TruthSeekers Chain: leveraging Invisible CAPPCHA, SSI and Blockchain to combat disinformation on social media

Meriem Guerar[1,3][0000−1111−2222−3333] and Mauro Migliardi[1,2,3][0000−0002−3634−7554]

[1] University of Padua, Padua 35131, Italy name.surname@unipd.it
https://www.unipd.it
[2] Centro per l'Ingegneria delle Piattaforme Informatiche (CIPI), Genova, 16145, Italy
name.surname@cipi.unige.it
[3] Cybertooth, Joint CIPI gruppo SIGLA CyberSecurity Lab
https://cybertooth.grupposigla.it/index.html

Abstract. Disinformation has become a worrisome phenomenon at a global scale, spreading rapidly thanks to the growth of social media and frequently causing serious harm. For instance, it can perplex and manipulate users, fuel scepticism on crucial issues such as climate change, jeopardize a variety of human rights, such as the right to free and fair elections, the right to health, to non-discrimination, etc.
Among the most used tools and techniques to spread disinformation are social bots, deep-fakes, and impersonation of authoritative media, people, or governments through false social media accounts. To deal with these issues, in this paper, we suggest TruthSeekers Chain, a platform which add a layer on top of the existing social media networks where I) the feed is augmented with new functionalities and reliable information retrieved from a blockchain II) a bot screening mechanism is used to allow only human generated content and engagement to be posted, III) the platform is open to integration of 3rd-party content verification tools helping the user to identify the manipulated or tampered content and IV) a self sovereign identity model is used to ensure accountability and to contribute building a reliable portable reputation system.

Keywords: Fake news · Social Media · Reputation system · SSI · NFT · CAPTCHA · Blockchain.

1 Introduction

During the last decade disinformation and fake news proved to be serious threats to democracies and to the freedom of citizens. Disinformation is defined as a subset of information that can be false, inaccurate, or misleading intentionally designed, published, and promoted for causing public harm or making a profit [1]. It is a force undermining citizens' faith in democratic institutions by distorting free and fair elections and, through the amplification of social division,

resentment, and fear, often resulting in fomenting violence and repression. Furthermore, disinformation is a danger for a range of economic, social and cultural rights [2]. The COVID-19 pandemic as well as the Russian invasion of Ukraine intensified disinformation related challenges and problems. In all cases, the role of social media platforms as major vectors of such disruptive phenomena has been questioned, especially after scandals such as Cambridge Analytica's misuse of data from Facebook [4], and court cases such as United States of America versus Internet Research Agency [5].

It is clear that a comprehensive and reliable solutions to fight fake news spreading and disinformation in social media networks is needed. Although several solutions have been proposed in the literature, either they focus on a specific content authenticity or they provide completely new platforms for social media content verification (e.g., [24, 6]). In the mentioned solutions, users have to check the veracity of each social media post separately which is unrealistic and time consuming. Aside from the fact that consumers must seek for the truth across numerous platforms and repeat the process for each piece of content, information about the source and its trustworthiness is unknown, and the verification process is available only to specific groups (e.g., accredited journalists). To the best of our knowledge, TruthSeekers Chain (TSC) is the first platform that augment the content of existing social media with reliable information and offer content verification and network analysis as features to the users while browsing their favorite social media feed. In addition, thanks to TSC design and Self-Sovereign Identity model (SSI), TSC is the first platform that can provide its members a set of verifiable credentials that links their real identity with their social media accounts and provides a portable social reputation score based on the user's behavior in multiple social media networks. Furthermore, TSC is also the first platform that offers the tokenization of evidence or social media contents by creating NFTs (Non-Fungible Tokens) and provides a marketplace for trading them. This way, TSC members can both prove ownership and monetize their evidence or content.

The objectives targeted by TSC vision are as follow: 1) leveraging beyond-state-of-the-art technological framework such as Self-Sovereign Identity, blockchain, Machine Learning-based tools and bots screening to increase trust and to ensure transparency and accountability; 2) create open and easy to use platform with transparent algorithms dedicated to content ordering ; 3) aggregate content from multiple social networks in one place where verification and social network analysis tools can be applied; 4) Build a portable decentralized social reputation system; 5) stop bot-generated content; 6) track content, the users and their engagement (individual or group); 7) create incentive mechanisms to share and verify contents; 8) build a censorship-resistant platform; 9) design algorithms based on the content veracity rather than the user's engagement; 10) access multiple social media networks with a single login.

2 Related work

The state of the art includes multiple blockchain-based solutions that aim at fighting fake content/news. However, most existing solutions focused on the authenticity of a specific content (e.g., image, video, article, document). So, the users of social media have to register in multiple platforms (e.g., Prover [7], Truepic [17], Po.et[14], D.tube [15], OriginalMy [16]) in order to verify the authenticity of a content and have to pay to use some of them.

EUNOMIA project [21] introduced a new decentralized social media platform with emphasis on trust instead of likes. The content is considered trustworthy if a high number of users vote that the content is trustworthy without using any mechanism to distinguish between human users and bots. Users need to rely on some undefined external tool to determine by themselves whether the content has been posted and/or voted by a human or a bot. Unlike EUNOMIA[21], TSC aims at fighting the fake news spreading in the existing dominant social media networks, keeping the interaction mechanism such as like/dislike to allow users to express their opinion but at the same time holding them accountable for their actions. In addition, TSC leverages a bot screening mechanism that prevents bots from posting or engaging with social media content.

SocialTruth project [20] integrates its content verification services which provide a specific type of content analytics (e.g. for text, image, video) and verification-relevant functionality (e.g. emotional descriptors, social influence mapping) with various platforms such as web search, journalist tools and a browser add-on. In order to check a content, users give an input to the SocialTruth search bar such as the URL of the content or website and get feedback regarding its type, source, trustworthiness etc. Unlike TSC, the content verification can be performed only by experts connected in a p2p network. So, the SocialTruth users have to trust the decision taken by unknown experts and have to verify each content in social media separately.

Recently, a project called WeVerify [24] is developing cross-modal disinformation detection and content verification tools. Similar to SocialTruth [20], WeVerify allows only professionals (journalists/Fact checkers) to verify and determine the reliability of the content without providing the users details about professionals and their reputation. So a leap of faith is required as users cannot check the level of trustworthiness of the people involved.

Trive [26]is a browser extension plugin, built on Ethereum. When a user browses a website, Trive plugin changes the story opacity based on how true/false it is. After the verification process performed by researchers and verifiers, a randomly selected group of 10 witnesses decide whether the content is true or false. Trive users have to pay to use the platform and it is not known whether the involved entities in the verification process are experts or not.

The main difference between the above-mentioned solutions and TSC is that their performance depends on results of verification and validation process, and that they don't take the threat posed by bots into consideration. It is known that the verification of content requires time, and it is not always obvious to find evidence and to prove whether the content/news is true or false. So, by the time

the verification results are provided, the fake news might be already widespread. In contrast to above mentioned projects, TSC doesn't depend on the content verification results to combat the spreading of fake news, it relies instead on the user's accountability and on bot screening mechanism among others to increase the level of trust in content recorded in the blockchain. TSC front-end will offer the users all the necessary information about the content, its sources, their reputation, and the evidence while browsing their favorite social media feed. In addition, it allows both experts and non-expert to contribute to check the content veracity by sharing their opinion and resources in a secure and transparent way. The expert's statements, votes, opinions will be highlighted. Furthermore, TSC provides a portable decentralized social reputation profile based on the user's behavior on multiple social media platforms. Besides the reputation system, different incentive mechanisms are used to encourage good and deter bad behaviour. Hence, TSC proposes a different approach to fight fake news spreading that completes the efforts performed by the existing projects (e.g., WeVerify, Truly Media, SOMA, etc) in designing content verification platforms and tools. The users would be able to access these tools while browsing their feeds to check the veracity of content as well as accessing the verification results of the other identified members. The TSC incentive mechanisms and reputation system are designed to encourage the users to engage only with the likely true content. This have a direct impact on the spreading of fake news in the existing social media where content sorting algorithms are based on the user's engagement regardless its veracity.

3 Truth Seekers Chain Concept

Truth Seekers Chain is an open ecosystem that aims at mitigating fake news spreading and the impact of tampered-with content posted on social media by increasing the user's awareness on the consequences of the engagement with likely fake contents and encouraging them to verify and engage with likely true content. TSC allows the users to access multiple social media networks with a single and passwordless login. The main idea is to aggregate news, facts, claims, and media content in one place where verification and social network analysis tools can be applied and multiple independent verifiers around the world can compete to check its veracity. On the other hands, TSC aims to return control back to the users by enabling them to select the way they want to see the posts in their feeds. By defaults, the posts which are likely true based on the users votes and the attached evidence to it will be on top. This feature protects users from micro-targeting and the algorithms used by TSC are transparent to the users.

In order to increase trust and to ensure transparency and accountability, TSC relies on cutting-edge technologies in the range of distributed ledgers, incorporating Self-sovereign identity and blockchain technology as well as an invisible mechanism for bots screening (i.e., Invisible CAPPCHA [18] or ascCAPTCHA [19]). The latter allows only actions performed by humans to be transferred to

existing social media networks or recorded in the blockchain. When a user submits a post to the blockchain, it is important to note that it's the content hash which will be recorded in the blockchain and not the content itself, hence the amount of blockchain storage needed is limited. By using the Self-sovereign identity (SSI) model, the user's identity, and its related claims such as ID, diploma, social reputation are directly and autonomously managed by the user through their SSI mobile wallet. To login, the users are required to present verifiable credentials with the following attribute: full name, photo, country and optionally a certificate of expertise from well-known trusted institutions (e.g. government, universities, etc). TSC will link these attributes to the user's social media accounts accessed through the platform. To the best of our knowledge, TSC is the first platform that links user's social media accounts to the user real identity and provides a portable decentralized social reputation profile based on the user's behavior on multiple social media platforms.

The main user-side component of the system is TSC User Interface (TSC-UI). Through TSC-UI, users will have a view of their favorite social networks contents augmented with information derived from the blockchain (see Figure 1). This augmentation will relate to the source (e.g., social reputation, membership and digital badges) as well as information related to post/content (e.g., whether the post hash has been recorded in the blockchain, rebuttals, sharings, endorsements by experts and non-experts and all the links to directly access the details and evidence). Furthermore, TSC is designed to be interoperable with third party's services such as Expert-Based and ML-based content verification tools, whose results can be accessed by all the members without leaving the platform. Besides, users will also be able to upload evidence on InterPlanetary File System (IPFS), rate evidence, participate in campaigns, tokenize pieces of evidence and sell them, and leverage social network analysis tools to visualize the network of users interacting with the content to have global views on the intention behind the viral spreading of a given content. The results will be displayed in the form of a network graph.

Hence, TSC saves user's time spent in reading fake news that might be posted by bots or looking for the truth from different places and unknown sources. Furthermore, one of TSC main feature is the fact that it increases the level of trust in content recorded in the blockchain even before its validation by verifiers. This is mainly due to two factors: i) Accountability and ii) bot screening mechanism. If the author submit his post to the blockchain through TSC, this means that content has been submitted by a real human and that he accepts full responsibility of his action. Since this will have a direct impact on his reputation, users will likely submit posts that they believe represent the truth.

4 Truth Seekers Chain Architecture

The TSC Architecture is depicted in the Figure 2. It consists of seven core components, TSC UI, SSI mobile wallet, MetaMask, Bot screening mechanism, IPFS, blockchain and smart contracts. As well as two other components that

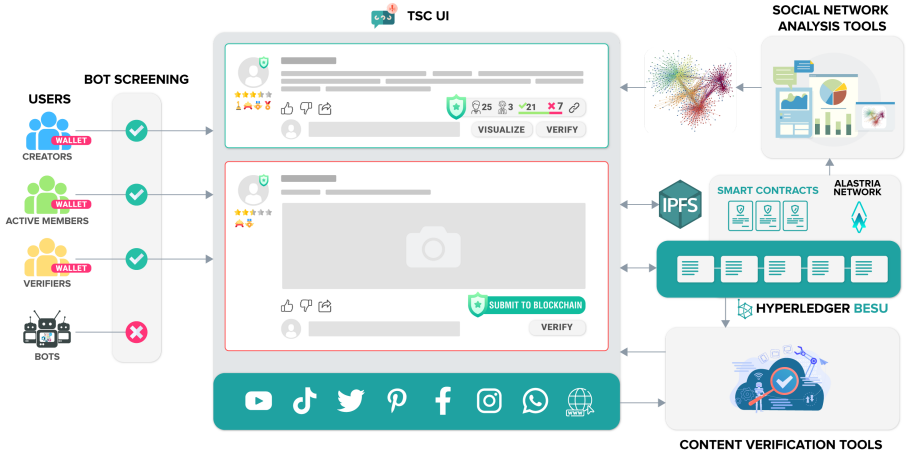

Fig. 1. TruthSeekers Chain overall concept.

allow TSC to interact with existing social media networks (i.e., social media API) and integrate external tools (i.e., open API).

TSC UI: the user interface is the main contact point for users, since all the user's interactions pass through it. The users will be able to sign up using the SSI model and interact with the system. The user's feed from the various social media platforms will be displayed in separate tabs and depending on whether the post is on-chain or not, users will have different options. For instance, the user can visualize the network using social network analysis tools only if the content (its hash) is already on-chain. The front-end is currently available as a Proof of concept and the final version will be developed using NextJS framework.

SSI Mobile Wallet: the mobile wallet is a mobile application that handles cryptographic keys and offers the potential to store and manage identity data in the form of verifiable credentials. Each verifiable credential is a representation of data which is cryptographically tamper-proof and traceable to its origin. Using this wallet, the user will be able to select some of these credentials to sign up to TSC. The credentials required by TSC are full name, photo, country and optionally certificate of expertise. For PoC implementation, we will use Trinsic ID wallet [8] or Alastria ID wallet [9].

Metamask: Metamask is a popular crypto wallet that will be used for managing rewards (TSC tokens) and NFTs. It is available as a browser extension or a mobile app [11].

Bot screening mechanism: Any action performed by the users will be filtered by a fully transparent bot screening mechanism, called invisible CAPPCHA [18] or ascCAPTCHA [19] depending on the device. The rationale behind a CAPPCHA is that the bot as a piece of code cannot perform a physical task. Since all social media networks requires users interaction with touchscreen or the keyboard, Invisible CAPPCHA leverages this natural interaction (e.g., post

a content, write a comment, tap like/dislike/share/submit to the blockchain button, etc) to distinguish between humans and bots (see Figure 3). In fact, such physical interactions cause micro-movements of the mobile device or generate a sound wave when the user taps on the keyboard. These can be detected easily by the microphone [19] or motion sensors such as the accelerometer [18, 22, 23].

Smart contracts: smart contracts will be responsible for identity management, reputation management, incentive management and content tracking. Any changes will be recorded in the blockchain in the form of transactions. For smart contracts development, we decided to use Truffle. The smart contracts are written in Solidity programming language and will be deployed in Alastria red B Network [10] which is a public-permissioned Blockchain network that uses the Hyperledger Besu technology, IBFT 2.0 consensus algorithm and it's managed by Alastria partners. It is important to note that the gas price in Alastria network is zero, the users don't need to pay anything for using TSC. We use web3.js library, which is an Ethereum Javascript API, that allows us to make requests to an individual Ethereum node with JSON-RPC in order to read and write data to the network.

Blockchain: the public-permissioned blockchain will be responsible for storing all the information that allows tracking of the contents/evidence, their sources, user's reputation profile, user's engagement with content and NFT trading. For instance, the link to social content, votes, like/share of content, IPFS hash of the content, etc. We selected a public-permissioned blockchain network that uses hyperledger besu technology (i.e., Alastria red B) to ensure data immutability, transparency and accountability. The Interaction with the hyperledger besu node is carried out via JSON-RPC API.

IPFS: IPFS is both a protocol and a peer-to-peer network for storing and sharing data in a distributed file system. All data that cannot be stored in the blockchain due to size will be stored in IPFS (e.g., , resources and evidence, NFT metadata, etc), while the IPFS hash will be recorded in the blockchain to ensure the data integrity. The communication to IPFS is carried out via HTTP-RPC API.

Social media API: it is a set of programmatic endpoints that allows TSC to communicate and exchange data with social media networks. Twitter API [12] for instance, can be used to find and retrieve, engage with, or create a variety of different resources such as Tweets, Users, Direct Messages, Trends, etc.

Open APIs: it is an open API that allows the integration of third-party content verification and social media analysis tools in TSC.

5 Comparison and discussion

The verification of content requires time and it is not always obvious to find evidence and to prove whether the content/news is true or fake. The performance of existing solutions depends on the results of the verification and validation process. So, by the time the verification results are provided, the fake news might be already widespread. Besides, the fact that the users have to search for

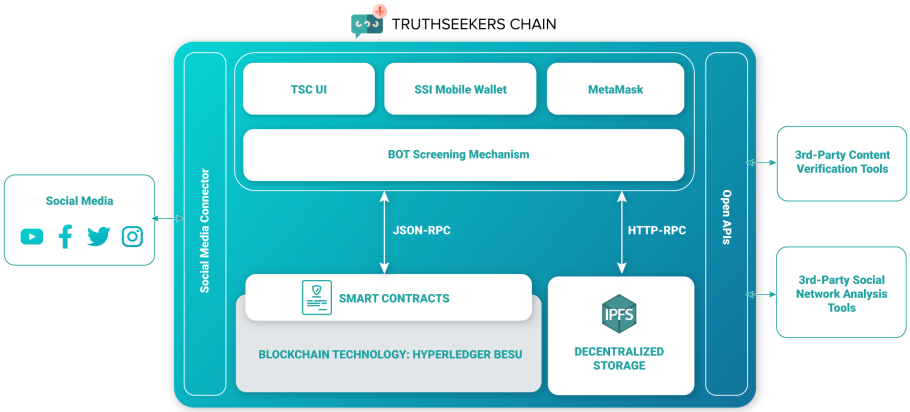

Fig. 2. TruthSeekers Chain architecture.

the truth across multiple platforms and repeat that for each content is extremely time-consuming, information about the source and its credibility is often scarce if not unavailable and sometimes the verification process is limited only to specific groups (e.g., accredited journalists). Furthermore, in all the solutions currently available, users will have to play the role of intermediary between existing social networks and content verification platforms. So, in the case in which the users do not fulfil this role, there is no real impact of these content verification platforms in combating the spreading of fake content.

In contrast, using TSC platform, users will be able to access multiple social media content with a single login and to see information about the content authenticity and the credibility of the person who posted them while browsing their favourite social media feed. These pieces of information help the user in differentiating between fake and true content from the very beginning. If expert or ML based verification tools are available, they can be used to detect deep fake or whether the content has been tampered with. When the verification results are available, they will be available in all the media networks accessed through TSC, users don't need to look for them. On the other hands, involving the users in the verification process saves the journalists and fact-checkers a lot of time. The users might witness an event or have an information which journalists don't have. In addition, the tools used by Truly Media for instance don't require high skills, any user can use them and the results would be available to journalists, fact-checkers and the other members. Furthermore, the users can filter the feed to see only posts that have been proved to be true or are from authors with a high reputation score, etc. This feature address Micro-targeting issue because the users take back control on what they see. Hence, TSC saves journalists time spent in the verification process as well as user's time spent in reading fake content or looking for the truth from different places and unknown sources.

Social bots represent a serious threat as they automatically produce content and mimic human social media behavior to influence the perception of reality and attempt to manipulate public opinion. Therefore a bot screening mechanism is crucial to combat fake news spreading. However, one of the big challenges that the existing solutions face today is to determine whether the content has been posted by a human or bot. In TSC, any user's input will be filtered by a fully transparent bot screening mechanism based on the physical nature of humans. Bot screening mechanism will reduce significantly the spreading of fake content, however this alone is not enough, as humans are also contributing in spreading fake news. Other mechanisms are built in TSC to achieve this goal: accountability and a fully historical reputation based on the blockchain, increasing the user's awareness to the consequences of his actions and limiting the fast gut-reaction by asking for explanations, linking to verification and analysis tools, incentivizing honest behavior and seeking for the truth through a rewarding system and competitions. These mechanisms aim at reducing the user's arousal, the engagement with fake contents/news and thus decreasing the visibility of such content in existing social media networks.

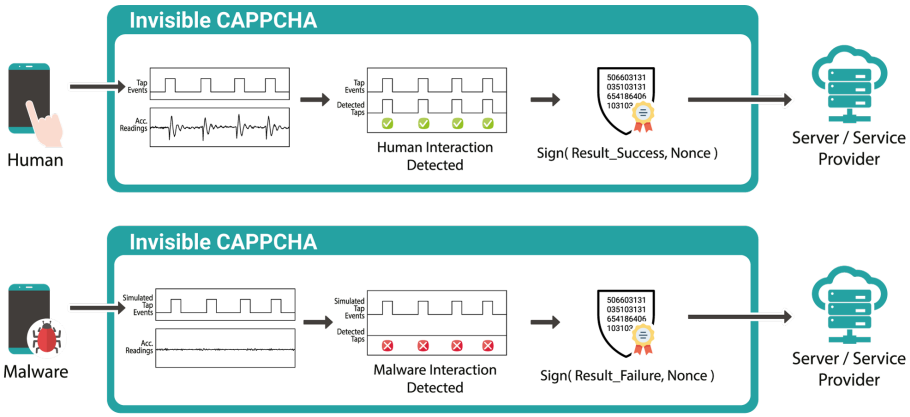

Fig. 3. Invisible CAPPCHA concept.

6 Security and privacy Analysis

TruthSeekers Chain platform as any other digital system is potentially vulnerable to cyber-attacks. In this section we analyse the security of TSC against the most common attacks and we discuss its privacy.

6.1 Distributed Denial of Service (DDOS)

Using an effective CAPTCHA mechanism [3, 22, 23, 25] prevents DDoS attacks because only humans would be able to pass the challenge and thus, prevent any attacking machines or zombified computers from passing this security checkpoint.

As we mentioned in the previous section, any user interaction with the TSC platform will be filtered by a fully transparent bot screening mechanisms [18, 19]. TSC uses Invisible CAPPCHA [18] or ascCAPTCHA [19] depending on the device to filter disruptive traffic and prevent bots from abusing social media networks APIs (e.g., Twitter API) and spreading the fake news. Unlike the traditional CAPTCHA methods[3], these mechanisms allow users to interact with the online services without the need to solve any challenge which makes them fully transparent and thus very usable.

6.2 Malicious Actors

TSC discourage malicious actors from giving unfair feedbacks (e.g., vote fake for a true content or provide low rating to a verifier to destroy the reputation of the user who created them) by incentivizing the users to act honestly. It rewards the users for their good behavior by offering them TSC tokens (ERC20 utility tokens) and increasing their reputation score and punishes them otherwise. In addition, TSC periodically checks the amount of likely fake news posted, shared or liked by each member, if the amount is higher than a threshold, the user's actions will appear in TSC platform but will not be transferred to existing social media networks to prevent the spreading of their posts or the posts that they engaged with. Unlike the existing social media networks, TSC sorts the posts in the user's feed based on their veracity, users' votes and the amount of evidence attached to it, rather than the users' engagement with it. So the risk of fake news going viral in TSC is culled; on the contrary, a permanent, blockchain attested proof of participating the spreading of fake news will be attached to the user's social reputation profile.

TSC also offers to the users the possibility to participate in campaigns by contributing in the verification process and earning an amount of cryptocurrency in Ether. So, the users are more likely to act honestly to get the reward and have this behavior stored in their blockchain-saved, permanent history.

It is important to mention that the TSC members can only vote or rate once the resources that don't belong to them and cannot evaluate their own resources. Furthermore, as the login to TSC is linked to the users real identities it is not possible to create false accounts to accrue votes.

6.3 Sybil attack

In this type of attack, the attacker creates many accounts (Sybils) to perform malicious activities in social network. For example, it can create phantom feedback in the system, spread fake news, ruin the reputation of honest users, etc. TSC is resilient to this attack because the users can not have multiple identities issued

by a trusted third party (e.g., Government) unlike email accounts. Thanks to SSI model and TSC design, all the user's social media accounts accessed through the platform will be automatically linked to the users real identity information shared through their SSI mobile wallet.

6.4 Whitewashing attack

The attacker behaves maliciously and after receiving negative ratings, he creates a new account to neutralize his reputation score. Although the user can have several social media accounts, in our system these accounts will refer to the same individual. To sign in, the users have to present verifiable credential which include information about their real identity signed by trusted entity such as the government. TSC links all their user's social media accounts accessed through TSC to their real identity. Thus, their social reputation score based on their behavior in all their social media networks accessed through TSC is permanent and cannot be neutralized.

6.5 51% attack

TSC smart contracts will be deployed in the Alastria red B network which uses Proof-of-Authority consensus (IBFT 2.0). Thus, the security against 51% attack depends on the Validator nodes. When the consortium selects these nodes, they have to ensure that these nodes will not collude and collaborate among them to make decisions that will adversely affect the rest of the nodes. The number of not fully trusted nodes should be less than one third of the total number of Validator nodes.

6.6 Data privacy

The user personal information requested by TSC like full name, photo and country are not considered sensitive information. Actually, these pieces of information and others are required also by the traditional social media platforms. However, traditional social platform do not verify whether they are correct or not. This allows some users to create accounts with fake data or use other person's data. Fortunately, using SSI model, TSC can ensure that the user's information are correct by verifying the signature of the verifiable credential issuer. By using TSC, users agree to share these pieces of information and accept responsability for their actions as in the real world.

Regarding the user's social media accounts, TSC also ensures that the registered social accounts (i.e., account ID) belong to a specific user. In order to access the existing social media accounts through TSC, users are required to authorize TSC to read and write data (e.g., get timeline, transfer like, post content, etc) in their social media on their behalf without sharing their usernames and passwords using Oauth protocol [13]. If TSC successfully receives the access token after the users' authorization, this means that the users have successfully signed in to their social media accounts and they are the rightful owners of these accounts.

7 Conclusion

Modern social media are public platforms where anyone, including news organizations, can post anything without being accountable and where fact-checking is extremely time-consuming. Furthermore, it is left to users to separate humans from bots, and fake news from truth inside their social feeds. In this paper, we proposed TruthSeekers Chain, an open platform that fights fake news spreading and helps users in recognizing fake news and tampered content. Using TruthSeekers Chain, users can I) access their feeds from multiple social media networks with a single login; II) adopt a transparent algorithm for the selection of what they see; III) contribute in the verification process as an expert or non-expert IV) monetize and prove ownership of their evidence or media content and finally V) they can receive a portable social reputation profile that can be used in other context and platforms. Journalists and fact-checkers can also benefit from the TSC platform, they would have access to resources that can help them in their investigation and they can as well buy NFTs that represent ownership of media files to use them in their blogs and articles. Involving the users in the verification process will save them a lot of time. In future work, we plan to provide a detailed description of TSC main components, its internal mechanisms, a Proof of Concept implementation and some preliminary experiments.

8 Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 957228 (TruBlo) and has also received financial support from Gruppo SIGLA s.r.l.

References

1. European Commission, Directorate-General for Communications Networks, Content and Technology, A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation, Publications Office, 2018, https://data.europa.eu/doi/10.2759/0156
2. COLOMINA, C., SÁNCHEZ MARGALEF, H., YOUNGS,R., :The impact of disinformation on democratic processes and human rights in the world, 2021.
3. Guerar,M., Verderame,L., Migliardi,M., Palmieri, F., Merlo, A., 2021. Gotta CAPTCHA 'Em All: A Survey of 20 Years of the Human-or-computer Dilemma. ACM Comput. Surv. 54, 9, Article 192 (December 2022), 33 pages. https://doi.org/https://doi.org/10.1145/3477142
4. Hu, M., 2020. Cambridge Analyticas black box. Big Data & Society, 7(2), p.2053951720938091.
5. Bastos, M. and Farkas, J., 2019. "Donald Trump is my President!": The internet research agency propaganda machine. Social Media+ Society, 5(3), p.2056305119865466.
6. TrulyMedia Homepage, https://www.truly.media. Last accessed 14 March 2022.
7. Prover Homepage, https://prover.io. Last accessed 14 March 2022.

8. Trinsic Wallet: It's like your physical wallet, but digital, https://trinsic.id/trinsic-wallet/. Last accessed 14 March 2022.
9. Alastria wallet, https://github.com/alastria/alastria-wallet. Last accessed 14 March 2022.
10. Alastria Network, https://alastria.io/en/la-red/. Last accessed 14 March 2022.
11. A crypto wallet & gateway to blockchain apps, https://metamask.io/. Last accessed 15 March 2022.
12. Twitter API, https://developer.twitter.com/en/docs/twitter-api. Last accessed 15 March 2022.
13. Oauth 1.0 wokflow, https://www.ibm.com/docs/en/tfim/6.2.2.7?topic=overview-oauth-10-workflow. Last accessed 15 March 2022.
14. Po.et Github Page, https://github.com/poetapp/documentation. Last accessed 14 March 2022.
15. D.tube Github Page, https://d.tube/. Last accessed 14 March 2022.
16. OriginalMy HomePage, https://originalmy.com/. Last accessed 15 March 2022.
17. Berkhead, S., 2017. Truepic app lets journalists instantly verify images, videos. International Journalists Network.
18. Guerar,M., Merlo,A., Migliardi,M., Palmieri, F., Invisible CAPPCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT,Computers & Security,Volume 78,2018,Pages 255-266,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2018.06.007.
19. Di Nardo Di Maio, R., Guerar, M., Migliardi, M., "ascCAPTCHA: an Invisible Sensor CAPTCHA for PCs Based on Acoustic Side Channel," 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), 2021, pp. 482-487, https://doi.org/doi: 10.23919/MIPRO52101.2021.9597134.
20. Chorań, M., Pawlicki, M.,Kozik, R. , Demestichas, K.,Kosmides, P., and Gupta,M., 2019. SocialTruth Project Approach to Online Disinformation (Fake News) Detection and Mitigation. In ¡i¿Proceedings of the 14th International Conference on Availability, Reliability and Security¡/i¿ (¡i¿ARES '19¡/i¿). Association for Computing Machinery, New York, NY, USA, Article 68, 1–10. https://doi.org/DOI:https://doi.org/10.1145/3339252.3341497
21. Toumanidis, L., Heartfield, R., Kasnesis, P., Loukas, G., Patrikakis, C. (2020) A Prototype Framework for Assessing Information Provenance in Decentralised Social Media: The EUNOMIA Concept. In: Katsikas S., Zorkadis V. (eds) E-Democracy Safeguarding Democracy and Human Rights in the Digital Age. e-Democracy 2019. Communications in Computer and Information Science, vol 1111. Springer, Cham. https://doi.org/DOI:https://doi.org/10.1007/978-3-030-37545-4_13
22. Guerar,M., Merlo,A., Migliardi,M., Completely automated public physical test to tell computers and humans apart: a usability study on mobile devices. Future Gen Comput Syst 2017. https://doi.org/doi:10.1016/j.future.2017.03.012.
23. Guerar, M., Migliardi, M., Merlo, A., Benmohammed, M., Messabih, B.: A completely automatic public physical test to tell computers and humans apart: a way to enhance authentication schemes in mobile devices. Proceedings of the 2015 international conference on high performance computing simulation (HPCS); 2015. p. 203–10. https://doi.org/doi: 10.1109/HPCSim.2015.7237041.
24. Marinova, Z. et al., "Weverify: Wider and Enhanced Verification for You Project Overview and Tools," 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2020, pp. 1-4, https://doi.org/doi: 10.1109/ICMEW46912.2020.9106056.

25. Guerar,M., Verderame,L., Migliardi,M., Merlo, A., "2GesturePIN: Securing PIN-Based Authentication on Smartwatches," 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2019, pp. 327-333, https://doi.org/doi: 10.1109/WETICE.2019.00074.
26. Mondrus, D., McKibbin,M., Barnetson,M., Trive Whitepaper, https://trive.news/Whitepaper.0.2.6x.pdf. Last accessed 14 March 2022.