfulness (PoT), a blockchain-based model to warm against fictitious content. The model has three mechanisms, a publisher, management protocol, and a Smart contract for news, as well as a news blockchain. The items are saved in a Merkle tree. Steve Huckle et al. [85] designed a structure called Provenator. The system keeps the metadata to check the veracity and origin of materials and, at the same time, assures its validity for later. Provenator utilizes smart contracts to maintain the origin state of the data inside Blockchain.

Table 4. Proposed models for avoiding fake contents

Reference	Proposed Model
[46]	Blockchain and keyed watermarking-based framework
[47]	Architecture of blockchain-based fictitious detection system
[48]	Architecture to store validation records in the blockchain
[49]	Rating system to detect the authenticity of news
[50]	A secure and privacy-preserving method
[51]	A framework for safely sharing information at the peer level
[52]	Machine Learning-based model using Blockchain
[56]	AI with a Proof-of-Stake smart contract algorithm architecture
[57]	Blockchain with Text Mining (TM) algorithm
[58]	Social media news-spreading model
[61]	A blockchain and watermarking-based social media framework
[63]	TRUSTD, a blockchain and collective signature-based ecosystem
[64]	A smart contract-based technique to avert fake posts
[66]	WhistleBlower, a decentralized fake news detection platform
[67]	Proof of Trustworthiness (PoT)
[69]	Avoiding false check-ins in Location-Based Social Networks
[72]	Method using the concept of decentralization
[73]	A blockchain-based social media notarization method
[74]	A blockchain consensus called Proof of Credibility (PoC)
[75]	A public opinion communication model
[77]	Architecture using data mining as a consensus algorithm
[78]	A prototype to counter the dissemination of fake news
[79]	Proof of Truthfulness (PoT) for news verification
[85]	Provenator, a blockchain-based distributed application

Another component used by many papers is the consensus protocol. Sakshi Dhall et al. [46] recommended a framework for fixing the problem of bogus or malicious articles on social media through examining messaging structure. The structure is based on Blockchain and keyed watermarking. The study used a Hyperledger Fabric Blockchain and its consensus algorithm, Practical Byzantine Fault Tolerance (PBFT). This system enables checking the veracity and responsibility of published items. However, this model cannot handle the problem of a masquerade attack situation, such as spoofing another user's profile, and can be cracked. In addition, it cannot be used with social media messaging platforms due to its considerable operation ratio. Subhasis Thakur et al. [50] designed a decentralized structure to avoid social bots by deploying a public PoW-based blockchain. Users can create a decentralized architecture, providing them with a safe environment and protecting their privacy. However, only the data from a neighbor can be received. To avoid social bots impacting users by receiving and propagating a hoax, users can exclusively include the credible neighbors in their contact group. Muhammad Saad et al. [78] suggest a model to address the standing issue of fake news. In this direction, they evaluated data produced on social media and built a model to identify fake news that can be efficiently installed with negligible upkeep using Byzantine Fault Tolerance (BFT) consensus. Users are detached from the consensus layer. They can create chain code connections, although article services and social media sites are involved in the consensus and operation validation. Gyuwon Song et al. [73] introduced a proof-of-concept instant messaging scenario involving a blockchain-based notarization structure that can assuredly store the items. Mohamed Torky et al. [74] presented PoC (Proof of Credibility), a method using Blockchain to spot fake news and delay its proliferation in social networks.

Several researchers have integrated artificial intelligence and machine learning into their models. Narayanan et al. [47] proposed an approach for perceiving fake content on social media. The system detects the propagation channels in order to define the problem. The authors use emotive investigation to evaluate spam posts. The content in spam is categorized by applying naïve Bayesian classification. Akash Dnyandeo Waghmare et al. [52] suggested a machine learning-based model that distinguishes fake content by employing Blockchain. The procedures of supervised machine learning are set up to recognize the certainty of definite data, although the Blockchain retains the difficult task of dispersing fake content. A blockchain context is produced through mining, a smart contract, and a PoW (Proof of Work) consensus. Yang Zen et al. [56] designed a model to identify fake content and regulate fallacious propagation. The framework associates artificial intelligence and a Proof-of-Stake (PoS) smart contract algorithm for externalizing in order to attain better veracity than a system exclusively based on Artificial Intelligence. Lakshmi Kanthan, Gowri Ramachandran et al. [66] introduced Whistleblower, a model associating machine learning/artificial intelligence algorithms, Blockchain, a confirmable computation framework, and a token-curated registry. It involves fake news execution algorithms. This system is trained by data gathered from social media platforms associated with several inspection kits. Data and text mining were introduced in Blockchain to detect fake news by Alsaawy Yazed et al. [57], who introduced a scheme mixing blockchain and text-mining algorithms. They used a unique blockchain architecture to produce a lightweight chain and settle the step along with algorithm and procedural information to identify fake contents. Iago Sestrem Ochoa et al. [77] presented FakeChain, a consensus on the Blockchain-based data mining systems for authenticating exchanged items via social media and recognizing false info. Data mining was used as an algorithm to validate the posted items. This structure can recognize bogus articles, prevent users from posting them, penalize the authors of fake content, and compensate people who post accurate items.

There are several studies focusing on the decentralized aspects and connection between the nodes of Blockchain. Md Arquam et al. [51] suggest a model founded on the Blockchain that partitions data safely at the peer level. The guarantee is determined between sender and receiver by employing local and global trust. The local trust is exclusively between neighbors of a node, while the global trust is updated according to the nodes implicated

in the data dissemination, the category of the data circulated, and the node's integrity grade. The system can find the origins of information diffusion nodes with the help of the blockchain. Dwivedi et al. [61] introduced a blockchain-based social networking structure by applying a BDN (Blockchain Distributed Network). They deployed this BDN through bloXroute servers to obtain a scalable system. Zakwan Jaroucheh et al. [63] suggest TRUSTD, an environment permitting a user to evaluate an element's accuracy and reliability. Shovon Gengxin Sun et al. [75] proposed a public opinion dissemination system for a social network based on Blockchain. The procedure takes up the impact of the stimulant structure formed by sensibly measuring rate involvement on data proliferation such social networks and builds an income–risk matrix below diverse dissemination deeds.

(b) Protecting Data and Privacy

Social media are maintained and regulated by their administrators, not the users. The distributed feature of blockchains removes an individual group's regulation and hands total data management to the members. Decentralized consensus mechanisms, which are privacy protocols, thus offer a higher level of user privacy. The existing social media platforms have poor safekeeping, and users are vulnerable to attacks that are known to expose their individual information. Different studies have suggested several methods to address these issues (see Table 5).

Table 5. Proposed models for protecting data.

Reference	Proposed Model
[45]	Model based on security data storage
[53]	Solution to managing the privacy preferences of a user
[55]	Autonomous decentralized online social network architecture
[59]	Blockchain-based data mining methodology
[60]	A blockchain-based privacy-preserving framework (BPP)
[62]	An auditable and trustworthy access control structure
[65]	A hierarchical blockchain-based attribute matching system
[68]	BCOSN, a blockchain-based Online Social Network
[70]	A decentralized social networking architecture
[71]	A blockchain-based model for data storage
[76]	An autonomous resource request transaction framework
[80]	Blockchain-enhanced version of social networking (BEV-SNSs)
[81]	Blockchain-based identity providers
[82]	A decentralized social network based on Ethereum and IPFS
[83]	RPchain, a blockchain based academic social networking platform
[84]	A protocol and authentication with a blockchain algorithm
[86]	Ushare: a blockchain scheme for social networks

Similar to the models proposed for detecting fake content, the models proposed for protecting data use Blockchain-based elements such as smart contracts and consensus algorithms. Dawei Xu et al. [45] recommended a novel truthfulness information storing system, CL-BC (Clark—Wilson), which contains a theoretical strategy, initial setting architecture, and comprehensive flux architecture to construct the entree regulator structure of a distributed veracity information storing system and optimize the safety of risks such as over-agreement and illegitimate completion in the storing of information. Smart contracts are deployed to ensure the integrity of predefined rules. Gianluca Lax et al. [53] suggested a way to handle the privacy setup on which a smart contract is employed to authenticate the modification in order to prove that the request is coming from the owner. Ningyuan Chen et al. [55] suggested a blockchain application for use in OSN (online social networks). The safety of user data is preserved by averting the risk of data outflow from a centralized system. There is no risk of a centralized unit crashing the system as long as the system is decentralized. Xiaoqiang Jia et al. [59] introduced a data mining system for social media based on blockchain concepts. This system offers safety and data mining exactness. The hash function is applied to encode social media content in order to increase its safety.

Zhang Shiwen et al. [60] used blockchain and public key cryptography methods to create a blockchain-based structure to safeguard privacy called BPP. It can accomplish secure information sharing, information recovery, and obtain information reasonably and without concern over potential harm to clients' interests. Mohsin Ur Rahman et al. [62] presented a perceptible and reliable access control model employing an ACL (access control list) to outline confidentiality rules. The client operates with a public key to express adaptable entrance regulator rules utilizing ACL. However, a private key connected with the client's Ethereum profile is employed to decode the confidential information when access authorization is confirmed on the blockchain. Feihong Yang et al. [65] introduced a friend-matching architecture based on a hierarchical blockchain to guarantee the client's confidentiality. The model uses ciphertext-policy attribute-based (CP-ABE) encryption and bloom screen to help users find friends. Le Jiang et al. [68] proposed BCOSN, a blockchain-based architecture for a decentralized OSN (Online Social Network). It considers the blockchain as a reliable server to execute the services that are deployed by central servers in traditional systems. Shuai Zeng et al. [70] customized a sharding architecture to boost their model's scalability while using a blockchain model to guarantee the veracity and uniformity of content and a character-based authority control system to enhance the safety of the model. Yun Chen et al. [71] introduced DEPLEST, an algorithm for the protection of users. A user can coordinate a certain number of securitized materials after joining to the social network, with the number of items relying on the workstation's ability during the process. Ke Gu et al. [76] presented a resource request transaction structure allowing users to trade content among community members. Suppose a user wants to obtain articles from a community. In that case, the user could make a request of a group inside the community via blockchain during the time the members freely discuss the arrangement. The structure allows community groups to distribute articles via smart contract by offering a motivating network. Renita M. Murimi [80] introduced a system providing users with control of access to information and value creation via social network site dealings named BEV-SNS (blockchain-enhanced version of social networking sites). Karl Pinter et al. [81] utilized a blockchain-based identity approach to boost safety and availability, and proposed the blockchain to improve the safety and accessibility of e-government facilities such as e-ID. Validating a KYC (know your customer) operation on a blockchain can address the problem of an identity earner tracing the exchanges of an operator within the facility structure. By employing several character earners, the operator has the option of obstructing illicit tracing and describing any attempts. Quanqing Xu et al. [82] made a DAPP (decentralized application) on the Ethereum blockchain employing smart contracts and IPFS (Interplanetary File systems). The IPFS can help maintain a considerable quantity of items, decreasing the Ethereum storing constraint. Dong Qin et al. [83] introduced a blockchain-based academic social network system called RPchain with the goals of providing irreversible peer review archives, status tracking, and suitable drives for data storage. They suggested a new consensus algorithm, PoRe (proof of reputation), that uses the status of members for consensus. Ruiguo Yu et al. [84] presented a privacy-preserving algorithm to maintain the confidentiality of material. The model deployed a blockchain to conserve clients' public keys in the system. The utility of a public key is to help check the client's identity and block hostile incursions. Antorweep Chakravorty et al. [86] introduced Ushare, a user-centric blockchain-reinforced social media platform that allows clients to manage, track, and preserve all articles they exchange. This model contains four main mechanisms: a blockchain, a hash table with encoded data exchanged by a client, a Turing-complete connection system to manage the large amount of exchanges achieved by the client's friend group, and a local individual credential authority to handle the client's groups and encode content to be exchanged before it is disseminated inside the system.

(c) Protecting Data Privacy and Detecting Fake Contents

Tee Wee Jing et al. [54] introduced a trust index model to preserve data privacy and avoid bogus content and deepfakes. Their proposed system uses a blockchain to generate a new structure to find the origin of contents, identify deepfakes, and estimate creators'

integrity through a trust index. The decentralized privacy structure, consensus algorithm, and smart contract features of the blockchain are applied ro ensure the tamper-proofing, immutability, and traceability of content.

These contributions present several different models for resolving existing issues in social media using different characteristics of blockchains. However, many of these studies have limitations, for a wide variety of reasons. In the next section, we analyze these limitations.

6.1.2. The Existing Challenges and Limitations of Blockchain Application in Social Media

There are substantial difficulties with the implementation of blockchain technologies.

(a) The immutability of data can be a handicap

Applying blockchains in social media networks cannot ensure that racist, homophobic, or culturally harmful comments will not be distributed. Any data that is stored in the blockchain will be there indefinitely. It cannot be removed or modified. Consequently, if a racist or offensive post is created on social media, the created information will remain there forever. It is almost impossible to punish the original user through the social blockchain because tracking the original user is impossible. In addition, members or site owners cannot remove members' data, even on request.

(b) Scalability issues can make the platform slow

Blockchains are not as scalable as their centralized counterpart systems. The scale of blockchain-based social media is relatively small, and blockchain nodes cannot afford to expand and deal with large flows of material. A centralized social platform can quickly and easily access its user database. With a blockchain, it may not be as quick and easy. A blockchain system does not scale proficiently, and has low scalability with massive amounts of information. These deficiencies have led to various attempts to manage social media's cumulative capacity, information, and content.

(c) Energy Consumption Challenge

In its initial introduction with bitcoin, blockchain employed the Proof-of-Work consensus algorithm. PoW relies on miners to accomplish a task, and miners are rewarded for resolving, for instance, a difficult mathematical puzzle. These complicated mathematical puzzles are not suitable for use in the real world due to their enormous energy consumption. On every occasion, the ledger is updated by any new deal, and the miners are required to resolve any issues, signifying the expenditure of a considerable amount of energy.

An alternative to proof-of-work now being widely proposed is proof-of-stake. In this consensus mechanism, block validation is based on miners' stake. The miners earn a portion as compensation from the operation. A transaction proposing more significant compensation has a higher chance of being added quickly. This consensus mechanism does not consume as much energy as PoW consensus; however, it is more vulnerable as a hacker can return the transactions and bribe the miners to approve them.

(d) Political Obstacles

Handling political dissent, for instance, how to handle sensitive published content about public authorities, is a challenging task. When miners are institutionally constrained, they may well consider false propaganda that has been posted in aid of particular party to be true. As a result, it is tough to trace articles based on political ideologies by employing the Ethereum blockchain. Online services must face job risks when using factual authentication mechanisms, which may force them to compete for evaluations [33,52].

(e) Security of blockchains

Blockchains can be safer than other systems. However, this does not signify that they are entirely safe. There are diverse methods by which a blockchain can be discredited. The safety of the blockchain itself requires being afraid. If a large portion of computing power is localized inside a specific group, individuals can target the blockchain and blockchain implementations, which is frequently referred to as a 51% attack [48]. After a successful attack, the attackers can change the stored content and obtain access to the personal information of users.

(f) Newness of the system

The popularity of blockchain-based social platforms may only be realized in ten or twenty years, as the technology is not mature at present. It is impossible to transplant the whole system that has formed on the basis of the scale of centralized social media to a decentralized platform. The main difficulty lies in dealing with the technology itself. Blockchain networks need to solve several design issues before they will be able to replace centralized client–server systems.

6.1.3. Knowledge Gaps Which Future Research Can Address

Blockchain technology provides much potential, however, many aspects remain to be specified in order to solidify the approach to their implementation in social media. Topics such as user authentication, the scalability of blockchains, elimination of sensitive content, etc., are all under development. The following represent a selection of suggested further research areas.

(a) Using persistent identifiers for authentication

An identifier is a symbol used to categorize an object. It has various senses in different application situations and is used to specify a thing or a person in daily life. Certain identifiers are persistent (PID, persistent identifier); these include long-lasting references to a file, web page, or other digital objects. Most of them have a unique identifier related to the current address of the metadata or content. Currently, two varieties are frequently employed, those for things (journals, information, or software, such as URN, DOI, ARK, and Handle) and those for persons (academics, authors, or contributors, such as ORCID and ISNI). ORCID (Open Researcher and Contributor ID) is an international, interdisciplinary, and open non-profit organization established in 2010 to deliver services to stakeholders, including academics, research organizations, research funders, and publishers. The ORCID identifier is a unique personal persistent identifier that every researcher can have. Simply, users with this ID do not have to worry about anyone having a similar appellation. This can resolve the problem of duplicate names; for researchers, an ORCID ID is similar to the ID number for every citizen. Even if your name is the same as other researchers, your ID distinguishes your identity. As long as you use this ID to publish articles on the associated platforms, your articles can be searched through your unique ID.

One suggestion is to apply the concept of ORCID to all the users of social media. A PID can be associated with a social media blockchain to store and save data and make identification quick, easy, and permanent. All users can know exactly who has posted fake content after a post is complete. With the use of a blockchain, a consensus protocol-based responsibility can be designed to punish such posters automatically. A consensus-based decision made by the majority of users can be fixed. A user can be suspended or a set time, or excluded according to the violation after a vote of members. This represents an interesting future research area to explore.

(b) Resolving scalability challenges

A scalable blockchain is required for better use of blockchains in social media contexts. Efficient blockchain scalability approaches are needed, and scalability seems the most serious current obstacle to widespread implementation. Several possible methods are being explored to handle the problem of blockchain scalability. As blockchain technology is embraced and deployed in more diverse applications, its scalability will remain a source of attention in the coming years.

(c) Coupling Blockchain and Machine Learning/Deep Learning Technologies

Several studies presented here have briefly combined these fields. However, there are limitations, and more research can certainly be carried out combining blockchain with deep learning or machine learning, particularly for hate and sensitive word detection and elimination.

6.2. Limitations of This SLR

The limited literature available on this topic determines the main boundaries of this review on the use of blockchain technology in social media. Regarding this article, even though the search and screening process was carried out in great detail and included eight

significant databases, there is a possibility that works have been left out. The screening and selection processes inevitably carry with them a dose of subjectivity. Authors may be attracted to documents that support their theories, while rejecting those that do not (i.e., selection bias). In order to ensure that our review was as consistent as possible, we used numerous search terms and recovered items from several different sources.

7. Conclusions and Future Work

One of the most substantial changes in communication services in the 21st century has been the expansion of social media. These new communication channels have refined many of the contemporary world's most dominant instants and facts. Traditional social media services are entirely centralized. They hold all information, control customer navigation, and control anything on their networks. This has significant repercussions for confidentiality, restrictions, and regulation, and concerns about this and many other problems have prompted requests for networks to reform their functionality and service models. Furthermore, whether anything whatsoever results from these concerns, it will likely only occur much later. Many studies combining blockchain with social media are trying to fix the problems of privacy and safety alternatives in social media.

This paper presents a detailed review of the existing literature using a systematic literature review process; based on this context, the current state of blockchain applications in social media is discussed. Our research aims to analyze the different models proposed in this domain. We report on several different models and techniques. We found that the models proposed are based mainly on certain characteristics and components of blockchain technology, particularly smart contract, consensus mechanisms, and decentralization. We found several studies that combined Blockchain with artificial intelligence and machine learning. The two main issues drawing the attention of researchers were data privacy and fake news. Blockchain provides solutions to several challenges in social media; however, certain obstacles to this application, such as scalability and storage capacity, affect the ability of blockchain and social media applications to work together efficiently. More research must be completed in this domain in order to make these two technologies work efficiently together.

In our future work, we plan to test several existing consensus protocols for their use in social media. We will focus mainly on those alternative protocols mentioned in Section 2. Furthermore, we intend to combine Blockchain with persistent identifiers in social media.

Author Contributions: Conceptualization, M.A.H.; methodology, M.A.H. and D.C.; validation, D.C. and X.Y.; formal analysis, M.A.H., D.C. and X.Y.; investigation, M.A.H. and X.Y.; data curation, M.A.H., D.C. and X.Y.; writing—original draft preparation, M.A.H.; writing—review and editing, M.A.H., D.C. and X.Y.; supervision, D.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cheung, C.M.K.; Lee, M.K.O.; Wagner, C. Introduction to Social Media and E-Business Transformation Minitrack. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; IEEE Computer Society: Washington, DC, USA, 2016; p. 908. [CrossRef]
2. Abawajy, J.H.; Ninggal, M.I.H.; Herawan, T. Privacy Preserving Social Network Data Publication. *Commun. Surv. Tutor.* **2016**, *18*, 1974–1997. [CrossRef]
3. Guille, A.; Hacid, H.; Favre, C.; Zighed, D.A. Information Diffusion in Online Social Networks: A Survey. *SIGMOD Rec.* **2013**, *42*, 17–28. [CrossRef]

4. MIT. The Social Media Summit @ MIT (SMS@MIT) 2021—MIT Initiative on the Digital Economy. 2021. Available online: https://ide.mit.edu/events/the-social-media-summit-mit-smsmit/ (accessed on 17 April 2022).
5. Kayes, I.; Iamnitchi, A. Privacy and security in online social networks: A survey. *Online Soc. Netw. Media* **2017**, *3–4*, 1–21. [CrossRef]
6. Shu, K.; Sliva, A.; Wang, S.; Tang, J.; Liu, H. Fake News Detection on Social Media: A Data Mining Perspective. *SIGKDD Explor. Newsl.* **2017**, *19*, 22–36. [CrossRef]
7. Vosoughi, S.; Roy, D.; Aral, S. The spread of true and false news online. *Science* **2018**, *359*, 1146–1151. [CrossRef]
8. Guidi, B.; Michienzi, A. The Decentralization of Social Media through the Blockchain Technology. In Proceedings of the 13th ACM Web Science Conference 2021, Virtual Event, 21–25 June 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 138–139. [CrossRef]
9. Xu, X.; Weber, I.; Staples, M. Introduction. In *Architecture for Blockchain Applications*; Springer International Publishing: Cham, Switzerland, 2019; pp. 3–25. [CrossRef]
10. Staff, C. Blockchain Social Media and Crypto Social Media. 2022. Available online: https://www.gemini.com/cryptopedia/blockchain-social-media-decentralized-social-media (accessed on 14 June 2022).
11. Haimoud, E. Blockchain-Based Social Media Will Be More Secure. 2022. Available online: https://cisomag.eccouncil.org/blockchain-based-social-media/ (accessed on 13 June 2022).
12. Benshahar, A. 6 Ways the Blockchain Is Revitalizing Social Networking. CryptoPotato. 2021. Available online: https://cryptopotato.com/6-ways-blockchain-revitalizing-social-networking/ (accessed on 3 June 2022).
13. Poongodi, T.; Sujatha, R.; Sumathi, D.; Suresh, P.; Balamurugan, B. Blockchain in Social Networking. In *Cryptocurrencies and Blockchain Technology Applications*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2020; Chapter 4; pp. 55–76. [CrossRef]
14. Sharma, T.K. How Will Blockchain Revive Social Media? 2018. Available online: https://www.blockchain-council.org/blockchain/how-will-blockchain-revive-social-media/ (accessed on 11 June 2022).
15. Fraga-Lamas, P.; Fernández-Caramés, T. Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. *IT Prof.* **2020**, *22*, 53–59. [CrossRef]
16. Kathryn, H.; Amelia, L. How Blockchain Can Help Combat Disinformation. 2021. Available online: https://hbr.org/2021/07/how-blockchain-can-help-combat-disinformation (accessed on 9 June 2022).
17. Chakravarty, S.R.; Sarkar, P. *Introduction to Blockchain*; Emerald Publishing Limited: Bingley, UK, 2020; pp. 137–143. [CrossRef]
18. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564. [CrossRef]
19. Seebacher, S.; Schüritz, R. Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review. In *Proceedings of the Exploring Services Science*; Springer International Publishing: Cham, Switzerland, 2017; pp. 12–23. [CrossRef]
20. Tama, B.A.; Kweka, B.J.; Park, Y.; Rhee, K.H. A critical review of blockchain and its current applications. In Proceedings of the 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, Indonesia, 22–23 August 2017; pp. 109–113. [CrossRef]
21. Sharma, G.; Kumar, A.; Gill, S.S. Chapter 4—Applications of blockchain in automated heavy vehicles: Yesterday, today, and tomorrow. In *Autonomous and Connected Heavy Vehicle Technology*; Krishnamurthi, R., Kumar, A., Gill, S.S., Eds.; Intelligent Data-Centric Systems; Academic Press: Cambridge, MA, USA, 2022; pp. 81–93. [CrossRef]
22. Frankenfield, J. Distributed Applications (DApps). 2021. Available online: https://www.investopedia.com/terms/d/distributed-applications-apps.asp (accessed on 18 April 2022).
23. Kramer, M. What Are Consensus Protocols? A Super Speedy Guide. 2019. Available online: https://decrypt.co/resources/consensus-protocols-what-are-they-guide-how-to-explainer (accessed on 10 June 2022).
24. Kaur, S.; Chaturvedi, S.; Sharma, A.; Kar, J. A research survey on applications of consensus protocols in Blockchain. *Secur. Commun. Netw.* **2021**, *2021*, 1–22. [CrossRef]
25. Oyinloye, D.P.; Teh, J.S.; Jamil, N.; Alawida, M. Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry* **2021**, *13*, 1363. [CrossRef]
26. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain Smart Contracts: Applications, challenges, and future trends. *Peer-Peer Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef]
27. Korobeinikov, A. 9 Most Common Smart Contract Vulnerabilities Found by Blaize. 2022. Available online: https://blaize.tech/article-type/9-most-common-smart-contract-vulnerabilities-found-by-blaize/ (accessed on 19 April 2022).
28. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.B.D.; Xia, X.; Feng, Y.; Chen, Z.; Xu, B. Smart Contract Development: Challenges and Opportunities. *IEEE Trans. Softw. Eng.* **2021**, *47*, 2084–2106. [CrossRef]
29. Sharma, T.; Zhou, Z.; Miller, A.; Wang, Y. Exploring Security Practices of Smart Contract Developers. *arXiv* **2022**. [CrossRef]
30. Górski, T. Reconfigurable Smart Contracts for Renewable Energy Exchange with Re-Use of Verification Rules. *Appl. Sci.* **2022**, *12*, 5339. [CrossRef]
31. Shahin, M.; Ali Babar, M.; Zhu, L. Continuous Integration, Delivery and Deployment: A Systematic Review on Approaches, Tools, Challenges and Practices. *IEEE Access* **2017**, *5*, 3909–3943. [CrossRef]
32. Górski, T. Towards Continuous Deployment for Blockchain. *Appl. Sci.* **2021**, *11*, 1745. [CrossRef]

33. Ahmed, M.; Dar, M.; Tahir, R.M.; Masood, F. Impact of social media on academic: A quantitative study. In Proceedings of the 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 3–4 March 2018; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2018; pp. 1–5. [CrossRef]
34. Garima, K. Different Types of Social Media Networks 2022. Available online: https://www.digitalvidya.com/blog/types-of-social-media/ (accessed on 11 June 2022).
35. Synapse. What Are the Different Types of Social Media? 2022. Available online: https://synapsereality.io/what-are-the-different-types-of-social-media/ (accessed on 11 June 2022).
36. Team, I.E. 10 Types of Social Media to Promote Your Brand. 2021. Available online: https://www.indeed.com/career-advice/career-development/types-of-social-media (accessed on 15 June 2022).
37. Bishop, A. 13 Awesome Professional Networking Alternatives to Linkedin. 2019. Available online: https://www.searchenginejournal.com/linkedin-alternatives/297409/#close (accessed on 15 June 2022)
38. Alfred, L. 20 Top Social Media Sites to Consider for Your Brand. Available online: https://buffer.com/library/social-media-sites/ (accessed on 19 April 2022)
39. EES. Blockchain Based Social Media Platforms To Know—EES Corporation. 2022. Available online: https://www.eescorporation.com/blockchain-based-social-media/ (accessed on 19 April 2022).
40. SOCIETY2. SOCIETY2—Own Your Digital Life—Decentralized Social Media. Available online: https://society2.com/ (accessed on 22 April 2022).
41. Peepeth. Peepeth | Peepeth. Available online: https://peepeth.com/about (accessed on 20 April 2022).
42. Giffin, K. Should Social Media Be More Rewarding? Sapien Thinks So—UC Berkeley Sutardja Center. 2020. Available online: https://scet.berkeley.edu/sapien-network-rewards-you-for-using-social-media/ (accessed on 23 April 2022).
43. Bhattacharya, R.; White, M.; Beloff, N. An Exploration of Blockchain in Social Networking Applications. In *Proceedings of the Intelligent Computing*; Springer International Publishing: Cham, Switzerland, 2021; pp. 858–868. [CrossRef]
44. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, 89. [CrossRef]
45. Xu, D.; Wang, W.; Zhu, L.; Zhao, J.; Wu, F.; Gao, J. CL-BC: A Secure Data Storage Model for Social Networks. *Secur. Commun. Networks* **2022**, *2022*, 5428539 . [CrossRef]
46. Dhall, S.; Dwivedi, A.; Pal, S.; Srivastava, G. Blockchain-based Framework for Reducing Fake or Vicious News Spread on Social Media/Messaging Platforms. *ACM Trans. Asian-Low-Resour. Lang. Inf. Process.* **2022**, *21*, 1–33. [CrossRef]
47. Narayanan, L.K.; Muralidharan, R.R.A.; Sampathkumar, R.; Gururajan, I.; Subbiah, P. Blockchain Based Fictitious Detection in Social Media. In Proceedings of the 13th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2021), Online, 25–17 December 2021; Springer International Publishing: Cham, Switzerland, 2022; pp. 226–236. [CrossRef]
48. Koly, W.; Jamil, A.; Rahman, M.; Bhuiyan, H.; Bhuiyan, M.; Al Omar, A. Towards a Location-Aware Blockchain-Based Solution to Distinguish Fake News in Social Media. *Commun. Comput. Inf. Sci.* **2022**, *1557 CCIS*, 116–130. [CrossRef]
49. Ush Shahid, I.; Anjum, M.; Hossain Miah Shohan, M.; Tasnim, R.; Al-Amin, M. Authentic Facts: A Blockchain Based Solution for Reducing Fake News in Social Media. In Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications (ICBTA 2021), Xi'an, China, 17–19 December 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 121–127. [CrossRef]
50. Thakur, S.; Breslin, J. Rumour prevention in social networks with layer 2 blockchains. *Soc. Netw. Anal. Min.* **2021**, *11*, 104. [CrossRef]
51. Arquam, M.; Singh, A.; Sharma, R. A blockchain-based secured and trusted framework for information propagation on online social networks. *Soc. Netw. Anal. Min.* **2021**, *11*, 49. [CrossRef]
52. Waghmare, A.; Patnaik, G. Fake news detection of social media news in blockchain framework. *Indian J. Comput. Sci. Eng.* **2021**, *12*, 972–980. [CrossRef]
53. Lax, G.; Russo, A.; Fascì, L. A Blockchain-based approach for matching desired and real privacy settings of social network users. *Inf. Sci.* **2021**, *557*, 220–235. [CrossRef]
54. Jing, T.; Murugesan, R. Protecting Data Privacy and Prevent Fake News and Deepfakes in Social Media via Blockchain Technology. *Commun. Comput. Inf. Sci.* **2021**, *1347*, 674–684. [CrossRef]
55. Chen, N.; Cho, D.Y. A Blockchain based Autonomous Decentralized Online Social Network. In Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering, ICCECE 2021, Guangzhou, China, 15–17 January 2021; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2021; pp. 186–190. [CrossRef]
56. Yang Zen, T.; Hong, C.; Mohan, P.; Balachandran, V. ABC-Verify: AI-Blockchain Integrated Framework for Tweet Misinformation Detection. In Proceedings of the 2021 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2021, Singapore, 11–12 December 2021; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2021. [CrossRef]
57. Alsaawy, Y.; Sen, A.; Bahbouh, N.; Alkhodre, A.; Nadeem, A. Lightweight Chain For Detection Of Rumors And Fake News In Social Media. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 515–525. [CrossRef]
58. Sari, R.; Ilmananda, A.; Romano, D. Social trust-based blockchain-enabled social media news verification system. *J. Univers. Comput. Sci.* **2021**, *27*, 979–998. [CrossRef]
59. Jia, X. Construction of online social network data mining model based on blockchain. *Soft Comput.* **2021**. [CrossRef]

60. Zhang, S.; Yao, T.; Arthur Sandor, V.; Weng, T.H.; Liang, W.; Su, J. A novel blockchain-based privacy-preserving framework for online social networks. *Connect. Sci.* **2021**, *33*, 555–575. [CrossRef]
61. Dwivedi, A.; Singh, R.; Dhall, S.; Srivastava, G.; Pal, S. Tracing the source of fake news using a scalable blockchain distributed network. In Proceedings of the 2020 IEEE 17th International Conference on Mobile Ad Hoc and Smart Systems, MASS 2020, Delhi, India, 10–13 December 2020; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2020; pp. 38–43. [CrossRef]
62. Ur Rahman, M.; Guidi, B.; Baiardi, F. Blockchain-based access control management for Decentralized Online Social Networks. *J. Parallel Distrib. Comput.* **2020**, *144*, 41–54. [CrossRef]
63. Jaroucheh, Z.; Alissa, M.; Buchanan, W.J.; Liu, X. TRUSTD: Combat Fake Content using Blockchain and Collective Signature Technologies. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 1235–1240. [CrossRef]
64. Tchakounté, F.; Amadou Calvin, K.; Ari, A.; Fotsa Mbogne, D. A smart contract logic to reduce hoax propagation across social media. *J. King Saud Univ.-Comput. Inf. Sci.* **2020**. [CrossRef]
65. Yang, F.; Wang, Y.; Fu, C.; Hu, C.; Alrawais, A. An Efficient Blockchain-Based Bidirectional Friends Matching Scheme in Social Networks. *IEEE Access* **2020**, *8*, 150902–150913. [CrossRef]
66. Ramachandran, G.; Nemeth, D.; Neville, D.; Zhelezov, D.; Yalcin, A.; Fohrmann, O.; Krishnamachari, B. WhistleBlower: Towards A Decentralized and Open Platform for Spotting Fake News. In Proceedings of the 2020 IEEE International Conference on Blockchain, Blockchain 2020, Rhodes, Greece, 2–6 November 2020; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2020; pp. 154–161. [CrossRef]
67. Praveen, S.; Nguyen, H.; Swapna, D.; Rao, K.; Kumar, D. The efficient way to detect and stall fake articles in public media using the blockchain technique: Proof of trustworthiness. *Int. J. Emerg. Technol.* **2020**, *11*, 158–163.
68. Jiang, L.; Zhang, X. BCOSN: A Blockchain-Based Decentralized Online Social Network. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1454–1466. [CrossRef]
69. Migliorini, S.; Gambini, M.; Belussi, A. A Blockchain-based solution to fake check-ins in location-based social networks. In Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Analytics for Local Events and News, LENS 2019, Chicago, IL, USA, 5 November 2019; Association for Computing Machinery, Inc.: New York, NY, USA, 2019. [CrossRef]
70. Zeng, S.; Yuan, Y.; Wang, F.Y. A decentralized social networking architecture enhanced by blockchain. In Proceedings of the 2019 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2019, Zhengzhou, China, 11–13 October 2019; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019; pp. 269–273. [CrossRef]
71. Chen, Y.; Xie, H.; Lv, K.; Wei, S.; Hu, C. DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks. *Inf. Sci.* **2019**, *501*, 100–117. [CrossRef]
72. Paul, S.; Joy, J.I.; Sarker, S.; Shakib, A.A.H.; Ahmed, S.; Das, A.K. Fake News Detection in Social Media using Blockchain. In Proceedings of the 2019 7th International Conference on Smart Computing Communications (ICSCC), Miri, Malaysia, 28–30 June 2019; pp. 1–5. [CrossRef]
73. Song, G.; Kim, S.; Hwang, H.; Lee, K. Blockchain-based Notarization for Social Media. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 1–13 January 2019; pp. 1–2. [CrossRef]
74. Torky, M.; Nabil, E.; Said, W. Proof of credibility: A blockchain approach for detecting and blocking fake news in social networks. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 321–327. [CrossRef]
75. Sun, G.; Bin, S.; Jiang, M.; Cao, N.; Zheng, Z.; Zhao, H.; Wang, D.; Xu, L. Research on public opinion propagation model in social network based on blockchain. *Comput. Mater. Contin.* **2019**, *60*, 1015–1027. [CrossRef]
76. Gu, K.; Wang, L.; Jia, W. Autonomous Resource Request Transaction Framework Based on Blockchain in Social Network. *IEEE Access* **2019**, *7*, 43666–43678. [CrossRef]
77. Ochoa, I.S.; de Mello, G.; Silva, L.A.; Gomes, A.J.P.; Fernandes, A.M.R.; Leithardt, V.R.Q. FakeChain: A Blockchain Architecture to Ensure Trust in Social Media Networks. In *Proceedings of the Quality of Information and Communications Technology*; Springer International Publishing: Cham, Switzerland, 2019; pp. 105–118. [CrossRef]
78. Saad, M.; Ahmad, A.; Mohaisen, A. Fighting Fake News Propagation with Blockchains. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–4. [CrossRef]
79. Qayyum, A.; Qadir, J.; Janjua, M.; Sher, F. Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News. *IT Prof.* **2019**, *21*, 16–24. [CrossRef]
80. Murimi, R. A Blockchain Enhanced Framework for Social Networking. *Ledger* **2019**, *4*. [CrossRef]
81. Pinter, K.; Schmelz, D.; Lamber, R.; Strobl, S.; Grechenig, T. Towards a Multi-party, Blockchain-Based Identity Verification Solution to Implement Clear Name Laws for Online Media Platforms. In *Proceedings of the Business Process Management: Blockchain and Central and Eastern Europe Forum*; Springer International Publishing: Cham, Switzerland, 2019; pp. 151–165. [CrossRef]
82. Xu, Q.; Song, Z.; Mong Goh, R.S.; Li, Y. Building an Ethereum and IPFS-Based Decentralized Social Network System. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 1–6. [CrossRef]
83. Qin, D.; Wang, C.; Jiang, Y. RPchain: A Blockchain-Based Academic Social Networking Service for Credible Reputation Building. In Proceedings of the Blockchain—ICBC 2018, Seattle, WA, USA, 25–30 June 2018; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; pp. 183–198. [CrossRef]

84. Yu, R.; Wang, J.; Xu, T.; Gao, J.; An, Y.; Zhang, G.; Yu, M. Authentication with Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network. *IEEE Access* **2017**, *5*, 24944–24951. [CrossRef]
85. Huckle, S.; White, M. Fake News: A Technological Approach to Proving the Origins of Content, Using Blockchains. *Big Data* **2017**, *5*, 356–371. [CrossRef]
86. Chakravorty, A.; Rong, C. Ushare: User Controlled Social Media Based on Blockchain. In Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication, IMCOM 2017, Beppu, Japan, 5–7 January 2017; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]