Combating fake news in social networks through the active participation of users: the approach of EUNOMIA project

Panagiotis Monachelis, Lazaros Toumanidis, Panagiotis Kasnesis and Charalampos Patrikakis*

Faculty of Engineering,
Department of Electrical and Electronics Engineering,
University of West Attica,
122 41, Greece
Email: pmonahelis@uniwa.gr
Email: laztoum@uniwa.gr
Email: pkasnesis@uniwa.gr
Email: bpatr@uniwa.gr
*Corresponding author

Abstract: With the rapid expansion of social networks, one of the most critical issues that have been emerged is the spread of fake news. The technology of blockchain in a combination of peer-to-peer networks can deal with the privacy and ownership of the users providing a tool that can overcome the issue of misinformation encouraging users to participate in a procedure of content's evaluation. This solution is proposed by EUNOMIA project, funded under H2020 research funding program of EU. The architecture adopted in the project in order to enable the users to actively engage in the detection of fake news, identify the provenance of information and protect their network from misinformation is presented here.

Keywords: decentralised social networks; blockchain; human as trust sensor; fake news; social networks; misinformation; peer-to-peer networks; content evaluation.

Reference to this paper should be made as follows: Monachelis, P., Toumanidis, L., Kasnesis, P. and Patrikakis, C. (2022) 'Combating fake news in social networks through the active participation of users: the approach of EUNOMIA project', *Int. J. Electronic Governance*, Vol. 14, Nos. 1/2, pp.131–144.

Biographical notes: Panagiotis Monachelis is a PhD student in the Electrical and Electronic Engineering Department at the University of West Attica (UniWA), Greece, and a teaching staff member in UniWA's Computer Networks & Services Research (CoNSeRT) Lab. His research focuses on big data mining and visualisation over online social networks. Currently, he is involved with the EUNOMIA project in the visualisation field. Previously, he worked in the domain of microcontrollers at a technical company and IT in the banking sector. He earned a bachelor's degree in Electronic Engineering from the Technological Educational Institution of Athens and a Master's degree in Networking and Data Communications from Kingston University, UK, in partnership with Piraeus University of Applied Science, Greece.

Lazaros Toumanidis has received his Electronics Engineering Bachelor's degree from the Piraeus University of Applied Sciences in 2014 and his Master of Science by research diploma from the University of West Attica in 2020. He was honoured with the 'Anastasiadis Award' for having the highest grade among the year 2014 graduates of the Department of Electronics. He has worked as a Software Engineer and has been a research associate of the Computer Networks & Services Research Lab of the University of West Attica (UniWA) since 2016. He has successfully participated in several European and National research projects and he has published more than 10 scientific papers in international journals and conferences His research interests include machine learning, web, mobile and wearable computing and the internet of things.

Panagiotis Kasnesis holds a PhD in Computer Science from the Department of Electrical and Computer Engineering at the National Technical University of Athens (NTUA). Moreover, he received his Diploma degree in chemical engineering and his MSc in Techno-Economic Systems from the NTUA, in 2008 and 2013 respectively. His research interests include machine/deep learning, Semantic Web technologies, multiagent systems, and the Internet of Things, while he has published and presented more than 25 scientific papers in international journals and conferences in these fields. He serves as a lecturer and Senior Researcher at the Department of Electrical and Electronics Engineering of the University of West Attica (UniWA) and has participated as a machine learning engineer in several European research and development projects. Finally, he is certified as Instructor and University Ambassador, by NVIDIA Deep Learning Institute (DLI), in the tasks of Natural Language Processing, Computer Vision and Recommender Systems.

Charalampos Patrikakis is a Professor at the Dept. of Electrical and Electronics Engineering of the University of West Attica on the Design and Implementation of Interconnected Electronic Systems and Services, with emphasis on data collection and processing. He has been an adjunct lecturer at the National Technical University of Athens and the Agricultural University of Athens, while he has worked for 20 years as a researcher at various laboratories of the Institute of Communications and Computer Systems, the National Technical University of Athens and the Agricultural University of Athens. He is currently the Director of CoNSeRT (Computer Networks and Services Research laboraTory) of the University of West Attica, which researches on Artificial Intelligence, Cloud Computing and Networking, Web and IoT and Blockchain technologies. He is also the Director of the MSc Program "Artificial Intelligence and Deep Learning". His research experience includes participation in in over 50 research projects.

1 Introduction

Online social networks (OSNs) have grown impressively over the last decade, and are still evolving rapidly. A plethora of social networks platforms and applications have been developed, promising direct and fast communication and information, reaching up to extreme levels of specialisation on topics they address. The number of SN users is constantly increasing while even the elderly are registered on at least one social network platform (Yangk and Lin, 2019). Users of different ages located all over the world, coming from different societies, produce a huge volume of data in social networks, consisting of opinions, news, photos videos and other media. All this chaotic information

raises doubts and questions about characteristics such as trustworthiness, subjectivity, validity and even risk. The importance of trustworthiness within social networks became particularly apparent in the last year of the COVID-19 pandemic, as many fake news were spread at the risk of public health. The management of such issues by the most popular centralised social networks has created skepticism, especially as regards content control, ownership, neutrality against ideas that are expressed by users, and censorship. As a result, new decentralised solutions gain more and more ground. The crowdsourced nature of social media can contribute to the assessment of their content (though a democratic, decentralised model) and thus, improve significantly the level of the trustworthiness. Mastodon (2020) is an excellent example of a decentralised social network, transforming the distributed, crowdsourced data model of SNs to an enabling architecture which deviates from the traditional centralised architectures of popular SNs. The 'Bluesky' project (Bluesky, 2019) announced in 2019 by Twitter CEO Jack Dorsey is a representative of the trend toward social network decentralisation. This paper focuses on the research performed in EUNOMIA (User-ori**e**nted, sec**u**re, trustful and dece**n**tralised s**o**cial **m**ed**ia**), a project funded under EU's Horizon 2020 program, which is in progress and is expected to be completed in 2021, and proposes an architecture based on blockchain and peer-to-peer (P2P) technology to address the following challenges: clarification of the original source-user of a piece of information, how this information has spread and been modified and how reliable this information is. EUNOMIA employs a decentralised architecture and a digital companion providing the user with intuitive indications of the content and context of the sources for defining user-specific trust criteria, and determination of the nodes (user and posts) along an information cascade derived by a machine learning approach. EUNOMIA addresses a key gap in the landscape of the social media information verification market. Current tools cover only a small subset of the requirements that EUNOMIA is addressing (source verification, cascade verification, trustworthiness score, open-source, decentralised, involved users and no needed expert curation). The most of them are websites, where expert curators analyse a variety of sources to establish the veracity of claims posted on social media, in a manner that is not scalable and generates one more intermediary (the group of expert curators employed). There are two alternatives that are available today, the add-on FiB (FiB, 2021) and the software Truthnest (Truthnest, 2021), that are not open-source, decentralised or able to involve the users in the information verification challenge.

EUNOMIA is powered by Mastodon, a decentralised social network where users can post text messages, photos, videos, share content, interact with other's posts and subscribe with each other. Mastodon is a free network that consists of separate websites installed on different units (instances) with the ability to easily integrate with each other. Users of different instances can interact with each other without the need of a central authority to moderate or control any action, as users are the sole owners of their posts. Below, we present a brief overview of two main underlying technologies that enable decentralisation while still providing a degree of trust between networked entities:

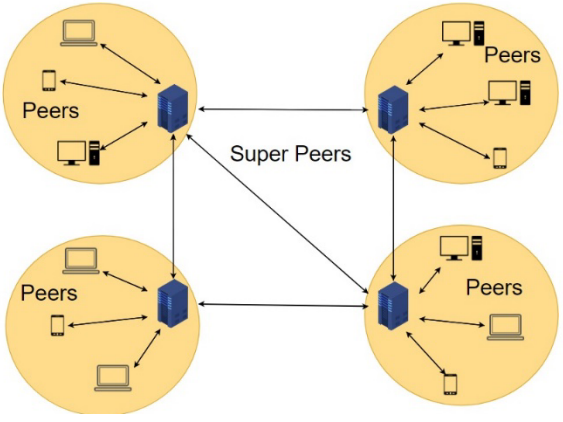
1 P2P social networks

2 blockchain technology.

2 Peer-to-peer technology

P2P technologies are widely used and have been embraced by internet users for resource sharing over the past decade. Therefore, in this section of the paper, we will not make an extensive presentation of P2P networks and architectures, but rather present the essential and necessary information, which is relevant to the paper. A P2P network uses a distributed architecture featuring networked devices called 'peers'. Peers interact with each other and share resources. All peers can share files, use instant messaging, make audio and video calls, interact with posts and photos, and join or leave the network at any time. The overall performance of the network increases with the number of peers. Peers can be combined into groups as they communicate, interact, and share bandwidth, allowing the network to continue to function, even if one or more peers disconnects. In a more complex interconnection, a P2P social network consists of small groups of peers, where each group has its own 'super peer,' a device that undertakes the role of mediator with the rest of the network via other super peers (see Figure 1).

Figure 1 P2P social network (see online version for colours)



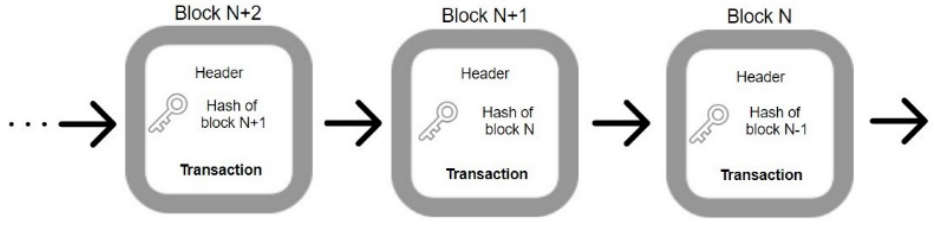
In this scheme, each peer connects with a super peer to route its data via the latter. Super peers manage the incoming messages and forward them to other super peers or peers, according to the content. If authentication is needed, it can be implemented between peers and super peers before connecting to the network. A popular file-sharing P2P system is BitTorrent (BitTorrent, 2020), which users can use to exchange files.

3 Blockchain technology

Blockchain Technology originally developed to support the Bitcoin cryptocurrency, blockchain technology has proven instrumental in supporting applications related to trust in several other distributed environments (Tama et al., 2017). In distributed social networks, the technology provides security and privacy through cryptography. In a blockchain structure, nodes (which can be physical or logical entities) interact with each other (e.g., making Bitcoin transactions recorded in the form of a decentralised digital ledger), and participating nodes on the blockchain network have the ability to validate, synchronise, and retain a copy of the ledger. Each user's action enters the network in the

form of a block. The blocks connect to each other, creating a chain in which each block (except the first) is connected to the previous with a hash function. Figure 2 provides a high-level overview of a blockchain. Typically, the blocks in a blockchain reference a specific user or system transaction.

Figure 2 A chain of blocks



However, blocks may also be designed to reference an immutable record of a 'state' of information trust or integrity. For example, in the case of social network posts, a blockchain ledger can be considered a reference state, recording votes of trustworthiness that have been anonymously recorded for specific post content. To uphold privacy, however, the 'right to be forgotten' must be upheld, whereby blockchain transactions can be deleted or expunged from the ledger. This is somewhat of a paradox for blockchain, as it was designed with the premise that the blockchain is an immutable record of events. To address this architectural limitation, rather than define blocks based on individual posts and their trustworthiness votes, it may be better to define blocks as a representation of the 'state' of the P2P database underpinning a decentralised social network platform (e.g., where a 'state' block is added periodically after either a predetermined amount of time, a set number of posts has been published, or a prescribed number of trust-worthiness votes have been cast). With this approach, if posts are revoked from the social media platform (and therefore the P2P database), it does not affect the immutability of the blockchain because each block references the P2P database 'state' of posts and votes cast against them, and not the posts or votes content themselves. Thus, registered actions (and, in this case, a post's trustworthiness votes) can be verified as a record by the most recent committed state, while ensuring posts that are revoked (and with them any trustworthiness votes stored in the P2P) do not compromise the integrity of the ledger. In a decentralised social network ecosystem, applying blockchain in this manner is highly attractive, as it provides a single source of intermediary-free 'truth' (i.e., verified state) for posts and trustworthiness votes that is resistant to manipulation of any single node in the network.

4 State-of-the-art

Various tools have been developed to face the issue of trustworthiness, following different approaches. Microsoft's News Guard, a plugin of Edge browser, relies on trained analysts (skilled journalists) to check the validity of the news. It provides a score of trustworthiness and information about non-fulfilment of specific criteria. Other tools as TextBox (TestBox, 2020) and FakeBox (FakeBox, 2020) are based on text analysis and fake news detection performing natural language processing, sentiment analysis, entity

and keyword extraction focusing on assessment whether newspapers are real or not. While other tools are oriented to check the source of a paper and other tools are oriented to users' contribution, EUNOMIA combines the services of source verification, cascade verification and involvement of users. The most of the tools that have been developed are services that are supported by expert curators who take into account data from a variety of sources to verify or not the content of posts on social media, in a manner that is not scalable and renders the need of existence one more intermediary (expert curators). The add-on for detection fake news in Facebook FiB (FiB, 2020) and the software Truthnest (Truthnest, 2020) seem to be alternative solutions but they are neither opensource, nor decentralised, and they don't involve the users in the process of information verification. Specifically, a scenario related to HaTS can involve two groups of validators. Trustworthy professional journalists validate the news and a random group of users with knowledge of the paper's subject validate it too. The validators hold different scoring weights, and the final rating of the paper is a combination of the validators' scoring. The weights of the validators' scoring change over time as valid votes increase a user's weight while incorrect votes decrease it. Validity is evaluated by the deviation of a validator's score from that of the professional journalists. This system is a step toward decentralising the process and more actively involving the user. As it is perceived, the contribution of users is important in the overall evaluation of the content.

A social media observatory has been developed on analysis and detection of crises of the contemporary society focusing on opinion dynamics related to cultural and societal issues in European spaces (Willaert et al., 2020). Founded by H2020, ODYCCEUS project includes 'Penelope', an open web-service-based infrastructure that different groups of users can consult and contribute as well, according to their analytical needs. The platform provides 'causation tracking' through linguistic analysis correlating posts through Natural Language Processing, and compare the semantic relationship for example of an paper and the comments underneath, so that is able to perceive if artificial bots interfere in online political debates.

Analysis on social media content in the context of COVID-19 pandemic has been performed by University of Southern California (Sharma et al., 2020) providing study results related to misinformation. The research is based on Twitter data and provides visualisations for specific hashtags according to their sentiment analysis. Also, the credibility of source for the shared newspapers has been considered to evaluate the tweet, based on fact-checking sources. The research provides also geographical distribution of tweets for trends presentation but does not provide any interactive tool for researchers to extract and visualise data.

An observatory has been deployed that is focused on Twitter dataset about COVID-19 vaccination. CoVaxxy (DeVerna et al., 2021) is an online set of tools that provides visualisations about misinformation on this topic. The extracted data come from United States and are filtered according to relevant keywords excluding non-English tweets. The terms of this dataset include the unique users, the number of the tweets they share, and the contained hashtags and URLs. The URLs in the posts characterise its credibility according to a third-party list, while a few URLs were evaluated manually.

Another study has also focused on combating fake news combining machine learning techniques (Kaur et al., 2020). Using data from New Trends, Kaggle and Reuters, the goal of this architecture is to find out which classification model has the optimal performance in automated detecting fake news procedure. It uses ML classifiers that are merged according to their metrics in order to form three voting classifiers which are then

merged in a final voting classifier for the final prediction. The voting classifiers are terms that refer to the self-assessment of the mechanism and there is no relation with exogenous voting. The architecture illustrates the fake news in word clouds with a prospect to provide a GUI.

A platform that aims to help researchers and journalist to study information diffusion in the social media (based on Discus and Twitter) is the social web observatory (Tsekouras et al., 2020). This observatory permit users to create account and visualise results related to trends, coverage, events, sentiment, stance, etc. The queries are made with a schema of entities containing title, name and keywords and the result can be public or private according to the user's selection. The results contain information about how many papers, comments and tweets exist that are related to the entity for a selected time period. It returns the domains with these papers and illustrates the results per source category (newspapers, tweets and comments). A sentiment analysis processing is visualised characterising the content as positive, negative and neutral.

EUNOMIA project aims to encourage citizen participation in content verification by voting on content trustworthiness. The goal is for users to take ownership of the problem of disinformation, rather than relying on third-party fact-checkers or computer software. The number of votes appears as one of several indicators that the user can visualise along the information cascade of each post.

5 Human as trust sensor

Methodology: Before proceeding to technical analysis of EUNOMIA, it is important to determine its methodology in the context of trustworthiness. Use of machine learning techniques and in particular natural language processing (NLP) is quite promising, in supporting the classification of papers posted in a SN into true or fake. However, the NLP evaluation process certainly can be improved with the additional involvement of users, contributing themselves to the content evaluation on the social networks (Shovon et al., 2019). Human-as-Trust-Sensor (HaTS) functions is one of the issues employed in EUNOMIA which addresses how human sensing capabilities are involved for evaluating trustworthiness. HaTS requires the following two facilities:

i a way to collect data and structure the information for human analysis and appraisal

ii a way that gives the ability to the users to interact with the visualised information, as voting.

The derived data create an information cascade that provides attributes for the purpose of HaTS analysis aiming at the optimal assessment and attempting to answer the following questions: what is the source of a post and importantly how its content might have changed. The post is accompanied by metrics which are created by the users' own contribution giving an assessment of the total trustworthiness score.

6 The EUNOMIA architecture

The EUNOMIA architecture contains three components that ensure its secure, decentralised nature:

1 a P2P network

2 a blockchain infrastructure

3 a security and privacy framework.

It also comprises four tools that assist a user in assessing information trustworthiness:

1 a human-as-trust-sensor component

2 a social media content and context data analysis component

3 trustworthiness scoring

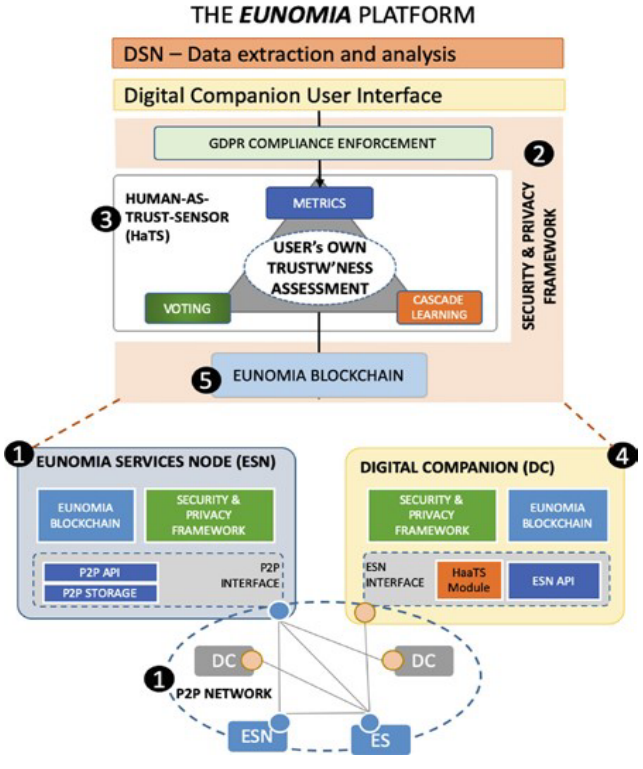
4 a user application in the form of a digital companion.

These tools and components are implemented in a network of interconnected services nodes, making their services available to end users through an application running on user devices (a 'digital companion'). The nodes communicate through a P2P network that features a distributed file system protocol. Data are collected and shared in accordance to a security and privacy framework, relating to data analytics and the HaTS component, and then are utilised to evaluate in near real-time the information trustworthiness with the support of machine learning information cascade learning and a user-driven assessment process. Reasoning is performed on the users' devices or on EUNOMIA servers, in a P2P schema and in line with the philosophy of Blockchain, avoiding the necessity of third party centralised cloud servers. A digital companion (DC) provides visualisations of possible indicators of information trustworthiness and an environment that allows users to get involved, e.g., by voting or other actions.

7 Decentralised platform architecture

EUNOMIA can be integrated as additional software to existing open-source distributed social media providing extended applications (Figure 3). The EUNOMIA architecture consists of five core components running in a decentralised manner: the first (1) is a peer-to peer network between EUNOMIA Services Nodes (ESN) which support and synchronise data and service components across EUNOMIA (and act as service nodes to users' Digtal Companion clients). The ESN P2P network enforces (2) a security and privacy framework which supervises a strict GDPRcompliant opt-in post data extraction policy for EUNOMIA users. The security and privacy framework directly enables (3) a Human-as-Trust-sensor mechanism with an integrated collection and extraction toolkit for analysis of social media post content and context, feeding output into a visualisation interface on (4) the EUNOMIA digital companion, where users able to make their own trustworthiness assessment for post content and metrics. Finally, an immutable record of EUNOMIA user trustworthiness votes (relating to a user's own trustworthiness scoring criteria) is stored and tracked in (5) a Blockchain infrastructure, supported and synchronised across the ES P2P network.

Figure 3 The overall EUNOMIA architecture (see online version for colours)



The components in EUNOMIA that comprise the services nodes include:

i The *P2P Infrastructure* which supports the storage and communication service for two types of peers: service providers (EUNOMIA services) and users (EUNOMIA digital companion). The P2P network has the following features:

- Any user has the ability to participate in the decentralised network without being controlled by any organisation.
- Users can contribute with their resources as a result the more users connected the more resources there are.
- Failures are significantly reduced because of the distributed architecture.
- Third party services are offered as distributed storage, peer-to-peer messaging (in DC) and network management.

ii The *Blockchain infrastructure* is able to cryptographically link the user posts to a Blockchain and create Blockchain-based signatures that can be used for verification purposes. The main functions of this infrastructure are:

- *Data aggregation*: all posts that are going to be published are collected and stored.
- *Data formatting*: the actual content of the post and the associated metadata are encoded.

- *Publishing*: Posts are published in the Blockchain after hashing procedure and stored.
- *Logger* where the information of transactions are maintained.
- *Transaction controller* that is responsible to control the transactions according to metrics as the number of posts that a single Blockchain transaction can serve and the frequency of transactions over time.
- *Verification*: Performing 'proof-of existence' procedure for a given post while successful verification returns the associated metadata.

8 Security and privacy regulation

EUNOMIA project is compliant with the security and privacy regulations and the following three elements serve this purpose:

i *the AAA server* which is responsible for authentication, authorisation and accounting

ii *the discovery server*, which provides the means to allow the discovery of other services and corresponding metadata, including public keys for sharing sensitive information

iii *the voting server*, through which users can react and express opinions on available content, features a voting mechanism that supports the submission, logging, and querying of votes by users for individual posts and cascades.

The above services provide high-level security features as:

Authentication of users and devices, implemented with keys derivation mechanisms in order to allow users to use more than one device, mitigating the risk of user's account hacking. The process of recording of relevant information and ensuring the transparency of the voting process including integrity forcing mechanisms, ensures integrity checking of voting and other user related information.

9 Digital companion

The digital companion, an application deployed on all types of devices (desktops/tablets and smartphones), features a responsive Web-based and a personal (mobile/wearable) app version, allowing for the active involvement of social media users. The digital companion client runs on the user's device and can communicate with one or more decentralised social networks, as well as one of the EUNOMIA services nodes. In the client, the end user can read a post from a decentralised social network, reply or 'like' the post, and also view computed EUNOMIA indicators about the post, such as its sentiment score. The user can also create a new post from the client and vote about the trustworthiness of a specific post. The result of the analysis is displayed on the client in the form of interactive visualisation graphs. All the queries between the client and the rest of the EUNOMIA services are implemented through the EUNOMIA services interface.

10 Workflow cases

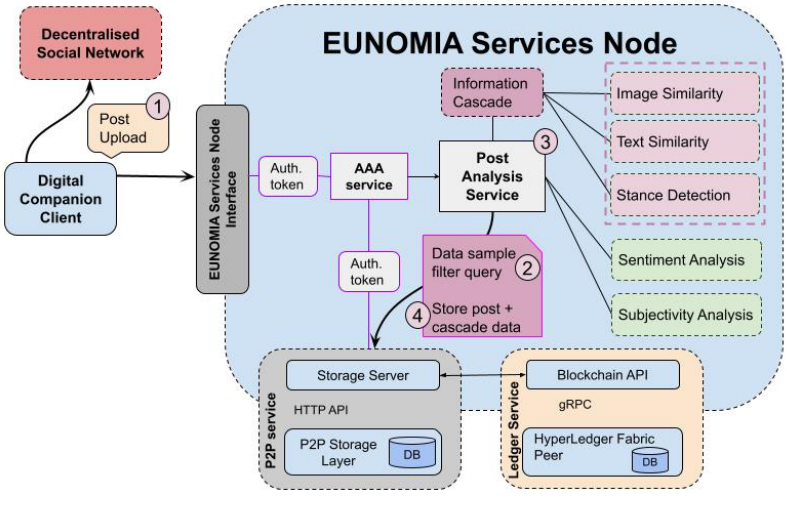
Following, two functions of EUNOMIA are described to clearly clarify the workflow during

i the creation of a new post

ii trustworthiness voting.

Figure 4 describes the workflow when a user makes a new post to one of the linked decentralised social networks (DSN), using the interface of digital companion (DC).

Figure 4 Creating a new 'EUNOMIA-enriched' post (see online version for colours)



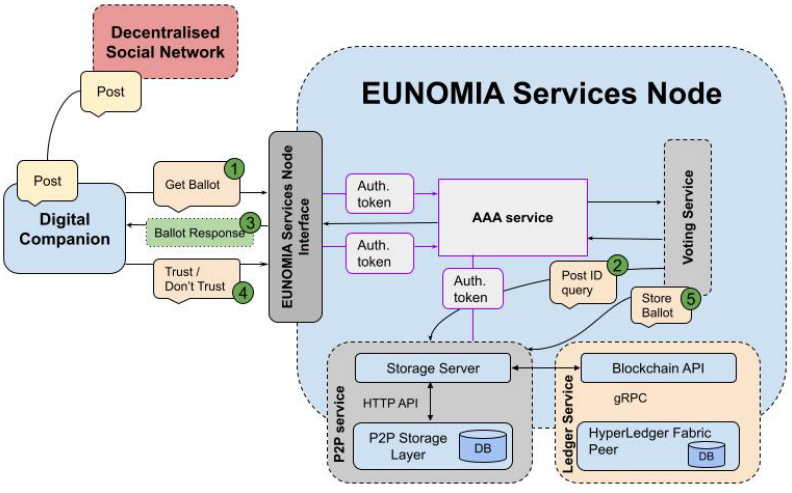
The client, after has been authorised as a user of the DSN uses its own Restful API services and forward the new post to one of the EUNOMIA Services Nodes (1). Through the authentication authorisation and accounting (AAA) Service, existing posts are queried from the Storage Service and passed as input to the post analysis service (PA). PA in its turn utilises the separate Sentiment, Subjectivity and Information Cascade services (3) in order to collect the computed post metadata and save the results to the Storage Service (4). For the Information Cascade service, the text and image similarity between the new post and existing ones are computed. The text similarity (paraphrase detection) service, relies on BERT model (Devlin et al., 2018) fine-tuned on the MRPC dataset (Dolan and Brockett, 2005). If a post is a reply to an existing one, the Stance Detection service is used, providing the possible relation (one of: 'support', 'deny', 'comment', 'query') between these two posts. The overall result of post analysis is stored back to the Storage whether the post is added to a (new or existing) cascade or not (4).

Figure 5 depicts the workflow during the procedure of trustworthiness voting.

Voting takes place in secure, fully decentralised way, where the request is forwarded to several peer nodes inside the EUNOMIA network. When a user wishes to vote on the trustworthiness of a specific post, a new ballot request (1) is sent to a EUNOMIA Services Node. After a successful user authentication, the Voting Service initialises a

ballot is for the queried post (2) and sends it back to DC(3). Using this ballot, the client sends the user's vote (4) back to ESN and the Voting Service, which stores the ballot, saving only the referenced post and the vote (5).

Figure 5 Voting trustworthiness in EUNOMIA (see online version for colours)



11 Future work

In the age of social networks, the information that is disseminated is chaotic. The effort for verification with a view to trafficking as much as possible trustworthy information seems to be imperative. Fake news and unreliable sources have a constant presence on the internet and this can be dangerous at critical issues. The project EUNOMIA proposes a decentralised solution which provides trustworthiness on social media. The first instance of EUNOMIA is deployed by University of Nicosia to support an online community discuss and quickly assess posts about the latest news, trends and rumours on cryptocurrencies and decentralised technology advancements. Subsequently, Blasting News publisher will be trailing EUNOMIA for a single vertical channel of theirs and for a limited time period. It will replace the static comment section under each paper with social media threads where users will benefit from EUNOMIA's trust functionalities, such as easily identifying similar posts from other papers or thematic groups, and assessing their trustworthiness. A third EUNOMIA instance is planned to serve a cluster of journalism students. The campaigns for attracting users will focus on Italy and Austria as per the existing consortium's contacts and initial engagement with universities. However, the instance will be open to any journalism student. Also, more services are planned to be added as instance messaging and notifications when EUNOMIA mobile app is delivered for Android and iOS. The main purpose is the development of a tool that can be embedded on social media with a friendly environment to guarantee the trustworthiness of the contents.

12 Conclusion

The misinformation on social media has become enormous and information technology has turned its attention to the validity of information. Techniques that have been developed for this purpose have to do with machine learning algorithms but as effective as it can be, user input is certainly not taken into account. The project EUNOMIA proposes an architecture based on P2P networks and blockchain technology through which users play a more active role. Users do not rest on technical solutions but they are encouraged to contribute to the evaluation of the content on social media. In an initial phase the tools of EUNOMIA are developed to be tested in the community of the partners and in a wider context of participants in a test environment, but in a final phase these tools can be a very important assistant in evaluating of information generally on social media fighting the spread of fake news effectively.

References

BitTorrent (2020) https://www.bittorrent.com/ (Accessed 6 October, 2020).

Bluesky (2019) https://twitter.com/bluesky (Accessed 6 October, 2020).

DeVerna, M., Pierri, F., Truong, B., Bollenbacher, J., Axelrod, D., Loynes, N., Torres-Lugo, C., Yang, K., Menczer, F. and Bryden, J. (2021) *CoVaxxy: A Global Collection of English-Language Twitter Posts About COVID-19 Vaccines*, arXiv:2101.07694v2

Devlin, J., Chang, M.W., Lee, K. and Toutanova, K. (2018) *BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding*, arXiv:1810.04805.

Diaspora (2020) https://diasporafoundation.org/ (Accessed 6 October, 2020).

Dolan, W.B. and Brockett, C. (2005) 'Automatically constructing a corpus of sentential paraphrases', *Proceedings of the Third International Workshop on Paraphrasing (IWP2005)*, Jeju Island, pp.9–16.

FakeBox (2020) https://machinebox.io/docs/fakebox (Accessed 6 October, 2020).

FiB (2020) https://devpost.com/software/fib (Accessed 6 October, 2020).

FiB (2021) https://devpost.com/software/fib (Accessed 1 July, 2021).

Kaur, S., Kumar, P. and Kumaraguru, P. (2020) 'Automating fake news detection system using multi-level voting model', *Soft Computing*, Vol. 24, pp.9049–9069, https://doi.org/10.1007/s00500-019-04436-y

Mastodon (2020) https://joinmastodon.org/ (Accessed 6 October, 2020).

Sharma, K., Seo, S., Meng, C., Rambhatla, S. and Liu, Y. (2020) *COVID-19 on Social Media: Analyzing Misinformation in Twitter Conversations*, arXiv:2003.12309

Paul, S., Joy, J.I., Sarker, S., Shakib, A., Ahmed, S. and Das, A. (2019) 'Fake news detection in social media using blockchain', *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, pp.1–5.

Tama, B.A., Kweka, B.J., Park, Y. and Rhee, K.H. (2017) 'A critical review of blockchain and its current applications', *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, pp.109–113.

TextBox (2020) https://machinebox.io/docs/textbox (Accessed 6 October, 2020).

Trusthnest (2020) https://www.truthnest.com/ (Accessed 6 October, 2020).

Truthnest (2021) https://truthnest.com (Accessed 1 July, 2021).

Tsekouras, L., Petasis, G., Giannakopoulos, G. and Kosmopoulos, A. (2020) 'Social web observatory: a platform and method for gathering knowledge on entities from different textual sources', *Proceedings of the 12th Language Resources and Evaluation Conference*, European Language Resources Association, pp.2000–2008.

Willaert, T., Van Eecke, P., Beuls, K. and Steels, L. (2020) *Building Social Media Observatories for Monitoring Online Opinion Dynamics*, Social Media + Society, April, doi:10.1177/2056305119898778

Yangk, H-L. and Lin, S-L. (2019) 'The reasons why elderly mobile users adopt ubiquitous mobile social service', *Computers in Human Behavior*, Vol. 93, April, pp.62–75.