applied sciences

MDPI

Article

Blockchain-Based Platform to Fight Disinformation Using Crowd Wisdom and Artificial Intelligence

Cristian Nicolae Buțincu * and Adrian Alexandrescu

Department of Computer Science and Engineering, Faculty of Automatic Control and Computer Engineering, Gheorghe Asachi Technical University of Iasi, 700050 Iasi, Romania; adrian.alexandrescu@academic.tuiasi.ro
* Correspondence: cristian-nicolae.butincu@academic.tuiasi.ro

Abstract: Disinformation and fake news are used by multiple actors to manipulate and influence the public with the purpose of gaining a series of advantages. This paper describes a promising solution to the increased spread of disinformation on the Internet. Our approach leverages blockchain technology combined with both crowd intelligence and federated artificial intelligence to develop efficient capabilities that address the disinformation phenomenon. The blockchain-based architecture of the platform creates a decentralized ecosystem that ensures transparency and trust, enabling the users to make correctly informed decisions in the face of disinformation. The key differentiating factor of the platform is the incorporation of both crowd and artificial intelligence in a system that can identify and respond to disinformation quickly and efficiently. The presented architecture can be used to build reactive and proactive platforms to effectively challenge disinformation.

Keywords: blockchain; fighting disinformation; crowd wisdom; artificial intelligence; governance protocol; cryptocurrency tokens

check for updates

Citation: Buțincu, C.N.; Alexandrescu, A. Blockchain-Based Platform to Fight Disinformation Using Crowd Wisdom and Artificial Intelligence. *Appl. Sci.* **2023**, *13*, 6088. https://doi.org/10.3390/app13106088

Academic Editor: Gianluca Lax

Received: 14 April 2023
Revised: 2 May 2023
Accepted: 11 May 2023
Published: 16 May 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Producing and publishing digital content on the Internet has become increasingly convenient and easy. Digital content (e.g., news, articles, images, videos) is being created and published at large scales today. Not only do humans are part of the information revolution, but also machines, AI (Artificial Intelligence) playing an important role in the generation of digital content. In this context, current and future generations will be overwhelmed with large amounts of digital content, impossible for the general user to sift through, analyze and consume. Therefore, information and information control are of paramount importance for a society and, as the future of almost everything is becoming more digital, information manipulation is becoming one of the most challenging aspects of the future.

Disinformation is becoming day by day more present at all levels of society, from the individual to the state. Now, the offensive in the information space is highly effective, cheap and difficult to counter. At the same time, defending against it is almost impossible, due to the huge flow of information that is generated on the Internet every day and the fact that social media algorithms are owned and controlled by companies rather than states. The reasoning for and the effects of disinformation vary, and mainstream media plays an important role [1]. Detecting disinformation is not trivial, but certain steps have been taken in order to fight this phenomenon [2].

Most of the population has no time nor the skills to check the authenticity of content published on news sites or social media platforms. Therefore, it has become essential to reach out the authenticity and truth behind the published information, i.e., where it has come from, who created it and its factuality.

Current fact-checking initiatives are small-scaled and human-led, which are prone to errors and interpretation. Having so many different fact-checking initiatives creates

confusion and huge duplication of work, which is not sustainable in the long run. Thus, even though the intention of fact-checkers is admirable it does not make them a viable solution to solve the issue of disinformation.

No technology can fully solve the challenges of establishing trust between people, nor eliminate the underlying motivations for profit and/or political gain that drive disinformation in the first place. This is why, to solve the problem of disinformation and fake news, society must fight back using various tools, ranging from technological tools (like blockchain [3] and AI [4]) to educational tools.

This paper describes a decentralized anti-disinformation platform for fact checking and trust assessment based on Blockchain, Crowd Wisdom and AI technologies.

At present, trust in mainstream media is lower than ever due to ever increasing disinformation levels and the amount of information that cannot be reliably checked. In the current media landscape, publications are driven by click-based ad revenue. To increase the number of views (and therefore to increase their income), publications tend to take journalistic shortcuts (like not thoroughly verifying the facts or presenting incomplete information just to be the first to announce some news). In this landscape, even reputable publications tend to favor engagement over clarity. This in turn impacts the readers' ability to distinguish the truth from disinformation and fake news.

A survey [5] regarding trust in the media (television, radio, written press, internet and social networks) was conducted in 2019 in all 28 EU countries. It was found that 41% of Europeans had medium trust in the media, 40% of the EU citizens had low or no trust in the media at all and only 19% of adults had high trust in the news media. So, the population in general is aware about the media quality and the spread of disinformation and fake news. That was in 2019 and since then, the sensitive geopolitical context further increased the spread of disinformation and fake news.

Because, in recent years, disinformation and misinformation spread increased to levels never seen before, the lack of trust in the media also increased in the general population. This affects all publishers, not only the ones responsible for spreading fake news. The lack of trust that consumes our society can be fixed by revealing, in a trusted way, what is true and what is not true. The platform described in this paper comes to address these issues, to expose disinformation and misinformation spread online by dishonest publishers and to finally restore trust to reputable publishers.

Currently, there are not enough platforms that can provide valuable and scalable fact-checking. This is in part because their operation is not sustainable for the long term, due to the dependency on paid human interaction.

Given the context, there is a real need for scalable and reliable tools that can be used at the level of society to fight against disinformation and fake news. In addition, when developing such tools, there are important questions to consider about who sets the standards, who is responsible for validation, and who manages the entire system. This is where blockchain technology comes into play since its decentralized nature can help address many of these concerns. Most importantly, it provides transparency since it eliminates the need for a single, trusted institution to make these decisions.

This paper describes the main drivers behind building such a platform, explores different solutions that try to solve the same problem and their drawbacks, and presents the overall architecture of the system.

The next section of the paper presents the current approaches to fighting disinformation and focuses on blockchain and smart contracts. The Related Work section of the paper describes the main approaches and the state of the art for blockchain-based solutions to fight disinformation, as well as their drawbacks and trade-offs. A detailed description of the proposed platform architecture is given in Section 4, which is divided into several subsections that discuss the general overview, blockchain and smart contracts, AI and human validators, system components, article extraction architecture, the platform protocol, the trust and security framework, and the provided APIs. In Section 5 we present some of the results obtained running the platform on a subset of publisher websites along with configu-

ration and runtime details. The paper ends with the conclusions section, where the main features of the platform are highlighted along with its current and future developments.

2. Background

2.1. Fighting Disinformation

In terms of fact-checking [6,7], there are a couple of current approaches to fighting disinformation, each with its own drawbacks:

1. Verification is performed by ***Professional Fact Checkers*** with accurate results following a standardized methodology for fact checking. This approach is time consuming, has little impact (since it is conducted most of the time in the "post-mortem" phase of the misinformation spreading) and it is very difficult to scale.
2. Verification is performed by non-professional communities—***Crowdsourced Fact Checking***, leveraging "cross wisdom" with no supporting tools. This approach has good potential to scale, but it is prone to becoming partisan or to be detoured. The level of impact is still low due to the "post-mortem" nature of the analysis.
3. Verification is conducted by software tools that utilize statistical algorithms mimicking the critical thinking process—***Non-assisted Automated Verification***. This approach has huge scaling and impact potential, but it cannot achieve the same level of accuracy as 1 and 2.

In the approaches mentioned above, the system must choose between scalability and accuracy. In any completely distributed system, consensus is considered one of the key properties when talking about a system that is considered reliable. The first blockchain has run on a public network since 2009 and opened the door to a new type of architecture, but at the same time, the technology offers just an infrastructure that must be combined with other techniques to offer solutions for today's problems.

The approaches for blockchain-based solutions to address the challenges of online disinformation are:

- ***Verifying provenance.*** This approach tracks and verifies the sources of online digital content. Examples of projects employing this approach are:
  - New York Times' News Provenance Project (https://newsprovenanceproject.com, accessed on 8 May 2023; https://www.nytimes.com/2020/07/06/insider/could-we-fight-misinformation-with-blockchain-technology.html, accessed on 8 May 2023)
  - Truepic (https://truepic.com/, accessed on 8 May 2023) notarizes content on the Bitcoin and Ethereum blockchains to establish a chain of custody from capture to storage
- ***Assessing identity and reputation.*** Blockchain-based solutions can track and verify the reputation of content creators in a transparent and decentralized way, thus eliminating the need for a trusted and centralized institution. Smart contracts built on blockchain offer the necessary mechanisms to achieve these goals.
- ***Incentivizing high quality content and content assessment.*** The blockchain generated cryptocurrency can be used to reward/penalize the actors that are responsible with trust assessment of both content and content creators. The trust score will be reflected upon content creators which will be incentivized to create high quality content. Pressland (https://pressland.com/, accessed on 5 August 2022) is another example of a system that stores online data on blockchain after it was analyzed using machine learning algorithms.

2.2. Blockchain and Smart Contracts

The blockchain technology was made popular by Bitcoin [8] and since then it was extensively adopted by the developer community into a broad range of different implementations such as Ethereum, Litecoin, Cardano, Tezos, and Solana, to name only a few. Instead of executing transactions through a centralized entity, transactions are executed by a net-

work of participants, mediated by smart contract programs. These smart contracts usually run using open-source software built and maintained by a community of developers.

The blockchain and smart contracts [9] technology enabled a wide range of applications in areas such as money transfer, cryptocurrencies [10], decentralized finance (DeFi) [11,12], Internet of Things (IoT) [13], Self-Sovereign Identity (SSI) [14], healthcare [15], logistics [16], Non-Fungible Tokens (NFTs) [17], government, media and so on.

The Blockchain and smart contracts technology enables the platform to inherently expose the following features:

- ***Zero downtime***—Since the smart contracts are deployed on the blockchain, the network will serve the clients. This also protects the platform from DDoS attacks.
- ***Privacy***—The access to the platform is guaranteed to be anonymous with no links to real world profiles.
- ***Resistance to censorship***—No single entity on the network can block users from interacting with the platform.
- ***Complete data integrity***—Data stored on the blockchain is immutable and indisputable; this is guaranteed by cryptographic primitives. Malicious actors cannot forge transactions or other data that has already been made public.
- ***Trustless computation and verifiable behavior***—Smart contracts can be analyzed and are guaranteed to be executed in predictable ways, without the need to trust a central authority.

Smart contracts are designed to be ***trustless***; this implies that the users don't have to trust third parties (developers, companies, or any other entities) to interact with a contract. By design, smart contracts are also ***immutable*** and cannot be altered; a contract will only execute the business logic defined in the code at the time of deployment.

Once the core of the platform is set on the blockchain, additional building blocks can come in place to provide a reliable and trusted anti-disinformation platform. These building blocks take the form specialized web crawlers and scrapers (distributed pieces of software fetching data from the Internet), Crowd Wisdom (human actors performing data analysis), and Artificial Intelligence Modules assembled into a federation.

3. Related Work

There is an increased scientific effort to develop new solutions based on blockchain that try to detect and fight against fake news. Many scientific papers that deal with different aspects of the fight against misinformation and disinformation were written.

In [18], the authors propose a blockchain platform focused on the "fact", where the news posted on the platform by news publishers will be analyzed by an AI component. This platform is similar to a social media platform where the content is generated and consumed within it. Having the content posted and reposted inside the platform, allows to easily track the source and the propagation path of the news.

Another solution is presented in [19], where the authors present an incentive-aware blockchain-based solution for internet of fake media things. The system architecture runs on a customized PoA (Proof-of-Authority) protocol. Here, news organizations must register to be able to publish news into the blockchain network, and the nodes, represented by news publishers, are also in charge of news validation.

The authors of [20] introduce a blockchain solution that uses a deep learning hybrid model to detect fake news. Their approach uses a pretrained GloVe (Global Vectors for Word Representation) embedding matrix for word embeddings. These embeddings are used as input for deep learning models to classify the news. The news is directly published into their system by reporters, analyzed by analyzers and validated by validators. There are three types of analyzers: deep learning, verified journalists and individuals.

In [21], the authors propose a combination of blockchain and machine learning techniques to detect fake news. They use NLP (Natural Language Processing) and reinforcement learning techniques and a customized blockchain consensus algorithm based on PoA protocol.

Another blockchain-based solution for fake news detection in social media is given in [22]. In this approach, the news is published into their system and random users are selected to act as validators. To select the users that are closer to the source of the news event, the system uses the BFS (Breadth First Search) algorithm to calculate the proximity of a user.

The authors of [23] propose a system where multiple news sources and social media platforms use the same blockchain to track how users share the news on their timeline. A modified version of a posted news can be easily tracked, flagged and removed from the system. However, this system assumes that the original published news is true and only detects if a user modifies the content on his timeline.

In another paper [24], the authors present a blockchain system featuring machine learning for mitigating the effects of fake news called Reliable News Sharing Platform. The news is published by publishers into the system. There are four entities involved in the system: reporters, machine learning analyzer, miners and readers. The system uses NLP and CNN (Convolutional Neural Networks) to analyze the news. The news articles are stored in the InterPlanetary File System (IPFS) and only a reference to IPFS id is stored on the blockchain.

A news verification blockchain system based on Ethereum and IPFS is presented in [25]. In this system, the journalists use a smart contract to publish news on the blockchain, after which they are validated by validators. The news content is stored on IPFS and the IPFS id is stored on blockchain, similar to the approach presented in [24].

In [26], a private blockchain and watermarking based social media framework is proposed to control the fake news propagation. In this system, users must register and provide their identity. The model focuses on identifying the source of news and verifies the fake news based on user reports.

Most solutions, which are trying to solve the problem of fake news, try to establish a news platform where publishers publish their news articles. The main problem with this approach is that it is extremely hard if not impossible to get all news agencies and publishers to use a particular platform. Another problem is that using only one approach for news analysis, AI or humans, is close to impossible to get things right in all cases.

4. Solution Description

This paper presents a way to fight disinformation using a coordinated approach between technologies and human intelligence in a unique way that will strengthen the defensive mechanisms against manipulated information and offers the reader an easy way to identify and verify the authenticity and factuality of the information. This solution enables building a system that counters disinformation using decentralized actors featuring AI, crowd wisdom, smart contracts and blockchain technologies.

The blockchain technology creates accountability and traceability. Artificial intelligence and human crowd wisdom help in detecting fake news. With the traceable, transparent and decentralized nature of the blockchain, it is possible to verify the authenticity of the information or its sources and build trust on the news available on the Internet.

The solution we are currently proposing consists of designing and deploying a scalable, decentralized anti-disinformation platform with the core of the platform built upon Blockchain technology and where verification is performed by Crowd Wisdom with support from Non-assisted Automated Verification through federated Artificial Intelligence modules.

Our proposal follows a similar approach to search engines and does not require news agencies and publishers to publish their news on a particular platform. Instead, a series of specialized web crawlers crawl their sites and index their content on blockchain. It is this blockchain stored content that is further verified for authenticity and trust using AI based algorithms and human crowd wisdom. This ensures that a large amount of content is verified and authenticated in a decentralized manner by the AI and human curators.

The platform will incentivize publishers to promote trustworthy content to reach a higher reputation score and increase the trust of their readers. The power of blockchain combined with crowd wisdom and AI will apply constant pressure on media outlets to scrutinize their content and promote trusted, high-quality content.

The platform architecture described in this paper stands at the core of the FiDisD project (https://www.trublo.eu/fidisd/, accessed on 8 May 2023). The FiDisD project provides an efficient and trusted solution to the problem of misinformation and disinformation by taking both a reactive and a proactive approach to effectively challenge the disinformation phenomenon.

4.1. General Overview

All the solutions proposed by various authors, which have been previously discussed, have some limitations. A major drawback is the fact that news publishers must use a particular platform to publish their news. This is the main reason why these solutions were not adopted by the mainstream. To address this problem, our solution does not impose a unique news platform. We let news agencies and publishers complete freedom as to where to publish their news and crawl their sites to fetch the news content into our blockchain-based system. Here, federated AI modules and crowd wisdom take over and analyze this content in a transparent and decentralized manner.

The system architecture described in this paper integrates the blockchain technology, artificial intelligence, human actors, off-chain distributed data storage and web crawlers. Online news from different agencies and news publisher sites are automatically fetched, aggregated and analyzed in parallel by federated AI modules and human validators. The end results are made available through a web portal where everyone can come and check the truth behind online news articles together with detailed analysis proofs.

Figure 1 presents the main features of overall architecture of the system.

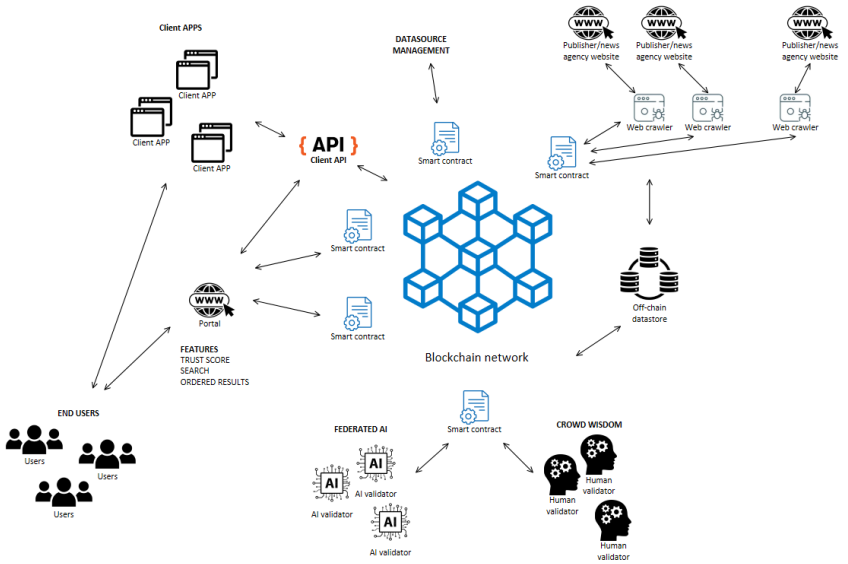

Figure 1. System Architecture Overview.

The main components are:

- the FiDisD blockchain network, which stores information regarding the news items from the off-chain datastore,
- the web crawlers, which include the web scrapers, which are used to extract the news articles from the publisher agencies,
- the datasource management, which is used to determine what article URLs are used by which web crawlers and what web scrapers extract the actual article information,
- the off-chain datastore, which stored the extracted article information,

- the federated AI and the crowd wisdom, which are used to validate the articles,
- the FiDisD portal application, which allows the users to view the extracted and validated articles,
- the client APIs, which can be used by third-party application to interrogate and obtain the information provided by the FiDisD solution.

Regarding the implementation of the conceptual architecture from Figure 1, for simplicity's sake, the datasource management, the communication with the off-chain datasource, and other business logic required for exposing the required APIs are all encapsulated in the Offchain Core component.

4.2. AI and Human Validators

The platform's architecture integrates a federated AI component that is formed by separated autonomous AI modules. These AI modules perform, in parallel, along with human actors, the analysis of the news and assign a trust score to each of them. Moreover, each of these modules can provide additional information as to why a certain trust score was given.

The platform is designed to support a plugin-like architecture while also exposing well defined interfaces, so that anyone can develop an AI module and register it in the platform. The AI modules are subject to reputation and incentivization/penalization schemes, such as human validator components.

An AI module usually employs a mix of NLP, Deep Learning and Neural Networks to extract the relevant entities from the news, to perform sentiment and bias analysis, to detect clickbait, to check for semantic similarities and to automatically classify the news items. A Cross-Lingual Semantic Textual Similarity can also be considered, which will allow the use pretrained models on multiple languages.

The platform combines the AI modules and the human validators effort through a recommender system that selects which news will be validated by humans. This system must consider at least the following three factors:

- Validator affinity: a human validator receives news on topics and areas that he is familiar with, based on previously validated news. This approach is similar to the behavior of classic recommender systems.
- Confidence scores of the AI validators: the fake news detection can be seen as a semi-supervised learning problem. Most news articles are unlabeled data, with few data being labeled by human validators. Uncertainty sampling will allow the recommender system to select the news for which the AI validators are least certain to be validated by humans.
- A random factor to reduce the assignments predictability and to prevent malicious actors from exploiting the system and to modify the verdict for certain news. An entity that spreads fake news might try to add bot-like human validators to our system to manipulate the news assessment.

4.3. System Components

4.3.1. Blockchain Network

This component provides a decentralized ledger used for the cryptographic proofs of system data: Crowd Wisdom and Federated AI modules score assessments, news timestamps and content proof hashes, user activity tracking (used to distribute token awards). The blockchain technology through its inherent decentralized nature provides transparency and eliminates the need for a single, trusted institution to make these decisions.

The blockchain network component stores transactions that indicate what news items are stored in the off-chain datastore and the identity of the entities that fetched the data. The blockchain stores cryptographic proofs of off-chain data to guarantee its validity and the fact that it was not tampered with.

4.3.2. Smart Contracts/Platform Protocol

Smart contracts record the validators activity (AI modules and crowd wisdom). These smart contracts encapsulate mathematical models for calculating trust scores for news articles and reputation scores for validators and publishers. The penalization and incentivization schemes are also implemented at this level.

This component comprises all smart contracts developed to provide a decentralized and verifiable business logic that resides at the core of the platform. End users through Portal, Crowd Wisdom, AI Modules, private and public client APIs, all interact with these smart contracts to create, read and update data into blockchain. Therefore, through blockchain cryptographic proofs, anyone can check the data validity and be assured that no one can manipulate this data except through clear and transparent access protocols.

These contracts form a decentralized protocol that gives its users access to a DAO-like (Decentralized Autonomous Organization) structure. A governance module together with governance and activity tokens, timelocks and access control primitives are used at the core of the protocol.

4.3.3. Web Crawler

The Web Crawler component has two subcomponents:

- Web Crawler;
- Web Scraper.

Both these components are completely distributed. The Web Crawler extracts the URLs from news publishers' web pages and compiles a list of URLs that identify news articles. This list is fed into the Web Scraper component.

Each news page is processed by multiple scrapers in such a way that they will not become blacklisted or banned from crawling on a particular website. This also guarantees that a particular news site serves the same content to its readers.

The Web Scraper component performs a targeted extraction from each news page depending on the extraction template for each news website. The extraction template contains the information of interest from a news webpage: article name, author, published date, referenced articles, and the news content in rich-text format (i.e., html with the associated multimedia content). For each considered website there is a predetermined extraction template with update triggers in place for the case in which the website's structure changes and the template is no longer applicable.

To prevent malicious actors from inserting invalid or altered data into our system, each site is crawled and scraped in parallel by multiple entities, and the majority gives the final data that will be recorded into our systems. All data transfers are cryptographically signed using public-key cryptography. Moreover, the platform incorporates an algorithm that deterministically allocates the resources to be fetched based on entities public keys and resource hashes.

4.3.4. Off-Chain Core

This component contains all business logic executed off-chain. It is responsible for providing public and private (internal) APIs to the other components. The storage off-chain core is datastore agnostic, meaning that any storage technology can be used without triggering modifications into the upper layers. The off-chain storage access is performed through the Data Persistence component (see Figure 2), that provides the data storage abstraction.

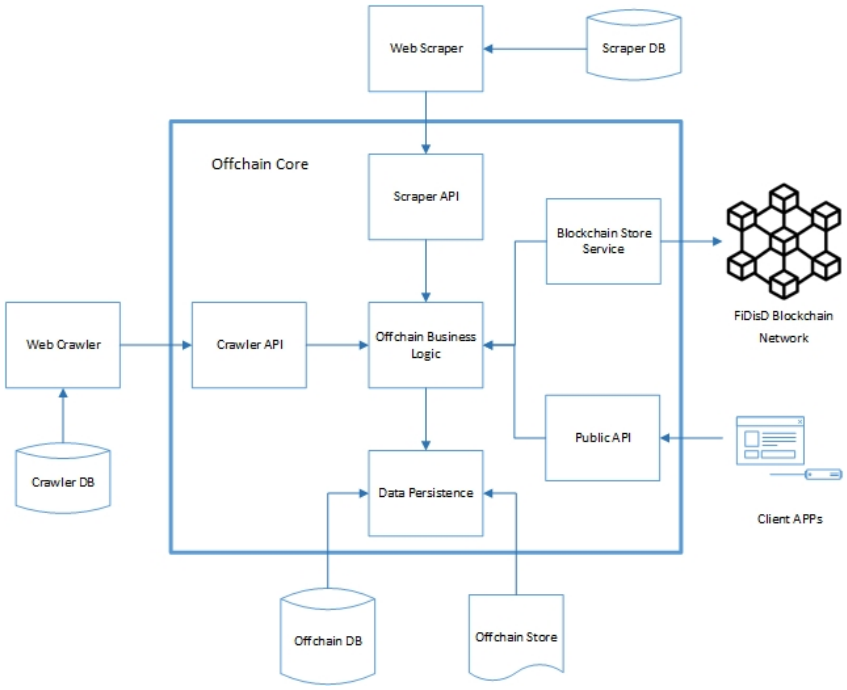

Figure 2. Article Extraction Architecture.

4.3.5. Off-Chain Datastore

This component provides off-chain storage. It is accessed by Off-chain Core component and, together with blockchain storage, stores all the data in the system. Curated data extracted from the distributed crawlers/scrapers is stored off-chain, in a separate distributed storage system; hashes of the data will be stored on-chain.

The off-chain datastore component persists a bundle (text and media resources) of the processed piece of news for each news URL; it also includes the list of crawler ids that processed that piece of news along with the corresponding hash. This component is distributed to ensure redundancy, scalability and a high degree of fault tolerance.

The component acts as a database for keeping track of stored and processed news items and integrates a distributed file system for storing the actual information and the multimedia content.

The interaction with the off-chain datastore is agnostic of any underlying storage implementation and it is performed via a facade API, which ensures the abstraction of the communication from the Web crawler component, the smart contracts from the Blockchain network, and the Client API. The implementation provides an interface to easily integrate different storage solutions in the off-chain datastore.

4.3.6. Federated AI

The Federated AI component employs validator modules based on artificial intelligence and machine learning techniques for determining the trust scores of news articles. The platform also provides an AI implementation to be used as a proof-of-concept/reference implementation.

The main job of an AI module is to analyze the news provided by the system. Similar to the Crowd Wisdom component, each AI module will assign a trust score to news articles and will participate in activity tokens rewards. This way, AI module development entities will be encouraged to join our ecosystem and will further expand the platform AI capabilities.

Any AI module that performs information analysis can be integrated with the platform, using the provided API. We expect that a 3rd party AI module to contain some form of Natural Language Processing based on Deep Learning and Neural Networks to extract

the relevant entities from the news, check pieces of text for semantic similarities, and automatically classify the news items.

The service provided by this component may also be used by the Crowd Wisdom (i.e., human validators) to help them assess the trust scores.

4.3.7. Crowd Wisdom

The Crowd Wisdom component is the other validator component on the blockchain system. Together with the Federated AI component, it forms the overall validator logic. This component is composed of human entities and any person is free to join this system to provide insights regarding the truthfulness behind news articles. For analysis, it may leverage the insights from AI components.

Like AI modules, each human actor analyzes the news and provides a trust score, participating in activity token rewards. This way, more human participants are incentivized to join our system and will further expand the platform analysis capabilities.

To prevent malicious human validators to defraud voting on different news articles, the system uses an algorithm that deterministically allocates human validators to news articles based on human validator public keys and news articles hashes.

The system also tracks the reputation scores of Crowd Wisdom entities and AI modules. This reputation impacts the voting on the news. In addition, with the integrated reward and penalization schemes, the validator components are incentivized to provide objective analysis on news articles.

4.3.8. Client API

The Client API offers integrated access to the system based on access permissions. Software developers can develop 3rd party applications that integrate with the system using this API.

Parts of this component are also used by the Web Crawler component to trigger storing data in the off-chain datastore and storing the news URLs, crawler ids and the hashes in the blockchain network.

The Portal uses the exposed services from the Client API to show end-users the news with their trust scores.

4.3.9. Portal

This component represents the front-end of the platform in the form of a publicly accessible web portal. Here, any user can access the news and the original source, check the trust scores of news articles from both Crowd Wisdom and Federated AI modules and inspect the distribution of scores.

Searches can be performed based on the identified news categories and keywords, and the search result order is tailored to favor high trust articles. The users are also presented with the reasoning of why a particular trust score was given.

4.4. Article Extraction Architecture

One of the main elements of the FiDisD solution is the article extraction architecture, which includes three main components: Web Crawler, Web Scraper and Offchain Core (Figure 2). Multiple web crawlers and web scrapers are employed to identify and extract the article information from various news websites, while the Offchain Core gathers and manages that data.

The role of the Web Crawler is to go through each page of specific websites, identify if the page represents an article and extract all the URLs. The website seed list is obtained from the Offchain Core component. Each Web Crawler has an associated account (i.e., username and password), which is used to authenticate to the Offchain Core. As the crawling is performed, the URLs that are identified as containing article information are sent to the Offchain Core.

Actual article extraction is performed by the Web Scrapers, which extract article information from the pages that were identified by the Web Crawlers. That data is then sent to the Offchain Core together with a hash on the extracted contents; the latter, gets put on the blockchain to ensure trust.

The considered news websites from which to extract information are managed by the Offchain Core. The bootstrap process of the components involves reading the website seed list and the corresponding extraction templates. These are stored on the Offchain Database by the Data Persistence module. Another aspect of bootstrapping is populating the database with the users that are allowed to crawl and scrap the websites.

In order to ensure trust in the system, multiple crawlers and scrapers process the same information. That data together with hash used to check the data integrity are sent to the Offchain Core, which, in turn, stores the information in the database. As soon as a large enough number of crawlers/scrapers obtain the same information then consensus is achieved. At this point, the hash on the article content is stored in the blockchain (by means of the Blockchain Store Service) and a status field is marked accordingly in the database to signify that the article data is available to be retrieved by external Public API clients.

4.5. The Platform Decentralized Protocol

The platform protocol is a decentralized news trust assessment protocol running on blockchain. At its core, it is composed of a series of smart contracts for decentralized governance (voting, proposals, executions), access control, time locks, token contracts for governance and activity tokens, news article score assessment.

4.5.1. Tokens

The protocol uses two types of tokens:

- a governance token, used by community to control the future direction of the project;
- an anti-disinformation activity token, minted and rewarded to users for their work in news analysis.

In general, governance tokens are minted and distributed to the community either via an airdrop to all users that interacted with the platform (according to a predefined release schedule) or via token exchanges (a user might trade his accumulated activity tokens to governance tokens), or a combination of both. The governance token serves the purpose of enabling shared community ownership in the growth and future development of the protocol. This will allow governance token holders to participate in the governance of the protocol in a neutral and trustless manner. As the platform adoption increases, it will positively impact the governance token value and will further incentivize token holders to contribute to the self-sustaining development of the platform.

4.5.2. On-Chain Governance

The protocol is governed and upgraded by governance token holders, using three distinct components implemented as smart contracts: the governance token, a governance module, and a timelock. Taken together, these contracts will allow the community to propose, vote, and implement changes to the protocol.

In general, a good governance design enables the core development team to eventually step out of the decision-making process entirely, achieving a truly self-sustaining and completely decentralized protocol.

The governance token acts to secure the future development of the platform, creating a decentralized voting system that ensures bad actors cannot propose and force development upgrades that may damage the reputation and security of the platform.

In addition, the governance protocol allows governance token holders to delegate their voting power. Users can also choose to delegate themselves.

4.5.3. Access Control

Access control is extremely important in the world of smart contracts. The access control of a contract may govern who can mint or burn tokens, who can vote, cancel or execute proposals or freeze transfers, and many other things.

The most common and basic form of access control is the concept of ownership: an account is the owner of a contract and can perform administrative tasks on it. This approach is best suited for contracts that have a single administrative user.

4.5.4. Role-Based Access Control

While the simplicity of ownership can be useful for simple systems or quick prototyping, different levels of authorization are often needed. Role-Based Access Control offers this kind of flexibility. Under this paradigm, one defines multiple roles, each allowed to perform a different set of actions.

4.5.5. Delayed Operation

Access control is essential to prevent unauthorized access. However, it does not address the issue of a malicious user with administrator rights to attack the system to the prejudice of the other users. This issue is addressed by timelocks.

A timelock acts as a proxy that is governed by proposers and executors. When set as the owner of a smart contract, it ensures that any operation ordered by the proposers will be delayed a certain amount of time. Thus, the users of the smart contract are protected by giving them enough time to review the proposed changes and exit the system before these changes take effect if they consider so.

4.6. Trust and Security Framework

In the process of designing a solid Trust and Security Framework we have integrated into the system the following aspects.

4.6.1. Decentralized Autonomous Organization (DAO)

The underlying principle of the platform is decentralization and transparency thus the implementation of DAO is at the core of our architectural design. DAO is implemented through a series of smart contracts that form the backbone of the whole system. To participate in the platform protocol, members need to hold governance tokens that will enable them to be part of the decision-making process and the future evolution of the project.

On-chain governance refers to a kind of governance where the rules for making changes are encoded into the blockchain protocol. In this system, smart contracts play a fundamental role in executing collective decisions taken through a voting mechanism.

On-chain governance operates in an autonomous and transparent way, and all changes are recorded on the blockchain and are accessible to anyone.

Community members of a DAO can collectively make decisions about the future directions of the project, such as technical updates and token allocation directives, to name only a few. The governance allows members to make proposals and to vote on them. If a proposal passes the voting phase, then it will be executed. Therefore, each member of the DAO can influence the future of the project regardless of his identity.

Power in such systems is fluid as actors can form alliances or delegate their votes, depending on the issues that are at stake. Participants in on-chain governance are free to make decisions according to their best interests that also coincide with the best interest of the protocol itself, since they need to be token holders to be able to participate.

In a DAO, members are also incentivized to be active participants, because the final decisions will affect them and their resources directly. Moreover, on-chain governance is performed by voting through governance tokens, and incentives for engaging in the voting process are usually offered to encourage user participation. As opposed to traditional voting, on-chain voting successfully addresses some of its challenges such as lack of

accountability, low transparency and external influence. Since everything is recorded on a blockchain and is openly available, external influence is very difficult.

The key advantages of on-chain governance:

- security provided by blockchain technology: the smart contracts run on a distributed network with thousands of computers that reach consensus, therefore altering the voting results, a huge amount of processing power is required (at least 50% of the entire network), not to mention that the community can fight back and with the help of honest miners can revert the attack. Moreover, the costs to conduct such an attack usually greatly exceeds the benefits;
- the decision-making approach is effective and decentralized because it is achieved through the community and it is not influenced by a single entity;
- maximum transparency because everyone can look at the code and see how the majority is established and how the decisions are made and executed.

4.6.2. Dynamic Validator Sets

Once a news article is fetched into the system by web scrapers, a series of blockchain accounts will be selected to be eligible for its trust assessment. This selection is performed by a specially devised algorithm that selects accounts based on their public keys and the news article hash. This approach will generate dynamic validator sets for each news article to be assessed. This way, we protect the system against a malicious attack that can use a large number of accounts to bias the final trust scores assigned to articles, since only a subset of accounts that match the selection scheme will be eligible for assessment.

The dynamic validator sets will change the validator sets constantly and randomly reducing the risk of centralization. Slashing is a set of techniques which incentivize actors to act honestly through the obligation to put some of their stake as collateral and enforce the threat of slashing their stake if they are proven to act maliciously and not follow the protocol. The threat of losing a significant part of their stake will incentivize users to act correctly.

4.6.3. Dishonest Behavior

Malicious actors that gain in spreading disinformation might try to attack and defraud the news article assessment system of the platform protocol by using multiple blockchain accounts that assign high trust scores on articles that contain disinformation. To address this aspect, the system implements dynamic validator sets so that the probability of forming a majority around a particular news article is extremely low. Moreover, each eligible selected account that enters the new article assessment procedure stakes tokens as collateral. All tokens from participating accounts are locked into an article assessment pool, until the assessment period ends. Once the assessment period ends, the tokens from the pool are redistributed among participants based on their assessments. Therefore, malicious voters, that will likely be on the minority side, will lose tokens in favor of the accounts whose assessment is clustered near a particular trust score. This in turn acts as a big deterrent to dishonest behavior.

4.6.4. Reputation System

By putting in place a reputation system, the platform protocol makes sure that its members are held responsible for their actions and that malicious users are reduced to insignificance. The voting power of users that consistently vote erroneously will decrease, while the voting power of the users that make correct assessments will increase over time. Activity tokens are rewarded for correct assessments. These tokens can be later transformed into governance tokens of the platform protocol. A smart contract incorporates the logic of tracking user reputation over time and distributes the activity tokens rewards or applies penalties.

The platform protocol, as it was designed, is expected to withstand the attacks from malicious individual or collective actors while also inflicting damage upon them by making them lose their tokens.

4.6.5. Governance Tokens and Quadratic Voting

The platform protocol governance features a token based voting system to ensure that major platform decisions are taken by the community. A scheme of governance tokens or activity tokens offering will favor the users that reach higher reputation levels. The governance token represents the users' ownership and stake in the platform protocol. A voting system based on Quadratic Voting [27,28] ensures that the cost to cast additional votes grows quadratically, while the number of the cast votes grows linearly. This in turn prevents a Sybil attack or 51% attack, where malicious actors try to gain control over the governance tokens to make changes in the platform's underlying architecture.

4.6.6. Randomized Voting System

After reaching a significant user base, a randomized voting system is planned to be employed. This system will assign voting rights on a specific article to several random accounts, taking into consideration aspects such as geographical location for specific news articles. Together with the aforementioned dynamic validator sets, this approach will significantly reduce the risk of vote manipulation, ensuring that only a percentage of the user base has voting rights on a specific news article, being randomly enforced each time a new news article arrives into the system.

4.6.7. DDoS (Distributed Denial of Service) Protection

Blockchain technology is inherently decentralized. Thousands of nodes participate in the network and a successful DDoS attack would mean a successful attack on all of them. Therefore, the blockchain component of the system is protected against DDoS attacks.

The only components exposed to the exterior are the front-end servers that provide the web portal application and client APIs accessible to anyone who wishes to integrate with the system. In the discussed system architecture, these front-end components are designed to be horizontally scalable, meaning that a successful DDoS attack would have to bring down all front-end servers.

4.7. APIs

4.7.1. Authentication API

The Offchain Core exposes an authentication API, which is used to obtain access to the other APIs, depending of the actor's role: Crawler API, Scraper API and Public API.

The role of this module is to provide authentication and authorization of the identified actors (i.e., crawler, scraper and public). The exposed API routes are shown in Table 1. The response status for invalid username-password pairs or for an invalid JWT is 401 Unauthorized. Unless otherwise specified, the response status for a proper request is 200 OK.

4.7.2. Crawler API

The role of this module is to provide the web crawler instances the seed data required to know which sites to crawl and to provide the means for the web crawlers to send the acquired and identified URLs to the Offchain Core. The web services that are exposed to the crawler instances are presented in Table 2.

4.7.3. Scraper API

The role of the Scraper module is to provide the web scraper instances the article URLs required to know from which to extract information, the extraction templates, and to provide the means for the web scrapers to send the extracted article information to the

Offchain Core. The web services that are exposed to the scraper instances are shown in Table 3.

Table 1. Authentication API routes.

URL Path	Method	Description
/api/auth/signin	POST	Receives two parameters (username and password) and returns a JWT with the user roles Request payload: username: string, password: string Response payload: JWT object
/api/auth/signup	POST	Receives three parameters (username, password and email) and creates a new user with the PUBLIC role Request payload: username: string, password: string, email: string Response status-payload: 201 Created or 409 Conflict—Username already exists

Table 2. Crawler API routes.

URL	Method	Description
/api/crawler/sites	GET	Returns the list of sites that have to be crawled by the user identified in the JWT used for authorization. Request payload: - Response payload: [{ siteName: string, urlBase: string, pageTypeClassifier: jsonString }, . . .]
/api/crawler/pages	POST	Receives a list of page URLs representing articles, which were identified by the crawler. The article list is associated to the user identified in the JWT used for authorization. The user can only send page URLs from the sites it was previously assigned to. Request payload: { siteName: string, pages: [urlString1, . . .] } Response payload: -

Table 3. Scraper API routes.

URL Path	Method	Description
/api/scraper/ extractor-templates	GET	Returns the list of extractor templates used to extract information from article URLs. Request payload: - Response payload: [siteName: string, templateVersion: versionNumber, removeElements: stringArray, title: stringArray, contents: stringArray, featuredImage: stringArray, publishDate: stringArray, author: stringArray , . . .]
/api/scraper/ article-urls? page=pageNumber &size=pageSize	GET	Returns the list of URLs representing articles that have to be scraped by the user identified in the JWT used for authorization. The list of URLs is organized by site and templateVersion, and are returned paginated; each page is identified by pageNumber and contains pageSize article URLs. Request payload: - Response payload: [siteName: string, templateVersion: versionNumber, urls: [urlString1, . . .] , . . .]
/api/scraper/articles	POST	Receives a list of objects representing article extracted information. The article information is associated to the user identified in the JWT used for authorization. Request payload: [siteName: string, articles: [url: string, title: string, contents: string, featuredImage: base64String, publishDate: string, author: string, extractedDate: string , . . .] , . . .] Response payload: -

4.7.4. Public API

Access to the stored articles is provided by the Public API module. It can be used by any entity to obtain article information, i.e., title, author, publish date, extracted date, publisher, featured image, contents. It is mainly used by the application frontend and the web services that are exposed are shown in Table 4.

Table 4. Public API routes.

URL Path	Method	Description
/api/public/articles	GET	Returns a paginated and filtered list of articles. Request payload: it allows the following query params: pageNumber, pageSize, publisher, start date, end date, title, author, and order by date. Response payload: [id: number, title: string, lastUpdated: string, extractedDate: string, publishDate: string, publisher: string, author: string, url: string, contentsHash: string , . . .]
/api/public/articles/{article-id}	GET	Returns information regarding the requested article-id. Request payload: - Response payload: single article information similar to the previous web service.
/api/public/articles/{article-id}/featured-image	GET	Returns the featured image. Request payload: - Response payload: byte array containing the featured image.
/api/public/articles/{article-id}/contents	GET	Returns the article contents with the HTML tags stripped. Request payload: - Response payload: Text representing the article contents.
/api/public/articles/{article-id}/contents-full	GET	Returns the article contents, including the HTML tags. Request payload: - Response payload: Text representing the article contents.

5. Use-Case Validation

5.1. Configuration of the Article Extraction Components

The Offchain Core is configured to handle seven news websites. For each website specific information is required in order to perform the URL and article extraction. This information is stored in JSON format with the following properties:

- name—news website name, which must be unique,
- urlBase—website base URL address,
- logoUrl—URL of the news outlet's logo,
- pageTypeClassifier—JSON object which contains information that differentiate article pages from other, irrelevant, pages from the website; it has two object arrays:
  - containsList—array with strings that are present in article web pages,
  - containsNotList—array with strings that must not be present in order to identify a page to be an article,
- extractorTemplate—CSS selectors and other metadata are used to identify the various properties that need to be extracted from an article page; all the JSON property values are in array format—the first string represents the selector and other optional strings represent from where the identified element(s) the information must be extracted:
  - removeElements—contents that must be removed from the extracted data,
  - title—article title,
  - contents—article contents,
  - featuredImage—URL location of the main image associated with the article,
  - publishDate—publish date as it appears on the article web page (if any),
  - author—author name or URL as it appears on the article web page (if any).

Both the crawler and the scraper are configured with the credentials to access the Crawler API and Scraper API, respectively, from the Offchain Core. Other configurations include access to the local database for each crawler/scraper and logging configurations.

In terms of actual gathering information from the news websites, the following parameters and corresponding values were used for each crawler/scraper instance:

- minimum waiting time between crawls from the same site (in milliseconds): 1800,
- maximum waiting time between crawls from the same site (in milliseconds): 2700,
- number of crawler instances running at the same time: 1
- recrawl type—can be interval (recrawlInterval is used) or time (recrawlTime is used): interval,
- recrawl time interval (in ISO 8601 format for durations): PT0H20M,
- recrawl time of day (in HH:mm:ss format for time): 08:00:00,
- recrawl time of day delta (in ISO 8601 format for durations); recrawl will occur at recrawlTime/recrawlInterval +/− rand(recrawlTimeDelta), depending on recrawlType: PT1H.

Those parameters were used so not to stress the news web servers with concurrent or many consecutive requests, and so not to get the crawler's/scraper's IP address blacklisted. Using the aforementioned configuration, the time between crawls is a random value between 1.8 and 2.7 s. In addition, the recrawl is triggered at a somewhat random time each day.

5.2. Extracted Articles

In order to demonstrate the efficiency of the proposed solution, seven news websites were crawled and scraped. Table 5 shows each news website, the total number of pages processed from each website, the number of extracted articles, and the percentage of pages representing articles compared to the total number of processed pages.

Table 5. Number of crawled pages and extracted articles for each considered news website.

Site Name	Site URL	Number of Pages	Number of Articles	Article Percentage
Adevarul	https://adevarul.ro	2516	482	19%
AgerPres	https://www.agerpres.ro	2636	490	19%
DCNews	https://www.dcnews.ro	1649	1302	79%
Digi24	https://www.digi24.ro	2695	2245	83%
G4Media	https://www.g4media.ro	2745	2391	87%
Hotnews	https://www.hotnews.ro	3521	1626	46%
Stiripesurse	https://www.stiripesurse.ro	1468	860	59%

The difference between the percentages among the considered websites is due to the fact that some of the websites had malformed URLs (especially representing email addresses or telephone numbers) or has more pages containing snippets of multiple articles on the same page. The information from these latter pages was ignored. Information regarding the 9.396 extracted articles can be obtained using the Public API.

5.3. Results Validation

News articles are extracted, stored in the Offchain Core, and validated by the federated AI and crowd wisdom. For each article, the Offchain Core calls an exposed service from the FiDisD Blockchain network, and sends the hash string obtained by applying the SHA3-256 algorithm on the article contents. The contents hash is stored on the blockchain network for later verification and in order to ensure trust in the system.

Validation of the results is obtained by the Frontend application, which is basically an aggregator portal that presents articles from those seven news websites. The Frontend application uses the Public API from the Offchain Core, which allows filtering and paginating the article list. Each piece of news shown contains the extracted article information and the

article score, which is stored on the blockchain. Anyone can validate the accuracy of the stored data by accessing the transactions that are stored on the blockchain network.

6. Discussion

There has been much innovation on the offensive side of threat actors, yet the defensive side is still lacking the innovation force to properly respond to these kinds of threats. This represents a key reason of why innovation is required in this space, and the platform proposed in this paper represents a powerful alternative to what is available on the fact-checking space, a rather reactive approach that does not have sufficient backbone to scale and effectively counteract the disinformation phenomenon.

The complex information environment that is aggressively developing in the digital ecosystem is threatening the way information is perceived. With high amounts of disinformation being spread on the Internet, AI-generated content that has the capacity to sky-rocket disinformation, and a diverse range of threat actors, humanity's access to information is threatened like never before. Not long from now, every piece of information on the Internet will be questioned because people will soon realize that it is no longer possible to separate truth from fiction. In this context, the platform described in this paper is set to fight disinformation using a coordinated approach between technologies and human intelligence in a unique way that will strengthen the defensive mechanisms against manipulated information and will offer the reader an easy way to identify and verify the authenticity of information.

In current stages, the anti-disinformation market is immature. The majority of the fact-checking initiatives are entirely dependent on funding, not being sustainable in the long-term, and also lacking scaling capability. There has not been any initiative that can be pinpointed as an important effect in effectively combating disinformation at scale, so the proposed system architecture can open the way for true scalable, decentralized and trusted platforms that can be used by all members of a society. Currently, there are no scalable and trusted solutions that can assess online information, and centralized solutions have the drawback of being controlled by a small number of entities that might influence the overall analysis. Therefore, our solution that uses decentralized blockchain technologies and a combination of human and artificial intelligence would naturally appeal to all the members of society that want to check the trust of online information.

Our system does not require publishers and news agencies to publish their news on a dedicated platform. Instead, our approach is to let the sites retain their identity and fetch their content using web crawlers that analyze and index the content on blockchain (proof of data) and off-chain (data). This content is further verified for authenticity and trust using AI based algorithms and human crowd wisdom.

The platform intends to help regular users to check the information available on the Internet, providing them with the necessary tools to verify the main triggers of disinformation and give a vote of confidence to the information they consider trustworthy. The platform aims to rally a fact-checking community where all the information can be aggregated and checked by human actors and AI modules. This will ensure an efficient alignment of fact-checking efforts and will allow people from all over the world to engage in the voting process, thus validating content that can be trusted in a truly decentralized fashion.

7. Conclusions

This paper describes a scalable system that can counter online disinformation using decentralized actors featuring artificial intelligence, crowd wisdom, smart contracts and blockchain technologies. The proposed solution uses distributed crawlers and scrapers to extract articles from news websites, federated AI and crowd wisdom to validate the information, and the blockchain network to ensure trust in the system.

The platform design enables both a reactive and proactive approach to fighting disinformation, firstly by significantly strengthening the fact-checking process through a

machine-human model, secondly by incentivizing publishers to adjust, verify and improve their content through an objective yet impactful way of voting that in turn reflects over their overall reputation.

Author Contributions: Conceptualization, C.N.B.; methodology, C.N.B. and A.A.; software, C.N.B. and A.A.; validation, C.N.B. and A.A.; formal analysis, C.N.B. and A.A.; investigation, C.N.B. and A.A.; writing—original draft preparation, C.N.B. and A.A.; writing—review and editing, C.N.B. and A.A.; supervision, C.N.B. All authors have read and agreed to the published version of the manuscript.

Funding: The research presented in this paper is part of the FiDisD project. FiDisD is the acronym for "Fighting disinformation using decentralized actors featuring AI and blockchain technologies". The FiDisD project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 957228. FiDisD is developed in the context of TruBlo ("Trusted and reliable content on future blockchains") which is part of the European Commission's Next Generation Internet (NGI) initiative.

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.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
BFS	Breadth First Search
CNN	Convolutional Neural Networks
DeFi	Decentralized Finance
DAO	Decentralized Autonomous Organization
DDOS	Distributed Denial of Service
FiDisD	Fighting disinformation using decentralized actors featuring AI and blockchain technologies
GloVe	Global Vectors for Word Representation
IoT	Internet of Things
IPFS	InterPlanetary File System
NFT	Non-Fungible Token
NLP	Natural Language Processing
PoA	Proof-of-Authority
SSI	Self-Sovereign Identity

References

1. Tsfati, Y.; Boomgaarden, H.G.; Strömbäck, J.; Vliegenthart, R.; Damstra, A.; Lindgren, E. Causes and consequences of mainstream media dissemination of fake news: Literature review and synthesis *Ann. Int. Commun. Assoc.* **2020**, *44*, 157–173. [CrossRef]
2. Shu, K.; Wang, S.; Lee, D.; Liu, H. Mining disinformation and fake news: Concepts, methods, and recent advancements. In *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–19. [CrossRef]
3. Fraga-Lamas, P.; Fernandez-Carames, 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]
4. Choraś, M.; Demestichas, K.; Giełczyk, A.; Herrero, Á; Ksieniewicz, P.; Remoundou, K.; Urda, D.; Woźniak, M. Advanced Machine Learning techniques for fake news (online disinformation) detection: A systematic mapping study. *Appl. Soft Comput.* **2021**, *101*, 107050. [CrossRef]
5. Guttmann, A. Survey: Index of Respondents' Trust towards Media in European Union (EU 28) Countries in 2019. 2023. Available online: https://www.statista.com/statistics/454409/europe-media-trust-index/ (accessed on 8 May 2023).
6. Walter, N.; Cohen, J.; Holbert, R.; Morag, Y. Fact-checking: A meta-analysis of what works and for whom. *Political Commun.* **2020**, *37*, 350–375. [CrossRef]
7. Nakov, P.; Corney, D.; Hasanain, M.; Alam, F.; Elsayed, T.; Barrón-Cedeño, A.; Papotti, P.; Shaar, S.; Martino, G. Automated fact-checking for assisting human fact-checkers. *arXiv* **2021**, arXiv:2103.07769.

8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 8 May 2023).
9. Zheng, Z.B.; Xie, S.; Dai, H.N.; Chen, W.L.; Chen, X.P.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput.-Syst.-Int. J. eSci.* **2020**, *105*, 475–491. [CrossRef]
10. Hardle, W.K.; Harvey, C.R.; Reule, R.C.G. Understanding Cryptocurrencies. *J. Financ. Econom.* **2020**, *18*, 181–208. [CrossRef]
11. Chohan, U.W. *Decentralized Finance (DeFi): An Emergent Alternative Financial Architecture*; Critical Blockchain Research Initiative (CBRI) Working Papers; Critical Blockchain Research Initiative: Islamabad, Pakistan, 2021. [CrossRef]
12. Schar, F. Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets. *Fed. Reserve Bank St. Louis Rev.* **2021**, *103*, 153–174. [CrossRef]
13. Atlam, H.F.; Wills, G.B. Technical aspects of blockchain and IoT. *Adv. Comput.* **2019**, *115*, 1–39. [CrossRef]
14. Ferdous, M.S.; Chowdhury, F.; Alassafi, M.O. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access* **2019**, *7*, 103059–103079. [CrossRef]
15. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. *Int. J. Healthc. Manag.* **2020**, *15*, 70–83. [CrossRef]
16. Vijay, C.; Suriyalakshmi, S.M.; Elayaraja, M. Blockchain Technology in Logistics: Opportunities and Challenges. *Pac. Bus. Rev. Int.* **2021**, *13*, 147–151.
17. Ante, L. Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations. *Econ. Innov. New Technol.* **2022**. [CrossRef]
18. Shae, Z.; Tsai, J. AI Blockchain Platform for Trusting News. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–9 July 2019; pp. 1610–1619. [CrossRef]
19. Chen, Q.; Srivastava, G.; Parizi, R. M.; Aloqaily, M.; Ridhawi, I.A. An incentive-aware blockchain-based solution for internet of fake media things. *Inf. Process. Manag.* **2020**, *57*, 102370. [CrossRef]
20. Agrawal, P.; Anjana, P.S.; Peri, S. DeHiDe: Deep Learning-based Hybrid Model to Detect Fake News using Blockchain. In Proceedings of the International Conference on Distributed Computing and Networking 2021, Nara, Japan, 5–8 January 2021; pp. 245–246. [CrossRef]
21. Shahbazi, Z.; Byun, Y.-C. Fake Media Detection Based on Natural Language Processing and Blockchain Approaches. *IEEE Access* **2021**, *9*, 128442–128453. [CrossRef]
22. 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]
23. 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]
24. Katal, A.; Singh, J.; Kundnani, Y. Mitigating the Effects of Fake News using Blockchain and Machine Learning. In Proceedings of the 2021 2nd International Conference for Emerging Technology (INCET), Belagavi, India, 21–23 May 2021; pp. 1–7. [CrossRef]
25. Ramadhan, H.F.; Putra, F.A.; Sari, R.F. News Verification using Ethereum Smart Contract and Inter Planetary File System (IPFS). In Proceedings of the 2021 13th International Conference on Information & Communication Technology and System (ICTS), Surabaya, Indonesia, 20–21 October 2021; pp. 96–100. [CrossRef]
26. Dwivedi, A.D.; Singh, R.; Dhall, S.; Srivastava, G.; Pal, S.K. 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 Sensor Systems (MASS), Delhi, India, 10–13 December 2020; pp. 38–43. [CrossRef]
27. Lalley, S.; Weyl, E.G. Quadratic Voting: How Mechanism Design Can Radicalize Democracy. *Am. Econ. Assoc. Pap. Proc.* **2018**, *108*, 33–37. [CrossRef]
28. Lalley, S.; Weyl, E.G. Nash Equilibria for Quadratic Voting. *arXiv* **2014**, arXiv:1409.0264.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.