RAUN

Regional Academy on the United Nations

Positive Impacts of Blockchain Technology on The Digital Safety of Journalists: An Explorative Study

Authors:

Susanna Bottaro, Vienna University of Economics and Business

Dheeraj Raja Kumar, Universitat Politècnica de Catalunya

Kimsey Zajac, University of Göttingen

Agency: OSCE

Mentor: Daliborka Jankovic

Peer+: Konrad Gertz

Abstract

The freedom of media and the safety of journalists are crucial elements in democratic societies. Despite global efforts to increase the safety of journalists, the profession remains plagued by perilous working conditions. With increasing digital threats to journalists' security and ability to work, blockchain technology might offer practical solutions to counteract specific vulnerabilities in the digital realm. This exploratory paper investigates the possible scopes of blockchain technology applications in improving the digital safety of journalists. With a qualitative analysis of semi-structured interviews with investigative journalists and blockchain experts, the study examines the threats journalists face in the digital realm and aims to understand the current and future opportunities and challenges of using blockchain technology for the digital safety of journalists. The results suggest that blockchain technology might already aid in protecting identities and communications, logging security breaches, and enabling decentralized data storage, among others. However, significant challenges exist in various dimensions, such as technical (e.g., scalability), political (e.g., lack of clear regulations), and social (e.g., acceptance). More research is needed to understand the full potential of blockchain technology in improving the digital safety of journalists and the steps and challenges ahead for a smooth adoption of this technology.

Table of Contents

List of Abbreviations

BCT	Blockchain Technology
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
DSoJ	Digital Safety of Journalists
NGO	Non-Governmental Organizations
OSCE	Organization for Security and Co-Operation in Europe
PoS	Proof of Stake
PoW	Proof of Work
RSF	Reporters Without Borders
SDG	Sustainable Development Goal
SLAPP	Strategic Lawsuit Against Public Participation
UI/UX	User Interface / User Experience
UN	United Nations
VPN	Virtual Private Networks

1. Introduction

"By defending journalists' safety and preserving a free and diverse press we make democracy stronger."
(Council of Europe, 2015, 8)

Media freedom has deteriorated globally over the past decade, with new forms of oppression taking root in both open societies and authoritarian states (Repucci, 2019). Some governments and other actors moreover exploited the ongoing COVID-19 outbreak as a pretext to undermine human rights, including the freedom of expression and press. Simultaneously, the pandemic highlighted the need for accessible, fact-based information to counteract malicious disinformation. Quality journalism plays an integral part in educating the people, with media actors serving as public watchdogs contributing to creating an informed and transparent public debate. The freedom of media is crucial in democratic societies as it provides accurate, fact-based and well-researched information to the public. This information is critical in enabling people to make informed decisions and hold those in power accountable. Free media acts as a watchdog, detecting wrongdoings by those in power, big businesses, corruption, and crimes. The safety of journalists is therefore essential as it not only protects their own human rights, but also strengthens and reinforces democracies. It furthermore directly relates to the successful outcome of Sustainable Development Goal (SDG) 16.10: ensuring public access to information and protecting fundamental freedoms[1].

The safety of journalists[2] is defined as the ability to provide an environment where journalists can write and report freely and independently. Journalists' safety can thus be considered "an all-embracing concept that includes the physical, psycho-social, digital and the legal domains equally" (Free Press Unlimited, 2022). However, despite global efforts to increase the safety of journalists, the profession remains plagued by perilous working conditions in both physical and digital spheres. With threats ranging from harassment, imprisonment, and torture to death – violence against journalists is a global phenomenon undermining human rights and the core foundation of a democratic society by restricting the public debate (Council of Europe, 2020). Over the past decade, at least 950 professional journalists and media workers lost their lives due to their journalistic activities, according to Reporters Without Borders (RSF), many being deliberately killed due to the nature of their investigations (RSF, 2022). Nine out of ten of journalists' suspicious death cases remain unsolved or yield no repercussions for the perpetrators (UNESCO, 2021). These statistics do not include the reported and unreported disappearances and incidents of torture, intimidation, imprisonment, harassment, and other forms of censorship[3].

Over the last decades, not only the physical but also digital threats to journalists' personal security and their ability to work increased rapidly. However, it becomes increasingly challenging to distinguish between the physical and the digital realm due to psychological injuries caused by continued online harassment, effects on one's livelihood due to mental stress and defamation, or physical violence due to the deliberate spread of misinformation or personal information (Posetti et al.,

[1] The successful outcome of SDG 16.10 is measured by the number of verified cases of killing, kidnapping, enforced disappearance, arbitrary detention and torture of journalists, associated media personnel, trade unionists and human rights advocates in the previous 12 months and the number of countries that adopt and implement constitutional, statutory and/or policy guarantees for public access to information.

[2] Journalists are understood to be "individuals who are dedicated to investigating, analysing, and disseminating information, in a regular and specialized manner, through any type of written media, broadcast media […], or electronic media." (UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom of Expression, 2010)

[3] See the RSF barometer for a disaggregated list of recorded abuses in real-time: https://rsf.org/en/barometer.

2020). Like other industries, journalism underwent a profound transformation due to the rise of the internet and digital media. Internet-enabled mobile devices facilitate the real-time capture and instantaneous sharing of events with people worldwide (Deibert, 2017). While incorporating technological advances introduced conveniences such as more accessible communication with sources and colleagues, adopting digital media also heightened journalists' exposure and opened them up to new vulnerabilities. Examples of how journalists and their sources can be targeted and endangered online are astroturfing, trolling, harassment, mob censorship, spoofing, and doxing (Posetti, 2017; Waisbord, 2020). In a survey conducted in Türkiye, Çalışkan (2019) outlines journalists' reports of personal threats followed by wiretapping, geo-tracking, online disinformation campaigns, cyber-attacks, denial of service (DOS), and access to personal accounts on other platforms. The survey points out that most journalists believe their government has likely collected data about their online activity. Nevertheless, only a fraction of the respondents uses data encryption or other protective measures to contact sources and store sensitive information. Various United Nations (UN) agencies, particularly UNESCO, and the Organization for Security and Co-Operation in Europe (OSCE), have published reports covering journalists' digital safety for different actors across levels ranging from individuals and news organizations to non-governmental organizations (NGOs) and governments[4]. Other than research and policy suggestions, international organizations have engaged with trend and violation identification and trainings for journalists, editors, and public officials[5]. While advocating for and underlying the importance of technical novelties, the development of innovative tools is often up to private companies or NGOs.

Considering the existing digital threats, blockchain technology (BCT) might offer compelling solutions to counteract specific vulnerabilities journalists and their sources face in the digital realm. Due to its diffused, anonymous, and validated nature, BCT might aid in protecting identities, reliably and transparently logging security breaches, enabling decentralized data storage, or securely localizing journalists in the field. Contrary to popular belief, BCT is not only pertinent for financial transactions but has been employed for all kinds of civil and social purposes in recent years, such as healthcare, government elections, identity management, logistics, and supply chain management (Taherdoost, 2022). In this exploratory paper, we examine the threats journalists face in the digital realm and investigate the possible scopes of BCT applications in improving the digital safety of journalists (DSoJ). Specifically, we aim to understand the current and future opportunities for and challenges of using BCT regarding the DSoJ by conducting semi-structured interviews with journalists and BCT experts. Our presented findings on the BCT-journalism nexus thus gives an insight into the feasibility of integrating BCT solutions into journalists' daily duties. This paper further aims to spark more research into innovative technical solutions designed to enhance the DSoJ and redirect the image of BCT from mainly being a tool for the financial industry towards also being a valuable instrument for social causes.

We found that BTC, considering the current development of the technology, can aid journalists in various digital activities increasing their safety thanks to its decentralized, anonymous, immutable and tamper-proof nature. BCT could for example make communication more secure, fight censorship, or provide a safe storage of sensitive data. Still, there are many obstacles to the technology

[4] See, e.g., "The Chilling" paper series (UNESCO, 2021), which can be retrieved from: https://en.unesco.org/publications/thechilling, "Online Safety and Digital Security for All Journalists – A Prerequisite for Media Freedom" (OSCE, 2022), which can be retrieved from: https://www.osce.org/representative-on-freedom-of-media/522169, and "Safety of Female Journalists Online" (OSCE, 2020), which can be retrieved from https://www.osce.org/files/f/documents/2/9/468861_0.pdf.

[5] See, e.g., the Multi-Donor Programme for Freedom of Expression and Safety for Journalists: https://en.unesco.org/themes/fostering-freedom-expression/mdp.

implementation, not only technical but also financial, legal, and sociopolitical. Journalists are open to new technological solutions as long as the resulting tool is effective and easy to use. The preferable provider of such tool are not-for-profit organizations and civil society associations, ideally with an open-source software. The exponential developments of BTC could present new unimaginable opportunities for enhancing the DSoJ.

The paper is structured as follows. Section 2 delineates the methodology employed during the research. Section 3 focuses on the DSoJ, including existing threats and current strategies journalists utilize to combat digital attacks. Section 4 expounds the technical basics of BCT and explores potential areas where BCT could be integrated to enhance journalists' digital safety. Section 5 discusses the findings. Section 6 concludes.

2. Methodology

In order to investigate the potential synergies of BCT and the DSoJ, we adopt a qualitative research approach. Semi-structured interviews (Table 1) were conducted on two themes: the DSoJ and BCT. On the one hand, we aimed to identify specific (digital) threats that journalists face in their daily work and to inquire whether journalists would value potential blockchain solutions. We concentrated on investigative journalists, given the elevated risk they face as a result of the nature of their work, bringing to light various local and international grievances. On the other hand, we investigate the possible applications of BCT to improve the DSoJ. Potential experts for the interviews were identified through desk research and social media and contacted through e-mail and LinkedIn. The interviews were conducted via video call or email and were held in English or Italian, depending on the preferred language of the interviewee. The data collected from the interviews is systematically analysed through qualitative content analysis, defining significant themes and categories relevant to the given research question.

Table 1 Interview partners

#	Name	Expertise	Affiliation	Mainly active in
1	Armando Strofaldi	Web3 business developer	Dverso	IT
2	Farhana Javed	Blockchain technology	UPC	ES
3	Federico Feggi	BCT development	Aesthetes	IT
4	Gabriele Cruciata	Investigative journalism	Freelancer	IT
5	Giancarlo Fiorella	Investigative journalism	BellingCat	CA & Latin America
6	Journalist #1	Investigative journalism	/	Arab region
7	Karim Maassen	Crowd-based journalism start-up	Nwzer	NL
8	Lorenzo Bagnoli	Investigative journalism	IRPI, freelancer	IT
9	Paul Simroth	BCT development	/	AT
10	Wilmer Daza	Start-up and BCT	La Fabrique	FR
11	Manisha Ganguly	Investigative journalism	The Guardian	UK

Limitations, which could have potentially influenced the results, were identified at various stages in the research. First, due to time and resource constraints, we decided to investigate how BCT might improve the DSoJ and not address how the technology might create new threats. Secondly, due to the limited number of participants (5 journalists, 6 BCT experts), the results might not be representative and exhaustive. In particular, saturation has not been reached on the topic of blockchain applications and of 11 interview partners only 2 identified as female. This poses a particular bias in the findings on journalists' experiences with digital safety, as background literature has demonstrated that females are targeted and perceive threats differently than their male counterparts. There could further be a selection bias leading to people who find the introduction of BCT in journalism unnecessary deciding not participating. Lastly, the field of BCT, both in research and business, is fast evolving, therefore our findings might be quickly surpassed.

3. Current digital safety threats on journalists and protective measures

Digital safety is a critical concern for journalists, who often rely on technology to gather, research, and disseminate information. In the current digital era, journalists run the risk of having their gadgets infiltrated, their online identities taken over, and their private data made public among other threats. This may endanger them and impair their capacity to carry out their duties effectively.

The definition and understanding of DSoJ are not straightforward, as interviewees framed it slightly differently, depending on their personal experiences. In any case, the journalists conceptualize DSoJ along the lines of the threats they encounter. One interviewed journalist argued: "*the issue of security is very complex because, in my opinion, it is expressed in so many different areas, in so many different things that do not necessarily speak to each other*" [6] (G. Cruciata, personal communication, 2022). Indeed, the digital realm hosts a vast array of risks and threats, from financial and related to the workflow to psychological, and is continuously influenced by the physical realm and vice versa.

3.1 Digital threats to journalists

Journalists face digital threats that aim to unsettle both their personal and professional lives. Damages from the various digital violations can result in poor working conditions, stress, and financial strain, among others, up to emboldening and enabling physical violence.

The personal lives of journalists can be affected in several ways. One common threat is **online harassment** and abuse on social media, which can take many forms, including bullying, trolling, doxing, and threats of violence. This can be especially prevalent for journalists who cover controversial or sensitive topics and can seriously impact their mental health and wellbeing. Conspiracy theorists and religious patriots are identified as the major perpetrators of online harassment. The interviewees and literature highlight a gender divide in the severity of harassment, as women tend to be attacked online more often and more violently (Chocarro et al., 2020). The severity further increases by intersecting with racism. As a coping mechanism, journalists report that they tend to ignore malicious messages and comments because engaging with them would have psychological repercussions. Another potential threat is **hacking and divulgating personal information**, which can put journalists at risk of identity theft and other forms of cybercrime to discredit their work and persona or intimidate the journalist into dropping an investigation. Hacking could also be used to put the journalist under psychological stress by, for example, triggering all accounts' passwords to reset or hacking bank accounts and threatening financial safety. Finally, journalists may also be subjected to **digital tracking of their activities online** and **geolocation**, compromising their privacy and, potentially, even physical safety. Pegasus was mentioned multiple times as a spyware tool that governments utilize for surveillance of potential national security threats but is often used on journalists, human rights activists, and others.

The workflow of journalists and their ability to produce high-quality journalism can also be affected in several ways. One threat is **identifying journalistic sources**, which can put both the journalist and their sources at risk of harm. The interviewed journalists highlighted this point unanimously as one of the most pressing. Indeed, journalists hold the professional responsibility to

[6] Original quote in italian language: "è complessa la questione della sicurezza, perché si esprime secondo me in tanti settori diversi, in tante cose diverse che non necessariamente si si parlano".

assure as best as possible the anonymity and safety of their journalistic sources. Were this trust to be broken, repercussions would be widespread, affecting the journalist's reputation and intimidating sources from speaking with journalists out of fear of retribution, making it more difficult for journalists to gather information and report on important stories. Source identification can be pursued through hacking conversations (written or oral) or by finding the name on a journalist’s confidential documents and notes. Connected to this, hackers may also attempt to hack into a journalist's computer and **access and/or divulge/destroy critical investigative data or sensitive information**, which can hinder their ability to report on a story and disrupt the work. This type of digital threat is particularly damaging for investigative journalists, as it can put their entire body of work at risk. As one of the journalists illustrated, this violation can also be carried out legally by the prosecution via subpoena of all documents and sometimes even laptops related to a specific case, leaving (maybe correctly so, according to another journalist) little to no means of protection to the journalists. Another significant digital threat journalists face is **surveillance of their online activities and research**. Journalists may be monitored online, with their activities and conversations tracked and recorded. This can make it difficult for journalists to work efficiently and confidentially gather information, incurring the severe consequence of exposing confidential sources. Governments, as well as private individuals and organizations, may engage in the surveillance of journalists in order to gather information about their work or to intimidate them. Notable examples include the use of the Israeli Pegasus spyware, as well as the involvement of the Russian cyber espionage group known as Fancy Bear and the Saudi Arabian government, which was reported to have bribed a Twitter employee to monitor the direct messages of journalists and other political dissidents. This type of surveillance can have a chilling effect on journalism, making it more difficult for journalists to do their job and resulting in the suppression of critical reporting. Finally, journalists may face **digital censorship**. This can be government- and mob- or self-imposed, depending on the story investigated and the connected fear of retaliation. Government-imposed censorship is a particularly serious issue, as it can make it difficult for journalists to report on important stories and hold those in power accountable in the media’s role as a public watchdog. Self-imposed and mob censorship[7] is also a problem, as journalists may be hesitant to report on certain topics out of fear of backlash or other consequences, most commonly harassment, defamation trials, and SLAPP lawsuits[8]. Censorship can limit the information available to journalists and make it more difficult for them to report freely, accurately, and objectively.

The digital threats mentioned above are carried out by numerous actors. These can include governments, international authorities, institutions, organized crime groups, corrupt officials, businesspeople, criminals, and ordinary individuals. Governments are unanimously identified as the main perpetrator of most digital incursions listed. The Russian government, with its intelligence unit (GRU), and Israel were often mentioned as the countries, in the interviewed journalists’ experiences, that are most dangerous to investigate. Indeed, the specific actor that poses the most significant threat to a particular journalist usually depends on the story they are working on and the country in which they are located. Considering the rather borderless cyberspace, we found that

[7] Mob censorship is the suppression of speech or expression through mob tactics, such as online mobs or social media mobs, which can involve large numbers of people expressing their disapproval or outrage towards a particular person or group. One way this can happen on social media is by involving an army of bots to report an account continuously until this is blocked.

[8] A SLAPP (strategic lawsuit against public participation) lawsuit is a lawsuit that is filed with the intention of silencing, intimidating, or punishing an individual or group for exercising their right to freedom of speech, typically on a matter of public concern. A SLAPP lawsuit's main objective is frequently not to prevail in court but rather to exhaust the defendant's financial and emotional resources. A journalist mentioned the UK as being a place where this type of lawsuits can be easily filed, in comparison to other nations where legislation is in place to protect against SLAPPs.

most of the digital threats faced by journalists are common across communities and countries. Of course, the possibility of these threats transforming and materialising into physical harm heightens when the journalist is located in the area or country at the centre of the investigative story. Interestingly, the journalists displayed a clear demarcation between physical and digital threats by highlighting that they fear physical harm mainly from criminals and ordinary individuals or groups and digital harm and surveillance from States and big criminal organisations. This is most likely attributable to the level of skills, devices, and knowledge necessary to carry out digital attacks versus physical ones.

3.2 Protective measures: tools and practices against digital threats

Following the approach designed by UNESCO, considering safety to be based on three pillars, the so-called *three Ps* (Prevention, Protection, and Prosecution), we framed the measures that the interviewed journalists use to operate digitally safely.

Prevention of digital threats refers to creating a safe digital environment for media actors to operate in, which can be achieved, for example, through clear legislation, governments speaking out against any attack on free media, education, and training of both journalists and public officials, and mechanisms to report potential threats. The journalists emphasised the importance of **trainings** in educating journalists about the threats they face due to their profession and in updating their safety procedures: due to the fast-paced profession, "*it is the only moment in which you manage to realize what you can do, what can happen and how much you yourself are exposed*"[9] (L. Bagnoli, personal communication, 2022). While professional trainings are common, most journalists reported to have not taken any courses on digital safety. Governance structures in the form of **risk assessment** sessions at the start of an investigative project and of inclusion of **safety officers** in the media company or directly in the team are vital for developing good prevention strategies and having a support system in place. There are significant differences among countries in the prevention stage. These differences can include the laws that regulate intrusions into journalistic activities, such as surveillance and data collection, as well as laws related to defamation and online speech. Some countries may have stricter laws that aim to protect the journalists' digital privacy and safety. In contrast, others may have more permissive laws that make it easier to file defamation lawsuits. Additionally, there are cultural differences in the attention given to digital privacy and safety and in the levels of digital literacy among the general population.

While in the physical realm of journalistic safety, protection is triggered in case of an impendent threat, the digital space's borderless, instantaneous, or sometimes atemporal nature entails that preventive and protective measures tend to fuse in most circumstances. Indeed, journalists need to operate with the mindset that anything on the internet might be hacked, surveilled, or deleted, making protection a necessary step in almost all activities. In any case, it is essential - for the protective measures to be efficient and effective - to measure them against the risks faced in a particular investigation. Always applying all the measures can lead to a waste of time and paranoia. Journalists adopt a series of tools, habits, and practices to protect themselves from digital perils. Yet, it is impossible to be 100% secure; the only thing one can do is *"to make it more difficult for someone to gain access to your digital life"* (G. Fiorella, personal communication, 2022). To protect themselves from digital threats, journalists take several precautions. These can include using strong, unique passwords for all online accounts, regularly changing them and allowing multi-step and multi-fac-

[9] Original quote in italian language: "è l'unico momento in cui riesci un po' a renderti conto di che cosa puoi fare, che cosa può succedere e quanto sei esposto anche tu stesso".

tor authentication (**password management**); avoiding clicking on suspicious links or downloading unknown files; using **secure communication** tools such as encrypted messaging apps (e.g., Signal, ProtonMail, GlobalLeaks); and providing **safe storage to data** through encryption of sensitive files, having also offline storage (hardware or paper), having secure clouds. Using **secure internet networks** and virtual private networks (VPN) is a practice largely adopted to mask online activity, conceal personal identity, and protect against surveillance. Journalists also tend to be **mindful of their online presence** and take steps to protect their personal information. This can include using privacy settings on social media platforms and being cautious about what information they share online. In case of an impendent threat, from the banality of a phishing email to a sophisticated hacking attack, having **systems and protocols** in place to deal with these stressful and impetuous situations is fundamental in effectively assuring the digital safety of the journalists and their work. Freelancers tend to be more vulnerable as they do not have a team or media outlet backing their activities.

As a last step in the digital safety of journalists, prosecution intervenes when prevention and protection have failed, and journalists have indeed faced infringements of their rights. Investigation and pursuit of justice then become important steps not only for the reparation of the victim but also as a deterrent for future acts against journalists. Impunity can also have a chilling effect on other journalists (Council of Europe, 2020). **Prosecution for digital violations is still sparse**, considering the general rise in cybercrimes and still low level of prosecution. The legal response is thus failing (Amell & Faturoti, 2022). The interviews suggested that journalists tend to report only more serious digital crimes (e.g., hacking) while ignoring others, such as online harassment.

Overall, the journalists argue that a vast array of tools and habits are at their disposal to operate safely online. What is often missing is the awareness of which threats they should protect themselves from and the expertise to utilize technical tools, apps, and software. Of course, improvements can be made and some challenges are unresolved. These will be addressed in the next section.

3.3 Open challenges and ideal solutions

There are still many challenges and open points in assuring that journalists can operate safely digitally. One major challenge is the **difficulty in identifying perpetrators of digital crimes against journalists and in having them prosecuted**. This can be due to a lack of expertise on the part of law enforcement agencies, jurisdiction issues (considering that digital crimes often cross international borders), a lack of international cooperation, and the difficulty in gathering and preserving digital evidence, which can more or less be easily altered or destroyed. A second significant challenge is the **lack of awareness** of the threats they may face. Many journalists may not be aware of the various ways in which they can be targeted online, or they may not understand the potential consequences of such attacks, leaving them vulnerable to digital attacks. This challenge relates to the **rapid evolution of digital technologies**, which can make it difficult for journalists to stay updated on the latest threats and how to protect against them. The constantly changing nature of the digital landscape can be overwhelming for journalists, who may struggle to keep up with the latest tools, technologies, and best practices for protecting themselves online. Another challenge is the **difficulty in implementing security measures** to protect journalists' identities and work online. Journalists often do not find the time to adopt all the necessary measures and tools, or they may lack the technical knowledge to do so effectively. The sheer number of tools and methods available can also be overwhelming, leading journalists to skip steps or become confused.

During the interviews, journalists illustrated a number of potential improvements when it comes to their digital safety:

- **Better education about digital literacy**, also in universities and for the general public, which includes potential whistle-blowers.
- **Making communications more secure**. This includes not only protecting their own communication channels but also ensuring that the sources they work with are able to communicate with them securely.
- **Fewer and simpler tools** for protecting their digital safety. Simplifying the process of digital safety would make it easier for journalists to adopt good security practices.
- **Reduce time and stress constraints** by changing the culture in the newsrooms from quantity to quality. This would allow the journalists to dedicate more time to ensuring that they are taking the appropriate measures to protect themselves.
- **Extra security on social media**. Platforms could provide certified journalists with more layers of security to access accounts and prevent or contain trolling, spoofing, and other online harassment.
- **More funding for not-for-profits and associations dedicated to journalistic safety**. These organizations provide valuable support and resources to journalists, but they often rely on external funding.
- **Easier channels to report violations** to both authorities and social media moderators (e.g., a direct hotline for journalists, activists, etc.)
- A generally **more conducive environment for journalists** that allows journalists to be proactive in their protection, better assurances for whistle-blowers, and better regulations.

Regarding new technological solutions, journalists had diverging opinions on whether the technical tools should be created specifically for journalists or whether the tools should be addressed to the general population. Less diverging opinions were presented about the array of actors that should actively intervene or create the conditions for innovative solutions to flourish. First and foremost, while the government would need to play an important role in regulating the new technologies and could potentially fund them, the journalists agree that, being the government the primary perpetrator of digital threats, a digital tool (or even trainings) provided or partially controlled by the governments would be undesirable. Not-for-profit organisations and journalistic associations are the preferable actors to develop new solutions for journalistic safety as the users would trust the good intention to empower the journalists. The private sector would also be an acceptable provider of new technical tools, with some hesitation towards the people and interests behind the company. Open-source software would be preferable.

4. Blockchain applications to digital safety of journalists

Blockchain can be viewed as a growing chain of data (often referred to as blocks) that are linked to each other securely by the principles of cryptography. Despite cryptographers supporting tamper-proof documents since the 1990s, the first ever implementation of blockchain was in 2008. The most well-known use case of BCT is its usage in cryptocurrencies, the popular ones being Bitcoin and Ethereum. The system users are identified by random alphanumeric characters, thus enabling anonymity. Other potential use cases, of which some are currently being developed and deployed as in-house applications in companies, are applied in supply chain operations, copyrights management, distributed storage, healthcare data management, marine industry day-to-day operational management, and digital identity system. The tremendous attraction to BCT is due to its characteristics: decentralized data storage, the anonymity of users, the immutable record of data, and a timestamp log.

Based on the interviews conducted with technical experts, blockchain technology offers features that help address the DSoJ, but the technology is still at its nascent stage. The experts' opinions on the use cases of BCT for journalists seem promising, but it remains limited to specific features. They come with numerous open technical issues; hence, the advice is to navigate and find solutions that work for each use case. The most crucial issue raised was regarding the visibility (or anonymity) of the users of a given BCT platform. The degree of transparency of users (and functions) depends on the type of blockchain used; for example, an unverified person on a public blockchain could pose as a journalist to spread fake news, whereas an enterprise-based private blockchain could limit access and transparency of the internal functions to the general public. Another important issue with respect to BCT deployment is that it essentially makes data more accessible, as "*the data would be replicated and distributed through a higher number of computers, therefore, being more easily retrievable by third parties*" (F. Feggi, personal communication, 2022).

To illustrate the potential application of BCT to address the DSoJ, considering the technological status and maturity of the solution and the issues raised by the interviewed journalists, we identified four main use cases, as summarized in the table below.

The inspiration of initiatives (A) and (B) currently use key features of BCT for its operations/functioning. The features of timestamp entry and hash generation would help in guaranteeing immutability and accountability of edits/changes made to the report. Although paper wallets are presently used to store cryptocurrencies, it could soon be used to securely store personal digital assets, which could be used by journalists to store sensitive content offline, that can be accessed on any device.

The basics of Blockchain Technology

What is Blockchain Technology?
BCT offers a decentralized environment that has been popularly used for storing committed transactions (in the form of blocks). Any changes made to these blocks are recorded with timestamps, making it easier for auditing. The users (or peers) of the system can remain anonymous by using several core technologies of cybersecurity: digital signatures, cryptographic hash, and distributed consensus algorithms (Monrat, 2019).
Though being a decentralized ecosystem, as the number of users grows and based on the type of application of BCT, the platform users need to agree on a few rules of conduct for the efficient functioning of the whole system. This could be in the form of consensus algorithms (as used in Bitcoin) or through a central in-charge that gives mining and writing rights. The 'decentralized' part most often refers to the elimination of a central authority (like banks, governments, middlemen, or third parties) and also to the fact that storage of data in BCT is not centralized on a single server, instead it is recorded on a peer-to-peer (P2P) network enabled by the Distributed Ledger Technology (DLT).

Main characteristics of Blockchain:

- Decentralization: There is no third-party central authority required to verify transactions; instead, peer-to-peer validation is carried out by consensus algorithms or protocols.
- Anonymity of the users: Users are identified by a randomly generated alphanumeric address.
- Immutability of the records: BCT architecture (chain of blocks) keeps a record of all the previous actions/transactions (by means of a hash of all previous blocks in the chain). Any (malicious) alterations of any block in the chain will need alterations of all the previous blocks (high energy and computation cost) and require validations from multiple users in the system, thus making BCT tamper-proof.
- Auditing: The storage of blocks also includes a timestamp, thus making it easy to track the history of edits.

Types of Blockchain:
There are three main types of blockchain: public, private, and consortium (or federated).

- Public: There is no central administrator; all the decisions are taken as per the various decentralized consensus algorithms (e.g., Proof of Stake *PoS*, Proof of Work *PoW*).
- Private: Only authorised users are allowed to join the network, thus having a central in-charge assigning rights to the different users. Compared to a public blockchain, the transaction cost and speed are significantly less in private blockchain as it is a private asset of an institution or organization.
- Federated: Multiple entities assign users and oversee the system's functioning (Namasudra, 2020).

General challenges/concerns of Blockchain:
The challenges are particular to the type of BCT used and the application use case. The ones below highlight the general concerns of deploying the technology.

- Deployment cost: The setup cost, the technical personnel, and the deployment of core tools for the system's functioning are quite demanding and costly.
- Database size: As the number of users grows, the higher number of transactions performed would increase the chain size and database size.
- Redundant copies: Every user in the system has a copy of the ledger database. For public BCT applications, this might not be useful as it adds to the network speed and cost.
- Energy concerns: Public BCT drains a lot of energy to perform the consensus algorithms. However, there are few algorithms and protocols (for private and federated BCT) that require less consumption of energy, and the carbon footprint might be comparable to the usage of existing technologies.
- Uncertainty in the regulatory landscape.

Table 2 Use cases for potential application of BCT for DSoJ

	Use Case	Main feature of BCT used	Type of Blockchain	Characteristics	Inspiration
A.	Editing history of report/articles	Timestamp entries	Private	Immutability, easier auditing.	Nwzer[10]
B.	Paper wallet for storing sensitive content offline	Storing sensitive information/digital content with secured access	Private	Highly secure, offline storage. Added steps required for hiding geolocation.	BitBox2[11]
C.	Anonymous whistleblowing	Anonymity	Public or Hybrid	Anonymity (depending on the use case), securely diffuse information for the public good	SecureDrop[12]
D.	Reporting and storing evidence(s) of digital (and/or physical) harassment	Immutable record of digital content (Screenshots of deleted tweets, conversations, IP address)	Private or Hybrid	Immutable record, cryptography	Callisto[13]

Initiatives (C) and (D) are existing use cases that do not employ BCT but could benefit from its application. As journalists routinely receive anonymous tips/leads for their investigations, the use of BCT could make the process more secure, appropriately validate the sources, conduct anonymous communication during the duration of the investigation. Though initiative (D) has been implemented to aid the victims of sexual harassment/abuse, the same could be used to address the digital (and physical) safety of journalists. The possibility to report and maintain an immutable record of the digital content of such incidents would amplify the safety measures of journalists.

Apart from the above presented use cases, some other noteworthy features of BCT were highlighted during the interviews. BCT could be leveraged to carry out communication with journalistic sources through smart contract, highlighting the use of Ethereum smart contracts and the creation of a Decentralized Autonomous Organization (DAO). An alternative to the source-journalist communication link could be by "*replacing it with a two-step source-blockchain and blockchain-journalist procedure, thus eliminating all the threats posed by direct communication such as information interception and tracking or identification of the sender*" (F. Feggi, personal communication, 2022). The cryptocurrency feature

[10] Nwzer, a Netherlands-based start-up uses Ethereum blockchain for recording all the user actions and the reputation score.

[11] BitBox 2 is currently used for offline storing of cryptocurrencies. It would soon be find potential use cases for storing digital assets offline.

[12] SecureDrop is an open-source "whistleblower submission system" which has many prominent news organisation and NGOs such as The Washington Post, The Guardian.

[13] Callisto uses a cryptographic feature that lets a harassment survivor to enter their name in a database, together with identifying details of their assailant, such as social media handle or phone number, which are encrypted meaning the details are anonymous. If the same perpetrator is named by two people, the website registers a match and triggers an email to two lawyers.

could be used to fight censorship by addressing the financial needs (and/or safety) of journalists by means of anonymous private donations to specific projects/organizations, complemented by the transparency of all the financial operations of a media organization.

The interviews also clarified how a new blockchain does not need to be created, especially considering that the number of users of the platform would be (too) low (depending on the use case). It could be deployed as a layer on top of existing blockchains like Ethereum. Almost all the interviewees agreed that there does not exist a "one-size fits all" blockchain: they vary depending on the needs of the solution required and also on the solution provider. There are different blockchains for (i) a fast, scalable, fee-less payment system; (ii) a censorship-resistant ledger to store information persistently; (iii) for performing anonymous monetary transactions; (iv) interoperable BCTs to interconnect business with other decentralized applications/service providers.

A constant sub-topic raised in the interviews with tech experts was the social acceptance side of BCT. There remain negative perceptions on the use of BCT among the general public, such as: its high consumption of energy, its large carbon footprint, doubts towards its security, the belief that a new cryptocurrency is needed for new application use-case, and others. The interviewees stressed the need to debunk myths and clarify the points of contention as these are limiting the application of the technology. As mentioned in one of the interviews, "*Cryptocurrencies are just one part of the puzzle and simply serve as a digital currency*" (P. Simroth, personal communication, 2022). They only act as an incentive for growing the community of users and are not an absolute requirement, although, as of now, no other large-scale project has implemented an incentive for validation different than cryptocurrencies. Regarding the power consumption, there are significant differences among blockchains attributable to the specificities of their validation mechanism (e.g., PoW or PoS). For example, an interviewee founder of a BCT-based start-up highlighted that energy consumption "*comes from running the validation algorithms, we do not use this feature of BCT*" (K. Maassen, personal communication, 2022). Social acceptance also depends on the UI/UX efforts to present the benefits of the technology, alongside the user manual (because most of the platforms require set up VPN, correct usage of public/private keys of encryption, digital authentication, among others). Although the next generation Web3[14] principles have the potential to address these, an 'easy-to-use' and 'ease-of-access' to such technologies would determine the success of the BCT initiatives.

Although currently there are no start-ups directly addressing the DSoJ, few of the initiatives in the past decade were centred around using blockchain technology: for helping in the operational activities of journalists (Civil), crowd-based journalism (Nwzer), storing editing history of articles (Mogul News), decentralized content publishing (PUBLIQ). Most of the initiatives were unsuccessful in their vision for case-specific reasons:

- Civil, started in 2016 was not able to sustain itself and had to merge in 2020 with ConsenSys. The team is now building a suite of solutions on top of Ethereum blockchain for use by enterprises.
- Mogul News, started in 2012, which offered subscriptions to handpicked stories from leading publishers, has not recorded any activity since January 2020 (the start of the COVID-19 pandemic).

[14] Web3 is the hyped next generation of world wide web that incorporates concepts of decentralization, blockchain technologies, and token-based economics.

- PUBLIQ, a non-profit foundation started in 2020, began with an ambition of creating ‘a decentralized independent communication platform for anyone who wants to post news and any type of articles’ and currently, the community of users are focused primarily on non-fungible token (NFT) and entertainment articles.

These developments illustrate the difficulties in creating startups centered around BCT.

5. Discussion

Digital threats faced by journalists are in continuous evolution and solutions must likewise evolve along the lines of new technological tools and better practices, habits, and expertise. As the use cases showed, BCT can already be utilized for some rudimental applications that might improve the DSoJ.

It is expected that BCT will exponentially develop and expand to more use cases and fields. The fast evolution is also to be attributed to the open-source nature of the code. Some experts believe that Web3 will become the new default, while others argue that Web3 and Web2 will coexist, potentially leaving the choice between decentralized and centralized options to each individual. An interviewee stated that "*centralized solutions will still exist as centralization is embedded in our human nature, in the form in which we tend to follow leaders, vote the same politicians, trust the same institutions and so on*" (F. Feggi, personal communication, 2022).

While the use of blockchain to improve the DSoJ is still in the early stages, it has the potential to offer a number of benefits in terms of securing communication channels, protecting sensitive information, and creating secure platforms for publishing articles. The use of BCT could lead to more secure, encrypted, and resistant to tampering or interception communication channels (beyond the current end-to-end technology). BCT could be a secure storage solution for sensitive information. Because data stored on a blockchain is cryptographically secured and can only be accessed by those with the appropriate keys or permissions, it could be used to store and protect sensitive information, such as sources or investigative data, potentially also offline. BCT could also be used to create secure platforms for journalists to publish their work, protecting it from tampering or censorship and, if on a public blockchain, giving access to everyone to the story.

The solution's maturity is determined by how the BCT ecosystem (and the associated tech community) evolves in terms of fixing existing issues, finding more eco-friendly alternatives to BCT processes, social acceptance, and interoperability of the many blockchains and cryptocurrencies in the market. All the above might result in new features or solutions that could be favorable for applying to the field of journalism. Social acceptance is particularly important for blockchain-based tools because they rely on a decentralized network of users to validate transactions and secure the network. If there is not enough adoption of and trust in the network, it will not function effectively, being more vulnerable to hacking attacks, and may not gain widespread usage. Currently, the general public lacks understanding of BCT, how it works or the potential benefits it offers. This in turn leads to misinterpreting the association of BCT with illegal activities connected to many cryptocurrencies, such as money laundering and sale of illegal goods. This harms blockchain-based solutions’ reputation and cause some people to distrust it.

Regarding the provider of the BCT solution to journalists, creating a startup would be challenging, especially after the attempts made in the past decade that were not able to succeed. Public institutions could direct more or higher investments into the research and development of BCT solutions specific to digital safety, which would serve as a booster for the evolution of the technology. Still, as journalists have emphasized, they would be reluctant to use a tool controlled or managed by the State, being governments one of the main perpetrators of digital threats. There is a lot of distrust in potential providers of an innovative technical solution for DSoJ. Asking the journalists who they would trust with novel digital tools, non-profit organizations and civil society groups yielded the most trust due to bad experiences with governments and private entities: *"I would say, ideally, in a perfect world, it would be governments and law enforcement and tech companies [who should provide innovative solutions]. […] I would be much more trusting of a civil society group."* (G. Fiorella, personal communication, 2022). Therefore, the usability of a potential BCT solution and its benefits to DSoJ are as important as the sponsor behind the tool to the actual usage in journalists' daily activities. In any case, the myriad of actors required to finalize suitable and functioning BCT-DSoJ tools significantly prolongs the development process. Next to front- and back-end, smart contract and blockchain developers, also node operators, application providers, legal specialists, regulators, and the journalists themselves (i.e., the users) are crucial parts of the validation and development process, which could impede the time required to deliver a functioning product to the market (Liu et al., 2022). Supporting and working closely with BaaS (Blockchain as a Service)[15] providers might help find feasible customized BCT solutions for journalistic use cases.

Furthermore, investors and developers need to consider journalists' needs and fears. A BCT developer illustrates: *"From my personal experience, [BCT] is mostly a bit of a scary concept, [because] there is no intermediate. It's decentralized, so you are fully responsible for what you put on there. And if you make a mistake, there's basically no going back. If you press send, if you send a transaction to the wrong address, they can't be reverted. Once the block is confirmed, you can't reverse the transaction because it's engraved in stone"* (P. Simroth, personal communication, 2022), underlining the need for digital literacy and proper technical education. For a BCT tool for DSoJ to be beneficial to and used by journalists, the knowledge and time investment from journalists in using a technological tool to protect themselves must be proportionate to the risks they currently face in their activities. There are already many tools and applications journalists use in their activities and they offer decent protection, according to the interviewees (e.g., VPNs, ProtonMail accounts, tools to publish anonymously, etc.). Hence, developers must continuously ask themselves *"am I creating a solution for a problem where there is no problem and there is* ***no*** *solution needed or* ***my*** *solution is not needed"* (P. Simroth, personal communication, 2022), highlighting the need to achieve proof of concept. However, it became evident that the journalists are not completely content with existing solutions due to the ever-changing evolvement of digital threats and the fear of not being able to keep up with the risks: *"I'm not totally satisfied with [the current solutions] because the world of it [technology] changes rapidly."* (Journalist #1, personal communication, 2022). Another journalist states that: *"The problem is that it's unrealistic for anybody to be perfectly secure, so it's sort of like a weird paradox. Like, yeah, there's enough tools out there. But at the same time, you're not perfectly secure, and you're never going to be, and it's because you can be attacked every single day, for the rest of your life."* (G. Fiorella, personal communication, 2022). Thus, the interviewees gladly recognize the possibility for improved technology if it does not entail a high-energy commitment in terms of time and education. Digital literacy, for both journalists and journalistic sources, was highlighted multiple times as a fundamental requisite for any technological tool for DSoJ to be successful.

While the commitment of journalists to understand and use a new tool is generally a requirement for its success, this condition is even more fundamental for BCT-based solutions developed specifically for journalists. Indeed, a specific tool would require a chain with restricted access (a private blockchain) that would have its own community of users and node operators. Considering that

[15] The term "blockchain-as-a-service" (BaaS) refers to third-party cloud-based infrastructure and management for businesses creating and running blockchain apps.

the immutable and untemperable nature of BCT rely on abundant users and transactions made, a blockchain with only few adopters would be unsecure and soon abandoned.

While BCT offers the possibility to greatly enhance journalists' safety, it is also crucial to consider possible adverse effects of introducing a new technology for the DSoJ. A journalist illustratively describes both advantages and disadvantages of a potential BCT solution using the example of secure storage: *"So, on the one hand, there's lots of stuff that gets deleted from the internet that is really important, because it's evidence of war crimes, for example, and it should not be deleted. But on the other hand, there's other stuff that gets deleted from the internet that should definitely be deleted, like disinformation, like deep fake pornography […]. So, you see, it's like anything else. It's a double-edged sword. There's a good application for it, but also some scumbag has got to find a way to use it for bad. It's the duality of humanity."* (G. Fiorella, personal communication, 2022). This viewpoint is also supported by the literature. González & Rodelo (2020) examine the perception of digital technologies among Mexican journalists and reinforce the suspicious attitude towards digital innovations due to the potential of misuse against journalists (e.g., through harassment or espionage). Developers must thus take these possible weaponization of new software into account and weigh the good and the bad to not create a tool that facilitates the disruption of journalists' ability to work safely.

6. Conclusion

Freedom of expression, access to information, and quality journalism are integral to creating an informed and transparent public debate. Making sure that journalists feel safe in carrying out their work and free from attacks or harassment thus plays a crucial role in strengthening and reinforcing democracies and protecting human rights. Over the last decades, not only the physical but also digital threats to journalists' personal security and their ability to work increased rapidly. Undermining journalists' legitimacy through disinformation and constant harassment through bots and trolls systematically threatens not only the journalists themselves but the very core of media freedom. This paper aimed to investigate the threats that target journalists in the digital realm and to explore the potential of BCT in aiding the enhancement of DSoJ by conducting semi-structured interviews with investigative journalists and experts on BCT.

Particular threats that journalists face in their daily activities are online harassment and abuse on social media, hacking and divulgation of personal information, digital tracking of journalists' activities online as well as their physical geolocation, and endangerment of their livelihoods by impeding their ability to work by identifying and threatening sources and/or accessing or destroying critical investigative data or sensitive information. To contribute to the discussion of increasing the DSoJ and combatting the existing threats, we found that BCT has the potential to aid journalists due to its decentralized, anonymous, immutable, and tamper-proof nature by, facilitating secure communication, facilitating the sharing of and access to important stories, or providing a safe, anonymised storage of sensitive data. While there may be various beneficial use cases of BCT for the DSoJ, many obstacles remain, alongside potential malicious uses of the technology. Despite BCT existing since 2008, the technology is still nascent and as of now cannot provide the necessary structure and practicability for a user-friendly interface that benefits the DSoJ. However, BCT is known for its rapid development, offering a hopeful glance into what will come. We cannot predict what the future will hold, and it is impossible to estimate the full potential of BCT, but it is clear that blockchain will bring about not only new tools based on its technology but also new ways of thinking, due to the principles of decentralization and transparency.

For BCT to positively impact DSoJ, more research and investment are needed to develop a suitable tool that is easy to use and protects against malicious digital attacks. However, as we have shown in this paper, private startups trying to do so failed, also due to a lack of investments brought on by the regulatory uncertainty surrounding BCT. Since journalists often lack trust in governments and are hesitant to use technologies sponsored by them, non-profit organisations, NGOs, and international organisations, such as the UN and the OSCE, must fill the gap by advocating for increased funding of research and development. This must go hand in hand with promoting digital literacy among journalists by intensifying trainings and especially supporting freelance journalists that are not backed by large media companies with their own digital security officers. Education should also clarify the distinction between blockchain and cryptocurrencies to enhance social acceptance. It is particularly crucial to encourage digital education of policymakers since they require digital knowledge to be able to make proper judgments regarding the regulatory framework and to provide appropriate legislation that favors rather than hinders innovation. Moreover, further research is required into possible negative effects of BCT on journalism, since new technologies are often weaponized and misused against the target group it was meant to aid. Understanding how the trust in institutions influences the social acceptance of blockchain solutions would also be an interesting field for further research.

With the continued crackdown on freedom of speech and the unceasing spread of hatred and misinformation online, the safety of journalists in the digital realm will only gain importance in the upcoming years. Focusing on increasing the DSoJ will be a first step in securing core democratic values and reinforcing human rights.

7. Bibliography

Amell, P., & Faturoti, B. (2022). The prosecution of cybercrime - why transnational and extra-territorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 1-23.

Çalışkan, B. (2019). Digital security awareness and practices of journalists in Turkey: A. *Conflict & Communication, 18*(1), 1-16.

Centre for Human Rights (2017, November 24). Mr Frank La Rue: Module 3 - The safety of journalists. Youtube. https://youtu.be/VhsIEDX3rls

Chocarro, S., Clarke, S., Gutiérrez, P., Taing, J., Olson, K., & Organisation fuer Sicherheit und Zusammenarbeit in Europa, R. on F. of the M. (2020). *Safety of female journalists online a #SOFJO resource guide*. https://www.osce.org/files/f/documents/2/9/468861_0.pdf

Council of Europe. (2015). *Journalism at risk: Threats, challenges and perspectives.* Strasbourg: Council of Europe Publishing.

Council of Europe. (2020). *How to protect journalists and other media actors?* . Strasbourg: Council of Europe Publishing.

Deibert, R. (2017). Digital Threats Against Journalists. In *Journalism After Snowden* (pp. 240–257). Columbia University Press.

Free Press Unlimited. (2022). *Safety of journalists.* Retrieved June 25, 2022, from https://www.freepressunlimited.org/en/themes/safety-journalists

Freedom House. (2022). *Media Freedom.* Retrieved August 31, 2022, from https://freedomhouse.org/issues/media-freedom

González, R. A., & Rodelo, F. V. (2020). Double-edged knife: Practices and perceptions of technology and digital security among Mexican journalists in violent contexts. *Tapuya: Latin American Science, Technology and Society*, *3*(1), 22–42. https://doi.org/10.1080/25729861.2020.1746502

Hogan, J., Dolan, P., & Donnelly, P. (2009). Introduction. In J. Hogan, P. Dolan, & P. Donnelly, *Approaches to Qualitative Research: Theory and Its Practical Application* (pp. 1-18). Cork: Oak Tree Press.

Lewis-Beck, M., Bryman, A., & Liao, T. (2004). *The SAGE Encyclopaedia of Social Science* (3 ed.). London: SAGE Publications.

Monrat, A., Schelen, O., & Anderson, K. (2019). A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access, 7*, 117134-117151.

Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2021). The Revolution of Blockchain: State-of-the-Art and Research Challenges. *Archives of Computational Methods in Engineering, 28*(3), 1497-1515.

Posetti, J. (2017). *Protecting journalism sources in the digital age.* UNESCO Publishing.

Posetti, J., Aboulez, N., Bontcheva, K., Harrison, J., & Waisbord, S. (2020). *Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts*. UNESCO.

Reporters Without Borders. (2022). *Abuses worldwide in real time*. Retrieved August 31, 2022, from https://rsf.org/en/barometer

Repucci, S. (2019). *Freedom and the Media 2019 - Media Freedom: A Downward Spiral.* Freedom House.

UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Freedom of Expression. (2010). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development* (Report to the UN General Assembly A/HRC/14/23). Human Rights Council. https://doi.org/10.1163/2210-7975_HRD-9970-2016149

UNESCO. (2020). *Journalism, press freedom and COVID-19*. UNESCO Publishing.

UNESCO. (2021). *62 journalists killed in 2020, just for doing their jobs: UNESCO*. Retrieved from UN News: https://news.un.org/en/story/2021/11/1104622

United Nations. (2015). *Sustainable Development Goals.* Retrieved from https://sdgs.un.org/goals

Waisbord, S. (2020). Mob Censorship: Online Harassment of US Journalists in Times of Digital Hate and Populism. *Digital Journalism*, *8*(8), 1030–1046. https://doi.org/10.1080/21670811.2020.1818111

RAUN
REGIONAL ACADEMY ON THE UNITED NATIONS

Policy Brief
February 2023

OSCE

Journalism in the Digital Age

Improving the digital safety of journalists by setting the stage for innovative blockchain solutions

Executive summary

Improving the **digital safety of journalists** is a much-needed step in protecting human rights and supporting democracies. Some of the digital threats faced by journalists could be addressed through the **creation of new tools based on blockchain technology**. To make this possible, **various stakeholders, from governments to universities and journalists themselves, need to take action in the realms of regulation** (e.g., clear regulation of blockchain technology and better international regulation of digital crimes)**, education** (e.g., digital literacy, digital safety training in universities)**, and social practices** (e.g., encourage more reporting of digital attacks), amongst others. The proposed policy recommendations bear the potential to improve journalists' digital safety, digital literacy of all, and encourage and govern technological innovation alongside social change for a stronger democracy.

Freedom of expression, access to information, and quality journalism are integral to creating an informed and transparent public debate. **Journalists serve as public watchdogs bringing to light various local and international grievances** and, through their investigations, continue to protect human rights. However, despite global efforts to increase their safety, **journalists remain plagued by perilous working conditions in physical and digital spheres**, with the latter rapidly gaining importance over recent years. Undermining journalists' legitimacy through disinformation and constant harassment through bots and trolls threaten not only the journalists themselves but the very core of media freedom. **Considering the existing digital threats, blockchain technology (BCT) might offer compelling solutions** to counteract specific vulnerabilities journalists and their sources face in the digital realm. Due to its diffused, anonymous, and validated nature, BCT might aid in protecting identities, reliably and transparently logging security breaches, enabling decentralized data storage, or securely localizing journalists in the field. However, the technology remains misunderstood and online dangers for journalists are often underestimated.

> *"Journalists remain plagued by perilous working conditions in physical and digital spheres"*

> *"Blockchain technology might offer compelling solutions"*

Against this background, this policy brief outlines **necessary steps to ensure the digital protection of journalists through raised awareness and new technologies**. A particular focus is placed on requirements to create a policy landscape that facilitates the introduction of technological advances by constituting **sound regulations** that favor rather than hinder innovation.

The UNESCO considers the **safety of journalists to be based on three pillars**, the so-called Three Ps: **Prevention**, **Protection**, and **Prosecution**. Following the UNESCO framework, this policy brief presents policy implications and recommendations for journalists, media actors, international (IOs) and nongovernmental organizations (NGOs), policymakers and governments that are designed to facilitate the achievement of the Three Ps and thus enhance journalists' digital safety.

The policy implications and recommendations in this policy brief are derived from the findings in the paper "**Positive Impacts of Blockchain Technology on The Digital Safety of Journalists: An Explorative Study**" (Bottaro, Kumar, Zajac, 2022).
Available on ra-un.org.

CONTACTS
http://www.ra-un.org
Susanna Bottaro - susanna.marie.bottaro@gmail.com
Dheeraj Raja Kumar - dheeraj.raja.kumar@upc.edu
Kimsey Zajac - kimzajac@gmx.de

POLICY RECCOMANDATIONS

Prevention

A general lack of digital literacy of relevant actors and a constant underestimation of digital threats by policymakers, cooperations, and journalists themselves endanger not only journalists' ability to work, and thus their livelihoods, but also their physical and mental well-being. Prevention is about creating a safe digital environment for media actors to operate in, which can be achieved, for example, through the education and training of both journalists and public officials, mechanisms to report potential threats, clear legislation, and governments condemning any attacks on media freedom.

Digital Literacy, Education & Trainings

→ IOs, NGOs, Governments, and Policymakers

Advocate for the topic of the digital safety of journalists and raise awareness about the dangers of cyber-attacks for journalists' physical and metal safety as well as their ability to work. Promote investments into continued digital education and trainings of journalists and policymakers alike to keep up with the ever-increasing complexity of cyber-attacks. Promote the education of the civil society as to the possibilities of BCT beyond cryptocurrencies.

→ Schools and Universities

Include education on digital security as a compulsory subject in the curriculum of schools but especially also during the specific trainings for journalists.

→ Media Corporations and Journalists

Have standardized procedures to assess the potential risks of digital attacks, data and human security of new investigative projects and mitigate vulnerabilities.

Protection

Protection is related to providing safety to journalists in case of an impending threat. Technological instruments are a primary tool to combat data breaches and hacking attacks, such as appliances designed to stop viruses, detect break-ins, or stop malicious access. To create a fertile ground for vital innovations in the cyber security domain, the following recommendations are proposed.

Support technical innovation

Clear legal framework

→ Governments and Policymakers

Create a regulatory environment that supports innovative technologies rather than hinder developments in web3 and BCT. So-called regulatory sandboxes will support the adaption and finalization of emerging technologies without burdening the developers with unnecessary regulations while simultaneously protecting the consumer.

→ Governments and Policymakers

Define clear but flexible legislation on BCT that safeguards the freedom of development but protects against the infringement on other people's rights (i.e., the right to be forgotten) to reduce the uncertainty around investments into new technologies like blockchain.

Prosecution

Sound investigation and strict pursuit of justice of unlawful attacks online are crucial not only for restitution for the victim but also act as deterrent for future acts against journalists. Prosecution thus poses the ultimate stage of safety for journalists as it is vital when prevention and protection have failed, and journalists have indeed faced infringements of their rights. Considering the general rise in cybercrimes and persistent low levels of prosecution, current legal measures are failing.

Prosecution for severe digital misconduct

Reporting mechanisms for digital harrassment

→ IOs, Governments and Policymakers

Due to the digital sphere being a borderless environment, the international community must cooperate to ensure the prosecution of perpetrators. The development of an international legal framework that ensures the digital safety of journalists and makes severe digital misconduct (e.g., data leaks, unlawful access of personal accounts, surveillance, etc.) illegal and punishable across borders must be supported.

→ IOs, NGOs, Governments and Policymakers

While a legal framework exists that dictates what is legal and what is not, the process of reporting harassment is time consuming and confusing, making people less likely to report misconduct. Supporting the development of centralized collection systems that facilitates the reporting of harassment online is thus crucial to obtain proof of continued harassment and infringement of the rights of the journalists (e.g., threats, spread of rumors and misinformation).

REFERENCES

Amell, P., & Faturoti, B. (2022). The prosecution of cybercrime - why transnational and extra-territorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 1-23.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Polizzi, G. (2020). Digital literacy and the national curriculum for England: Learning from how the experts engage with and evaluate online content. *Computers & Education*, 152, 103859.

UNESCO. (2021). *Global toolkit for judicial actors: international legal standards on freedom of expression, access to information and safety of journalists*. Retrieved from UNESDOC Digital Library: https://unesdoc.unesco.org/ark:/48223/pf0000378755

UNESCO. (2022). Retrieved from Freedom of Expression and the Rule of Law: https://www.unesco.org/en/freedom-expression-rule-law

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75, 547-559.