COIMBRA UNIVERSITY
European Master's Degree in Human Rights and Democratisation
A.Y. 2018/2019

Blockchain and Journalism:

the intersection between blockchain-based technology and freedom of the press

Author: Meredith Veit
Supervisor: Jónatas Machado

Biography:

Meredith has worked as a writer, multimedia journalist and researcher in Kenya, Botswana, Zimbabwe, the Democratic Republic of the Congo, South Africa, Namibia, Burkina Faso, Côte d'Ivoire, Argentina, Chile, and Mexico. She holds a B.A. in Communication & Public Culture from The George Washington University and following the completion of her undergraduate degree, she interned for former Vice President Joe Biden at the White House. This research is inspired by her experiences and the inspirational journalists that she has met along the way.

Abstract:

Quality journalism is essential to democracy, as it is a means of empowering people with information. Yet, journalists, and press freedom itself, are under threat. The number of journalist assassinations and forced disappearances is increasing as the World Press Freedom Index rankings achingly decline across the board. Most State protection mechanisms are currently insufficient in shielding journalists from escalating violence—irrespective of whether or not these journalists report from a country in peacetime or at war. As a result, technologists have begun developing powerful tools in an effort to ensure that journalists and human rights defenders alike are more prepared in the face of danger.

Yet, technological integration as an added safety and security mechanism is far from seamless. This paper critically reviews the new technologies offered to journalists—those that have succeeded and failed—in an attempt to consolidate the lessons learned from both journalistic and technological perspectives. Resultantly, there is a theoretical gap in how the offerings of modern technology, namely blockchain, could serve as an indispensable tool to better protect journalists and the journalistic process, if applied correctly and realistically. This paper examines the convergence of blockchain and journalism; combining theoretical proposals from academia with the pragmatic technological developments underway and ultimately expanding upon the suggestions for potential applications.

Furthermore, this paper proposes blockchain-based smart contracts as an innovative tool for combating the high impunity rates for those who commit crimes against journalists—particularly assassinations and disappearances. The author argues that an important use of blockchain could be to establish a journalistic version of a 'last will and testament.' This will ensure that essential stories do not die along with journalists who are assassinated while covering them and that those investigating the murders have greater access to pivotal evidence. However, any and all blockchain-based applications must first be vetted through an anti-techno-solutionist lens to assure that they are the most fitting tool for achieving the aim.

Keywords: blockchain, journalism, freedom of the press, technology, smart contracts, techno-solutionism, violence against journalists, decentralization

Acknowledgements:

I would like to sincerely thank Coimbra University's Human Rights Centre for hosting my research. More particularly, I want to offer my utmost gratitude to Carla de Marcelino Gomes and Jónatas Machado, who have not only exhibited a tremendous amount of support throughout this entire process, but also serve as wonderful role models for those doing critical human rights work through academia.

A special thank you and an awed appreciation goes to the RightsCon community, which is a group of some of the most inspiring human rights defenders that I have ever met. To Mohammed Al-Maskati, thank you not only for making that experience possible and better informing my research, but for being such an exceptional person. To Laura Thomi for her encouragement and insights. And thank you to João Machado and Amanda James for keeping me motivated.

To all of the journalists who continue to dig deeper regardless of the risks, especially those fighting for the credibility of journalism through the power and impact of their work.

Table of Abbreviations:

ASIC	Application Specific Integrated Circuits
BTC	Bitcoin tokens
CIA	The United States Central Intelligence Agency
CJFE	Canadian Journalists for Free Expression
CPJ	Committee to Protect Journalists
CVL	Civil Media Company token
DApp	Decentralized Application
ETH	Ethereum tokens
GCHQ	British Government Communications Headquarters
ICCPR	International Covenant on Civil and Political Rights
IoT	Internet of Things
IWMF	The International Women Media Foundation
NGO	non-governmental organization
NSA	The United States National Security Agency
OHCHR	The Office of the United Nations High Commissioner for Human Rights
OS	Operating System
RSF	Reporters Without Borders
UAT	Universal Attention Token
UN	United Nations
UNESCO	The United Nations Educational, Scientific and Cultural Organization
UNDG	The United Nations Development Group
UNDP	The United Nations Development Programme
UNHCR	The United Nations High Commissioner for Refugees

UNICEF	The United Nations Children's Fund
UNOPS	The United Nations Office for Project Services
USAID	United States Agency for International Development
Will	A Last Will and Testament
WFP	The World Food Programme

Table of Contents:

List of Graphics:

Introduction

Violence against journalists and impunity for those who commit crimes against them are the principal threats to freedom of expression worldwide, and this has a ripple of consequences which affect other inalienable rights—most directly related, but not limited to: freedom of assembly, freedom of thought, conscience and religion, and freedom of association.[1] Freedom of expression is what stimulates communication needed to institute positive change and societal growth, and that expression also allows for informed citizens to participate in civil and political spheres.[2] Quality journalism plays an essential role in educating the public, and the best argument for providing greater protection for journalists is imagining a dystopian democratic system without the investigatory nature of journalism itself. For every journalist that dies or disappears, there are countless stories left uncovered, truths that will never come to light, and connections that may never be made—referring not only to current investigations, but the research and fact-finding contributions that would have taken place throughout their lifetime. This paper seeks to explore how journalists should implement technology as a tool to improve protection for journalists while working in the field and to highlight new ideas surrounding these technological advancements that are worthy of further exploration.

The paper develops as follows: Part 1 first explains the gravity and increasing frequency of attacks—both physical and digital—on the media and subsequently analyzes how technology has proved or attempted to prove itself useful for safeguarding the journalistic process as well as journalists themselves. The comparisons and critical reviews of existing technological applications provide a fundamental understanding of how technology and journalism already overlap in regards to safety and security. This is followed by an explanation of a theoretical gap in academia and practice—which is the potential for decentralized information storage and blockchain-based systems in reinforcing freedom of the press and protecting journalists. Though this is a non-technical paper, the basics of blockchain technology are explained in Part 2 through analogies that are relevant to the news industry; this is to provide a more suitable theoretical approach to blockchain's potential journalistic applications. Part 3 further contextualizes how the media has attempted to implement blockchain and accumulates the current theories in circulation concerning how this technology could alleviate some of the industry's most dire pains. Having analyzed current practical and theoretical applications of blockchain to journalism, it is apparent that academia and practitioners fail to consider blockchain's potential for aiding in the protection of individual journalists, which is proposed in Part 4. Finally, Part 5 expands upon the previous arguments to outline how smart contracts in particular—a functionality only possible through blockchain technology—have the potential to streamline and provide more evidence for judicial

[1] Article 19, 'Acting on UN Human Rights Council Resolution 33/2 on the Safety of Journalists' (2017) 48 <https://www.article19.org/wp-content/uploads/2018/02/safety_of_journalists_WEB_23.10.pdf> accessed 12 May 2019.

[2] As stipulated in point 1.4 of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity, freedom of expression is an individual and collective right. This means that not only should no individual be in danger of death or persecution as a result of their expression, but this freedom is what "empowers populations through facilitating dialogue, participation and democracy, and thereby makes autonomous and sustainable development possible." Based on this logic, freedom of the press must also be both an individual and collective right, and protected to a more serious degree.
UNESCO, 'UN Plan of Action on the Safety of Journalists and the Issue of Impunity' (2016) <https://en.unesco.org/un-plan-action-safety-journalists> accessed 16 May 2019.

proceedings related to crimes against journalists—particularly murder and forced disappearances—and reduce the impunity rates for said crimes.

This paper both accumulates and qualitatively analyzes academic articles and civil society reports, providing a comprehensive overview of the potential for the intersection of blockchain and journalism. In addition, it incorporates first-hand reviews for technologies aimed at protecting journalists, and after testing the existing software, programs and applications available, the aim of this research is to gauge whether or not adding a blockchain-based tool is necessary or practical. An additional aim is to find out if blockchain is a techno-solutionist approach to solving a problem too complex for any computer code to resolve by itself. Considering blockchain is the most well-known decentralized storage technology, this paper aims to unpack its uses, pitfalls and benefits within the context of a global decline in press freedom. The research questions are: What are the most promising applications of blockchain to protect journalists, if any? More importantly, would blockchain technology work in practice?

Scholars often say that technology is neither inherently good nor bad, but its evaluation depends on its application. The same idea applies to whether or not the government, a non-governmental organization (NGO), or a company using technology to accomplish human rights endeavors has properly valued its true impact. Techno-solutionism is the oversimplified and overly optimistic belief that technology is the be-all-end-all for resolving complex societal issues.[3] For example, some techno-solutionists argue that self-driving tractors will solve an impending global food shortage;[4] blockchain based voting apps will fix broken democracies;[5] or even that energy-efficient cars will eliminate climate change.[6] The idealization of technology and its impacts can cause great discrepancies between the desired and actual outcomes of utilizing it,[7] and the proliferation of tech-buzzwords used in substitution for well-elaborated impact assessments has shifted the definition of 'innovation' to now require some kind of technological aspect.[8] Technology certainly plays an important role in today's challenges, and though its use can potentially provide targeted solutions, new technology can never be a stand-alone fix. It is important that those wishing to employ new technologies, especially in human-rights-related situations, ask these questions: Will this technology be worth the investment? Does a better, low-tech solution exist? And who will this technology really benefit most? While many technological

[3] Seyram Avle, David Li and Silvia Lindtner, 'Responsible IoT after techno-solutionism' (*Medium*, 27 August 2018) <https://medium.com/the-state-of-responsible-iot-2018/responsible-iot-after-techno-solutionism-cf583e5f9b9a> accessed 20 June 2019.

[4] Natalie Gagliordi, 'How self-driving tractors, AI, and precision agriculture will save us from the impending food crisis' (*TechRepublic*, 12 December 2018). <https://www.techrepublic.com/article/how-self-driving-tractors-ai-and-precision-agriculture-will-save-us-from-the-impending-food-crisis/> accessed 20 June 2019.

[5] Connie Loizos, 'Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it' (*TechCrunch*, March 2019) <https://techcrunch.com/2019/03/07/voatz-the-blockchain-based-voting-app-gets-another-vote-of-confidence-as-denver-agrees-to-try-it/> accessed 20 June 2019.

[6] Meghan L. O'Sullivan, 'Technology & Ideas: If All Vehicles Go Electric, That's Just Step One' (*Bloomberg Opinion*, 14 January 2019) <https://www.bloomberg.com/opinion/articles/2019-01-14/electric-vehicles-are-just-one-step-to-address-climate-change> accessed 20 June 2019.

[7] Christo Sims, *Disruptive Fixation: School Reform and the Pitfalls of Techno-Idealism* (Princeton University Press, 2017) pages 51-59.

[8] Oren Levine, Director of innovation for the International Center for Journalists side-event (Speech at RightsCon, 12 June 2019).

innovations or applications have roots in good intentions, relying on technology to be a silver-bullet solution will only lead to lost time, money, and resources.[9]

Blockchain has been a buzzword in newspaper headlines, executive boardrooms, university centers for innovation, and also within the human rights community in recent years. Conclusively, blockchain is useful for three types of uniquely attributable applications: ensuring tamper free evidence; decentralization from a single authority; and the transparency of data flow. Projects focused on achieving those aims should consider blockchain, while all other projects should not. These applications could be useful in protecting journalists' work and potentially journalists themselves by permanently and transparently logging security breaches, decentralizing control over stored and shared information, and securely localizing journalists in distress. Furthermore, smart contracts could be used to establish a journalistic version of a 'last will and testament' (hereafter referred to as a Will), which would ensure the flow of valuable information in dire circumstances. The suggestions proposed by the author in Parts 4 and 5 are positioned as particular solutions for specific problems facing a targeted group, but these suggestions are by no means autonomous nor are they implying that the need for grander societal changes are irrelevant.

Part 1: Journalists' under attack — in both the physical and digital spheres

1.1 Targeting journalists

Journalists face mortal threats daily in the course of their investigations, and often become targets for assassination, over a variety of motives. For example, consider:

- drug traffickers kidnapped and murdered Paúl Rivas Bravo, a photojournalist for Ecuadorian daily *El Comercio,* along with journalist Javier Ortega and driver Efraín Segarra;
- criminals with concealed identities abducted Musa Abdul Kareem of the Libyan newspaper *Fasanea;*
- an unknown individual shot and left Jefferson Pureza Lopes, a radio presenter in Brazil for dead in his living room;
- Ján Kuciak, an investigative journalist for the Slovakian news website *Aktuality.sk*, and his fiancée Martina Kušnírová were also found murdered in their home, sparking mass protests;
- a man walked into the *Capital Gazette* newsroom in Maryland with a shotgun, killing Rob Hiaasen and four other journalists (the perpetrator himself a disgruntled former subject of the paper's articles);
- an assassin shot Leslie Ann Pamela Montenegro del Real, a YouTuber and online news publisher, at the restaurant she owned;
- one of the most egregious examples of violence against the press in recent history was the suicide bombing that killed at least nine journalists in Afghanistan, including Maharram Durrani, a producer at *Radio Azadi.*

[9] Satvik Shukla, 'Get to Know Berkman Klein Fellow Dragana Kaurin' (*Berkman Klein Center for Internet & Society at Harvard University*, 5 February 2019) <https://cyber.harvard.edu/story/2019-02/get-know-berkman-klein-fellow-dragana-kaurin> accessed 20 June 2019.

The above list,[10] courtesy of *The Guardian*, pays tribute to several of the over seven dozen journalists assassinated in 2018. Locating a safe working environment as a journalist is more difficult now than ever. Today, journalists are warned to take extra precautions while covering protests and elections. The U.S. Press Freedom Tracker finds that newsworthy events with large gatherings of people—formerly neutral grounds in the United States—are now 'hot zones' for attacks. This intrinsically states that the media is no longer safe, not only in its own right, but also alongside the activities of citizens expressing their freedom of expression or assembly.[11] Journalists working in unsafe-for-press zones such as Mexico are warned that, statistically, their own homes are the most dangerous places for them to be.[12]

At least 702 professional journalists were murdered over the past decade, with an additional 62 journalists reported missing according to Reporters Without Borders (RSF).[13] The International Federation of Journalists confirmed that at least 88 journalists and media workers were assassinated in 2018, which is a double-digit increase from the year prior.[14] Approximately 61% of those 702 journalists previously mentioned were deliberately killed due to the content of their investigations, proving that journalists—not just those operating in conflict zones—are at a greater risk, merely because of their profession.[15] In fact, nearly half of 2018's media fatalities occurred in countries at peace.[16] Incarceration of journalists is also up by 7%, with a total of 348 journalists currently detained in connection with their work.[17] China, Turkey, Egypt, Iran, and Saudi Arabia combined are imprisoning more than half of the world's detained journalists.[18] These statistics do not include the reported and unreported incidents of torture, intimidation, harassment, and censorship of the press.

1.2 The importance of press freedom

These assaults on the press are not only an offense against the individual right to freedom of expression, but they more potently infringe upon the right to information, further denying the public access to facts they have a right to know, as stipulated under Article 19 of the International

[10] Aamna Mohdin and Bibi van der Zee, ''Killed for speaking the truth': tributes to nine journalists murdered in 2018' *The Guardian* (London, 5 December 2018) <https://www.theguardian.com/media/2018/dec/05/journalists-murdered-khashoggi-kuciak-panama-papers> accessed 13 May 2019.

[11] U.S. Press Freedom Tracker, 'All Incidents' (2019) <https://pressfreedomtracker.us/all-incidents/?search=protes> accessed 13 May 2019.

[12] This was a closed workshop that took place at the Club de Periodistas in CDMX on March 27, 2018. The event name was "Acciones de fortalecimiento para la prevención de agresiones en medios" run by USAID and the OHCHR.

[13] RSF, 'Worldwide round-up of journalists killed, detained, held hostage, or missing in 2018' (2019) 1-24. <https://rsf.org/sites/default/files/worldwilde_round-up.pdf> Accessed 13 May 2019.

[14] Al Jazeera, 'Number of journalists killed on the job in 2018 rises' (30 December 2018) <https://www.aljazeera.com/news/2018/12/number-journalists-killed-job-2018-rises-181231021858196.html> accessed 13 May 2019.

[15] RSF (n. 13) 7.

[16] According to RSF numbers. Section 3.3. ibid 10.

[17] ibid 13.

[18] ibid 14.

Covenant on Civil and Political Rights (ICCPR).[19] Depriving society of quality journalism inherently reduces governmental accountability, and human rights NGO *Article 19* explains that, “Stories that people would literally kill to suppress are often the most important for the public to know. They detail organized crime, conflict, environmental degradation, corruption; the journalists on these beats play an essential role in society.”[20] International human rights treaty bodies have further stipulated that the right to information plays a critical role in the enjoyment of other basic rights, such as: the right to privacy; the right to take part in public affairs; the right to a fair trial; the right to life; and numerous social and economic rights.[21]

Quality journalism is critical for democracy and transparency, as well as combating corruption. The role of journalism is to seek truth, and a republic needs truthful information in order to function.[22] Journalism is also a check on those in power, bringing to light critical issues that go unnoticed or are purposefully suppressed. In particular, the media is crucial in uncovering human rights violations, such as: *The Dallas Morning News*’ reports on thousands of sick and disabled citizens who were denied life-sustaining medicine and their right to health; PBS uncovering the labor trafficking of migrant children working on egg farms in the United States, which highlighted the importance of children's rights; ProPublica’s investigation of two men’s wrongful convictions, pushing for the right to their fair trial.[23] Furthermore, the press is an instrument for collecting and disseminating impartial information and without it, corruption is left unbridled.[24] The Panama Papers grew out of reporting that uncovered secret financial havens for wealthy and powerful figures across the globe, and the investigations the International Consortium of Investigative Journalists sparked had the result of revealing $1.2 billion in back-taxes and penalties owed to governments and the general public.[25]

Both French and American revolutionaries established freedom of the press as a basic right in the founding of their democracies. The United States Constitution, given life by a nation that claims to be one of the strongest proponents of freedom of expression, embodies anti-corruption principles, rooted in a system for the separation of governing powers, but also in an empowered

[19] OHCHR, ‘International Covenant on Civil and Political Rights’ (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> accessed 15 May 2019.

[20] Article 19, ‘UN must translate words into action on journalists’ safety’ (20 September 2018) <https://www.article19.org/resources/un-must-translate-words-into-action-on-journalists-safety/> accessed 13 May 2019.

[21] Maeve McDonagh, ‘The Right to Information in International Human Rights Law’ (March 2013) 13(1) Human Rights Law Review <doi:10.1093/hrlr/ngs045> accessed 13 May 2019.

[22] Dan Rather and Elliot Kirschner, *What Unites Us: Reflections on Patriotism* (Kindle edn, Algonquin Books of Chapel Hill 2017) page 26.

[23] Harvard Kennedy School Shorenstein Center on Media, Politics, ‘2019 Goldsmith Prize Finalists: Shorenstein Center Announces Seven Finalists for 2019 Goldsmith Prize for Investigative Reporting; Marty Baron to Receive Career Award’ (6 February 2019) <https://shorensteincenter.org/2019-goldsmith-prize-finalists/> accessed May 23 2019.

[24] OECD, ‘The role of media and investigative journalism in combating corruption’ (27 March 2018) pages 16-18 <https://www.oecd.org/corruption/the-role-of-media-and-investigative-journalism-in-combating-corruption.htm> accessed 23 May 2019.

[25] International Consortium of Investigative Journalists, ‘Panama Papers Helps Recover More Than $1.2 Billion Around The World’ (2019) <https://www.icij.org/investigations/panama-papers/> accessed 23 May 2019.

free press.[26] The First Amendment explicitly prioritizes freedom of the press alongside freedom of speech, insinuating that the 'press' plays a separate yet important role in the functionality of a corruption-free democratic republic.[27] Wiebke Lamer argues that press freedom is more important than free speech, as the press serves as a quasi-political institution, a source of information and context and a social glue that holds communities together.[28] Press freedom is distinct from an individual's right to freedom of expression, in that the press has the power of mass distribution as well as being an organized accountability mechanism. Thus, the impact of the press on society is more influential than the average individual opinion or expression.[29]

Specific cases supporting the importance of freedom of the press can be elucidated from domestic and international law. The U.S. case of *People v. Croswell* in 1804, permitted the 'truth' to be a reasonable defense against libel accusations, laying the groundwork for other historical cases that protect freedom of the press as an engine for informed, accountable governance. United States Supreme Court cases such as *Near v. Minnesota*, *New York Times v. Sullivan*, *Curtis Publishing Co. v. Butts and AP v. Walker*, *New York Times v. United States*, and *Nebraska Press Association v. Stuart* position the press as a critical megaphone for truth, regardless of a subject's job title or political standing, or the government's desire for censorship based on claims of defamation or national security.[30] The European Court of Human Rights (ECtHR) also established the importance of preserving several important aspects of journalism, including: journalists' sources in *Goodwin v. the United Kingdom*; journalists' access to public or official documents in *TASZ v. Hungary*; whistleblowers in *Guja v. Moldova*; and the right of newsgathering in *Dammann v. Switzerland.* Part of the journalistic process requires that the government does not surveil investigative journalists, a principle which ECtHR[31] has also discussed. More currently, this principle came under fire in Germany with the Bundesnachrichtendienst (BND) law which permits Germany's intelligence agency to spy on foreign journalists. An alliance of NGOs and journalists' associations are currently fighting the law with a lawsuit, coupled with the No Trust, No News initiative.[32] Finally, the European Court reiterated the State's positive obligation to "create a favourable environment for participation in public debate by all the persons concerned, enabling them to express their opinions and ideas without fear" with cases relating to violent attacks against journalists in *Uzeyir Jafarov v. Azerbaijan and Huseynova v. Azerbaijan.*[33] Judicial bodies have

[26] Zephyr Teachout, 'The Anti-Corruption Principle' (2009) 94 (2) Cornell Law Review <https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=3123&context=clr> accessed 23 May 2019.

[27] Peter Greste, 'The Case For A Media Freedom Act' (*Alliance for Journalists' Freedom*, 5 February 2019) <https://www.journalistsfreedom.com/case-for-media-freedom-act/> accessed 23 May 2019.

[28] Wiebke Lamer, *Press Freedom as an International Human Right* (Kindle edn, Palgrave Pivot 2018) 17-41.

[29] ibid 40-41.

[30] Bill of Rights Institute, 'Freedom of the Press' <https://billofrightsinstitute.org/educate/educator-resources/landmark-cases/freedom-of-the-press/> accessed 23 May 2019.

[31] Rachel Oldroyd, 'The Bureau wins landmark press freedom case at the European Court of Human Rights' (*The Bureau of Investigative Journalism*, 13 September 2018) <https://www.thebureauinvestigates.com/stories/2018-09-13/bureau-wins-case-to-defend-press-freedom-at-the-european-court-of-human-rights> accessed 21 May 2019.

[32] No Trust No News, 'We have filed a lawsuit against the BND Law' (2018) <http://notrustnonews.org/?lang=en> accessed 21 May 2019.

[33] Dirk Voorhoof and others and Tarlach McGonagle (Ed. Sup.), Freedom of Expression, the Media and Journalists: Case-law of the European Court of Human Rights (2017) IRIS Themes 3, *European Audiovisual Observatory* 351 422
<https://rm.coe.int/freedom-of-expression-the-media-and-journalists-iris-themes-vol-iii-de/16807c1181> accessed 24 May 2019.

continually reaffirmed that freedom of the press is important to a democratic society, and it can strengthen the rule of law.

Yet, justice systems seldom resolve individual crimes against journalists, suggesting murder to be a viable solution for perpetrators that do not want journalists to leak incriminating stories or allow sensitive investigations to continue. The ratio for global impunity leaves nine out of ten of these crimes unsolved and without consequence, which compounds the violent acts and contributes to their recurrence.[34] On the International Day to End Impunity for Crimes Against Journalists in 2018, Audrey Azoulay, Director-General of UNESCO, noted that "it is our responsibility to ensure that crimes against journalists do not go unpunished. We must see to it that journalists can work in safe conditions, which allow a free and pluralistic press to flourish."[35] Her remarks coincide with a steadily increasing journalist-mortality rate, which has been on the rise since the start of this millennium. Relatedly, the murder and impunity rates correspond with an expected decline in healthy media coverage, which factors into an ongoing 'global slump' in press freedom.[36]

1.3 Using technology against journalists

The spread of malware creates greater risk for journalists to be susceptible to cyber-attacks, putting both journalists and their sources "increasingly at risk of identification, prosecution, and persecution by powerful entities, threatening efforts in investigative reporting, transparency, and whistleblowing."[37] In Mexico, for example, there were reports of the government using advanced spyware to collect information on prominent journalists and human rights activists.[38] Specifically, a software called Pegasus infected the cellphones of some of Mexico's most famous journalists and lawyers. Pegasus is capable of reading text messages, hacking the phone's camera and microphone, tracing and recording calls, keystroking passwords, tracking the location of the phone, and gathering sensitive information from its applications. These activists were either involved in investigations related to cartel activity[39] or researching the infamous case of 43 missing students who mysteriously disappeared after encountering the police.[40] Pegasus was sold to the

[34] Elisabeth Witchel, 'Getting Away with Murder' (*CPJ*, 2018) 3 <https://cpj.org/reports/2018/10/impunity-index-getting-away-with-murder-killed-justice.php> accessed 13 May 2019.

[35] International Programme for the Development of Communication, '2018 DG Report on the Safety of Journalists and the Danger of Impunity'(UNESCO, 2018) CI-18/COUNCIL-31/6 REV.2 <https://unesdoc.unesco.org/ark:/48223/pf0000265828> accessed 15 May 2019.

[36] Freedom House, 'Freedom of the Press 2017: Press Freedom's Dark Horizon' (2017) <https://freedomhouse.org/report/freedom-press/freedom-press-2017> accessed 15 May 2019.

[37] Susan E. McGregor and others, 'Investigating the Computer Security Practices and Needs of Journalists' (USENIX 2015) 399 <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf> accessed May 14 2019.

[38] Azam Ahmed, 'Mexico to Investigate Spying Campaign Against Journalists and Activists' *New York Times* (Mexico City 21 June 2017) <https://www.nytimes.com/2017/06/21/world/americas/mexico-pena-nieto-spying-hacking-surveillance.html> accessed 13 May 2019.

[39] John Scott-Railton and others, Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague' (*The Citizen Lab*, 27 November 2017) <https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/> accessed 15 May 2019.

[40] Azam Ahmed and Nicole Perlroth, 'Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families' *New York Times* (Mexico City 19 June 2017)

Mexican government by the Israeli cyberarms company NSO Group.[41] A recent *DNS Cache Probing* study uncovered that the spyware was sold to operators in 45 different countries,[42] and that journalists were frequently on the list of targeted actors. Citizen Lab researchers have also found that Pegasus was involved in Saudi Arabia's intricately organized murder of journalist Jamal Khashoggi in 2018.[43]

Other examples of government surveillance of journalists include the United States Justice Department's covert collection of journalists' phone records and investigations,[44] the French government's illegal interception of phone records from *Le Monde* reporters,[45] the British intelligence agency GCHQ's monitoring of journalists' emails,[46] and the State-sponsored hacking of journalists for pervasive surveillance in China.[47] For example, the Chinese government created a fake survey embedded with malware and sent it to the employees of a Beijing-based news office, which they then used to track 10 of the office's employees.[48] Germany,[49] Russia,[50] and Israel[51] all have similar incidents on record of using invasive technology to spy on foreign journalists. Most recently, the U.S. government was secretly logging a database of activists and journalists that worked in relation to the 2018 'migrant caravan' of refugees traveling from Central America

<https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html?module=inline> accessed 14 May 2019.

[41] Redacción AN, 'La denuncia y el informe completo sobre #GobiernoEspía (Documentos)' (*Aristegui Noticias*, 20 June 2017) <https://aristeguinoticias.com/2006/mexico/la-denuncia-y-el-informe-completo-sobre-gobiernoespia-documentos/> accessed 15 May 2019.

[42] Algeria, Bahrain, Bangladesh, Brazil, Canada, Côte d'Ivoire, Egypt, France, Greece, India, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Mexico, Morocco, the Netherlands, Oman, Pakistan, Palestine, Poland, Qatar, Rwanda, Saudi Arabia, Singapore, South Africa, Switzerland, Tajikistan, Thailand, Togo, Tunisia, Turkey, the United Arab Emirates, Uganda, the United Kingdom, the United States, Uzbekistan, Yemen, and Zambia. Bill Marczak and others, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' (*The Citizen Lab*, 18 September 2018) <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> accessed 15 May 2019.

[43] CNN, 'Saudi's use social media to hunt down dissenters' (*Quest Means Business*, 22 October 2018) <https://www.youtube.com/watch?v=A1xgYWxl6fQ&feature=youtu.be> accessed 15 May 2019.

[44] Charlie Savage and Leslie Kaufman, 'Phone Records of Journalists Seized by U.S.' *New York Times* (Washington 13 May 2013) <http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html> accessed 15 May 2019.

[45] Jean-Paul Marthoz, 'Spying on media exposes French government's dark side' (*CPJ*, 3 September 2011) <https://cpj.org/blog/2011/09/spying-on-media-exposes-french-governments-dark-si.php> accessed 15 May 2019.

[46] James Ball, 'GCHQ captured emails of journalists from top international media' *The Guardian* (London 19 January 2015) <http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post> accessed 15 May 2019.

[47] Shane Huntley and Morgan Marquis-Boire, 'Tomorrow's News is Today's Intel: Journalists as Targets and Compromise Vectors by Shane Huntley' (*Black Hat*, 3 August 2014) <https://www.youtube.com/watch?v=7mI-qCRohWU> accessed 14 May 2019.

[48] ibid.

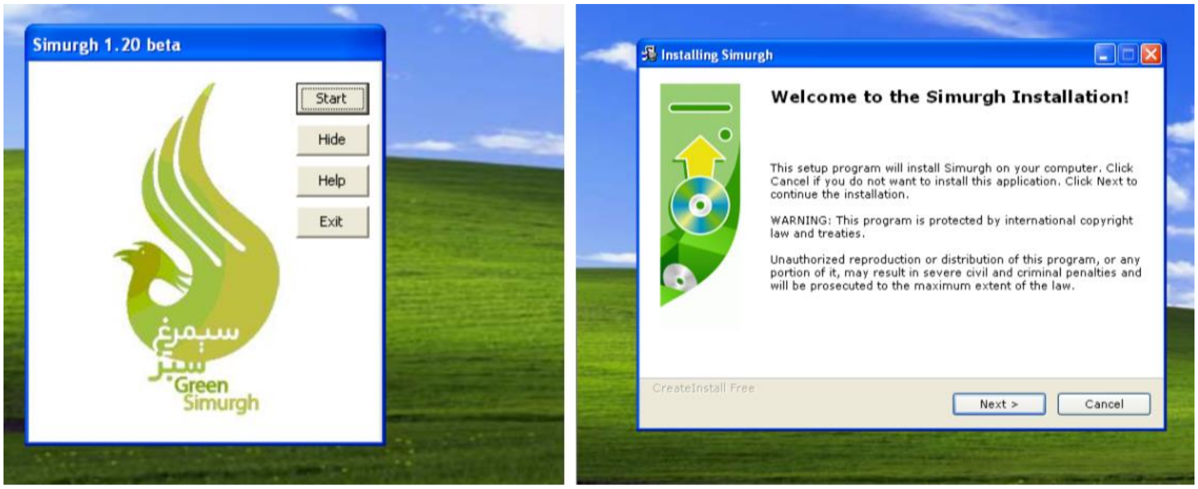
[49] Maik Baumgärtner, Martin Knobbe and Jörg Schindler, 'Documents Indicate Germany Spied on Foreign Journalists' (*Der Spiegel*, 24 February 2017) <https://www.spiegel.de/international/germany/german-intelligence-spied-on-foreign-journalists-for-years-a-1136188.html> accessed 15 May 2019.

[50]Scott Shane, 'When Spies Hack Journalism' *New York Times* (Washington 12 May 2018) <https://www.nytimes.com/2018/05/12/sunday-review/when-spies-hack-journalism.html> accessed 15 May 2019.

[51] Nicole Perlroth and Ronen Bergman, 'WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone' *New York Times* (San Francisco 13 May 2019) <https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html> accessed 13 May 2019.

towards the United States, placing alerts on these media employees' passports and ordering further scrutiny in their interrogations.[52]

Susan McGregor notes that many journalists are illiterate when it comes to cybersecurity protections and the use of secure applications for media-related communication.[53] She suggests that journalists are overwhelmed by the frequency of technological updates on which apps are the most secure to use in the field, just to give one example. Not only are new applications constantly in development, but cybercriminals are creating fake versions of these supposedly liberating circumvention tools. For example, Simurgh is a proxy tool used to overcome censorship in Syria and Iran; however, a fake and trojan-ized version was also developed so governments could identify potential users. False recreations of digital safety and security tools like Tor and FreeGate are also in circulation,[54] which shows how difficult it is for journalists to stay one step ahead of phishing schemes and hackers, as well as their own governments.



Welcome to the Simurgh Installation!

This setup program will install Simurgh on your computer. Click Cancel if you do not want to install this application. Click Next to continue the installation.

WARNING: This program is protected by international copyright law and treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties and will be prosecuted to the maximum extent of the law.

Figure 1: Display of the real Simurgh (left) compared to the fake Simurgh (right) which actually contains malware[55]

1.4 A familiar paradox of State accountability

While there have been advancements in terms of overall visibility for the issue of violence against journalists, more favorable jurisprudence in international human rights courts, and new measures have been adopted from regional human rights bodies,[56] aggressions against journalists

[52] Esha Bhandari and Hugh Handeyside, 'The Government Is Detaining and Interrogating Journalists and Advocates at the US-Mexico Border' (*ACLU*, 7 March 2019) <https://www.aclu.org/blog/free-speech/freedom-press/government-detaining-and-interrogating-journalists-and-advocates-us> accessed 16 May 2019.

[53] McGregor and others (n. 37) 403-404.

[54] Aditya Tiwari, 'Don't Use This "Fake TOR Browser" — Scammers Are Fooling People' (*Fossbytes,* 13 July 2017) <https://fossbytes.com/fake-tor-browser-rodeo-scan/> accessed 14 May 2019.

[55] Huntley and Marquis-Boire (n. 47).

[56] In 2015 the East African Court of Justice ruled in favor of journalists' necessity to disseminate information and that journalists cannot be forced to reveal their sources in the *Burundian Journalists Union v. Burundi.* The African Court on Human and Peoples' Rights heard *Konaté v. Burkina Faso* in 2016 ruling in favor of freedom of expression stating that journalists cannot be criminally charged for defamation. The European Court of Human Rights ruled in favor of journalists in 2018, in *Ivashchenko v. Russia* stating the governments cannot make copies of a journalist's laptop and storage devices. In 2018, the Inter-American Commission on Human Rights adopted

continue to occur faster than any established procedure can manage to fix. At the intergovernmental level, the United Nations Plan of Action on the Safety of Journalists and the Issue of Impunity provides a framework for UNESCO to guide the United Nations' activities concerning improving safety for press on the ground.[57] Meanwhile, the Office of the United Nations High Commissioner for Human Rights (OHCHR) monitors the situation of journalists working around the world, reports on violations committed against the press and makes recommendations on their behalf in accordance with international human rights laws. Perplexingly, UNESCO and the OHCHR, which are both entities within the same overarching UN system, follow different standards and classifications concerning the monitoring of journalists, and even produce different statistics on those that are missing or assassinated—which metaphorically highlights a larger global misalignment on the realities of this issue.

The Human Rights Council's non-binding Resolution 33/2, which was adopted in 2016, pushes for States to better prevent attacks, protect journalists, and prosecute offenders, while protecting the journalistic process in law, policy and practice.[58] A long list of countries led and co-sponsored the Resolution, some of which are now among the greatest offenders against press freedom—such as Brazil, Mexico, Honduras, Russia, and Yemen.[59] Without heavy-handed consequences, elected officials continue to reap the benefits of impunity for crimes against the press. The work of the United Nations is critical for amplifying attention to the need for press freedom, and it is pushing a multilateral approach to solving the current problems, yet there is little evidence to show that the mechanisms currently in place will be able to reduce the frequency of violence against journalists, or diminish the impunity rate.

The Resolution also recognizes that State actors, though not the only perpetrators, are often involved in attacks against journalists,[60] and many high-level elected officials around the world perpetuate a culture of criticism and violence against journalists by feeding a vicious anti-media narrative. In the thick of corruption, overreaching surveillance and a tightened grip on media, many more journalists are working in an environment where they cannot rely on the State for protection; the number of countries considered 'safe' for journalists also continues to decline.[61] In fact, many government-run protection programs fail to properly execute their functions,[62] with Mexico being a prime example. Recently, Rafael Murúa Manríquez[63] was killed under the watch of Mexico's

resolution 3/2018, which contained measures to expedite the processing of requests for precautionary measures regarding the safety of journalists. OHCHR, Safety of journalists: Report of the United Nations High Commissioner for Human Rights (10–28 September 2018) A/HRC/39/23 <https://www.ohchr.org/Documents/Issues/Journalists/A_HRC_39_23_EN.docx> accessed 13 May 2019.

[57] UNESCO (n. 2).

[58] Article 19 (n.1) 33-40.

[59] ibid 6.

[60] ibid 37-38.

[61] RSF, '2019 World Press Freedom Index – A cycle of fear' (2019) <https://rsf.org/en/2019-world-press-freedom-index-cycle-fear> accessed 16 May 2019.

[62] Daniela Pastrana, 'Protection of Journalists Fails in Latin America' *IPS* (Mexico City 29 April 2017) <http://www.ipsnews.net/2017/04/protection-of-journalists-fails-in-latin-america/> accessed 16 May 2019.

[63] CPJ, 'Rafael Murúa Manríquez' (2019) <https://cpj.org/data/people/rafael-murua-manriquez/index.php> accessed 16 May 2019.

Federal Mechanism for the Protection of Human Rights Defenders and Journalists, as were Pedro Tamayo Rosas,[64] Jesus Eugenio Ramos Rodriguez,[65] and others.

As the journalism industry leans more on freelance writers, photographers, and videographers for content, more media workers will station themselves in the field and operate entirely on an "at-your-own-risk" basis. Amid a "post-industrial capitalist desire for flexibility and dexterity in staffing" as well as journalism's current need to adapt to the digital revolution of news, the number of freelancers is growing quickly, relative to the overall amount of employed journalists.[66] Freelance journalism by definition is "a person who works as a writer, designer, performer, or the like, selling work or services by the hour, day, job etc., rather than working on a regular salary basis for one employer."[67] Without a full-time employment contract, freelancers are not likely to receive oversight benefits or safety evacuations from any particular company or news outlet, hence why local freelancers often receive the most threats and endure the vast majority of murders, imprisonments and abductions.[68] The number-one item on the list of Freelance Journalist Safety Principles from the Columbia Journalism School is: "Before setting out on any assignment in a conflict zone *or any dangerous environment*, journalists should have basic skills to care for themselves or injured colleagues."[69] This principle demonstrates the necessary assumption that journalists must always prepare for physical harm, as most environments are dangerous for media.

Even big-name news organizations that send journalists to conduct investigative reports are unable to guarantee safety. On May 14, 2019, Greek CNN Reporter Mina Karamitrou's car was destroyed by a bomb.[70] On October 2, 2018, *Washington Post* columnist Jamal Khashoggi was assassinated by a team of Saudi Arabian agents inside the Saudi consulate in Istanbul.[71] Myanmar detained *Reuters* journalists Wa Lone and Kyaw Soe Oo for 18 months in prison and the two were finally released in May 2019.[72] Those that are killing journalists know that knowledge is power,[73] and more often than not, perpetrators equate killing journalists with killing the stories they cover. Many times, when journalists are murdered, critical evidence also dies with them—

[64] PEN International, 'Mexico: failure of protection mechanisms exposed by murder of third print journalist in Veracruz this year' (27 July 2016) <https://pen-international.org/news/mexico-failure-of-protection-mechanisms-exposed-by-murder-of-third-print-journalist-in-veracruz-this-year> accessed 16 May 2019.

[65] Tanja Biscevic, 'Mexico: Second Journalist Murder of 2019' (*OCCRP*, 12 February 2019) <https://www.occrp.org/en/27-ccwatch/cc-watch-briefs/9226-mexico-second-journalist-murder-of-2019> accessed 16 May 2019.

[66] Brian L. Massey and Cindy Elmore, 'Freelancing in Journalism' (*Oxford Research Encyclopedias*, June 2018) <DOI: 10.1093/acrefore/9780190228613.013.818> accessed 16 May 2019.

[67] The Writers Bureau, 'What is Freelance Journalism?' <https://www.writersbureau.com/writing/what-is-freelance-journalism.htm> accessed 16 May 2019.

[68] Dart Center for Journalism & Trauma, 'Freelance Journalist Safety Principles' (12 February 2015) <https://dartcenter.org/content/global-safety-principles-and-practices> accessed 15 May 2019.

[69] ibid.

[70] CPJ, 'Greek CNN reporter Mina Karamitrou's car destroyed by bomb' (14 May 2019) <https://cpj.org/2019/05/greek-cnn-reporter-mina-karamitrous-car-destroyed-.php> accessed 16 May 2019.

[71] Washington Post, 'Jamal Khashoggi' (2018) <https://www.washingtonpost.com/people/jamal-khashoggi/?utm_term=.c7d57fafb6a1> accessed 16 May 2019.

[72] Reuters, 'Reuters Journalists Freed from Myanmar Prison' <https://www.reuters.com/subjects/myanmar-reporters> accessed 15 May 2019.

[73] Louise Williams, 'Censors: At work, censors out of work' in Louise Williams and Roland Rich (eds), *Losing Control: Freedom of the Press in Asia* (ANU Press 2013) <https://www.jstor.org/stable/j.ctt5vj71c.5> accessed 16 May 2019.

which makes destruction of this evidence another principal motive behind these crimes. In situations where the State is unwilling or unable to fulfil its obligation to protect the press—which includes both freelancers and mainstream news media—technology may be a necessary tool to better equip journalists for an increasingly hostile news environment.

1.5 Trials and tribulations of technology

As States, extremist groups, and other human rights offenders use technology for offensive attacks, journalists must better integrate equally, if not more, sophisticated technical defensive strategies into their workflow. However, typically only seasoned reporters with full-time positions at international media houses carry SOS locators and satellite phones. Those that cannot afford such expensive equipment rely on traditional smartphones, email, or social media for their everyday workload.[74] "The needs for security tools that journalists around the world have are vast and diverse," writes Mexican journalist Javier Garza Ramos. In 2016, Garza Ramos found that 60% of journalists (from a sample size of 154) do not regularly use digital security tools to protect themselves.[75]

Digital security for journalists can refer to a combination of encryption strategies, geo-tracking, or circumvention routers.[76] "Cryptography shifts the balance of power from those with a monopoly on violence to those who comprehend mathematics and security design," states Jacob Appelbaum, activist and core member of the Tor project.[77] Surveys show, however, that device, file storage, and communication encryptions remain scarce. Only around 30% of professional journalists use encrypted communications between colleagues and sources, only 17% have encrypted their laptops, mobile phones and tablets to avoid searches,[78] and the vast majority are not visually obscuring their collected information (i.e. blurring photos or videos).[79] Respondents also claimed to use Google Drive or Dropbox as "encrypted tools" for storing and sharing files, unaware that neither platform used any actual encryption at the time. McGregor notes that it is imperative for the technology community to protect media by understanding "the practices, constraints, and needs of journalists, as well as the successes and failures of existing tools."[80] An entirely secure and consolidated tool, made specifically for journalists to store their work, log security breaches, or track their location without fear of government surveillance or hacking, has yet to exist.

In 2012, Amnesty International, Google, The Engine Room and Frontline Defenders began developing an app called 'Panic Button,' that would function as an alert system for human rights

[74] Javier Garza Ramos, 'Journalist Security in the Digital World: A Survey Are We Using the Right Tools?' (CIMA, March 2016) 3 <https://www.cima.ned.org/resource/journalist-security-in-the-digital-world/> accessed 18 May 2019.

[75] ibid 3.

[76] Frontline Defenders, 'Digital Security Resources' <https://www.frontlinedefenders.org/en/digital-security-resources> accessed 23 June 2019.

[77]Andy Greenberg, *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World's Information* (Kindle edn, Dutton 2012) 94.

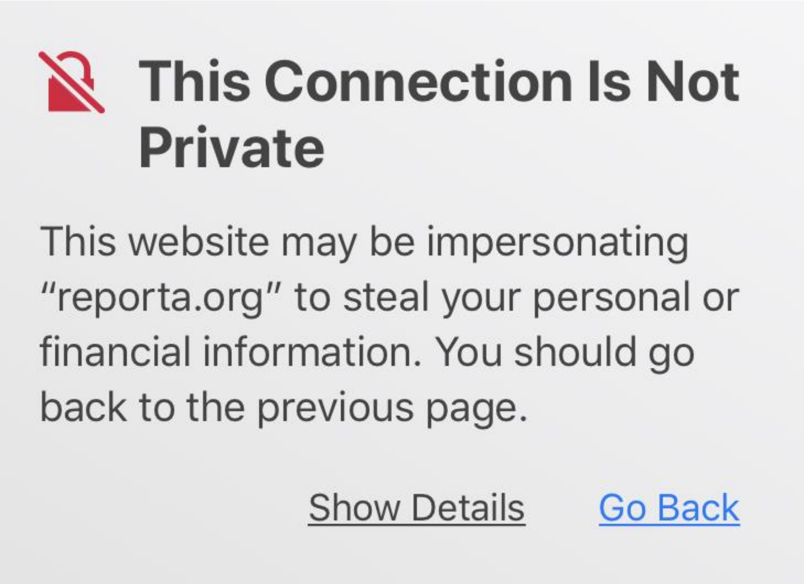
[78] Garza Ramos (n.74) 6.

[79] McGregor and others (n. 37) 407.

[80] ibid 339.

defenders in danger.[81] An activist could activate an SOS signal from their phone, which the app would relay to a trusted inner circle of contacts for someone to take appropriate action. After five years of iterations and development, the collective decided to cease support for the project, citing three main reasons for the discontinuation: lack of funding for sustainable maintenance, inability to resolve a major technical issue with false alerts, and lack of human resources in order to sustain engagement with users.[82] However, the suspension of this project is not a testament to its lack of worth. The location of a journalist or human rights defender in distress is likely the most valuable piece of information for those intending to come to his or her aid.

In 2015, the International Women Media Foundation (IWMF) launched a similar initiative called Reporta, which is a freely downloadable app aiming to serve the same alert system function as Panic Button. Elisa Lees Muñoz, executive director of IWMF, stated in the Reporta press release that “Now more than ever, it is critical to equip journalists with a free tool to help them stay safe and best positioned to continue to tell the significant stories of our time.”[83] Reporta would send an email with the journalist’s location to his or her ‘trusted emergency contact’ if he or she failed to check in at a predetermined time. The email message could also include a photograph, video or voice recording. After a failed check-in, the app would automatically lock and could only be reactivated with a code sent to the listed contact. Within a few days of the app’s release, however, the security community launched criticism at the app, stating that the device can just as easily be used by actors with malintent, because the sensitive information collected on the IWMF server is a likely target for hackers. This assumption is proven true when one visits the Reporta.org webpage; the following message appears:



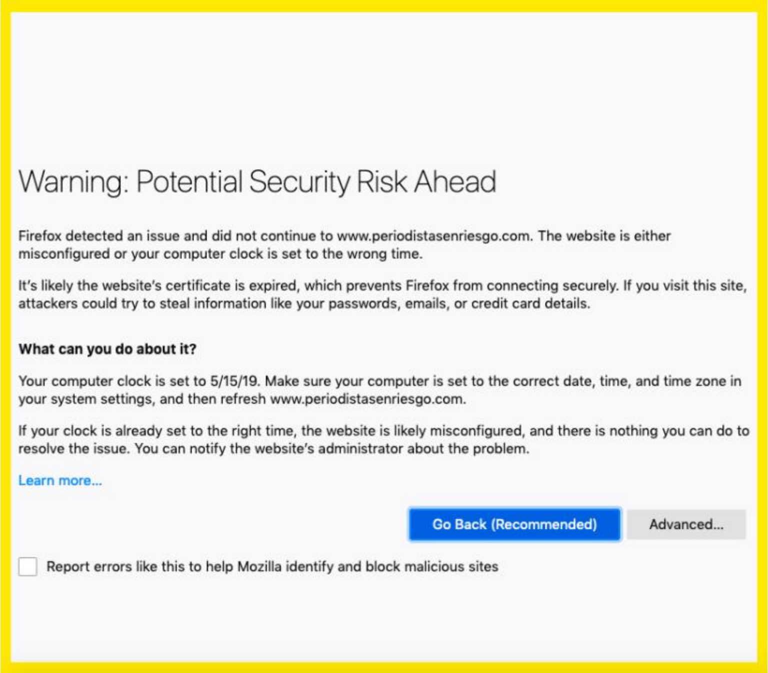
This Connection Is Not Private

This website may be impersonating “reporta.org” to steal your personal or financial information. You should go back to the previous page.

Figure 2: Text displayed when attempting to visit Reporta’s website[84]

[81] Tanya O’Carroll, Danna Ingleton and Jun Matsushita, ‘Panic Button: Why we are retiring the app’ (*The Engine Room*, 1 September 2017) <https://www.theengineroom.org/panic-button-retiring-the-app/> accessed18 May 2019.
[82] ibid.
[83] International Women’s Media Foundation, ‘Reporta™: Using Technology to Help Tackle Increasing Risks to Journalists’ (19 February 2015) <https://www.iwmf.org/2015/02/reporta-using-technology-to-help-tackle-increasing-risks-to-journalists/> accessed 16 May 2019.
[84] Reporta <https://www.reporta.org> accessed 13 May 2019.

Those seeking out journalists are aware of the applications and information platforms that the press uses to protect itself. The site Periodistas en Riesgo (Journalists at Risk), which monitors violence against journalists in Mexico and provides safety updates, is also a victim of malicious tampering. When visiting periodistasenriesgo.com, the web browser again indicates an alert of foul play (see image below). Thus, hacking should be a principal concern for those developing safety-centric applications. If a journalist cannot trust the website, it is not very likely that they will also trust the actual application or service.



Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to www.periodistasenriesgo.com. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

Your computer clock is set to 5/15/19. Make sure your computer is set to the correct date, time, and time zone in your system settings, and then refresh www.periodistasenriesgo.com.

If your clock is already set to the right time, the website is likely misconfigured, and there is nothing you can do to resolve the issue. You can notify the website's administrator about the problem.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

Figure 3: Text displayed when attempting to visit Periodistas en Riesgo's website[85]

Journalists must be able to trust the tools that they use, in order for sources in turn to place trust in the press; that their identity and information will be kept secret. Confidentiality is key to journalists' ability to investigate, and many types of private search engines, encrypted messaging apps, VPN providers, and add-ons exist as a means of enhanced security for all digital-delvers and Internet-users alike (see Annex 1). The NGO Canadian Journalists for Free Expression encourages journalists to "Explore the list [of tools/applications] below—but don't limit yourself to these. Do some research to find the ones that best suit your needs."[86] As platforms change, stagnate, or fail, journalists need to continually research which aids are the most trusted—TrueCrypt has now been replaced by VeraCrypt, for example.[87] Understanding how to best keep oneself technologically safe requires significant time and attention, and has become a job requirement that runs parallel to the true work of journalism itself.

[85] Periodistas en Riesgo <https://www.periodistasenriesgo.com> accessed 13 May 2019.

[86] Canadian Journalists for Free Expression,'Journalists in Distress: Securing your Digital Life' <https://www.cjfe.org/journalists_in_distress_securing_your_digital_life> accessed 17 May 2019.

[87] Both TrueCrypt and VeraCrypt are encryption softwares.

Also on the list of protective technology is an app called Umbrella, which is a much-needed security literacy platform that guides the user through critical lessons on password protection, data security precautions, proper incident response, emergency support numbers and more. The application can disappear from the phone screen when the user quickly shakes the device back and forth, which can be very useful during situations where a journalist becomes vulnerable due to his or her profession—while crossing borders or during protests, for example.[88] The dashboard also displays safety and security alerts from UN bodies, notifying users of floods or earthquakes, protests or riots. Umbrella is helpful as an educational tool for journalists aware of their own need for improved security in a digital world. The International Center for Journalists attempted to create a similar risk assessment app, called Salma, which scores a journalist based on their current security risk level and provides suggestions as to how they could improve.[89] Salma, however, has not gained as much traction, and some have criticized it as a bare-minimum solution for proactive self-protection.

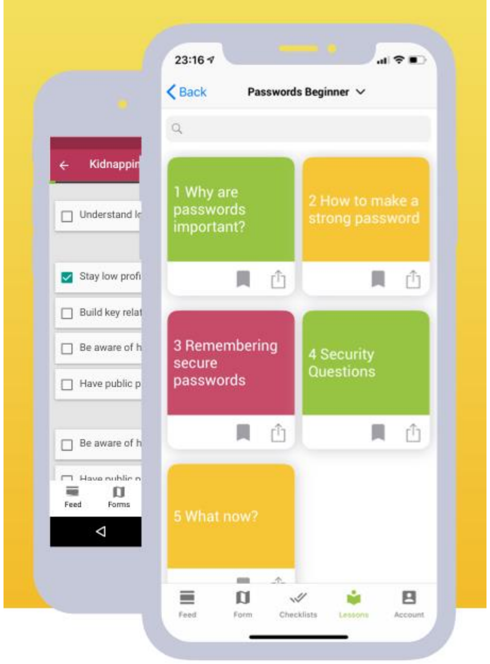


Figure 4: Screen display of the Umbrella application[90]

Investing in journalists' safety is increasingly necessary for press organizations, and taking advantage of technology's capabilities is an avenue surely worth exploring. "Journalists have become more vulnerable not only while on assignment in dangerous places, but also in their daily routines, at home, in the newsroom, or on the road, as digital surveillance increases," notes Garza Ramos.[91] Any technology put towards this cause will require an extensive process of trial and error, but each attempt provides more insight into which tools are most valuable. One such

[88] Security First, 'What is Umbrella?' <https://secfirst.org/umbrella/> accessed 17 May 2019.
[89] International Center for Journalists, ''Salama' App Aims to Keep Journalists Safe?' (23 August 2015) <https://www.icfj.org/news/salama-app-aims-keep-journalists-safe> accessed 16 May 2019.
[90] Security First (n. 88).
[91] Garza Ramos (n. 74) 1.

technology that deserves examination is blockchain. Though not a cure-all elixir for every journalist's digital ailments, blockchain technology could be a dependable tool for avoiding foul play throughout the journalistic process, if applied and used properly. The journalism industry has displayed a vested interest in blockchain for various reasons (to be further explained in Part 3), but there has yet to exist academic research concerning the viability of a blockchain-based platform for protecting journalists in the field and streamlining judicial processes to combat impunity.

Part 2: Introduction to blockchain

> "Blockchain is quickly becoming one of the most important emerging technologies since the Internet."
> —Brian Forde, Director of Digital Currency Initiative, MIT Media Lab
>
> "Blockchain technology has the potential to revolutionize industry, finance, and government—a must for anyone interested in the future of money and humanity."
> —Perianne Boring, Founder and President, Chamber of Digital Commerce

Blockchain, like the Internet, is proving to be confusing during its early adoption phase. Both technologies are variations of a global computer network, a concept that is difficult to grasp due to its seeming intangibility. The harshest critics argue that blockchain will never be widely adopted by the general public, or even within businesses, because it is "exclusively for 'smart' people within the tech world", or because its slow lag in computing transactions makes it inefficient, or that it is a "technology for the rich"—all of which were also arguments against the widespread adoption of the Internet in 1993 and 1994.[92] The many parallels between the two technologies have led early adopters to lean on the unexpected, and at the time unbelievable, impact of the World Wide Web as a foundation for explaining what blockchain has the potential to be; "blockchain technology does for trust what the Internet did for information."[93]

However, the over-hype around blockchain diminished its credibility within the tech-world. At the 2019 RightsCon Conference, the annual gathering of expert practitioners for a summit on human rights in the digital age, there was a panel entitled "If you keep suggesting blockchain, I swear to God I'll f---ing scream."[94] The panelists discussed the over-application of blockchain, adding that the tool should not be seen as a simple solution for complex development and humanitarian issues. Based on blockchain's actual capabilities and limitations, it should only be used when it is the proper tool, and the only tool, able to achieve an aim. Opportunity costs for funding one project over another are always high for human rights organizations, meaning blockchain would need to be the most viable and economic option in comparison to all others. Research stated that the following situations are the best applications of blockchain to date:

[92] Armit, 'Confused by Blockchain Technology? No worries. Let's talk about it!' (*Medium*, 24 March 2018) <https://medium.com/@amrit_sharma/confused-by-blockchain-technology-no-worries-lets-talk-about-it-8e444637e46d> accessed 25 May 2019.

[93] ibid.

[94] Rights Con 2019, 'Rights Con Tunis 2019' <https://rightscon2019.sched.com/event/PvjZ/if-you-keep-suggesting-blockchain-i-swear-to-god-i-will-fing-scream> accessed 9 June 2019.

ensuring tamper free evidence; decentralization from a single authority; and the transparency of data flow.[95]

2.1 What is blockchain?

At its core, blockchain is a new technology that can securely store information without the need of a centralized authority. Though it was first applied in the financial sector and is primarily associated with cryptocurrencies, its applications have significantly evolved over the past decade to include self-executing smart contracts and the development of decentralized apps (DApps) across many industries, which will be further explained in Part 5.

In 1991, Stuart Haber and W. Scott Stornetta first hypothesized about a system where document timestamps could not be altered.[96] Two decades later, however, a person or group of people under the pseudonym Satoshi Nakamoto,[97] launched Bitcoin, which became the first real-world application of blockchain technology.[98] Since Bitcoin's unveiling in 2009, tech experts argue that blockchain developed into one of today's most significant ground-breaking technologies, with the potential to impact nearly every industry—from banking to healthcare, voting to supply chain management, property tendering to education and more.[99] Blockchain's appeal is apparent through its foundational pillars, which are decentralization, transparency, and immutability; but one of the main obstacles to its practical adaptation is the need for its demystification. In essence, blockchain is a secure way to verify, store and keep track of data; due to its properties, it cannot be faked or hacked.[100]

Blockchain technology is defined as a distributed ledger-based database that disperses data across a network of participating nodes using cryptographic proofs, removing the necessity for a centrally controlling entity to hold information.[101] Instead, streams of information interweave into a chain of data, and the blockchain becomes more secure as it becomes more complex. Nodes are defined as individual computers connected to the network.[102] Each node receives a copy of the blockchain, or, in other words, the complete history of the blockchain at hand. This means the same information can replicate across thousands of independent computers.

[95] Lukas Marx, 'Storing Data on the Blockchain: The Developers Guide' (*Malcodad*, 5 July 2018) <https://malcoded.com/posts/storing-data-blockchain/> accessed 20 July 2019.

[96] Stuart Haber and W. Scott Stornetta, 'How to Time-Stamp a Digital Document' (Bellcore) 5 <https://www.anf.es/pdf/Haber_Stornetta.pdf> accessed 22 May 2019.

[97] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (*Bitcoin*, 2018) <https://bitcoin.org/en/bitcoin-paper> accessed 21 May 2019.

[98] Bitcoin is a cryptocurrency that utilizes blockchain technology, and while cryptocurrencies are now one of the main applications of blockchain, 'cryptocurrency' and 'blockchain' are not interchangeable terms.

[99] Ameer Rosic, 'What is Blockchain Technology? A Step-by-Step Guide For Beginners' (*Blockgeeks*, 1 March 2019) <https://blockgeeks.com/guides/what-is-blockchain-technology/> accessed 17 May 2019.

[100] Bernat Ivancsics, 'Blockchain in Journalism' (*Tow Center for Digital Journalism*, 25 January 2019) <https://www.cjr.org/tow_center_reports/blockchain-in-journalism.php#blockchain> accessed 19 May 2019.

[101] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (2nd edn, Kindle edn, Portfolio/ Penguin 2018) 365.

[102] Luke Fortney, 'Blockchain, Explained' (*Investopedia*, 21 May 2019) <https://www.investopedia.com/terms/b/blockchain.asp> accessed 22 May 2019.

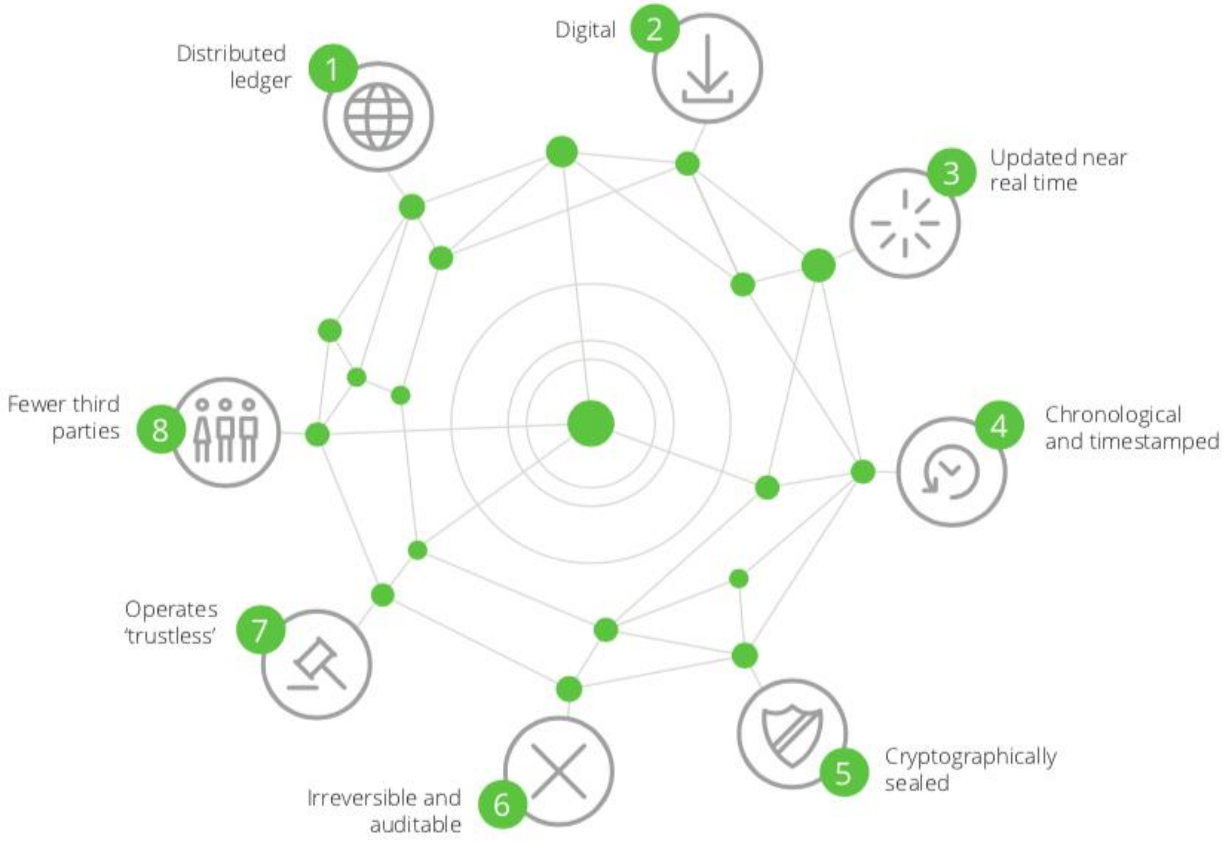


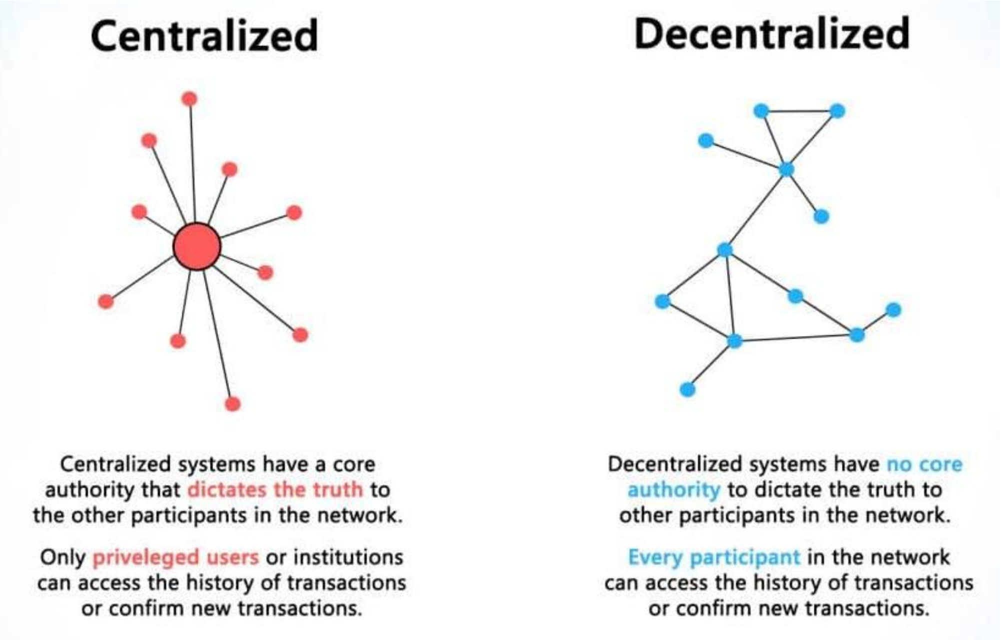
Figure 5: Visualization of blockchain's properties and characteristics[103]

The integrity of the system is maintained through data miners, verifying the same sets of transactions which consolidate into universally-agreed-upon blocks.[104] Each block of records is encoded with a timestamp, its history, and a unique identifying code called a hash. Independent of the size of the original file, or the piece of data being stored, hash codes remain the same length and no two hashes are the same. Each block contains its own hash, as well as the hash of the block before it, allowing for the two to be linked and the chain of blocks to be subsequently arranged in chronological order. If a hacker were to try and break into a block, they would need to recode all other blocks from multiple different nodes all at the exact same time, which is virtually impossible.[105] Breaking one block has an avalanche effect on all other blocks linked behind it on the chain; therefore, any changes made to one part of the system would be immediately and permanently visible to the entire node network.

[103] Deloitte Blockchain @ Media, 'A new Game Changer for the Media Industry?' (*Deloitte and Blockchain Institute*) 6 <https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/ZA_PoV_Blockchain_Media_250817.pdf> accessed 14 May 2019.

[104] This process is called Proof of Work (PoW), which requires that miners compete against each other to solve algorithms, in order to produce a new block for the chain. Miners are incentivized to create blocks with crypto-payments.

[105] The possibility of a 51% attack occurring is discussed later on in this section.



Centralized systems have a core authority that dictates the truth to the other participants in the network.

Only priveleged users or institutions can access the history of transactions or confirm new transactions.

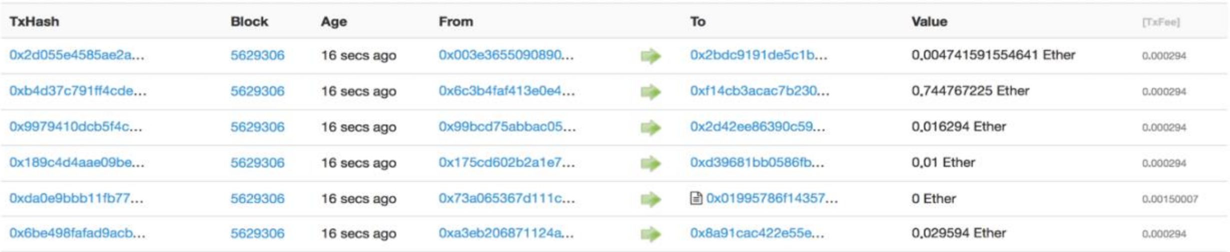
Decentralized systems have no core authority to dictate the truth to other participants in the network.

Every participant in the network can access the history of transactions or confirm new transactions.

Figure 6: Visualization of the difference between a centralized and decentralized network[106]

Due to blockchain's decentralized nature, no single entity can control what is happening in the blockchain ecosystem. Therefore, no State or non-State actor can control the information or reverse an action logged in the blockchain. The peer-to-peer network model eliminates any kind of authority figure from overseeing the process, rather, individuals on the same plane are independently verifying a transaction's 'truth'. Another key property of blockchain is that it is open and accessible, meaning anyone with an Internet connection can theoretically engage in transactions.

Blockchain is entirely transparent, and creates a digital fingerprint that allows one to trace, track, and authenticate information. At the same time, its use of public and private keys provides anonymity and privacy. While seemingly paradoxical, the transparency of the technology lies in its overarching structure; privacy, on the other hand, is kept by means of its complex cryptography and a stand-in digital signature that hides users' identities, not unlike a username. For example, the public ledger would not read "Bob Woodward" sent 3 files to "*The Washington Post*". Instead, it would read "1MF1bhsFLkB5zz9vpFYEgvwt2dbyct7n" sent 3 files to "7f83kfndFdbsSftisAjit8395Kfhfod3". See the sample blockchain ledger below.



TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	➡	0x2bdc9191de5c1b...	0,004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...	➡	0xf14cb3acac7b230...	0,744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	➡	0x2d42ee86390c59...	0,016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	➡	0xd39681bb0586fb...	0,01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	➡	0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	➡	0x8a91cac422e55e...	0,029594 Ether	0.000294

Figure 7: An example of how the Ethereum transactions are publicly ledgered[107]

[106] Rosic (n.99).
[107] ibid.

2.2 What is a block?

Blocks consist of a long string of numbers and letters that are meaningless unless decoded. The average size of any particular block is around 1 megabyte (MB) of data; bytes being the basic unit for digital information.[108] Within each block, there can be any number of transactions that are grouped together. In Bitcoin blocks, for example, there are an average of 500 transactions.[109] In addition to all of the recorded transactions and data transfers, each block consists of a:

- height or version number - which indicates the position of the block on the chain
- header hash - the unique code of the previous block
- Merkle root - a data structure which summarizes the content of the block
- nonce - a randomized number used to standardize mining difficulty and create the output hash of the block
- timestamp - which marks when the block was created
- output hash - unique code of reference specific to the newly created block; reflects all of the above information

2.3 What can be stored via blockchain?

Blockchains can store nearly any kind of data, ranging from monetary transactions, contracts, source code, documents,[110] photos, videos, GPS locations, and more. Storing large amounts of data on blockchain, however, can become expensive. Thus, bit-torrent-based solutions were developed—such as StorJ and the InterPlanetary File System (IPFS)—that can break down the file into more digestible pieces and provide a 'compressed' hash for storing on the blockchain. This guarantees that the file is secure, permanently stored, and impossible to tamper with and at a lower cost.[111]

2.4 How does blockchain work?

Once a transaction occurs, it must be verified based on a consensus of the network. For instance, a source may send a journalist a photograph of a local protest. This transaction is then listed as a record containing the digital signatures of both parties, meaning neither the source nor the journalist's identities are exposed. The photograph itself and the metadata it contains will not be available for public viewing, as it is encrypted. The record of this transaction then travels to the network—which consists of many computers that have Application Specific Integrated Circuits (ASIC) and specialized mining software—to verify the details of the transfer. Once verified, the transaction is collected into a grouping of other verified transactions in order to create a block of records, which is also encrypted. This block also gets a unique hash, which would be automatically

[108] Blockchain, 'Average Block Size: The average block size in MB' (May 2019) <https://www.blockchain.com/charts/avg-block-size> accessed 19 May 2019.

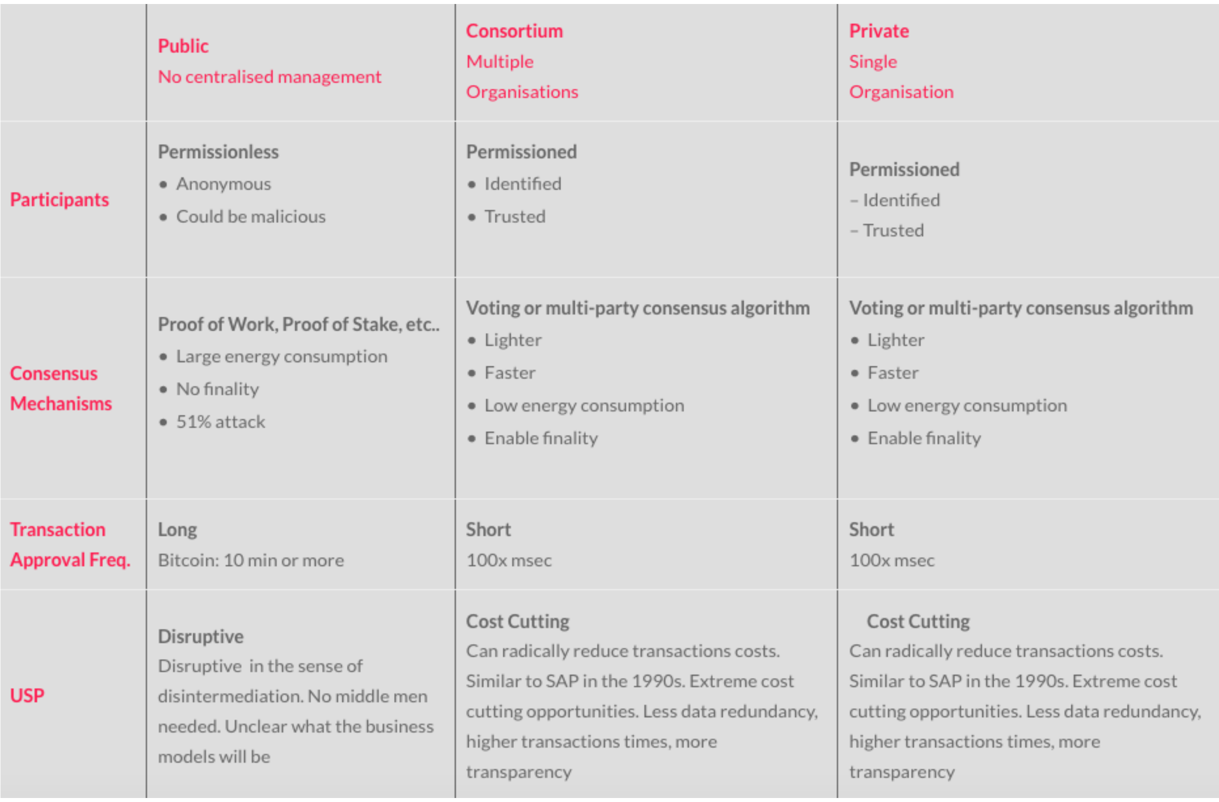
[109] Damien Cosset, 'Blockchain: what is in a block?' (*DEV*, 27 December 2017) <https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo> accessed 21 May 2019.

[110] Ben Whittle, 'Storing Documents on the Blockchain: Why, How, and Where' (*Coin Central*, 23 December 2018) <https://coincentral.com/storing-documents-on-the-blockchain-why-how-and-where/> accessed 19 May 2019.

[111] Abhishek Singh, Answer ' Are there any Altcoins I can invest in 2019 and why? There are too many scams and it's hard to find a good one for a long-term investment' (*Quora*, 14 March 2018) <https://www.quora.com/How-would-I-store-digital-documents-on-the-blockchain-rather-than-just-record-transactions> accessed 17 May 2019.

altered if any piece of information within the block (all of its consolidated records) were to change. Therefore, if anyone alters the photo in any way, the hash would change. Since each block also contains the hash of the previous block (for linking it to the chain) altering the photo would unlink the entire blockchain, by way of a domino effect. However, the chain of blocks is stored on many computers in the network, and therefore it can be easily restored. As explained by Bernat Ivancsics, "There is no centralized, shared database, and edits can't be tracked by clicking on an 'edit history' button. Instead of rewriting the same page or database, blockchain is cumulative, or in other words, append-only. It's not a palimpsest; it's more like a lot of pages stacked on top of each other in a fixed order."[112] Thus, the photograph that the source sent to the journalist is protected by cryptography, and additionally verified by community consensus, before being added to a single, non-editable public record of data.

While public blockchains allow for any computer to act as a node in the network, private blockchains require that members of the community hold stakes in the network and establish rules of operation. Private blockchains can even operate by ratification of a constitution, and violations of the prescribed rules would eliminate a node from the network. In private blockchains there is a stronger element of trust, and the network is very tight-knit. Most of the journalistic applications of blockchains discussed in Part 3 are based on private networks[113] where stakeholders are held to a stricter set of guidelines.



	Public No centralised management	Consortium Multiple Organisations	Private Single Organisation
Participants	Permissionless • Anonymous • Could be malicious	Permissioned • Identified • Trusted	Permissioned – Identified – Trusted
Consensus Mechanisms	Proof of Work, Proof of Stake, etc.. • Large energy consumption • No finality • 51% attack	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality
Transaction Approval Freq.	Long Bitcoin: 10 min or more	Short 100x msec	Short 100x msec
USP	Disruptive Disruptive in the sense of disintermediation. No middle men needed. Unclear what the business models will be	Cost Cutting Can radically reduce transactions costs. Similar to SAP in the 1990s. Extreme cost cutting opportunities. Less data redundancy, higher transactions times, more transparency	Cost Cutting Can radically reduce transactions costs. Similar to SAP in the 1990s. Extreme cost cutting opportunities. Less data redundancy, higher transactions times, more transparency

Figure 8: Types of blockchains[114]

[112] Ivancsics (n. 100).

[113] ibid.

[114] Blockchain Hub, 'Blockchains & Distributed Ledger Technologies' <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/> accessed 21 May 2019.

2.5 What are the disadvantages to blockchain?

The challenges of implementing blockchain are not only technical but also political, because regulations concerning the use of the technology are far from standardized. Firstly, while blockchain is freely open and accessible, it is not free or efficient to operate. There is an infrastructural cost to keep the blockchain running, considering the data miners need to be compensated for their work, and maintaining a growing blockchain consumes vast amounts of computational power.[115] A Bitcoin specialist at PwC estimates that Bitcoin's servers are consuming approximately 67.33 terawatt-hours (TWh) per year and growing,[116] which is a rate greater than the entire nation of Ireland.[117] By another comparison, Google consumed just 8.03 TWh worldwide in 2017.[118] Another critique from businesses has been blockchain's inefficient processing time. Bitcoin or Ethereum can process approximately seven and fifteen crypto-transactions per second, respectively, while Visa can process approximately 1,700 transactions per second, decimating the theoretically instantaneous benefit of blockchain's microtransaction capabilities.[119] While a business model based on profits is less likely to be a concern of the human rights community, it does frame important apprehensions related to scalability. Therefore, blockchain projects that are worthwhile must add a "minimum threshold of viability," to ensure they add value beyond what a more traditional technology can provide.[120]

Secondly, public blockchain networks came under heavy criticism for illegal trading and illicit activity. In 2013, the U.S. Federal Bureau of Investigation shut down a platform called Silk Road, where anonymous buyers were making illegal purchases with Bitcoin.[121] More generally, government wariness of blockchain has roots in the technology's nuanced form of digital governance and consensus, which may impact and call into question established democratic systems.[122] In addition, there is yet to be success concerning international policy standardization, and there are even inconsistencies at domestic levels. In the United States, the U.S. Securities and Exchange Commission, the U.S. Commodity Futures Trading Commission, the Financial Crimes Enforcement Network, and state governments all have "differing and, at times conflicting, policies related to blockchains and crypto-assets."[123]

[115] Jeff, 'Bitcoin Mining Costs Throughout the World' (*Elite Fixtures*, 26 February 2018) <https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/> accessed 20 May 2019.

[116] Digiconomist, 'Bitcoin Energy Consumption Index' (June 2019) <https://digiconomist.net/bitcoin-energy-consumption> accessed 12 June 2019.

[117] Alex de Vries, 'Bitcoin's Growing Energy Problem' (2018) 2(5) Joule <DOI:https://doi.org/10.1016/j.joule.2018.04.016> accessed 20 July 2019.

[118] T. Wang, 'Energy consumption of Google from 2011 to 2017 (in gigawatt hours)' (*Statista*, 31 May 2019) <https://www.statista.com/statistics/788540/energy-consumption-of-google/> accessed 21 June 2019.

[119] Kenny Li, 'The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed' (*Hackernoon*, 30 January 2019) <https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44> accessed 20 May 2019.

[120] Nelson Granados, 'How Blockchain Is Making Waves In Media And Entertainment' (*Forbes*, 3 December 2018) <https://www.forbes.com/sites/nelsongranados/2018/12/03/how-blockchain-is-making-waves-in-media-and-entertainment/#44859b7d3f6c> accessed 21 June 2019.

[121] Jake Frankenfield, 'Silk Road' (*Investopedia*, 26 October 2016) <https://www.investopedia.com/terms/s/silk-road.asp> accessed 20 May 2019.

[122] Ryan Osgood, 'The Future of Democracy: Blockchain Voting' (*Tufts University*, 14 December 2016) 17-18 <http://www.cs.tufts.edu/comp/116/archive/fall2016/rosgood.pdf> accessed 20 May 2019.

[123] Timothy G. Massad, 'It's Time to Strengthen the Regulation of Crypto-Assets' (*Bookings*, 18 March 2019) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwix0PuU5KLiAhUNDm

Most importantly, newer blockchains are more susceptible to 51% attacks, which is when younger blockchains are overrun by attackers that would be able to "prevent new transactions from gaining confirmations, allowing them to halt payments [or data transfers] between some or all users."[124] If a person or group controls the majority of the nodes on the network, then they can interfere with the process of recording new blocks by monopolizing the process. This has taken place on the Krypton, Shift and Bitcoin Gold blockchains in the past, all of which are cryptocurrencies, meaning the hackers were likely looking for a heftier financial profit. The only solution to this problem is having either a robust or completely closed network.[125] While there are many grayscale faults to blockchain that still require elucidation, the dormant benefits are too promising to completely ignore.

2.6 How is blockchain currently being used?

The Financial Times' technology reporter Sally Davies explains, "[Blockchain] is to Bitcoin, what the Internet is to email. A big electronic system, on top of which you can build applications. Currency is just one."[126] Cryptocurrencies are the most widely known development of blockchain realization—likely due to the popularity and newsworthiness of Bitcoin, the original blockchain based system—but the technology is diversifying quickly. Deloitte surveyed 1,386 senior executives from countries across the world who run companies in FinTech, technology, media, telecommunications, life sciences, health care, and government, and 53 percent of the respondents said that blockchain became a "critical priority" for their organizations in 2019.[127] Microsoft and Ernst & Young recently deployed a blockchain-based payment system for video game developers;[128] Spotify acquired the blockchain-based startup Mediachain to better handle copyright and licensing attribution in its music streaming;[129] Starbucks is building a blockchain-based, fair-trade coffee-tracking platform;[130] The Walt Disney Company created Dragonchain, a

MBHR5lD4YQFjAAegQIABAC&url=https%3A%2F%2Fwww.brookings.edu%2Fwp-content%2Fuploads%2F2019%2F03%2FTimothy-Massad-Its-Time-to-Strengthen-the-Regulation-of-Crypto-Assets-2.pdf&usg=AOvVaw3_iGe88rOISfaqWOgaYTIt> accessed 21 May 2019.

[124] Jake Frankenfield, '51% Attack' (*Investopedia,* 6 May 2019) <https://www.investopedia.com/terms/1/51-attack.asp> accessed 21 May 2019).

[125] ibid.

[126] Sally Davies,. 'How bitcoin and its blockchain work' (*Financial Times*, 3 February 2015) <https://repository.gchumanrights.org/handle/20.500.11825/1013> accessed 17 May 2019.

[127] Linda Pawczuk, Jonathan Holdowsky and Rob Massey, 'Deloitte's 2019 Global Blockchain Survey: Blockchain gets down to business' (*Deloitte Insights*, 6 May 2019) <https://www2.deloitte.com/insights/us/en/topics/understanding-blockchain-potential/global-blockchain-survey.htm> accessed 17 May 2019.

[128] EY, 'EY and Microsoft launch blockchain solution for content rights and royalties management for media and entertainment industry' (21 June 2018) <https://www.ey.com/en_gl/news/2018/06/ey-and-microsoft-launch-blockchain-solution-for-content-rights> accessed 18 May 2019.

[129] Sarah Perez, 'Spotify acquires blockchain startup Mediachain to solve music's attribution problem' (*TC*, 2017) <https://techcrunch.com/2017/04/26/spotify-acquires-blockchain-startup-mediachain-to-solve-musics-attribution-problem/?guccounter=1> accessed 19 May 2019.

[130] Max Boddy, 'Starbucks Working With Microsoft for Blockchain-Based Coffee Tracking Platform' (*Cointelegraph*, 6 May 2019). <https://cointelegraph.com/news/starbucks-working-with-microsoft-for-blockchain-based-coffee-tracking-platform> accessed 18 May 2019.

developer platform for enterprises;[131] and Facebook recently launched Libra, a new attempt at a global currency backed by a financial reserve.[132] Countless startups are still emerging with visions concerning how blockchain can solve industry-specific problems, and journalism is no exception.[133] It remains relatively unclear, however, as to which innovations will be the most sustainable.

More industries have been able to attain blockchain technology due to the creation of platforms such as the Ethereum Virtual Machine (EVM), which is a blockchain-based system that provides other developers with the necessary tools to build their own decentralized applications with a shared memory.[134] The best analogy for Ethereum is that it functions as the iOs or Android application store; it is the foundation for where other applications can be stored, reviewed and verified.[135] Anyone can create an app, access it, download it and run it from the store. Since Ethereum is a blockchain that understands a more general programming language, it works in a similar way. One can also understand it as a starting point for building something over top of a pre-established system, as-per the functionality of WordPress for all those that wish to create a website. The complex coding, cryptography and mathematics are all pre-set, allowing for those less-versed in programming to adapt to blockchain without becoming lost in technicalities. In the current blockchain market, 89% of the best-ranked projects are built using Ethereum.[136] Starting a blockchain from scratch can take years, and they are very expensive to commission.[137] In 2017, the average annual income for a blockchain developer was between $150,000-$200,000 USD.[138] Thus, the creation of platforms like Ethereum has made blockchain more accessible to human rights organizations. These platforms reduce, to some degree, the fixed costs required to develop and maintain a blockchain-based project.

2.7 How is the human rights community using blockchain?

The human rights community is investing in blockchain heavily, to the extent that the United Nations Office for Project Services (UNOPS) assigned Yoshiyuki Yamamoto to the newly-

[131] Dragonchain, 'Blockchain as a Service for Enterprises and Developers' <https://dragonchain.com/> accessed 18 May 2019.
[132] Josh Constine, 'Facebook announces Libra cryptocurrency: All you need to know: The use cases, technology and motive behind the new digital money (*TechCrunch*, 17 June 2019) <https://techcrunch.com/2019/06/18/facebook-libra/ > accessed 21 June 2019.
[133] Karen Taylor Quinn, 'Can Blockchain Fix Journalism? How one technology—and a handful of insurgent startups—could revive an industry in crisis' (*Medium*, 6 November 2018) <https://medium.com/the-slowdown/can-blockchain-fix-journalism-946418d4fac6> accessed 18 May 2019.
[134] Ameer Rosic, 'What is Ethereum? [The Most Comprehensive Guide Ever!]' (*Blockgeeks*, 2016) <https://blockgeeks.com/guides/ethereum/> accessed 17 May 2019.
[135] Vitalik Buterin and Naval Ravikant, 'Decentralizing Everything with Ethereum's Vitalik Buterin | Disrupt SF 2017' (*TechCrunch*, 18 September 2017) <https://www.youtube.com/watch?v=WSN5BaCzsbo> accessed 19 May 2019.
[136] Torsten Hartmann, 'Ethereum (ETH) Price Analysis and Prediction 2019 – Market Takes A Nosedive And Takes ETH With It (June 4th Update)' (*Capital Coin*, 4 June 2019) <https://captainaltcoin.com/ethereum-eth-price-prediction-update-06-04-2019/> accessed 22 June 2019.
[137] Jackt, 'Blockchain Development: A Complete Guide For Innovators' (2019) <https://byjakt.com/blockchain-development-nyc-complete-guide/> accessed 23 June 2019.
[138] 4IRE labs, 'How Much Does It Cost to Hire a Blockchain Developer?' (2018) <https://4irelabs.com/how_much_does_it_cost_to_hire_blockchain_developer> accessed 23 June 2019.

created post of Special Advisor for UN Engagement and Blockchain Technology in 2016.[139] Separately, the newly-established UN Blockchain Group[140] pulls interested specialists from the World Food Programme (WFP), The United Nations Development Programme (UNDP), The United Nations Children's Fund (UNICEF), UN Women, the UN High Commissioner for Refugees (UNHCR) and the UN Development Group (UNDG) to propose technologically-charged solutions for some of the agencies' most pressing problems. Additionally, the Blockchain Commission for Sustainable Development[141] came into being in 2017, with a mandate to host an annual Blockchain for Impact Summit that focuses on incubating a collaborative space; allowing activists to brainstorm blockchain applications for positive social change.[142]

Blockchain-based platforms are already used for the promotion of human rights and towards the achievement of a variety of Sustainable Development Goals. In 2017, the WFP partnered with the startup Parity Technologies to provide over 10,000 Syrian refugees with cryptocurrency-based food vouchers that could be redeemed in participating markets, since most of the refugees did not have access to a bank account.[143] They have since expanded the initiative, and now the WFP is using Parity Ethereum to serve more than 100,000 refugees each month.[144] In Venezuela, where the national currency is rapidly devaluing, citizens have turned to cryptocurrencies in order to maintain an adequate standard of living: "Venezuelans have been using cryptocurrency for years now to protect their capital from inflation. But now with Dash, it has opened a new window as a means of payment. It is an easy way to receive something that is stronger than the Bolivar and is within the law," explained a Dash cryptocurrency co-founder.[145] In combining Internet-of-Things (IoT) with blockchain, companies can connect GPS-based tracking with a public ledger, that shows where goods and services are coming from in real time. Walmart and Costco are using an Ethereum-based private blockchain to track the fish they sell from its source, working to ensure that slave labor is not involved in the process.[146] De Beers began a pilot program for tracking the journey of their diamonds following a UN mandate that requires an update to the Kimberley Process Certification Scheme, imposing requirements that all diamonds be verified on the blockchain in order to certify suppliers as conflict-free.[147]

[139] Axiom Technologies, 'A Reasonably Comprehensive Outline of Blockchain in the United Nations' (1 March 2019) <https://www.axiomtech.io/blog-feed/2019/3/1/blockchain-in-the-united-nations> accessed 17 May 2019.

[140] UN Blockchain <https://un-blockchain.org/> accessed 18 May 2019.

[141] Blockchain Commission for Sustainable Development [Linkedin] <https://www.linkedin.com/company/blockchain-commission/about/> accessed 17 May 2019.

[142] Blockchain for Impact <https://www.blockchainforimpact.org/> accessed 26 May 2019.

[143] George Levy, 'United Nations Expanding Blockchain Use to Help Syrian Refugees' (*Bitsonline*, 8 May 2018) <https://bitsonline.com/united-nations-blockchain-refugees/ > accessed 17 May 2019.

[144] Gautam Dhameja, 'UN World Food Programme uses Parity Ethereum to aid 100,000 refugees' (*Parity*, 18 February 2019) <https://www.parity.io/un-world-food-programme-uses-parity-ethereum-to-aid-100-000-refugees/> accessed 19 May 2019.

[145] Christina Comben, 'How Blockchain Is Being Applied to Human Rights' (*Coin Central*, 5 September 2018) <https://coincentral.com/blockchain-and-human-rights/> accessed 18 May 2019.

[146] Dean Pinkert, James Ton-that and Ravi Soopramanien, 'Blockchain technologies offer transparency that could improve human rights practices' (*Open Global Rights*, 24 January 2019) <https://www.openglobalrights.org/blockchain-technologies-offer-transparency-that-could-improve-human-rights-practices/> accessed 20 May 2019.

[147] Zoe Biehl, '6 Ways Blockchain Is Radically Improving Global Human Rights' (*Invest in Blockchain*, 2 April 2018) <https://www.investinblockchain.com/blockchain-improving-human-rights/> accessed 20 May 2019.

Activists are also using Ethereum tokens (ETH) to practice freedom of expression, particularly as a means of disseminating information under authoritarian rule. On April 23rd, 2018, an anonymous activist in China completed a transaction of no value (0 ETH), sending information to his or herself.[148] The transfer contained the text of a letter written by a student at Peking University, explaining instances of when the school threatened her, due to her attempts to investigate claims of a professor's sexual assault. The letter had originally been posted on the State-owned and monitored social media platform WeChat, but government censors ensured that all copies vanished from the platform. Because every computer running a full Ethereum node had the complete history of the blockchain, the letter was replicated across thousands of independent computers, making it virtually impossible to remove its content from the network. Fighting censorship is one of the common missions behind startups interested in using blockchain-based journalism platforms, which will be further elaborated upon in Part 3.

Part 3: Journalism's current applications and considerations for blockchain

There are many challenges facing the journalism industry today,[149] including the need for greater confidence in media in the age of fake news and post-truth politics. Additionally, the basis for journalism's business model has deteriorated since the emergence of the Internet. Public trust in the media is at an all-time low; exemplified by the fact that a majority of adults in the United States feel diminished confidence in the media's ability to report unbiased and accurate news.[150] The extensive use of misinformation as a political strategy has confused the public about the meaning of 'fake news', and unsubstantiated allegations have started to target credible news organizations as an attempt to destroy their credibility. Happening in parallel, both print and digital media outlets are struggling to find sustainable revenue streams due to readers' lack of willingness to pay for content. Many news organizations have yet to find the correct balance between making content affordable, nuanced and accessible, while at the same time managing operational costs. *The Rocky Mountain News, The Buenos Aires Herald,*[151] *The Baltimore Examiner, The Kentucky Post, The Cincinnati Post, and The Pittsburgh Tribune* are just a few of the newspapers that have gone out of business since 2007, while *The Minneapolis Star-Tribune, The Boston Herald, The*

[148] Walker Flynn, 'Uncensored Content on Ethereum: How Chinese Activists Inspired Civil' (*Medium*, 13 August 2018) <https://blog.joincivil.com/uncensored-content-on-ethereum-how-chinese-activists-inspired-civil-f09f095a9e91> accessed 21 May 2019.

[149] Robert G. Picard, 'A Business Perspective on Challenges Facing Journalism' in David A. L. Levy and Rasmus Kleis Nielsen (eds), 'The Changing Business of Journalism and its Implications for Democracy' (*Reuters Institute for the Study of Journalism,* 2010) 17-24 <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/The%2520Changing%2520Business%2520of%2520Journalism%2520and%2520its%2520Implications%2520for%2520Democracy.pdf#page=23> accessed 19 May 2019.

[150] The poll also found that a staggering nine out of ten U.S. citizens that consider themselves Republican do not trust the media. Republicans are much more likely to share ideologies with the current U.S. President Donald Trump, who considers the media to be an 'enemy of the people'. Gallup and Knight Foundation, 'Indicators of News Media' (*Knight Foundation,* 11 September 2018) <https://www.knightfoundation.org/reports/indicators-of-news-media-trust> accessed 21 May 2019.

[151] Teresa Mioli, 'One of the last English-language newspapers in Latin America, *The Buenos Aires Herald* to close after 140 years' (*Knight Center for Journalism in the Americas*, 1 August 2017) <https://knightcenter.utexas.edu/blog/00-18659-one-last-english-language-newspapers-latin-america-buenos-aires-herald-close-after-140> accessed 24 May 2019.

Philadelphia Inquirer, Canwest, Canada's Postmedia,[152] the Chilean branch of Grupo Televisa S.A.,[153] the South African Broadcasting Corporation (SABC),[154] and *Financial Times Deutschland*,[155] have all experienced bankruptcy or near bankruptcy within the past decade, and these are merely the most renowned examples.[156] Quality journalism is by no means cost-free, yet readers have become accustomed to the open-access Internet, forcing more well-known news outlets with a wide-scale and loyal audience to charge for online subscriptions; to afford to use the platform and still pay their journalists. Smaller publications are more reliant on advertising, donations or sponsorship to stay afloat which are options that are becoming less and less dependable.

Academics, entrepreneurs, and journalists alike pose blockchain as a potential solution to these problems, and some have invested increasing amounts of energy into discovering if these newly developed frameworks could be sustainable solutions for their respective industries. In March of 2019, *The New York Times* posted a job opening announcing their search for an experienced innovator in the blockchain space; someone to help "design a blockchain-based proof of concept for news publishers."[157] The job description is not particularly clear as to how the *Times* would apply blockchain, but a "proof of concept" for a project could be related to the *Times'* business model, a truth-seeking initiative, or, perhaps, a completely new idea that has yet to be discussed publicly.

[152] Robert Hiltz and Bruce Livesey, 'Postmedia continues its downward spiral' (*Canada's National Observer*, 25 October 2018) <https://www.nationalobserver.com/2018/10/25/analysis/postmedia-continues-its-downward-spiral> accessed 24 May 2019.

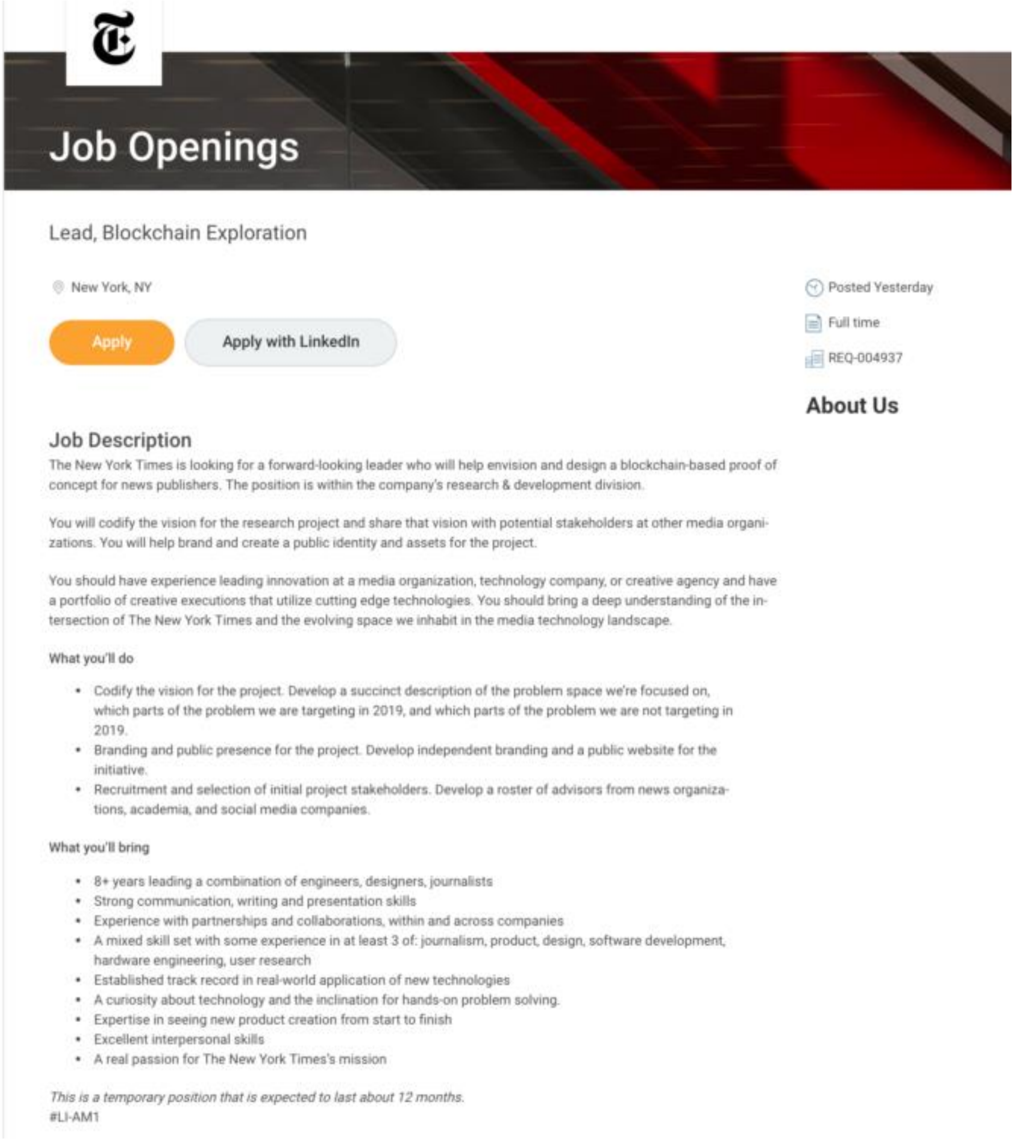
[153] Nelson Quiroz, 'Closing of Editorial Televisa in Chile: The end of Condorito?' (*Chile Today*, 22 February 2019) <https://www.chiletoday.cl/closing-of-editorial-televisa-in-chile-the-end-of-condorito/> accessed 24 May 2019.

[154] Luke Daniel, 'The SABC is bankrupt, admits CEO Madoda Mxakwe' (*The South African*, 31 October 2018) <https://www.thesouthafrican.com/news/sabc-bankrupt-confirmed-ceo-2018/> accessed 24 May 2019.

[155] Spiegel Online, 'The End of Financial Times Deutschland Germany Hit by Wave of Newspaper Bankruptcies' (23 November 2012) <https://www.spiegel.de/international/business/media-woes-hit-germany-as-financial-times-deutschland-goes-under-a-869001.html> accessed 24 May 2019.

[156] Paul Gillin, 'North American metro dailies that have closed since this site was created in March, 2007' (*Newspaper Death Watch*) <http://newspaperdeathwatch.com> accessed 19 May 2019.

[157] Anna Baydakova, 'The New York Times Is Planning to Experiment With Blockchain Publishing' (*CoinDesk*, 13 March 2019) <https://www.coindesk.com/the-new-york-times-is-planning-to-experiment-with-blockchain-publishing> accessed 19 May 2019.



Lead, Blockchain Exploration

New York, NY

Posted Yesterday

Full time

REQ-004937

About Us

Job Description

The New York Times is looking for a forward-looking leader who will help envision and design a blockchain-based proof of concept for news publishers. The position is within the company's research & development division.

You will codify the vision for the research project and share that vision with potential stakeholders at other media organizations. You will help brand and create a public identity and assets for the project.

You should have experience leading innovation at a media organization, technology company, or creative agency and have a portfolio of creative executions that utilize cutting edge technologies. You should bring a deep understanding of the intersection of The New York Times and the evolving space we inhabit in the media technology landscape.

What you'll do

- Codify the vision for the project. Develop a succinct description of the problem space we're focused on, which parts of the problem we are targeting in 2019, and which parts of the problem we are not targeting in 2019.
- Branding and public presence for the project. Develop independent branding and a public website for the initiative.
- Recruitment and selection of initial project stakeholders. Develop a roster of advisors from news organizations, academia, and social media companies.

What you'll bring

- 8+ years leading a combination of engineers, designers, journalists
- Strong communication, writing and presentation skills
- Experience with partnerships and collaborations, within and across companies
- A mixed skill set with some experience in at least 3 of: journalism, product, design, software development, hardware engineering, user research
- Established track record in real-world application of new technologies
- A curiosity about technology and the inclination for hands-on problem solving.
- Expertise in seeing new product creation from start to finish
- Excellent interpersonal skills
- A real passion for The New York Times's mission

This is a temporary position that is expected to last about 12 months.
#LI-AM1

Figure 9: Screenshot of the job posting published by the New York Times[158]

Also, for seemingly ambiguous reasons, the Chinese Communist Party's *People's Daily Online* news group partnered with the technology company Xunlei Limited in order to create a blockchain lab within the People Capital's Blockchain Research Institute.[159] The news site has been called the "official mouthpiece" of the government, with a circulation reaching approximately 3 million people. The announcement of the news-tech collaboration noted that the focus would be on supporting blockchain-based startups, without specifying industry-related goals. These initiatives may or may not be an explicit sign that journalism is adopting blockchain-based solutions. Perhaps,

[158] New York Times, 'Lead, Blockchain Exploration' (*Indeed*) <https://www.indeed.com/jobs?q=Blockchain&sort=date&fromage=last&start=10&vjk=0dec9afbb9cb507e> accessed 19 May 2019.

[159] Shalin Soni, 'China's People's Daily Online to Deploy Blockchain Lab in Association with Xunlei Limited' (*Crypto NewZ*, 24 October 2018) <https://www.cryptonewsz.com/chinas-peoples-daily-online-to-deploy-blockchain-lab-in-association-with-xunlei-limited/2482/> accessed 19 May 2019.

news outlets with enough resources are proactively and precariously taking necessary measures in order to stay ahead of their competition (be it ideological or business model oriented).

The speculative promise and potential of blockchain as the 'technology of the future' remains in flux, in turn contextualizing the fact that many applications of blockchain to journalism are still in very experimental phases. "Blockchain technology can create both chains of authenticity and a level of security … Journalism [is] in a highly distributed world [and] is in need of solutions," noted Emily Bell, director of the Tow Center for Digital Journalism at Columbia University.[160] Despite blockchain's nascency, there are a few noteworthy initiatives that already exist; the main categories concerning how interested parties presume blockchain can, or will, intertwine with journalism are designated within four overarching themes:

1. Blockchain-based payment systems
2. Increasing access to quality and verified information
3. Accessing public data secured in government blockchains
4. Reduce government surveillance, imposed censorship and better respect for privacy

These four categories have the most forthright correlational effects with key human rights principles, as stipulated in Articles 19 and 23 of the Universal Declaration of Human Rights.[161]

> Article 19 - Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
>
> Article 23 - (3) Everyone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection.

3.1 Blockchain-based payment systems - right to a fair wage

Ensuring that journalists and news agencies are fairly compensated for their work has been a challenge for the industry since the advent of the Internet. CareerCast ranked 'being a newspaper reporter' as the worst job in the United States in 2015,[162] based on poor job security and diminishing salaries. According to a Pew Research Center report, journalists' salaries have not kept up with inflation over the past ten years,[163] and newsrooms are shrinking their editorial staff as they fight for more revenue to keep papers running. Between 2014 and 2017, approximately

[160] Nicky Woolf, 'What Could Blockchain Do for Journalism?' (*Medium*, 13 February 2018) <https://medium.com/s/welcome-to-blockchain/what-could-blockchain-do-for-journalism-dfd054beb197> accessed 20 May 2019.

[161] United Nations, 'Universal Declaration of Human Rights' (2015 adopted 10 December 1948) <https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf> accessed 19 May 2019.

[162] Career Cast, 'The Worst Jobs of 2015' <https://www.careercast.com/jobs-rated/worst-jobs-2015> accessed 19 May 2019.

[163] Alex T. Williams, 'The growing pay gap between journalism and public relations' (*Pew Research Center*, 11 August 2014) <https://www.pewresearch.org/fact-tank/2014/08/11/the-growing-pay-gap-between-journalism-and-public-relations/> accessed 23 May 2019.

5,000 media jobs were cut from the market,[164] highlighting the trend of mass layoffs taking place over the past two decades.[165] The startups described below are working to reverse this bleak trend, while better empowering journalists and newsrooms through turning a more sizable profit and providing members of the media with just and livable wages.[166]

Monetization of viewership is traditionally achieved strictly through advertising, but blockchain is potentially a method of calculating the value of viewership differently. "An ecosystem of micropayments, in which everyone pays fractions of a penny for every article they read, has long been thought of as the holy grail for online journalism, the theoretical future solution. But there has never been a way to process payments like that in reality—until now," says Jarrod Dicker, the CEO of the startup Po.et.[167] Ensuring appropriate compensation for all parties involved in the creation, accreditation, and distribution of content online is a complex and often incomplete process, as most of those working in online media do not receive their fair share of revenue. Po.et is working to implement a system that would allow content creators in media—musicians, writers, artists, filmmakers, etc.—to earn more by receiving credit each time an individual simply comes in contact with their work. Dicker, the platform's founder, is now also *The Washington Post*'s vice president of innovation and commercial strategy, and he aims to take advantage of blockchain's ability to transparently and permanently log original content by using its metadata, such as timestamps, copyright and authorship.[168] The content's distribution is then trackable and linked to micro-transactions, which would mean that instead of charging readers one larger, upfront fee for an annual subscription, consumers will have the option of pay-as-you-go micro-payments, made each time they open a link to an article online, within an email, or even on a social media post. Not all of the content recorded on the Po.et blockchain needs to be shared publicly, but once shared, the micro-payments would not only be sent to the author but also to the publisher and the platform from which the reader sourced the material. This ensures that writers earn fairer compensation for their intellectual property. Additionally, writers, photographers and videographers could potentially benefit from a constant stream of payment for their work, for as long as it is publicly available on the Internet, rather than a flat rate per article. While Po.et is a noble cause, its functionality requires that all institutions involved utilize some kind of token-to-currency-based system. The robustness of the start-up's wide-scale adoption will determine how powerful of a tool Po.et can be.

The platform Snip was also created with the intent of providing writers with additional income, whereby they can earn SnipCoin (SNIP) in exchange for publishing brief, explanatory 'snippets' of news articles. Authors could post concise summaries of news stories and verify content for audiences to consume information quickly and update themselves on the rapid news

[164] Elizabeth Grieco, Nami Sumida and Sophia Fedeli, 'About a third of large U.S. newspapers have suffered layoffs since 2017' (*Pew Research Center*, 23 July 2018) <https://www.pewresearch.org/fact-tank/2018/07/23/about-a-third-of-large-u-s-newspapers-have-suffered-layoffs-since-2017/> accessed 2 July 2019.

[165] Robert McChesney and John Nicols, *The Death and Life of American Journalism: The Media Revolution that Will Begin the World Again* (Nation Books 2010) 1-20.

[166] It is important to note that the descriptions of the nuanced business models listed below are simplified versions of complex and technical White Papers.

[167] Whitepaper Database, 'Po.et (POE)-Whitepaper' (15 March 2018) <https://whitepaperdatabase.com/po-et-poe-whitepaper/> accessed 24 May 2019.

[168] Adrian Zmudzinski, 'CEO of Blockchain Media Company Po.et Leaves for Washington Post' (*Cointelegraph*, 25 January 2019) <https://cointelegraph.com/news/ceo-of-blockchain-media-company-poet-leaves-for-washington-post> accessed 25 May 2019.

cycle. Since the snippet summaries appeared on its blockchain-based platform, the content was then "verified by users rather than by centralized publishers" and authors are rewarded for valuable contributions because "writers can make legitimate income from generous readers."[169] Poorly covered news was subsequently de-incentivized. However, earning a more lucrative wage as a contributor is only possible through mass-participation, and at the close of 2018 the company's executives released a statement explaining that Snip[170] had failed to gain enough traction for the mission to achieve fruition, rendering SnipCoins essentially valueless.[171] Cryptocurrencies (of all acronyms and abbreviations) infamously experience value volatility as a consequence of their hype or uncertainty, which is a concern for all crypto-based business models in the making. Snip's failure is emblematic of an importunate apprehension towards journalism's reliance on crypto.

Tackling the job security aspect of journalism, AdChain[172] and SocialFlow[173] are startups that focus on the enhanced distribution and monetization of news media content for publishing houses.[174] In these applications, blockchain becomes a means of cutting intermediary costs, bolstering overall readership, and strengthening the financial stability of traditional news organizations. Businesses spend substantial amounts of time and money on the verification of marketing and advertising-related data before signing contracts, insisting on operating based on informed decision-making, and newsrooms are no exception in their dealings with advertising companies. The due diligence process was born from opacity, but in a more transparent business environment, news outlets could divert their funds and attention to their core functionality: news production.

AdChain is a platform that adds transparency to advertising contracts and keeps a public registry of which news organizations partner with which advertisers, eliminating the need for costly ad brokers as intermediaries. Instead, the registry keeps track of verified media companies and vetted ad agencies, relying on the public accountability aspect of blockchain to reduce fraud in reporting mechanisms. The database stores all of the relevant performance metrics and data around each advertisement, which can show where the ad is coming from and the number of genuine impressions—irrespective of bots—providing a confirmed impact report of advertising campaigns. Thus, the news agencies can make sure that they are receiving the most value for their advertising dollars, in an attempt to receive more subscriptions. Perhaps more importantly, those that wish to advertise on a news agency's platform can obtain irrefutable statistics concerning the reach and performance of their content, adding credibility to a newspaper's visibility value for businesses. The instability of cryptocurrencies likely signifies that newspapers will rely on

[169] Omri Barzilay, 'How Blockchain Is Reinventing Your News Feed' (*Forbes*, 28 August 2017) <https://www.forbes.com/sites/omribarzilay/2017/08/28/how-blockchain-is-reinventing-your-news-feed/#5217e5777bf4> accessed 25 May 2019.

[170] Rather than focusing on the daily news, Snip's creators adopted a more niche, go-to-market strategy that focuses on publishing user-friendly summaries of highly technical papers, concerning advancements in artificial intelligence. Their new platform is called LyrnAI. LyrnAI <https://www.lyrn.ai> accessed 22 May 2019.

[171] Rani Horev, 'Snip - December Update & 2018 Summary' (*Medium*, 3 January 2019) <https://medium.com/snip-news/snip-december-update-2018-summary-fb7bebdb89f2> accessed 25 May 2019.

[172] Mike Goldin, Ameen Soleimani and James Young, 'The AdChain Registry' (*adChain*, 2017) 2-16. <https://adtoken.com/white-paper.pdf> accessed 25 May 2019.

[173] Sarah Donna, 'White Paper: Data Continues to Drive Social Performance 2016' (*SocialFlow*, 3 March 2017) <www.socialflow.com/resources-2/white-papers> accessed 24 May 2019.

[174] SocialFlow <http://www.socialflow.com/> accessed 25 May 2019.

advertising in some capacity for years to come, which is why AdChain and SocialFlow already entice numerous big names in the media industry.

SocialFlow is working to capitalize on the value of strong readership by rewarding users for their advertising engagement. The Associated Press, *The New York Times*, Reuters, *The Washington Post, The Wall Street Journal*, the BBC, CBS, NBC, HuffPost, Bloomberg, Al Jazeera and others, are already working with SocialFlow to algorithmically enhance their social media presence and increase their digital impression numbers. SocialFlow's Universal Attention Token (UAT) launched in 2018; a cryptocurrency allowing readers to access media content online without encountering paywalls while directly rewarding publishers with data concerning audience engagement. The SocialFlow business model is comparable to that of Spotify, where users are given free content until they reach a certain limit and an advertisement airs before more content can be streamed. In relation to news consumption, readers would start with UAT to 'spend' on viewing articles, mini-documentaries, etc. until their tokens are spent. Watching advertisements or engaging in advertising-related surveys could replenish UAT, and advertisers then pay publishers more for stimulating active readers. Reports of which news agencies are actively involved in the crypto-currency portion of the SocialFlow project are yet to be released, but the greatest barrier to entry for this type of business model would be consumers' willingness to educate themselves on the functionality of tokens like UAT.

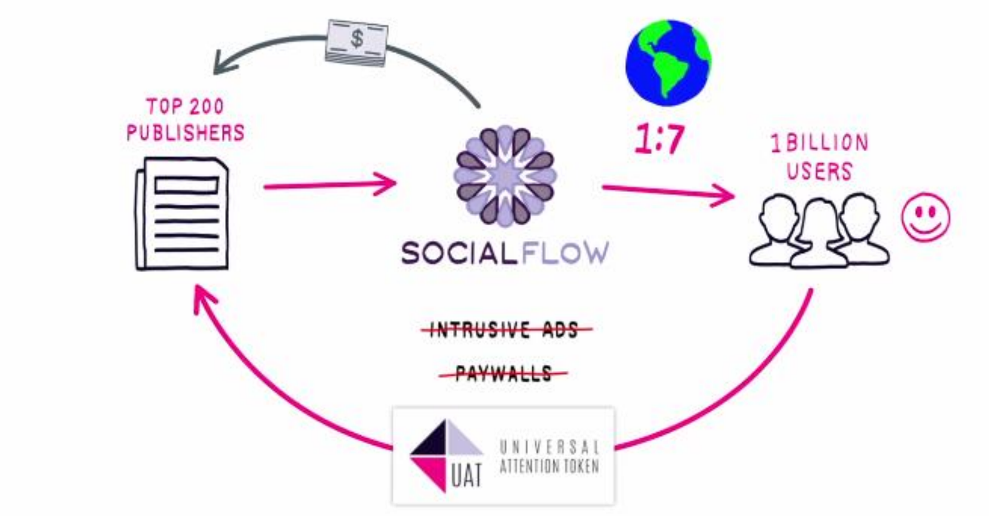


Figure 10: Visualization of Social Flow's business model[175]

3.2 Increasing public access to quality and verified information - right to information

A potentially positive side-effect of a blockchain-based business model could be an increase in the quality of journalism, due to a reduction in editorial interference and misinformation. Newly emerging news-dissemination platforms are testing blockchain as a means of providing citizens with accurate and unexpurgated information, which could impact decision-making at the local, state or national levels. The following initiatives are rooted in the right to information, rooted in the understanding that information is empowering.

[175] SocialFlow, 'What is the UAT Ecosystem?' (Facebook 29 August 2018) <https://www.facebook.com/socialflow/videos/1790864651028711/?v=1790864651028711> accessed 24 May 2019.

All too often, board decisions silence journalists that work to expose the truth, citing conflicts of interest. Financial dependency on sponsors, donors and advertisers can cultivate a soft policy of avoiding negative coverage for those they support, which is apparent in the case of both the *Las Vegas Review Journal* and *The Denver Post*. In 2015, Sheldon Adelson, a billionaire with several business interests in the Las Vegas area, bought the *Las Vegas Review Journal*. James Wright, former deputy editor of the *Journal,* admits that any articles about Adelson or his affiliated businesses go through an extra review process: "In this review process, things are changed, added, removed with no explanation as to why, and there is no appeal…There are things done because it is known that this is the way Sheldon Adelson wants it to read. And it could be something very minor or it could be something very big."[176] Similarly, in 2018, a group of *Denver Post* employees decided to quit the paper due to the *Post*'s hedge-fund owners having too much control over its editorial coverage.[177] The former employees have since created a competing paper, *The Colorado Sun*, partially funded by the Civil Media Company's crypto-business model.[178] *The Sun* hopes to participate in the reclamation of journalistic authority, rather than corporate interference, to decide which stories are told and to provide the public with a less-filtered version of the truth.

The Civil Media Company is making the most jarring moves thus far in the blockchain-based journalism space and is focused on reviving the definition of quality and credible journalism through community accountability. The Civil platform directly reconnects news creators to news digesters and eliminates advertising from its business model; instead, the theory behind the platform is that readers, journalists, and newsrooms will invest—via Ethereum blockchain-based token CVL—in assuring that the content shared on the platform is independent, original, and in accordance with ethical journalism. News agencies, on the other hand, still rely on a hybrid-sourced income: CVL and advertising revenue.

News organizations can join Civil by purchasing memberships of at least $1,000 USD in CVL; once a member, they can permanently archive their content on the Civil blockchain and accept CVL payments or donations from readers that support the organization. Anyone interested in upholding the project's mission can also purchase CVL in order to become a member of the private blockchain community, and this pool of journalists and critical eyes collectively work to verify posts on the platform and police contributors' abidance of the Civil Constitution. Therefore, rather than giving a parent company or sponsor the choice of what content readers can consume, a decentralized network of people curates the content. The Civil Constitution is the cornerstone of this principally self-governing platform, which all community members must agree upon in order to contribute content. Section III of the Civil Constitution outlines:

> "Civil is dedicated above all else to the public, which journalism is intended to serve. Its purpose is to provide citizens with information that enables them to fully participate in society. Civil seeks to establish the conditions for journalism to fulfill that purpose with minimal interference from government, commercial pressures, or

[176] John Oliver, 'Journalism: Last Week Tonight with John Oliver (HBO)' (LastWeekTonight, 7 August 2016) <https://www.youtube.com/watch?v=bq2_wSsDwkQ> accessed 25 May 2019.

[177] Jaclyn Peiser, 'Goodbye, Denver Post. Hello, Blockchain' *New York Times* (17 June 2018) <https://www.nytimes.com/2018/06/17/business/media/denver-post-blockchain-colorado-sun.html> accessed 24 May 2019.

[178] Civil, 'The Civil white paper' <https://civil.co/white-paper/> accessed 24 May 2019.

> other interests that inappropriately attempt to influence, control or stop the gathering and dissemination of facts, opinions and ideas in the public sphere through unjust laws, commercial pressure, intimidation or violence."[179]

If anyone posts content—be it audio, video, illustration, photography, data visualizations, animations or text—in conflict with the Constitution's prescribed code of conduct, any member of the community can challenge that contribution and initiate a voting process, whereby all community members are able to agree or disagree on whether a piece of content should be removed from the platform. Therefore, the Civil community acts as a jury on the matter, but there is also an appeal process where the Civil Council (made up of proven constitutionally conscious journalists) can reverse decisions if there is extemporaneous cause. A graphic illustration of the Civil model is shown on the following page.

[179] Vivian Schiller, 'The Civil Constitution' (*Civil*) <https://civil.co/constitution/> accessed 24 May 2019.

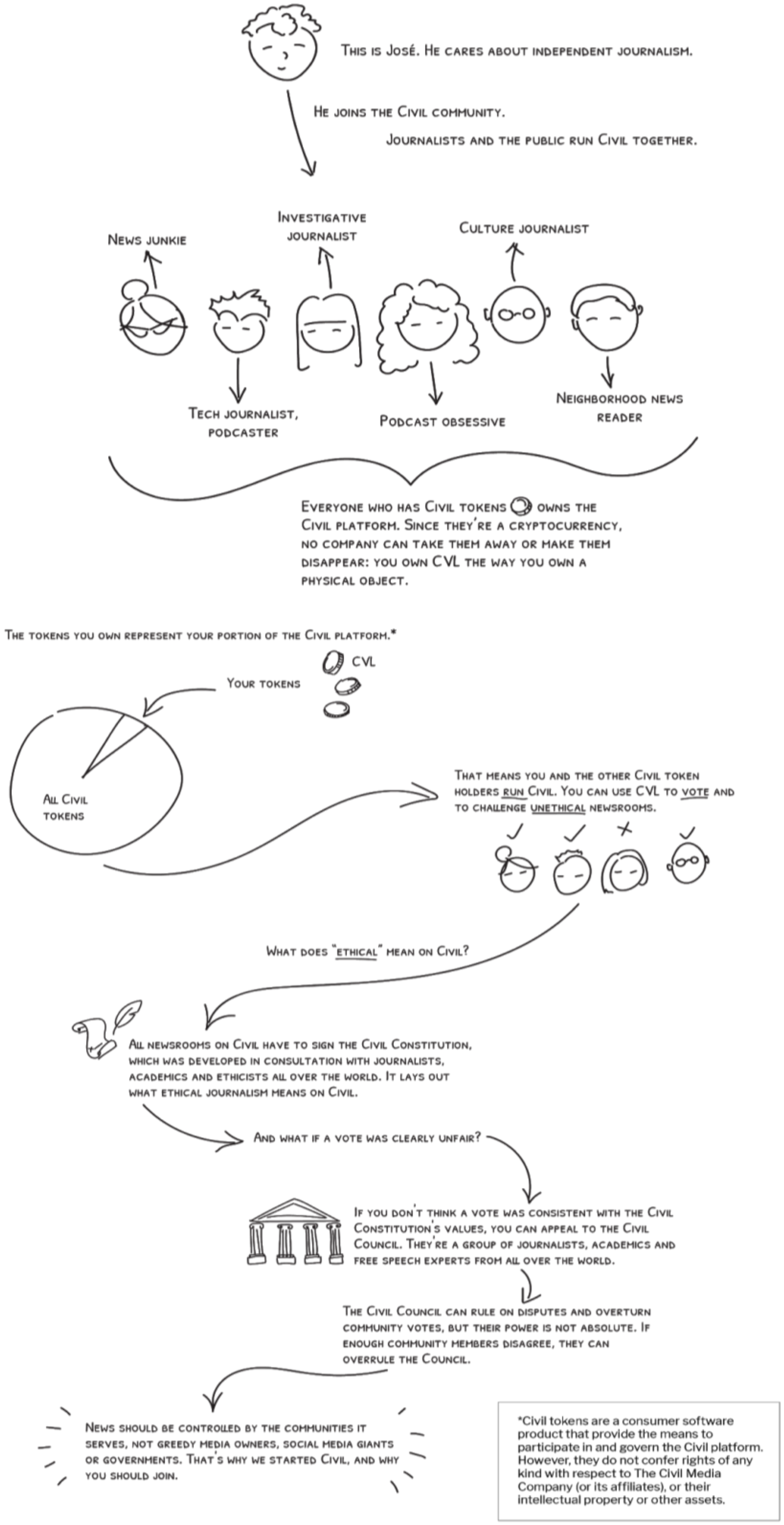

This is José. He cares about independent journalism.
He joins the Civil community.
Journalists and the public run Civil together.
News junkie
Investigative journalist
Culture journalist
Tech journalist, podcaster
Podcast obsessive
Neighborhood news reader
Everyone who has Civil tokens owns the Civil platform. Since they're a cryptocurrency, no company can take them away or make them disappear: you own CVL the way you own a physical object.
The tokens you own represent your portion of the Civil platform.*
CVL
Your tokens
All Civil tokens
That means you and the other Civil token holders run Civil. You can use CVL to vote and to challenge unethical newsrooms.
What does "ethical" mean on Civil?
All newsrooms on Civil have to sign the Civil Constitution, which was developed in consultation with journalists, academics and ethicists all over the world. It lays out what ethical journalism means on Civil.
And what if a vote was clearly unfair?
If you don't think a vote was consistent with the Civil Constitution's values, you can appeal to the Civil Council. They're a group of journalists, academics and free speech experts from all over the world.
The Civil Council can rule on disputes and overturn community votes, but their power is not absolute. If enough community members disagree, they can overrule the Council.
News should be controlled by the communities it serves, not greedy media owners, social media giants or governments. That's why we started Civil, and why you should join.
*Civil tokens are a consumer software product that provide the means to participate in and govern the Civil platform. However, they do not confer rights of any kind with respect to The Civil Media Company (or its affiliates), or their intellectual property or other assets.

Figure 11: Explanatory flow chart of how the Civil Media Company's platform functions[180]

[180] Civil <https://civil.co/> accessed 22 May 2019.

The execution of this idea has proven to be very complicated, yet it is slowly gaining traction with journalists and publishers alike, including Forbes,[181] Sludge, Popula, the Associated Press[182] and approximately 100 other newsrooms of various sizes.[183] The proliferation of 'fake news' is partly due to the fact that the writers of falsified stories and disinformation campaign managers are not held accountable to the public they wrongly influence. In this new system, the public can directly fight not only disinformation, but low-quality clickbait journalism as well. Constitutionalizing online journalism emboldens the traditional social contract between news producers and consumers, in which the media and public work together towards a mutually beneficial outcome: reduced corruption, greater transparency, upholding the rule of law and good governance. The Civil Constitution stipulates the rights of media consumers and the responsibilities of media producers, reinstating the rules of earned credibility.

A blockchain platform solely aimed at fighting fake news has yet to exist; however, researchers have begun theorizing potential fact-verification frameworks. As discussed in Part 2, companies are working on blockchain-based supply-chain verification in order to create more transparency concerning 'organic,' 'free trade' or 'conflict free' products, and the same idea is applied to fact-checking the origins of news. Qayyum and others argue that blockchain has great promise in revaluing truth in a "post-truth" world; by harnessing blockchain's ability to carry out smart contracts,[184] decentralized consensus and tamper-proof authentication.[185]

Authentication, in this context, refers to checking the legitimacy of a news agency against lists of fake news sites that purposefully mimic news agencies, while they are simultaneously the cause of phishing attacks or hoaxes. Proof-of-Truthfulness (PoT) is a potential additional element of the standardized Proof-of-Work mining method. PoT would require that facts must be verified by hashes linked in the blockchain. Participating nodes would then be able to easily verify the source of referenced content, eliminating the possibility of an error message reading 'link not found' for in-text citations. Decentralizing the news would mean that fact-checking groups can play a more direct role in linking readers to credible articles and archiving falsified stories on a transparent platform that the government would have no power to delete. Activists, technology experts and academics can challenge the validity of an article, for the community to review. Furthermore, altered photo or video content could be more easily traced to the original, which would help eliminate the pervasive spreading of deep fakes. While images and videos on blockchain would be cryptographically stored, every interaction with the content is detectable.

[181] Forbes Corporate Communications, 'Forbes Becomes First Major Media Brand to Experiment with Publishing on Civil Platform' (*Forbes*, 9 October 2018) <https://www.forbes.com/sites/forbespr/2018/10/09/forbes-becomes-first-major-media-brand-to-experiment-with-publishing-on-civil-platform/#e1647b177c15> accessed 25 May 2019.

[182] Matt Coolidge, 'Civil and The Associated Press to Collaborate on Blockchain-Based Content Licensing' (*Medium*, 28 August 2018) <https://blog.joincivil.com/civil-and-the-associated-press-to-collaborate-on-blockchain-based-content-licensing-c7211f5ae7fa> accessed 26 May 2019.

[183] Matthew Iles, 'Civil means journalism' (*Medium*, 1 March 2019) <https://blog.joincivil.com/civil-means-journalism-3fd7a6be8aee> accessed 23 May 2019.

[184] Discussed further in Part 3

[185] Adnan Qayyum and others, 'Using Blockchain to Rein in The New Post-Truth World and Check The Spread of Fake News' (*Information Technology University,* 2019) 3-5 <https://arxiv.org/pdf/1903.11899.pdf> accessed 24 May 2019.

While Civil, or any existing platform, is not modeled off of Qayyum and others' research, it does embody some of their proposed verification concepts, including a variation of the Evolving Reputation Set where all newsrooms are invited to contribute with the understanding that their 'membership' in the community is at risk of being revoked with the post of each article. The quality of newsrooms—as it relates to accuracy, context, and bias—would evolve within a score-based system.

Blockchain would not likely be able to eliminate fake news all together, because the original upload would have eternal life. Yet the debunking of fake news would be logged in a linear and orderly ledger, which is more easily digestible than a multitude of anonymous opinions. Anonymity is also self-monitored, and experts or newsrooms can expose their credibility scores when voting to verify content through their digital signatures. Linking content to a verifiable source coincides with standardizing digital identities, and while it would be far into the future, theoretically, all news articles could be blockchain verified as legitimate prior to their ability to be shared on any social media platform.

3.3 Accessing public data secured in government blockchains - improved transparency

The right to information directly relates to the need for operational transparency in government, and over 100 countries have laws that codify a citizen's right to an open government.[186] Since blockchain is based on consensus, it could replace existing social hierarchies that fog visibility, including corruption and bureaucracy.[187] It also could be useful as a tool to increase efficiency and accountability in regards to the government's oversight of complex taxation protocols, federal budget spending, courtroom evidence authentication, tamper proof record storage for documents such as visas, property ownership, licenses, and more.[188] Governmental financial reports, speeches and voting records of elected officials, and even their tweets would be unassailable and undeletable.[189] All of these documents could be kept for journalists' investigative purposes, but also for generations to come—to analyze the impact of the policies and political discourse of today.

The government of Estonia is one of the first to fully embrace distributed ledger-based technologies, and in 2016 all 1.3 million Estonian residents' medical records were secured on the decentralized Healthcare Registry.[190] Using digital identities, Estonian citizens can access their records' activity log on a platform that stores all of their previous documents, showing which

[186] Toby Mendel and others, 'International Standards on Transparency and Accountability' (*Centre for Law and Democracy and Democracy Reporting International,* 2014) page 1 <http://www.law-democracy.org/live/wp-content/uploads/2014/04/Transparency-and-Accountability.final_.Mar14.pdf> accessed 26 May 2019.

[187] MyungSan Jun, 'Blockchain government - A next form of infrastructure for the twenty-first century' (2018) 4(7) Journal of Open Innovation: Technology, Market, and Complexity <DOI 10.1186/s40852-018-0086-3> accessed 26 May 2019.

[188] Blockchain, 'Blockchain Applications in *Government*: Blockchain Technology for Government' <https://www.blockchaintechnologies.com/applications/government/> accessed 26 May 2019.

[189] A website emerged d in order to monitor the tweets that Trump deletes, in an attempt to keep them as part of the public record. For other world leaders that do not have similar websites, important content is lost when deleted. Factba.se, 'Donald Trump- Deleted Tweets' (2019) <https://factba.se/topic/deleted-tweets> accessed 31 May 2019.

[190] Kaspar Korjus, 'Welcome to the blockchain nation' (*Medium,* 7 July 2017) <https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4> accessed 27 May 2019.

medical professionals viewed their information and when they did so. The records themselves remain in databases within the cloud, which is currently the data storage solution for many governments; the CIA logs their information in Amazon Web Services' cloud, for example. Adding a blockchain layer of security on top of the cloud allows for all instances of access to be traced. This kind of pellucidity allows for citizens to be more in control of what happens behind closed government doors, or ensure that the digital filing cabinets holding their sensitive personal information are actually locked. An increase in trust in government processes, as well as State institutions in general is a major incentive behind uncovering blockchain's potential, which is one of the reasons why the European Union Blockchain Observatory & Forum's Horizon 2020 program will invest €300 million in projects supporting the use of blockchain and policy-related actions.[191] Over the course of 2018 and 2019, 27 member States signed the Declaration for a European Blockchain Partnership (EBP) in order to "cooperate on the development of a European Blockchain Services Infrastructure."[192] Additionally, in 2018, the National Research Council of Canada (NRC) launched the first-ever live trial of a public blockchain for the transparent administration of government contracts.[193] E-governance, using digital tools to help with the business of governing, is inexorable, yet whether government-created blockchains will help or hinder watchdog journalism remains a point of contention.

Transparency and freedom of information need greater stature in the hierarchy of societal importance,[194] and the nature of freedom of information requests from journalists will likely change as more governments adopt blockchain-based transparency initiatives. As Ivancsics hypothesizes, journalists who request public records based in a blockchain from governments will be at greater risk of exposing the story they are working on. Freedom of Information requests would be publicly logged, which "could become highly problematic for journalists on the trail of a story wishing to act covertly before it breaks."[195] Concerning the safety of journalists, many corruption-infused States could view an individual's access of an article as a direct threat, which could set in motion an order for kidnapping or even assassination. The accession of blockchain in government operability would require that journalists continue to take extreme precaution in protecting their identities and the identities of their sources.

3.4 Reduce government surveillance, imposed censorship and better respect privacy - freedom of expression

A function of defending and practicing the right to freedom of speech is for the allowance of criticism against the government. The First Amendment to the United States Constitution protects citizens from their government in their expression of these criticisms—the impetus being the freer the speech the stronger the democracy—and what is considered "speech" has evolved

[191] European Commission, 'European countries join Blockchain Partnership' (10 April 2018) <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership> accessed 24 May 2019.

[192] ibid.

[193] CMSC Media, 'Canada using blockchain for transparent administration of Government contracts' <https://www.cms-connected.com/News-Archive/August-2018/Canada-Using-Blockchain-for-Transparency-of-Government-Contracts> accessed 27 May 2019.

[194] Patrick Birkinshaw, 'Transparency as a Human Right' (2006) 135 Proceedings of the British Academy <DOI: 10.5871/bacad/9780197263839.003.0003> accessed 26 May 2019.

[195] Ivancsics (n. 100).

alongside technology. Over the past two decades, courts reached a “near consensus” that “computer code, along with virtually every flow of data on the Internet” is protected as “speech” as it relates to freedom of expression.[196] At the twenty-ninth session of the UN Human Rights Council in 2015, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, released a report stating that encryption should also be protected as a means of promoting free speech:

> “Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks. The previous mandate holder noted that the rights to ‘privacy and freedom of expression are interlinked’ and found that encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40 and Corr.1). Echoing article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights specifically protects the individual against ‘arbitrary or unlawful interference with his or her privacy, family, home or correspondence’ and ‘unlawful attacks on his or her honour and reputation’, and provides that ‘everyone has the right to the protection of the law against such interference or attacks.’”[197]

Alex Gladstein, Chief Strategy Officer for the Human Rights Foundation, notes that there are 4 billion people living under authoritarian rule around the world, and many citizens are reliant on encryption-based technologies in order to practice free expression without interference from surveillance States.[198] The Russian government is repeatedly trying to access messages within the app Telegram; the Chinese government is constantly monitoring WeChat; the Brazilian government once blocked WhatsApp for 72 hours.[199] Tyrannical States are quick to overcompensate for the kind of liberation that technology has been able to provide critics, intellectuals and other diverse perspectives.

Journalists’ use of technology needs to progress a step ahead of oppressive rule, beyond the capabilities of State control, and blockchain is a potential tool to circumvent unwanted supervision. Mainframe, for example, serves as an operating system (OS) for surveillance-free communication.[200] Those using this blockchain-based program are able to navigate the network without being monitored, and it hosts applications that are censorship-free. All applications that run on the Mainframe OS must embody a privacy-focused mission statement and are impossible for any government to shut down. “The Internet was never meant to be controlled by anyone,”

[196] Kyle Langvardt, ‘The Doctrinal Toll of "Information as Speech"’ (2015) 47 Loyola University Chicago Law Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2674634> accessed 26 May 2019.

[197] Serge Schouterden, ‘Bitcoin and Encryption are Protected by Freedom of Speech’ (*Bitcoin.com*, 11 June 2015) <https://news.bitcoin.com/bitcoin-and-encryption-are-protected-by/> accessed 27 May 2019.

[198] Eric Wall, ‘Privacy and Cryptocurrency, Part I: How Private is Bitcoin?’ (*Medium*, 7 March 2019) <https://medium.com/human-rights-foundation-hrf/privacy-and-cryptocurrency-part-i-how-private-is-bitcoin-e3a4071f8fff> accessed 28 May 2019.

[199] Kate Conger, ‘WhatsApp blocked in Brazil again’ (*TechCrunch*, 2016) <https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/> accessed 27 May 2019.

[200] Steven Buchko, ‘Mainframe’s Mick Hagen on the Importance of Censorship Resistance and Charitable Endeavors [PART 1]’ (*Coin Central*, 21 May 2018) <https://coincentral.com/mainframe-mick-hagen-interview-part-1/> accessed 27 May 2019.

explains Neil Bly, vice president of product for Mainframe, “let alone be held hostage by a few.”[201] At its core, Mainframe attempts to offer an unbridled platform that protects citizens from NSA-esque, nefarious spying and empowers the individual voice, which is why the founders of Mainframe have directed a call to action towards the journalism industry. Mainframe donated 1,000 ETH to the Freedom of the Press Foundation, which works closely with journalists and whistleblowers, including Edward Snowden.[202] The donation is coupled with a push for the Foundation to “explore the potential to combat censorship and data compromise through decentralized technologies” and Mainframe is also granting “early access to test new features and functionality of [their] platform,” highlighting the importance of free speech, free press, and freeing people in a digital age. The most promising outcomes of platforms like Mainframe for journalists would be uninhibited messaging apps, unmonitored file-storage, or uncensored bulletins for local, national, or international news agencies.

Some journalists are attempting to use Bitcoin tokens (BTC) as a way to circumvent government surveillance of their purchases, making it more difficult for actors to geolocate them through their consumption—i.e. tracking them along the course of their investigations. However, when dealing with blockchain it is important to know how far encryption and anonymity will go for protection. Tech-experts have warned human rights defenders that Bitcoin’s node network is part of a public blockchain, and it only provides identity privacy to a certain extent. While all transactions use digital signatures, blockchain analytics firms have already emerged, employing specialists that work to uncover trends in transaction histories and source IP addresses. With the cooperation of service providers, IP addresses are easily traceable to a person’s real identity. The Tor browser, as discussed in Part 1, is a tool that journalists should use in conjunction with BTC in order to hide their IP address while making transactions for greater security.

Part 4: Applying blockchain to journalistic activity in the field

Academic research concerning blockchain and journalism has focused on how distributed ledger technology can salvage the industry of journalism itself, but prior research has not yet addressed how blockchain and, more broadly, the decentralization of content, can provide greater security for those doing ‘press’ jobs. As explained in Part 1, multiple mobile apps were developed in a targeted attempt to better inform and protect journalists against threats, yet many have been unsuccessful due to the fact that any single-host institution is susceptible to hacking or cyberattacks. Additionally, journalists seldom use more broadly-adaptable, cybersecurity-focused technologies—which can be primarily attributed to usability and design issues—seeing as there is a disconnect between the tech industry and the needs of the journalistic process.[203] While distributed networks, such as blockchain, are not simple to develop, building a user-friendly platform that focuses on protecting journalists and their work is a partial solution to the much grander insecurity issue. Once established and funded, decentralized platforms are operable in any country and beneficial for journalists of all nationalities, including freelancers working without dependable corporate or State protection.

[201] Mainframe OS <https://mainframeos.com/> accessed 27 May 2019.

[202] Mick Hagen, ‘Freedom of the Press Foundation & Mainframe’ (*Medium*, 18 June 2018) <https://blog.mainframe.com/freedom-of-the-press-foundation-mainframe-6ffb39918503> accessed 26 May 2019.

[203] McGregor and others (n. 37) 403-405.

As evidenced by the plethora of tech-based security developments, it is clear that journalists need a borderless solution for what has become a borderless safety issue. *The Washington Post* columnist Anne Appelbaum explains that prior to the existence of the Internet, censorship or expulsion were the more common means of silencing journalists, but "today, a writer like Khashoggi, working from abroad, could reach substantial audiences both inside Saudi Arabia and among the international business and political figures who might determine the success or failure of Crown Prince Mohammed bin Salman's reign."[204] Due to the international nature of the news coverage and information dissemination, the strategies for protecting journalists must also have a collective multi-State solution. However, considering that nations inconsistently hold one another accountable for protecting journalists—as per the situation between the United States and Saudi Arabia—State-independent solutions are needed in place of either non-existent political will or unenforceable conventions. A technology like blockchain may be able to stand in as a more dependable means of support, as its decentralized nature ensures that journalists take priority over State concerns.

Blockchain, however, is not an all-encompassing solution to ensuring journalists are physically or digitally secure. Rather, it can act as an additional layer of assurance to existing software and applications, weaving a more reliable safety net for those that risk their lives in search of the truth. As described in Part 2, the most promising use-cases for blockchain are ensuring that content is tamper-free, decentralizing content from a single authority, and securing transparency of data flow. In consideration of these functions, the specific methods of enhancing the safety of journalists throughout the news gathering process via blockchain are exemplified in the following applications:

- Secure file storage and sharing of documents, photos, videos, audios, agenda, emails, etc.
- Checkpoint verification
- Logging and sharing digital and physical security incidents

4.1 Secure file storage - using blockchain & bit-torrent[205]

In an ideal scenario, any materials collected during an investigation must be completely secret, sources must be kept private, and the transcripts, photos, videos taken or gathered should be inaccessible to anyone, except the journalist, throughout the investigative process. The most common and free way to store material is on cloud-based networks (such as iCloud, Google Drive, Dropbox etc.), but these platforms have suffered from massive data breaches in the past. To combat this risk, many major media houses use encryption platforms such as VeraCrypt, CryptPad and Cryptomator for additional file protection.[206] Nevertheless, all of these platforms rely on a centralized server, meaning all content, whether encrypted or not, is theoretically subject to the host company's control. Journalists undoubtedly recognize the value of secure file storage, but trusting a single company with valuable and sensitive information is risky, particularly if

[204] Freedom House, 'Violence against Journalists Is a Transnational Enterprise' (17 October 2018) <https://freedomhouse.org/blog/violence-against-journalists-transnational-enterprise> accessed 20 June 2019.

[205] Bit-torrent uses multiple computers to store and transfer files. The various pieces of a whole file are stored on different computers as a means of decentralization, as well as lowering the average bandwidth needed to download it.

[206] Garza Ramos (n. 74) 5.

governments place pressure on news companies to comply with content elimination requests. For example, the total number of government requests for Google to remove information from their products is increasing, with 25,534 requests submitted between January and June 2018.[207] A single government request may ask for the elimination of multiple items; therefore, taking into account each individual piece of content, governments called for the removal of 271,127 items within that same six month period in 2018.[208] According to Google, "governments cite defamation, privacy, and even copyright laws in their attempts to remove political speech from our services."[209] Google attempts to respond to these requests in accordance with the laws governing each country, and in many instances it is compliant or at least partially compliant to government requests or court orders.[210] Specifics concerning Google's approach to cooperating with oppressive governments and legal repression of freedom of expression are not outlined in the report, and Google is an example of a company that actually tracks and attempts to standardize this procedure. Other companies, particularly those based in authoritarian States, may not have any transparency to their content removal processes or even monitor their activity in this regard.

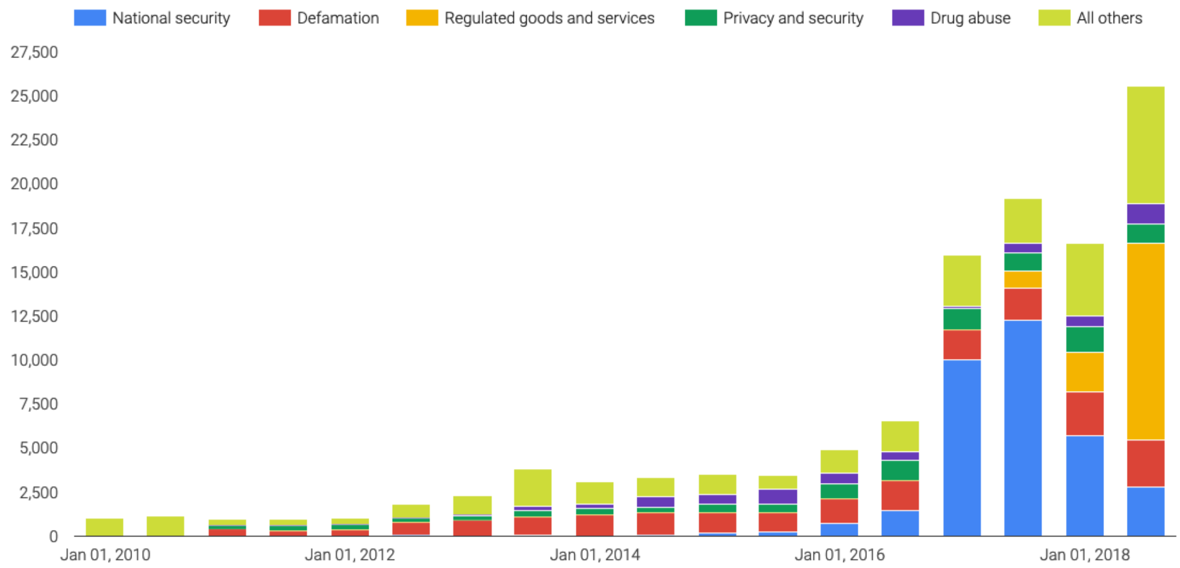


Figure 12: Breakdown of the cited reasons behind government requests to remove content or information from Google platforms/services[211]

[207] Google, 'Transparency Report: Government requests to remove content' <https://transparencyreport.google.com/government-removals/overview?hl=en&removal_requests=group_by:totals;period:&lu=removal_requests> accessed 25 June 2019.

[208] ibid

[209] ibid

[210] An extensive list and brief description of each request and the outcome is available on Google's Transparency Report webpage, where requests can also be viewed per country. ibid.

[211] ibid.

In regards to file-sharing, newspapers rely on external open-source systems like SecureDrop, where whistleblowers can safely and anonymously send files.[212] While these tools are reliable, they do not keep immutable records of the files, making it impossible to determine if some files have been deleted or if any of the content has been altered after submission. Hence, there is no evidence of how frequently this has occurred.

Therefore, using a decentralized storage tool could be a sure way for journalists to harbor the media and information collected in the news-gathering process. Such programs can ensure that the critical information needed for watchdog reporting, investigative journalism, and accurate storytelling is kept securely—and even permanently, if stored on the blockchain. Storj[213] and the InterPlanetary File System (IPFS)[214] are examples of decentralized storage platforms where the content is either duplicated across multiple nodes, or, once uploaded, it is shredded, encrypted, and spread across a network of nodes for safekeeping, until the journalist needs to access the file again. Storj is based on a bit-torrent system, while the IPFS is based on the blockchain. In the case of Storj, for example, the complete file is not in a single location, but rather its components are distributed across multiple locations; thus, a hacker in search of a single document would first have to locate all of the nodes containing its pieces, attack each node separately, and reconstruct the document in a sensical order. Additionally, the encryption keys are in the hands of the journalist rather than the company operating the digital drive, removing final decision-making authority from the hands of a third party. Consequently, it would no longer serve a purpose for governments to pressure companies—such as Amazon, Apple, Google and Facebook—to disclose users' personal data to authorities, because the individuals themselves hold the encryption keys. Even if the document is reconstructed, the hacker wouldn't be able to understand its contents without also knowing the journalists' encryption key. The likelihood of all of the above events taking place in favor of a cyber attacker is nearly impossible. However, prior research concerning journalists' adoption of technological best practices fails to mention the importance of decentralized storage and the potential benefits of permanently logging their content on the blockchain.

OpenArchive[215] is a recently-launched mobile app, created for human rights defenders to preserve and protect the audio/visual media content they capture and post on social media. This application, which currently only works for Android phones, was built to protect a person's content "in the event of Internet shutdowns, surveillance, device confiscations, content takedowns, limited bandwidth, and data loss."[216] The application allows for organizations within civil society to permanently save their media content on either the open Internet Archive, or an internal private server; in both cases, copies of the media are stored in multiple locations on various servers, with encryption limiting their accessibility. Within the wave of content takedowns and the proliferation of misinformation, governments or corporations have been free to subjectively deem certain media content as 'inappropriate' or in violation of a platform's Terms of Service. Regardless of intention, these posts, photos and videos containing hate speech, violence, racism, etc. should not be deleted from public memory, as they testify to important trends of societal angst and, in some cases,

[212] McGregor and others (n. 37) 400.

[213] STORJ <https://storj.io/> accessed 21 June 2019.

[214] Protocol Labs, 'Introducing Filecoin, a decentralized storage network' (19 July 2017) <https://www.youtube.com/watch?v=EClPAFPeXIQ> accessed 22 June 2019.

[215] It is important to note that OpenArchive is not based on blockchain but instead uses a similar method of decentralization of information. Open Archive <https://open-archive.org/> accessed 22 June 2019.

[216] ibid.

legitimize claims relating to violations of human rights.[217] Journalists, in particular, are often key witnesses to the critical, controversial and historical moments that shape how events will be remembered, giving their media collections significant value. While OpenArchive is available for numerous types of organizations, the application is currently marketing itself to journalists, as seen below:

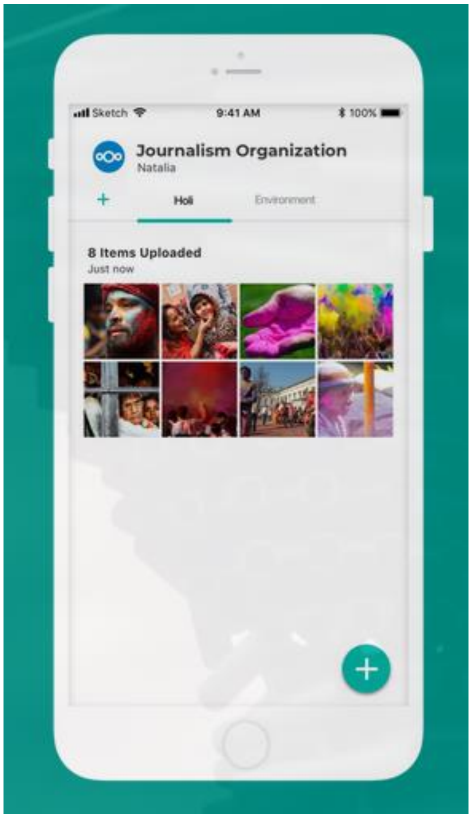


Figure 13: Screenshot of OpenArchive's app interface[218]

Using any of the above programs, journalists would be able to securely and privately store highly sensitive information—including important emails, audio or video testimonies, interview transcripts, photographs from protests or crime scenes, etc.—knowing that it cannot be deleted by any single point of failure, i.e. a company or government with centralized control. OpenArchive attempts to validate data with options to either manually input notes and locations, or tag people within each uploaded file. The latter can also take place with the ProofMode[219] extension, which is a program that maximizes metadata capture while taking photos or videos. Metadata is extremely

[217] The UC Berkeley Human Rights Center is working in collaboration with the International Criminal Court, the tech startup EyeWitness, the Commission for International Justice & Accountability (CIJA), along with other international legal and tech consultants in order to create an International Protocol for Open Source Investigations to address the issue of content removal which could be useful in trying authorities for war crimes and crimes against humanity. In doing so, hashing is an important part of verifying the originality and legitimacy of evidence, according to Enrique Piracés, manager of the Media and Human Rights Program at the Center for Human Rights Science and a consultant to the Protocol initiative. Rights Con 2019 (n. 94).

[218] Open Archive (n. 215).

[219] Nathan Freitas, 'proofmode' (*Why GitHub?*, 24 February 2017) <https://github.com/guardianproject/proofmode/blob/master/README.md> accessed 23 June 2019.

valuable in media verification and, by extension, investigative journalism and the disarming of mis- or dis-information. The content that journalists collect is soundly admissible in a courtroom or to a human rights body if they can provide immutable verification, which is possible via the blockchain. Collaborative layering of decentralized storage with blockchain hashing would act as a public notary for journalistically sourced evidence; a better use for the sensitive and triggering information that companies and governments are otherwise trying to delete.

4.2 Logging and sharing digital and physical security incidents

Security First's Umbrella app, as described in Part 1, is a valuable tool for activists, human rights defenders and journalists to become literate in digital safety and security. Within the app, self-reflective incident forms are available with step-by-step instructions on how to act once a digital or physical attack occurs. Incidents reported through the app are designed with the victim's personal experiences in mind, for the purpose of assuring that the victim knows the proper steps to take post-violation. For example, when completing the physical security incident form, question seven asks "Who has the incident been reported to locally?" followed by "Please suggest specific measures that may help avoid this type of incident in the future." Be that as it may, the impact of these forms is limited considering they do not ensure that relevant agents are actually notified. In this sense, it is a tool of support and guidance, rather than a mechanism for streamlining redress. There is also no way to review a collective log of these reports and therefore no opportunities to analyze the frequency or intensity of multiple incidents—within a particular region, at certain times, or from a specific group, for example. Umbrella's incident forms are only shareable if the host organization has programmed for that possibility, and for any given case, there is no assurance that the report will be stored in a secure location.

Adding a layer of blockchain to the Umbrella app could guarantee that digital and physical attacks against journalists are permanently recorded and accessible, for further action to take place. Blockchain acts as the most suitable technology to employ, considering its hashing function which timestamps events into an unchangeable historical ledger. These incidents could be logged on a topical ledger as well—with the Committee to Protect Journalists for example—for a supporting body or institution to follow through with resolving each report. Negative consequences could arise if privacy for the victims is not prioritized and respected. Once something is published on the blockchain it cannot be removed, thereby signifying that confidential details or personal information cannot be removed if published on the blockchain.

4.3 Checkpoint verification

As mentioned in Part 1, logistics companies are interested in integrating blockchain into their supply chain management for greater transparency. Capgemini is one such company, which has developed a 'Smart Container', which combines IoT with blockchain to track the location and condition of a product as it moves from point A to point B.[220] A chip equipped with sensors travels with the merchandise in order to continually send updates to the back-office which monitors each shipment. A similar feedback-type-system could be implemented for journalists to communicate with their editor, or colleagues, or loved ones when entering risky territory. If journalists' routes

[220] Capgemini, 'Capgemini Smart Container using Blockchain' (9 February 2018) <https://www.youtube.com/watch?v=6A0FMv-JXQE> accessed 23 June 2019.

are interrupted, or perhaps a certain number of check-ins are not registered, an alert can be triggered for a predetermined confidant to intervene. This type of tracking could be very beneficial to journalists entering dangerous areas; offering extra assurance that there is a system of trusted, precautionary supervision in place.

One of the primary issues with geolocation-based emergency response applications that have been developed in the past—such as Panic Button and Reporta—is the vulnerability of the GPS information due to hacker susceptibility. The centralized storage of the data is what puts activists and journalists in danger when using these applications; therefore, there is a lesser risk to implementing the same model, in which the GPS information is stored and then released to a trusted contact in the event of an emergency, using a decentralized network of servers. Instead, if these coordinates were to be encrypted and stored across various private nodes or a private blockchain, then the only way to access the information in an assembled and decrypted manner would be via the emergency trigger—and even then, only the trusted contacts would have the key to decode the coordinates.

Previous tracking applications also experienced difficulties in scalability, because providing 24/7 monitoring of human rights defenders around the world requires a great deal of human resources and time to assess when a person is actually in danger, or if they have triggered a false alarm. If built on a blockchain, the release of a journalist's GPS location could be executed via a smart contract,[221] even without the need of a button being pressed, and sent to one or multiple people that have agreed to be personally accountable for receiving and acting upon the alert. Journalists would need to pre-program the smart contract before leaving on each mission, according to the specifics of the journey. Therefore, the responsibility is more appropriately delegated and false-alarms are much less likely to occur, leaving it up to journalists themselves to choose who they would like to entrust as their emergency contacts.

4.4 Conclusions

These suggestions are not to say, however, that the creation of a decentralized storage system, a more trusted GPS tracking system, a more secure incident report, or any type of blockchain will be a catch-all solution for completely protecting journalists against the many threats they face in the field. There is no application that can stop a bullet and no technology that can replace human support systems provided by organizations such as the Committee to Protect Journalists, the International Center for Journalist and Frontline Defenders, among others. The suggested applications of decentralized networks provided above serve as a theoretical foundation for developing tools available for practical use that could aid the work of these organizations, within the near future. Journalists must not only continue to educate themselves on the most relevant preventative technological tools available (see Annex 1) but also rely on traditionally imperative journalistic best-practices—such as taking physical safety precautions, developing a strong intuition, training oneself on how to investigate inconspicuously, and adhering to professional conduct in the field.

[221] Automated smart contract execution is further explained in the following section. In summary, the journalist can pre-set conditions—such as inactivity for a certain number of days, or the GPS tracking is off route, etc—for the smart contract to automatically release the decryption key.

That being said, the above suggestions would provide greater confidence that information is stored without risk of being deleted, security incidents are not tampered with or stuck on a single phone application, and critical information (like a journalist's location) will be used more productively. Drawing back to the example of the creation of the Internet in Part 2, it took time for the technology to reach a certain level of maturity before the general public could have greater access to it. Similarly, there are still many necessary advancements in order for blockchain to be both more efficient and more widely adopted, but innovative applications continue to materialize, showing continual advancement. Importantly, considering blockchain is still a developing technology, the theoretical should not become actual until further research is done to war-game the possible negative outcomes of building these tools for human rights defenders and journalists in dangerous situations.

PART 5: Using smart contracts to streamline judicial processes and reduce the rates of impunity for the assassination of journalists

5.1 What is a smart contract?

Smart contracts are similar to paper contracts, in that they lay out certain terms and conditions for an agreement. The difference lies in that smart contracts are completely digital, and the programmed conditionalities and responses are stored inside of the blockchain. Essentially, smart contracts store, validate and self-execute rules based on an "if this, then that" logic. Smart contracts are immutable—meaning they cannot be changed—as well as distributable, meaning everyone on the blockchain network can validate the output of a contract. As described by Bitcoin News (NewsBTC), a smart contract "allows individuals to exchange data in a trusted, conflict free manner, without depending on a third party."[222]

Similar to existing systems, a smart contract will execute an agreed-upon process once a certain event takes place. For example, once a company receives the proper amount of money, a product will automatically be shipped. The aspect of additionality, however, lies in the fact that for the first time ever, software is holding the money, value and information—hence, the smart contract is programmed to do something with these assets without an intermediary, like a bank, stepping in.[223] For example, inheriting money will be much easier than entrusting money to an Escrow account. Rather than confiding in a bank or spending money on lawyers to ensure that someone's Will is carried out properly, one could use a smart contract to automatically distribute each portion of the allocated funds to the beneficiaries—including the taxes owed to the government as well as pay for the funeral. In this instance, the event that would trigger the smart contract is the contract owner's death, and that condition can be determined by a certain coded preset—for example, the person would have to log in to the system once every year, otherwise the funds will be distributed.

[222] Jayanand Sagar, 'Confideal: Smart Contracts Made Simple' (*News BTC*, 2017) <https://www.newsbtc.com/2017/10/23/confideal-smart-contracts-made-simple/> accessed 28 May 2019.

[223] Ivan on Tech, 'Difference between DAPPS and Smart Contracts? Programmer explains' (9 March 2018) <https://www.youtube.com/watch?v=4rczD8xKPJc> accessed 27 May 2019.

Conceptually, users can be confidant that smart contracts will do what they are programmed to do, and there is no need to trust a company, government authority, or any person to fulfill the contractual terms if all conditions are met.[224] Since it is impossible to alter information on the blockchain, any updates to the contract would also be logged, but tampering with the contract is nearly impossible.[225] Smart contracts are typically built into decentralized applications, which are programs that allow for the public to use blockchain more easily.

5.2 What is a decentralized application?

A decentralized application (DApp) looks similar to any other downloadable application for a phone or computer and is the entire architecture or infrastructure that makes smart contracts accessible on the blockchain. A DApp typically houses multiple smart contracts, all with specific functions, in order for the app to work. More often than not, the application takes a simpler form (on a server or interface) in order for people to interact with the smart contract in a user-friendly manner. Once a DApp is created, it will be forever on the blockchain for everyone to use and there is no centralized body that, when compromised, could lead to its dismantling.[226]

Take fundraising for example: a video journalist is looking for crowdsourced support in order to make a documentary about children living in prisons around the world, and for each donation of over $100 USD, the donor will receive a copy of the final product. Today, the journalist would most likely use the Internet-based platform called Kickstarter, which is the third-party operator that sits between the journalist and their supporters, collecting donations from people that believe in the importance of the story. The journalist can set a minimum fundraising goal, and once that goal is achieved, Kickstarter will close the crowdsourcing campaign and send the money to the journalist. However, there is no guarantee that the journalist will follow through with the project or distribute the completed product.[227] Kickstarter is also not the most trusted platform since its hacking in 2017, exposing the account information and passwords of nearly 14.5 million people.[228] In online exchanges, there is a great need for both users and donors to trust that their information will remain private and the fundraised money will be used properly.

[224] Smart contracts are programmed in a language called Solidity, which was specifically created by the Ethereum blockchain developers and is similar to the syntactical formatting of Javascript.Simply Explained - Savjee, 'Smart contracts - Simply Explained' (20 November 2017) <https://www.youtube.com/watch?v=ZE2HxTmxfrI&list=PLX_38LSoURa9lUR2VvacK763AWSQoA7hP> accessed 27 May 2019.

[225] Tapscott and Tapscott (n. 101) 47-48.

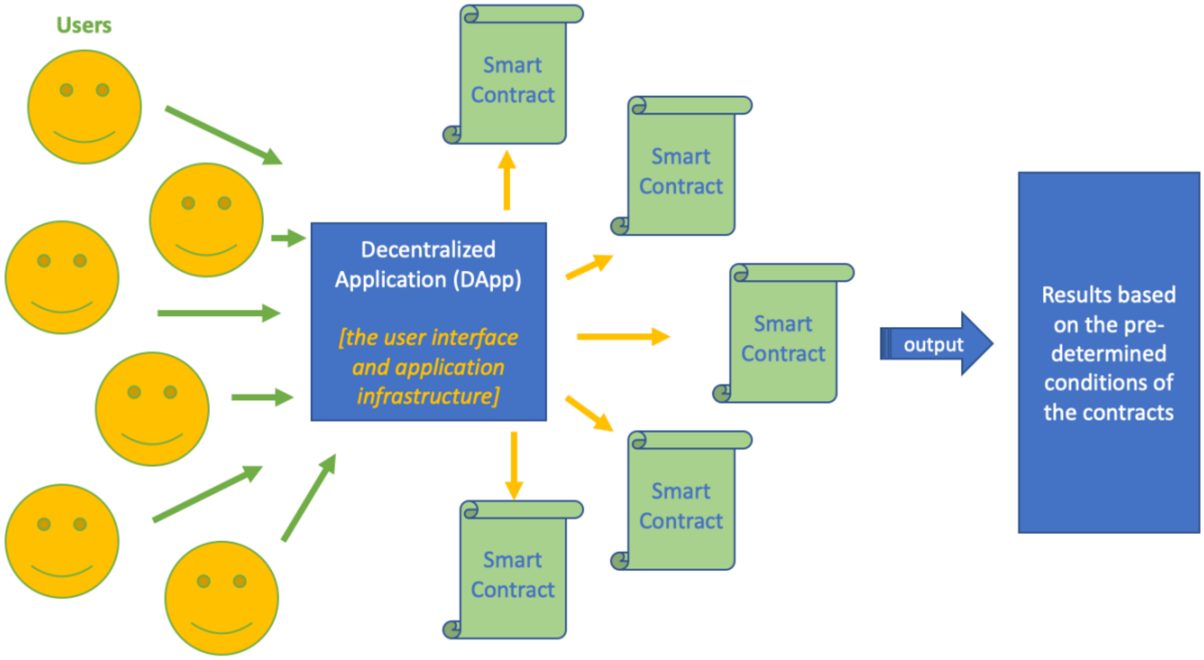
[226] Siraj Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology* (O´Reilly 2016) 10.

[227] There was the case of distrust in 2016 with the Kickstarter-funded minidrone Zano. The product developers raised $3.5 million USD and promised that once their drones were created, each contributor above a certain pricemark would receive a drone, yet the company had misled the public concerning their technological developments, claimed bankruptcy and never returned any of the money to the donors—even though the product was never created. Mark Harris, 'How Zano Raised Millions on Kickstarter and Left Most Backers with Nothing' (*Medium*, 28 January 2016) <https://medium.com/kickstarter/how-zano-raised-millions-on-kickstarter-and-left-backers-with-nearly-nothing-85c0abe4a6cb> accessed 28 May 2019.

[228] Nick Douglas, 'Info From 15 Million Breached Kickstarter and Bitly Accounts Is Now Publicly Available [Updated]' (*Lifehacker*, 10 June 2017) <https://lifehacker.com/15-million-hacked-kickstarter-and-bitly-passwords-are-n-1819216049> accessed 28 May 2019.

On the other hand, Lighthouse.cash is a DApp that eliminates the need for a third party such as Kickstarter, with the donations transferring directly from the supporters to the project's smart contract.[229] Lighthouse.cash fulfils the same objective as the Kickstarter model, except all conditions are logged in smart contracts to ensure validity of the initiative in addition to the donor receiving everything they are promised in return. Lighthouse.cash has no access or control over the money that is exchanged, or the users' information. There are multiple conditions built within a smart contract—i.e. once the fundraising goal is reached, the money is transferred to the journalist; if the goal is not reached the money is redistributed back to the donors; all those that donate over $100 USD are contractually obliged to receive a copy of the final product or their money is returned; the project must be finished within two years or the money is redistributed back to the donors, etc.—and the transactions would be registered and executed automatically. The DApp can host multiple smart contracts from multiple fundraising projects.

Figure 14: Model of how users interact with DApps


Users
Smart Contract
Smart Contract
Decentralized Application (DApp)
[the user interface and application infrastructure]
Smart Contract
output
Results based on the pre-determined conditions of the contracts
Smart Contract
Smart Contract

Source: Own elaboration based on districtOx's "Understanding Ethereum" course[230]

5.3 How can smart contracts be applied to fighting impunity for crimes committed against journalists?

> "Each year, one journalist gets a Pulitzer and one hundred get shot."
> - UNESCO's #TruthNeverDies campaign[231]

[229] Jamie Redman, 'Decentralized Crowdfunding Platform Lighthouse.cash Launches' (Bitcoin.com, 5 July 2018) <https://news.bitcoin.com/decentralized-crowdfunding-platform-lighthouse-cash-launches/> accessed 27 May 2019.

[230] district0x Educational Portal, 'Understanding dApps' (2018) <https://education.district0x.io/general-topics/understanding-ethereum/understanding-dapps/> accessed 27 May 2019.

[231] UNESCO, '#TruthNeverDies: Journalists are killed everyday to silence the truth. Share their stories to Keep them alive? (*Exposure*, 26 October 2018) <https://unesco.exposure.co/truth-never-dies> accessed 27 May 2019.

In regards to the most severe crimes against journalists, kidnapping or murder, the following rights are at risk: the right to life, freedom from torture, freedom of expression, and right to an effective remedy. These rights are enshrined in multiple human rights instruments, but the problem is not a lack of recognition of rights, it is a failure of States to uphold their positive obligation to protect the press. More often than not, the lack of prosecution for crimes committed against journalists is due to a lack of evidence, coupled with a lack of political will to investigate.[232] According the Council of Europe's 2019 *Democracy at Risk* report, the lack of proper police and judicial follow-up to crimes committed against journalists has allowed for violence to become the "new normal."[233] Even in regards to some of the most conspicuous cases of journalists' assassinations, law enforcement officials neglect their responsibility to follow leads, interview witnesses, or collect evidence.[234] The Maguindanao massacre victims of the Philippines,[235] Anna Politkovskaya of Russia,[236] Lasantha Wickramatunge of Sri Lanka,[237] Samir Qassir[238] and Gebran Tueni[239] of Lebanon, Armando Rodríguez of Mexico,[240] Soran Mama Hama of Iraq,[241] Deyda Hydara of Gambia,[242] Hayatullah Khan of Pakistan,[243] Elmar Huseynov of Azerbaijan,[244] and Norbert Zongo of Burkina Faso,[245] are all famously impactful journalists that were killed over a decade ago, but there has yet to be a single conviction in any of these cases.

As stated in a policy research and advocacy project from the Centre for Law, Justice and Journalism at City University London, and the Centre for Freedom of the Media at the University of Sheffield, the only effective mechanism the UN provides for journalists and their families to seek justice is the Human Rights Committee's quasi-judicial individual communications

[232] Article 19, 'Ending impunity for crimes against journalists' (2 November 2018) <https://www.article19.org/resources/ending-impunity-for-crimes-against-journalists/> accessed 2 July 2019.

[233] Partner Organisations to the Council of Europe Platform to Promote the Protection of Journalism and Safety of Journalists, 'Democracy at Risk: Threats and Attacks Against Media Freedom in Europe' (*Council of Europe*, 2019) <https://rm.coe.int/annual-report-2018-democracy-in-danger-threats-and-attacks-media-freed/1680926453> accessed 2 June 2019.

[234] CPJ, 'CPJ challenges authorities in 10 nations to bring justice and reverse culture of impunity' (29 April 2010) <https://cpj.org/reports/2010/04/ten-journalist-murders-to-solve.php> accessed 28 May 2019.

[235] Ellen T. Tordesillas, 'OPINION: Lila Shahani, Maguindanao massacre and impunity' (*ABS CBN News*, 26 November 2018) <https://news.abs-cbn.com/blogs/opinions/11/26/18/opinion-lila-shahani-maguindanao-massacre-and-impunity> accessed 31 May 2019.

[236] Deniz Yazici, 'Impunity for crimes against journalists in Russia is serious threat to media freedom, OSCE Representative says on anniversary of Anna Politkovskaya's killing' (*OSCE*, 7 October 2017) <https://www.osce.org/fom/348441> accessed 31 May 2019.

[237] CPJ, 'Civil case filed in US over murder of Sri Lankan journalist Lasantha Wickramatunga' (15 April 2019) <https://cpj.org/2019/04/civil-case-filed-in-us-over-murder-of-sri-lankan-j.php> accessed 31 May 2019.

[238] CPJ, 'Samir Qassir' <https://cpj.org/data/people/samir-qassir/> accessed 2 June 2019.

[239] CPJ, 'Gebran Tueni' <https://cpj.org/data/people/gebran-tueni/index.php> accessed 2 June 2019.

[240] CPJ, 'José Armando Rodríguez <https://cpj.org/data/people/armando-rodriguez/> accessed 31 May 2019.

[241] CPJ, 'Soran Mama <https://cpj.org/data/people/soran-mama-hama/> accessed 2 June 2019.

[242] Foroyaa, 'Who Killed Deyda Hydara?' (1 December 2018) <http://foroyaa.gm/who-killed-deyda-hydara/> accessed 2 June 2019.

[243] CPJ, 'Hayatullah Khan' <https://cpj.org/data/people/hayatullah-khan/> accessed 2 June 2019.

[244] Institute for Reporters' Freedom and Safety, 'Call to Combat Impunity on the 13th Anniversary of Journalist Elmar Huseynov Murder' (3 March 2018) <https://www.irfs.org/news-feed/call-to-combat-impunity-on-the-13th-anniversary-of-journalist-elmar-huseynov-murder/> accessed 2 June 2019.

[245] CPJ, 'Norbert Zongo' <https://cpj.org/data/people/norbert-zongo/> accessed 2 June 2019.

procedure.[246] However, considering its jurisdictional restrictions and non-binding nature, the effectiveness of the procedure is highly limited. UNESCO's International Programme for the Development of Communication is a similar mechanism,[247] but its sole focus is on journalist assassinations, excluding all other forms of violence and threats. The researchers from City University London and the University of Sheffield suggest that the most valuable action to take would be the adoption of a global and binding convention, alongside an ad hoc body of independent experts tasked with monitoring State compliance of the convention—with a streamlined complaints procedure. On the same page, however, they admit that while the need for a convention is urgent, "the legal inertia of the international community is likely to perpetuate the status quo."[248] Thus, the disruptive nature of technology as a part of the solution is two-fold: to break through political gridlock and begin to break-ground on new ways to execute protection mechanisms.

One of the main advantages to blockchain is its ability to securely maintain a complex system of records and through both hashing and smart contracts, the human rights community could ensure submission of evidence needed to prosecute crimes against journalists as verified records to a judicial body. Once a certain, predetermined condition is met (a journalist disappears for X number of days, a journalist is verifiably kidnapped, a journalist is murdered), an automated reaction occurs in the blockchain's programming, sending the journalist's information to the appropriate and trusted institutions. UN General Assembly Resolution A/RES/68/163[249] reinforces the UN Plan of Action on the Safety of Journalists and the Issue of Impunity, which states that: "Promoting the safety of journalists and fighting impunity must not be constrained to after-the-fact action. Instead, it requires prevention mechanisms and actions to address the root causes of violence against journalists and impunity for its perpetrators." While smart contracts appear to be an "after-the-fact" solution at the surface, the act of logging information in a blockchain-based platform and setting up an automated contract for disseminating that information in the event of an emergency would be a proactive measure for combating impunity. The same logic behind purchasing an insurance plan applies to pre-programing a smart contract: it is a more protection-oriented way of managing risks.

A DApp focused on streamlining judicial processes for crimes committed against journalists could be created to manage the smart contracts of journalists all around the globe. To further elaborate on how the DApp would work, its primary function would be to act as a single point of access for journalists to house all of their valuable research-oriented information—it could combine the potential of applications such as Storj and OpenArchive, Umbrella's incident reporting, and even Panic Button's geolocation capabilities. In the event of a journalist's death, the decryption key for access to the information stored on the application would automatically, by way of a smart contract, go to a trusted contact or institution. All of the information that had been

[246] CLJJ and CFOM, 'The Initiative on Impunity and the Rule of Law: A Policy Research and Advocacy Project of the Centre for Law, Justice and Journalism (CLJJ) at City University London, and the Centre for Freedom of the Media (CFOM) at the University of Sheffield' (2011) 11 <https://www.city.ac.uk/__data/assets/pdf_file/0017/106424/CLJJ-Impunity-Report.pdf> accessed 2 June 2019.

[247] UNESCO, 'International Programme for the Development of Communication' <https://en.unesco.org/programme/ipdc> accessed 23 June 2019.

[248] ibid.

[249] UN General Assembly, Resolution adopted by the General Assembly (18 December 2013) UN Doc A/RES/68/163 <http://undocs.org/A/RES/68/163> accessed 23 June 2019.

stored and hashed on the blockchain throughout the investigative process would then be viable evidence from the victim as a primary source[250]—potentially including the journalists' notes, agenda, transcripts, photos, video interviews, GPS location at the time of disappearance, previous incident reports, etc.—in an effort to resolve the case and seek justice.

Not only would prosecutors have greater access to evidence, but a murdered journalist's work could be given new life through the eyes of a fellow journalist. Due to the nature of their work, journalists are typically more isolated and secretive about the stories they develop. Protecting oneself and protecting sources requires that reporters conduct their research in a more covert manner, which inadvertently positions journalists as central to all of the auxiliary components of an investigative piece. In fact, most journalists are assassinated based on the logic that if the journalist dies, then the story dies with them—but giving a story life after death would nullify this motive. If journalists utilize a smart contract—in the form of a journalistic Will, so to speak—to automatically transfer their research to a colleague as their beneficiary, the investigation and the story can be seamlessly 'picked-up' by a fellow reporter. In fact, if this mechanism is known to assailants, it may even reduce the rate of kidnappings and assassinations; if criminals are aware that all documents related to the journalists' investigations will be released, there is less of an incentive to kill a journalist.

5.5 Conclusions

In theory, utilizing smart contracts could victual what are otherwise malnourished protection mechanisms. These programs could also be beneficial to human rights defenders from a variety of backgrounds and of any nationality. However, in practice, blockchain continues to be an expensive technology and most, if not all, blockchains are not powered sustainably. If journalists were to utilize these applications, they would need to be more cost-effective or subsidized by a sponsoring institution. Similarly, those developing these applications would need to ensure that the interface is as user-friendly as possible, in order for the tech to seamlessly integrate into a journalist's workflow. If journalists do not use these applications, like with any technology, they will be essentially useless, which is why careful iteration in terms of design is critical. More research must be conducted concerning journalists' workflow preferences and apps must be designed with an intended daily use in mind. With all of the above considerations taken into account, this type of smart contract-based tool would take several years for development.

Conclusion

From a human rights perspective, more research should be conducted to measure blockchain's power in terms of credibility and accountability. For example, in theory, if police body-cam videos could be publicly ledgered in real-time, the data would register in a distributed network before it could be cut or altered. Voters could both register and cast their ballots in a secure and un-editable system, ensuring the validity of election outcomes. Blockchain could even amplify boycott and divestment movements through ledgers that refuse any transactions with a history of conflict, illicit funds trading or slavery. Initiatives have even begun to use blockchain

[250] One of blockchain's principal functionalities is verifying a file's originality by hashing it permanently into existence, which is critically important when trying to classify something as tamper-free evidence.

for systematizing digital identity, nullifying the need for a State to instill personhood via a birth certificate—which would grant equal opportunity to the millions unrecognized by their governments around the world.[251] Specifically in terms of journalism, blockchain would not only work to provide journalists with a more dignified wage, better ensure that citizens are able to exercise their right to access information, improve government transparency, and promote freedom of expression, but protecting journalists themselves should be the issue at the center of its investment and innovation.

Admittedly, many have discredited implementing blockchain-based applications as a techno-solutionist reaction to problems that society cannot overly rely on computers to solve. At present, this argument generally holds true, considering blockchain's inefficiencies in relation to excessive energy use, cost and processing time. For blockchain to live up to the high standards theorists and optimists have set, it will take at least a few more decades for the technology to grow into its potential. However, theorizing possible applications for how the technology can better serve the human rights community in anticipation of blockchain's maturity allows for a proactive debate that keeps academia aware of the possibilities and problems that lie ahead. Nelson Granados, a tech-journalist from *Forbes Magazine* explains, "The hype will settle, the technology will mature, and the true applications [of blockchain] will emerge." [252] As argued in this paper, blockchain is, in fact, only necessary for three key functions: the verification of information via hashing, avoiding single points of failure through decentralization, and transparency of data flow. Applying these uses to better protect journalists and their work is achieved through blockchain's ability to securely store information related to journalistic investigations through decentralization techniques, to log a journalist's working information as tamper free evidence, and to improve upon the secure tracking of journalists working in dangerous environments.

In the same way that businesses and governments are beginning to take advantage of blockchain's capabilities, journalists and, more broadly, those working in human rights should strategize about how to reap benefits from the costly trial investments that are already taking place in other industries. Telecommunications companies have begun to use secure file storage for documents and media. Logistics companies are working to perfect blockchain-based checkpoint verification. The National Aeronautics and Space Administration (NASA) now logs and shares cyber-security incidents on the blockchain.[253] The successes of these applications are beginning to tangibly justify the theoretical arguments for how blockchain could protect journalists—both digitally and physically—while conducting investigative work in the field. With an interdisciplinary approach, there is no need to start building these initiatives from scratch. Human rights defenders, defending freedom of speech or otherwise, need technologists as allies in today's digital age.

Arguably the most valuable application of blockchain is the programming of smart contracts, which creates an automated and direct flow of critical information in the event of an

[251] Accenture, Microsoft, Gavi and the Rockefeller Foundation have been working with the United Nations to create the non-profit organization ID2020, created in alignment with SDG 16.9 for the purpose of using blockchain to provide "legal identity for all including free birth registrations." Axiom Technologies (n. 139).
[252] Granados (n.120).
[253] Ronald J. Reisman, 'Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy' (*NASA*, 2019) 1-11 <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190000022.pdf> accessed 25 June 2019.

emergency. Creating a more secure GPS-tracking system in the event of a disappearance or establishing an automated journalistic 'Will' in case of death could not only provide safety-nets for journalists but also, potentially, disincentivize their capture. Preparing for the worst-case scenario is considered best-practice for field practitioners in human rights, and journalists, too, need updated contingency plans in light of increased rates of disappearances and assassinations. Furthermore, the proactive nature of smart contracts could systematize a more effective procedure that reduces the rates of impunity for crimes committed against journalists—by granting human rights prosecutors and courts the additional raw evidence necessary for solving said crimes.

Human rights institutions and organizations, including academia, should place greater emphasis on properly analyzing if, and when, technological tools are useful for giving life to their respective mission statements. The UN Plan of Action on the Safety of Journalists and the Issue of Impunity, for instance, does not mention technology even once, completely neglecting its existence or potential. Technological tools have proven to be invaluable for freedom of expression, and there are many recent historical examples of how technology has provided critical channels of communication while citizens fight for their rights. Universities should remain up-to-date with technological developments, as they are responsible for preparing future generations of human rights defenders and should be arming their students with the most relevant and powerful tools at their disposal.

While we tend to hold novel technologies to an unrealistically high standard, aspirations of building a system—one that better protects human lives and allows for a more streamlined judicial process—are in-fact worth the patience of a sustainability-focused iteration process. Such a tool would surely not eradicate the problem, nor would it function perfectly in all cases, but even testing a minimum viable product is a step in the right direction towards saving individual lives and granting the issue of heightened violence against journalists its warranted urgency. Ideally, these investments would be coupled with better funded, robust, national and international safety mechanisms for journalists which, in turn, establish better human-based security guarantees such as a trusted police force, rapid response assistance, and the political will to resolve crimes and punish perpetrators. A multilateral approach is the only approach worth pursuing, and technology can assuredly be a valuable part of the solution if used properly.

Vadym Komarov. Norma Sarabia Garduza. Francisco Romero Díaz. Ahmed Hussein-Suale Divela. Raed Fares. Hamoud al-Jnaid. Chandan Tiwari. Sohail Khan. These are just a few of the many journalists that have been murdered within the past year. Since the Committee to Protect Journalists (CPJ) began monitoring violence against journalists in 1992, 1,345 members of the media have been killed to date.[254] The old 'sticks and stones' adage claiming that words will never hurt is disproven by their shared fate. Journalists are being assassinated for their words, and it is everyone's responsibility to introspectively reflect on how they can actively be a part of the solution. Digital dexterity and tech-based shields should be standardized, if not required, armor for those battling corruption, disinformation, injustice and hate, but as a society we should be doing more to fight for justice and protection for journalists. After all, the Fourth Estate is fighting on behalf of the 'we the people'.

[254] ibid 34.

BIBLIOGRAPHY

BOOKS

Greenberg A, *This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World's Information* (Kindle edn, Dutton 2012)

Lamer W, *Press Freedom as an International Human Right* (Kindle edn, Palgrave Pivot 2018)

McChesney R and Nicols J, *The Death and Life of American Journalism: The Media Revolution that Will Begin the World Again* (Nation Books 2010)

Rather D, and Kirschner E, *What Unites Us: Reflections on Patriotism* (Kindle edn, Algonquin Books of Chapel Hill 2017)

Raval S, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology* (O´Reilly 2016)

Sims C, *Disruptive Fixation: School Reform and the Pitfalls of Techno-Idealism* (Princeton University Press, 2017)

Tapscott D and Tapscott A, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (2nd edn, Kindle edn, Portfolio/ Penguin 2018)

BOOK CHAPTERS

Picard RG, 'A Business Perspective on Challenges Facing Journalism' in David A. L. Levy and Rasmus Kleis Nielsen (eds), 'The Changing Business of Journalism and its Implications for Democracy' (*Reuters Institute for the Study of Journalism,* 2010) <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/The%2520Changing%2520Business%2520of%2520Journalism%2520and%2520its%2520Implications%2520for%2520Democracy.pdf#page=23> accessed 19 May 2019

Williams L, 'Censors: At work, censors out of work' in Louise Williams and Roland Rich (eds), *Losing Control: Freedom of the Press in Asia* (ANU Press 2013) <https://www.jstor.org/stable/j.ctt5vj71c.5> accessed 16 May 2019

OFFICIAL DOCUMENTS

OHCHR, Safety of journalists: Report of the United Nations High Commissioner for Human Rights (10–28 September 2018) A/HRC/39/23 <https://www.ohchr.org/Documents/Issues/Journalists/A_HRC_39_23_EN.docx> accessed 13 May 2019

UN General Assembly, Resolution adopted by the General Assembly (18 December 2013) UN Doc A/RES/68/163 <http://undocs.org/A/RES/68/163> accessed 23 June 2019UNESCO, 'UN Plan of Action on the Safety of Journalists and the Issue of Impunity' (2016) <https://en.unesco.org/un-plan-action-safety-journalists> accessed 16 May 2019

REPORTS

CLJJ and CFOM, 'The Initiative on Impunity and the Rule of Law: A Policy Research and Advocacy Project of the Centre for Law, Justice and Journalism (CLJJ) at City University London, and the Centre for Freedom of the Media (CFOM) at the University of Sheffield' (2011) <https://www.city.ac.uk/__data/assets/pdf_file/0017/106424/CLJJ-Impunity-Report.pdf> accessed 2 June 2019

Freedom House, 'Freedom of the Press 2017: Press Freedom's Dark Horizon' (2017) <https://freedomhouse.org/report/freedom-press/freedom-press-2017> accessed 15 May 2019

Garza Ramos J, 'Journalist Security in the Digital World: A Survey Are We Using the Right Tools?' (*CIMA*, March 2016) 3 <https://www.cima.ned.org/resource/journalist-security-in-the-digital-world/> accessed 18 May 2019

Google, 'Transparency Report: Government requests to remove content' <https://transparencyreport.google.com/government-removals/overview?hl=en&removal_requests=group_by:totals;period:&lu=removal_requests> accessed 25 June 2019

International Programme for the Development of Communication, '2018 DG Report on the Safety of Journalists and the Danger of Impunity'(UNESCO, 2018) CI-18/COUNCIL-31/6 REV.2 <https://unesdoc.unesco.org/ark:/48223/pf0000265828> accessed 15 May 2019

Partner Organisations to the Council of Europe Platform to Promote the Protection of Journalism and Safety of Journalists, 'Democracy at Risk: Threats and Attacks Against Media Freedom in Europe' (*Council of Europe,* 2019) <https://rm.coe.int/annual-report-2018-democracy-in-danger-threats-and-attacks-media-freed/1680926453> accessed 2 June 2019

Reisman RJ, 'Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy' (*NASA*, 2019) <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190000022.pdf> accessed 25 June 2019

RSF, '2019 World Press Freedom Index – A cycle of fear' (2019) <https://rsf.org/en/2019-world-press-freedom-index-cycle-fear> accessed 16 May 2019

– – 'Worldwide round-up of journalists killed, detained, held hostage, or missing in 2018' (2019) <https://rsf.org/sites/default/files/worldwilde_round-up.pdf> Accessed 13 May 2019

Witchel E, 'Getting Away with Murder' (*CPJ*, 2018) <https://cpj.org/reports/2018/10/impunity-index-getting-away-with-murder-killed-justice.php> accessed 13 May 2019

JOURNAL ARTICLES

De Vries A, ‘Bitcoin's Growing Energy Problem’ (2018) 2(5) Joule <DOI:https://doi.org/10.1016/j.joule.2018.04.016> accessed 20 July 2019

Langvardt K, ‘The Doctrinal Toll of "Information as Speech"’ (2015) 47 Loyola University Chicago Law Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2674634> accessed 26 May 2019

Massey BL and Elmore C, ‘Freelancing in Journalism’ (*Oxford Research Encyclopedias*, June 2018) <DOI: 10.1093/acrefore/9780190228613.013.818> accessed 16 May 2019

McDonagh M, ‘The Right to Information in International Human Rights Law’ (March 2013) 13(1) Human Rights Law Review <doi:10.1093/hrlr/ngs045> accessed 13 May 2019

Teachout Z, ‘The Anti-Corruption Principle’ (2009) 94 (2) Cornell Law Review <https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=3123&context=clr> accessed 23 May 2019

Voorhoof D, and others and McGonagle T, (Ed. Sup.), Freedom of Expression, the Media and Journalists: Case-law of the European Court of Human Rights (2017) IRIS Themes 3, *European Audiovisual Observatory* <https://rm.coe.int/freedom-of-expression-the-media-and-journalists-iris-themes-vol-iii-de/16807c1181> accessed 24 May 2019

NEWSPAPER ARTICLES

Ahmed A, ‘Mexico to Investigate Spying Campaign Against Journalists and Activists’ *New York Times* (Mexico City 21 June 2017) <https://www.nytimes.com/2017/06/21/world/americas/mexico-pena-nieto-spying-hacking-surveillance.html> accessed 13 May 2019

Ahmed A and Perlroth N, ‘Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families’ *New York Times* (Mexico City 19 June 2017) <https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html?module=inline> accessed 14 May 2019

Ball J, ‘GCHQ captured emails of journalists from top international media’ *The Guardian* (London 19 January 2015) <http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post> accessed 15 May 2019

Mohdin A and van der Zee B, ‘'Killed for speaking the truth': tributes to nine journalists murdered in 2018’ *The Guardian* (London, 5 December 2018) <https://www.theguardian.com/media/2018/dec/05/journalists-murdered-khashoggi-kuciak-panama-papers> accessed 13 May 2019

Pastrana D, ‘Protection of Journalists Fails in Latin America’ *IPS* (Mexico City 29 April 2017) <http://www.ipsnews.net/2017/04/protection-of-journalists-fails-in-latin-america/> accessed 16 May 2019

Peiser J, ‘Goodbye, Denver Post. Hello, Blockchain’ *New York Times* (17 June 2018) <https://www.nytimes.com/2018/06/17/business/media/denver-post-blockchain-colorado-sun.html> accessed 24 May 2019

Perlroth N and Bergman R, ‘WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer’s Phone’ *New York Times* (San Francisco 13 May 2019) <https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html> accessed 13 May 2019

Savage C and Kaufman L, ‘Phone Records of Journalists Seized by U.S.’ *New York Times* (Washington 13 May 2013) <http://www.nytimes.com/2013/05/14/us/phone-records-of-journalists-of-the-associated-press-seized-by-us.html> accessed 15 May 2019

Shane S, ‘When Spies Hack Journalism’ *New York Times* (Washington 12 May 2018) <https://www.nytimes.com/2018/05/12/sunday-review/when-spies-hack-journalism.html> accessed 15 May 2019

INTERNET SOURCES

4IRE labs, ‘How Much Does It Cost to Hire a Blockchain Developer?’ (2018) <https://4irelabs.com/how_much_does_it_cost_to_hire_blockchain_developer> accessed 23 June 2019

Al Jazeera, ‘Number of journalists killed on the job in 2018 rises’ (30 December 2018) <https://www.aljazeera.com/news/2018/12/number-journalists-killed-job-2018-rises-181231021858196.html> accessed 13 May 2019

Armit, ‘Confused by Blockchain Technology? No worries. Let’s talk about it!’ (*Medium*, 24 March 2018) <https://medium.com/@amrit_sharma/confused-by-blockchain-technology-no-worries-lets-talk-about-it-8e444637e46d> accessed 25 May 2019

Article 19, ‘Acting on UN Human Rights Council Resolution 33/2 on the Safety of Journalists’ (2017) <https://www.article19.org/wp-content/uploads/2018/02/safety_of_journalists_WEB_23.10.pdf> accessed 12 May 2019

Article 19, ‘Ending impunity for crimes against journalists’ (2 November 2018) <https://www.article19.org/resources/ending-impunity-for-crimes-against-journalists/> accessed 2 July 2019

Article 19, ‘UN must translate words into action on journalists’ safety’ (20 September 2018) <https://www.article19.org/resources/un-must-translate-words-into-action-on-journalists-safety/> accessed 13 May 2019

Avle S. Li D. and Lindtner S, ‘Responsible IoT after techno-solutionism’ (*Medium*, 27 August 2018) <https://medium.com/the-state-of-responsible-iot-2018/responsible-iot-after-techno-solutionism-cf583e5f9b9a> accessed 20 June 2019

Axiom Technologies, ‘A Reasonably Comprehensive Outline of Blockchain in the United Nations’ (1 March 2019) <https://www.axiomtech.io/blog-feed/2019/3/1/blockchain-in-the-united-nations> accessed 17 May 2019

Barzilay O, ‘How Blockchain Is Reinventing Your News Feed’ (*Forbes*, 28 August 2017) <https://www.forbes.com/sites/omribarzilay/2017/08/28/how-blockchain-is-reinventing-your-news-feed/#5217e5777bf4> accessed 25 May 2019

Baumgärtner M, Knobbe M and Schindler J, ‘Documents Indicate Germany Spied on Foreign Journalists’ (*Der Spiegel*, 24 February 2017) <https://www.spiegel.de/international/germany/german-intelligence-spied-on-foreign-journalists-for-years-a-1136188.html> accessed 15 May 2019

Baydakova A, ‘The New York Times Is Planning to Experiment With Blockchain Publishing’ (*CoinDesk*, 13 March 2019) <https://www.coindesk.com/the-new-york-times-is-planning-to-experiment-with-blockchain-publishing> accessed 19 May 2019

Bhandari E and Handeyside H, ‘The Government Is Detaining and Interrogating Journalists and Advocates at the US-Mexico Border’ (*ACLU*, 7 March 2019) <https://www.aclu.org/blog/free-speech/freedom-press/government-detaining-and-interrogating-journalists-and-advocates-us> accessed 16 May 2019

Biehl Z, ‘6 Ways Blockchain Is Radically Improving Global Human Rights’ (*Invest in Blockchain*, 2 April 2018) <https://www.investinblockchain.com/blockchain-improving-human-rights/> accessed 20 May 2019

Bill of Rights Institute, ‘Freedom of the Press’ <https://billofrightsinstitute.org/educate/educator-resources/landmark-cases/freedom-of-the-press/> accessed 23 May 2019

Biscevic T, ‘Mexico: Second Journalist Murder of 2019’ (*OCCRP*, 12 February 2019) <https://www.occrp.org/en/27-ccwatch/cc-watch-briefs/9226-mexico-second-journalist-murder-of-2019> accessed 16 May 2019

Blockchain, ‘Average Block Size: The average block size in MB’ (May 2019) <https://www.blockchain.com/charts/avg-block-size> accessed 19 May 2019

Blockchain Commission for Sustainable Development [Linkedin] <https://www.linkedin.com/company/blockchain-commission/about/> accessed 17 May 2019

Blockchain for Impact <https://www.blockchainforimpact.org/> accessed 26 May 2019

Blockchain Hub, ‘Blockchains & Distributed Ledger Technologies’ <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/> accessed 21 May 2019

Boddy M, ‘Starbucks Working With Microsoft for Blockchain-Based Coffee Tracking Platform’ (*Cointelegraph*, 6 May 2019) <https://cointelegraph.com/news/starbucks-working-with-microsoft-for-blockchain-based-coffee-tracking-platform> accessed 18 May 2019

Buchko S, ‘Mainframe’s Mick Hagen on the Importance of Censorship Resistance and Charitable Endeavors [PART 1]’ (*Coin Central*, 21 May 2018) <https://coincentral.com/mainframe-mick-hagen-interview-part-1/> accessed 27 May 2019

Buterin V and Ravikant N, ‘Decentralizing Everything with Ethereum's Vitalik Buterin | Disrupt SF 2017’ (*TechCrunch*, 18 September 2017) <https://www.youtube.com/watch?v=WSN5BaCzsbo> accessed 19 May 2019

Canadian Journalists for Free Expression**,** ‘Journalists in Distress: Securing your Digital Life’ <https://www.cjfe.org/journalists_in_distress_securing_your_digital_life> accessed 17 May 2019

Career Cast, ‘The Worst Jobs of 2015’ <https://www.careercast.com/jobs-rated/worst-jobs-2015> accessed 19 May 2019

Civil <https://civil.co/> accessed 22 May 2019

– – ‘The Civil white paper’ <https://civil.co/white-paper/> accessed 24 May 2019

Comben C, ‘How Blockchain Is Being Applied to Human Rights’ (*Coin Central*, 5 September 2018) <https://coincentral.com/blockchain-and-human-rights/> accessed 18 May 2019

Conger K,‘WhatsApp blocked in Brazil again’ (*TechCrunch*, 2016) <https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/> accessed 27 May 2019

Constine J, ‘Facebook announces Libra cryptocurrency: All you need to know: The use cases, technology and motive behind the new digital money (*TechCrunch*, 17 June 2019) <https://techcrunch.com/2019/06/18/facebook-libra/ > accessed 21 June 2019

Cosset D, ‘Blockchain: what is in a block?’ (*DEV*, 27 December 2017) <https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo> accessed 21 May 2019

CPJ, ‘Civil case filed in US over murder of Sri Lankan journalist Lasantha Wickramatunga’ (15 April 2019) <https://cpj.org/2019/04/civil-case-filed-in-us-over-murder-of-sri-lankan-j.php> accessed 31 May 2019

– – ‘CPJ challenges authorities in 10 nations to bring justice and reverse culture of impunity’ (29 April 2010) <https://cpj.org/reports/2010/04/ten-journalist-murders-to-solve.php> accessed 28 May 2019

– – ‘Gebran Tueni’ <https://cpj.org/data/people/gebran-tueni/index.php> accessed 2 June 2019

– – ‘Greek CNN reporter Mina Karamitrou's car destroyed by bomb’ (14 May 2019) <https://cpj.org/2019/05/greek-cnn-reporter-mina-karamitrous-car-destroyed-.php> accessed 16 May 2019

– – ‘Hayatullah Khan’ <https://cpj.org/data/people/hayatullah-khan/> accessed 2 June 2019

– – ‘José Armando Rodríguez <https://cpj.org/data/people/armando-rodriguez/> accessed 31 May 2019

– – ‘Norbert Zongo’ <https://cpj.org/data/people/norbert-zongo/> accessed 2 June 2019

– – ‘Rafael Murúa Manríquez’ (2019) <https://cpj.org/data/people/rafael-murua-manriquez/index.php> accessed 16 May 2019

– – ‘Samir Qassir’ <https://cpj.org/data/people/samir-qassir/> accessed 2 June 2019

– – ‘Soran Mama <https://cpj.org/data/people/soran-mama-hama/> accessed 2 June 2019

Daniel L, ‘The SABC is bankrupt, admits CEO Madoda Mxakwe’ (*The South African*, 31 October 2018) <https://www.thesouthafrican.com/news/sabc-bankrupt-confirmed-ceo-2018/> accessed 24 May 2019

Dart Center for Journalism & Trauma, ‘Freelance Journalist Safety Principles’ (12 February 2015) <https://dartcenter.org/content/global-safety-principles-and-practices> accessed 15 May 2019

Davies S, ‘How bitcoin and its blockchain work’ (*Financial Times,* 3 February 2015) <https://repository.gchumanrights.org/handle/20.500.11825/1013> accessed 17 May 2019

Dhameja G, ‘UN World Food Programme uses Parity Ethereum to aid 100,000 refugees’ (*Parity*, 18 February 2019) <https://www.parity.io/un-world-food-programme-uses-parity-ethereum-to-aid-100-000-refugees/> accessed 19 May 2019

Digiconomist, ‘Bitcoin Energy Consumption Index’ (June 2019) <https://digiconomist.net/bitcoin-energy-consumption> accessed 12 June 2019

district0x Educational Portal, ‘Understanding dApps’ (2018) <https://education.district0x.io/general-topics/understanding-ethereum/understanding-dapps/> accessed 27 May 2019

Donna S, ‘White Paper: Data Continues to Drive Social Performance 2016’ (*SocialFlow*, 3 March 2017) <www.socialflow.com/resources-2/white-papers> accessed 24 May 2019

Douglas N, ‘Info From 15 Million Breached Kickstarter and Bitly Accounts Is Now Publicly Available [Updated]’ (*Lifehacker*, 10 June 2017) <https://lifehacker.com/15-million-hacked-kickstarter-and-bitly-passwords-are-n-1819216049> accessed 28 May 2019

Dragonchain, ‘Blockchain as a Service for Enterprises and Developers’ <https://dragonchain.com/> accessed 18 May 2019

EY, 'EY and Microsoft launch blockchain solution for content rights and royalties management for media and entertainment industry' (21 June 2018) <https://www.ey.com/en_gl/news/2018/06/ey-and-microsoft-launch-blockchain-solution-for-content-rights> accessed 18 May 2019

Flynn W, 'Uncensored Content on Ethereum: How Chinese Activists Inspired Civil' (*Medium,* 13 August 2018) <https://blog.joincivil.com/uncensored-content-on-ethereum-how-chinese-activists-inspired-civil-f09f095a9e91> accessed 21 May 2019

Foreign & Commonwealth Office '"I am placing the resources of @foreignoffice behind the cause of media freedom..."' [Twitter], 31 October 2018 <https://twitter.com/foreignoffice/status/1057723034331762688?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed&ref_url=http%3A%2F%2Ftheconversation.com%2Fdear-foreign-secretary-heres-how-to-protect-journalists-and-press-freedom-111128> accessed 23 June 2019

Foroyaa, 'Who Killed Deyda Hydara?' (1 December 2018) <http://foroyaa.gm/who-killed-deyda-hydara/> accessed 2 June 2019

Fortney L, 'Blockchain, Explained' (*Investopedia,* 21 May 2019) <https://www.investopedia.com/terms/b/blockchain.asp> accessed 22 May 2019

Frankenfield J, '51% Attack' (*Investopedia*, 6 May 2019) <https://www.investopedia.com/terms/1/51-attack.asp> accessed 21 May 2019)

– – 'Silk Road' (*Investopedia,* 26 October 2016) <https://www.investopedia.com/terms/s/silk-road.asp> accessed 20 May 2019

Freedom House, 'Violence against Journalists Is a Transnational Enterprise' (17 October 2018) <https://freedomhouse.org/blog/violence-against-journalists-transnational-enterprise> accessed 20 June 2019

Freitas N, 'proofmode' (*Why GitHub?*, 24 February 2017) <https://github.com/guardianproject/proofmode/blob/master/README.md> accessed 23 June 2019

Frontline Defenders, 'Digital Security Resources' <https://www.frontlinedefenders.org/en/digital-security-resources> accessed 23 June 2019

Gagliordi N,'How self-driving tractors, AI, and precision agriculture will save us from the impending food crisis' (*TechRepublic,* 12 December 2018)
<https://www.techrepublic.com/article/how-self-driving-tractors-ai-and-precision-agriculture-will-save-us-from-the-impending-food-crisis/> accessed 20 June 2019

Gallup and Knight Foundation, 'Indicators of News Media' (*Knight Foundation,* 11 September 2018) <https://www.knightfoundation.org/reports/indicators-of-news-media-trust> accessed 21 May 2019

Gillin P, 'North American metro dailies that have closed since this site was created in March, 2007' (*Newspaper Death Watch*) <http://newspaperdeathwatch.com> accessed 19 May 2019

Goldin M, Ameen Soleimani and James Young, 'The AdChain Registry' (*adChain,* 2017) <https://adtoken.com/white-paper.pdf> accessed 25 May 2019

Granados N, 'How Blockchain Is Making Waves In Media And Entertainment' (*Forbes,* 3 December 2018) <https://www.forbes.com/sites/nelsongranados/2018/12/03/how-blockchain-is-making-waves-in-media-and-entertainment/#44859b7d3f6c> accessed 21 June 2019

Greste P, 'The Case For A Media Freedom Act' (*Alliance for Journalists' Freedom*, 5 February 2019) <https://www.journalistsfreedom.com/case-for-media-freedom-act/> accessed 23 May 2019

Grieco E, Sumida N and Fedeli S, 'About a third of large U.S. newspapers have suffered layoffs since 2017' (*Pew Research Center,* 23 July 2018) <https://www.pewresearch.org/fact-tank/2018/07/23/about-a-third-of-large-u-s-newspapers-have-suffered-layoffs-since-2017/> accessed 2 July 2019

Haber S and Stornetta WS, 'How to Time-Stamp a Digital Document' (Bellcore) <https://www.anf.es/pdf/Haber_Stornetta.pdf> accessed 22 May 2019

Hagen M, 'Freedom of the Press Foundation & Mainframe' (*Medium*, 18 June 2018) <https://blog.mainframe.com/freedom-of-the-press-foundation-mainframe-6ffb39918503> accessed 26 May 2019

Harris M, 'How Zano Raised Millions on Kickstarter and Left Most Backers with Nothing' (*Medium*, 28 January 2016) <https://medium.com/kickstarter/how-zano-raised-millions-on-kickstarter-and-left-backers-with-nearly-nothing-85c0abe4a6cb> accessed 28 May 2019

Hartmann T, 'Ethereum (ETH) Price Analysis and Prediction 2019 – Market Takes A Nosedive And Takes ETH With It (June 4th Update)' (*Capital Coin,* 4 June 2019) <https://captainaltcoin.com/ethereum-eth-price-prediction-update-06-04-2019/> accessed 22 June 2019

Harvard Kennedy School Shorenstein Center on Media, Politics, '2019 Goldsmith Prize Finalists: Shorenstein Center Announces Seven Finalists for 2019 Goldsmith Prize for Investigative Reporting; Marty Baron to Receive Career Award' (6 February 2019) <https://shorensteincenter.org/2019-goldsmith-prize-finalists/> accessed May 23 2019

Hiltz R and Livesey B, 'Postmedia continues its downward spiral' (*Canada's National Observer*, 25 October 2018) <https://www.nationalobserver.com/2018/10/25/analysis/postmedia-continues-its-downward-spiral> accessed 24 May 2019

Horev R, 'Snip - December Update & 2018 Summary' (*Medium,* 3 January 2019) <https://medium.com/snip-news/snip-december-update-2018-summary-fb7bebdb89f2> accessed 25 May 2019

Institute for Reporters' Freedom and Safety, 'Call to Combat Impunity on the 13th Anniversary of Journalist Elmar Huseynov Murder' (3 March 2018) <https://www.irfs.org/news-feed/call-to-combat-impunity-on-the-13th-anniversary-of-journalist-elmar-huseynov-murder/> accessed 2 June 2019

International Center for Journalists, ''Salama' App Aims to Keep Journalists Safe?' (23 August 2015) <https://www.icfj.org/news/salama-app-aims-keep-journalists-safe> accessed 16 May 2019

International Consortium of Investigative Journalists, 'Panama Papers Helps Recover More Than $1.2 Billion Around The World' (2019) <https://www.icij.org/investigations/panama-papers/> accessed 23 May 2019

International Women's Media Foundation, 'Reporta™: Using Technology to Help Tackle Increasing Risks to Journalists' (19 February 2015) <https://www.iwmf.org/2015/02/reporta-using-technology-to-help-tackle-increasing-risks-to-journalists/> accessed 16 May 2019

Ivancsics B, 'Blockchain in Journalism' (*Tow Center for Digital Journalism,* 25 January 2019) <https://www.cjr.org/tow_center_reports/blockchain-in-journalism.php#blockchain> accessed 19 May 2019

Jackt, ‘Blockchain Development: A Complete Guide For Innovators’ (2019) <https://byjakt.com/blockchain-development-nyc-complete-guide/> accessed 23 June 2019

Jeff, ‘Bitcoin Mining Costs Throughout the World’ (*Elite Fixtures*, 26 February 2018) <https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/> accessed 20 May 2019

Levy G, ‘United Nations Expanding Blockchain Use to Help Syrian Refugees’ (*Bitsonline*, 8 May 2018) <https://bitsonline.com/united-nations-blockchain-refugees/ > accessed 17 May 2019

Loizos C, ‘Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it’ (*TechCrunch*, March 2019) <https://techcrunch.com/2019/03/07/voatz-the-blockchain-based-voting-app-gets-another-vote-of-confidence-as-denver-agrees-to-try-it/> accessed 20 June 2019

LyrnAI <https://www.lyrn.ai> accessed 22 May 2019

Mainframe OS <https://mainframeos.com/> accessed 27 May 2019

Marczak B and others, ‘Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries’ (*The Citizen Lab*, 18 September 2018) <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/> accessed 15 May 2019

Marthoz JP, ‘Spying on media exposes French government's dark side’ (*CPJ*, 3 September 2011) <https://cpj.org/blog/2011/09/spying-on-media-exposes-french-governments-dark-si.php> accessed 15 May 2019

Marx L, ‘Storing Data on the Blockchain: The Developers Guide’ (*Malcodad*, 5 July 2018) <https://malcoded.com/posts/storing-data-blockchain/> accessed 20 July 2019

Massad TG, ‘It’s Time to Strengthen the Regulation of Crypto-Assets’ (*Bookings*, 18 March 2019) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwix0PuU5KLiAhUNDmMBHR5lD4YQFjAAegQIABAC&url=https%3A%2F%2Fwww.brookings.edu%2Fwp-content%2Fuploads%2F2019%2F03%2FTimothy-Massad-Its-Time-to-Strengthen-the-Regulation-of-Crypto-Assets-2.pdf&usg=AOvVaw3_iGe88rOISfaqWOgaYTIt> accessed 21 May 2019

McGregor SE and others, ‘Investigating the Computer Security Practices and Needs of Journalists’ (USENIX 2015) 399 <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf> accessed May 14 2019

Mioli T, ‘One of the last English-language newspapers in Latin America, *The Buenos Aires Herald* to close after 140 years’ (*Knight Center for Journalism in the Americas,* 1 August 2017) <https://knightcenter.utexas.edu/blog/00-18659-one-last-english-language-newspapers-latin-america-buenos-aires-herald-close-after-140> accessed 24 May 2019

Nakamoto S, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (*Bitcoin*, 2018) <https://bitcoin.org/en/bitcoin-paper> accessed 21 May 2019

New York Times, ‘Lead, Blockchain Exploration’ (*Indeed*) <https://www.indeed.com/jobs?q=Blockchain&sort=date&fromage=last&start=10&vjk=0dec9afbb9cb507e> accessed 19 May 2019

No Trust No News, ‘We have filed a lawsuit against the BND Law’ (2018) <http://notrustnonews.org/?lang=en> accessed 21 May 2019

Li K, ‘The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed’ (*Hackernoon,* 30 January 2019) <https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44> accessed 20 May 2019

O’Carroll T, Ingleton D and Matsushita J, ‘Panic Button: Why we are retiring the app’ (*The Engine Room,* 1 September 2017) <https://www.theengineroom.org/panic-button-retiring-the-app/> accessed 18 May 2019

OECD, ‘The role of media and investigative journalism in combating corruption’ (27 March 2018) <https://www.oecd.org/corruption/the-role-of-media-and-investigative-journalism-in-combating-corruption.htm> accessed 23 May 2019

Oldroyd R, ‘The Bureau wins landmark press freedom case at the European Court of Human Rights’ (*The Bureau of Investigative Journalism,* 13 September 2018) <https://www.thebureauinvestigates.com/stories/2018-09-13/bureau-wins-case-to-defend-press-freedom-at-the-european-court-of-human-rights> accessed 21 May 2019

Open Archive <https://open-archive.org/> accessed 22 June 2019

Osgood R, ‘The Future of Democracy: Blockchain Voting’ (*Tufts University,* 14 December 2016) 17-18 <http://www.cs.tufts.edu/comp/116/archive/fall2016/rosgood.pdf> accessed 20 May 2019

O'Sullivan ML, ‘Technology & Ideas: If All Vehicles Go Electric, That’s Just Step One’ (*Bloomberg Opinion,* 14 January 2019) <https://www.bloomberg.com/opinion/articles/2019-01-14/electric-vehicles-are-just-one-step-to-address-climate-change> accessed 20 June 2019

Pawczuk L, Holdowsky J and Rob Massey, ‘Deloitte’s 2019 Global Blockchain Survey: Blockchain gets down to business’ (*Deloitte Insights*, 6 May 2019) <https://www2.deloitte.com/insights/us/en/topics/understanding-blockchain-potential/global-blockchain-survey.htm> accessed 17 May 2019

PEN International, ‘Mexico: failure of protection mechanisms exposed by murder of third print journalist in Veracruz this year’ (27 July 2016) <https://pen-international.org/news/mexico-failure-of-protection-mechanisms-exposed-by-murder-of-third-print-journalist-in-veracruz-this-year> accessed 16 May 2019

Perez S, ‘Spotify acquires blockchain startup Mediachain to solve music’s attribution problem’ (*TC,* 2017) <https://techcrunch.com/2017/04/26/spotify-acquires-blockchain-startup-mediachain-to-solve-musics-attribution-problem/?guccounter=1> accessed 19 May 2019

Periodistas en Riesgo <https://www.periodistasenriesgo.com> accessed 13 May 2019

Pinkert D, Ton-that J and Soopramanien R, ‘Blockchain technologies offer transparency that could improve human rights practices’ (*Open Global Rights*, 24 January 2019) <https://www.openglobalrights.org/blockchain-technologies-offer-transparency-that-could-improve-human-rights-practices/> accessed 20 May 2019

Quinn KT, ‘Can Blockchain Fix Journalism? How one technology—and a handful of insurgent startups—could revive an industry in crisis’ (*Medium*, 6 November 2018) <https://medium.com/the-slowdown/can-blockchain-fix-journalism-946418d4fac6> accessed 18 May 2019

Quiroz N, ‘Closing of Editorial Televisa in Chile: The end of Condorito?’ (*Chile Today*, 22 February 2019) <https://www.chiletoday.cl/closing-of-editorial-televisa-in-chile-the-end-of-condorito/> accessed 24 May 2019

Redacción AN, ‘La denuncia y el informe completo sobre #GobiernoEspía (Documentos)’ (*Aristegui Noticias,* 20 June 2017) <https://aristeguinoticias.com/2006/mexico/la-denuncia-y-el-informe-completo-sobre-gobiernoespia-documentos/> accessed 15 May 2019

Reporta <https://www.reporta.org> accessed 13 May 2019.

Reuters, ‘Reuters Journalists Freed from Myanmar Prison’ <https://www.reuters.com/subjects/myanmar-reporters> accessed 15 May 2019

RightsCon 2019, ‘RightsCon Tunis 2019’ <https://rightscon2019.sched.com/event/PvjZ/if-you-keep-suggesting-blockchain-i-swear-to-god-i-will-fing-scream> accessed 9 June 2019

Rosic A, ‘What is Blockchain Technology? A Step-by-Step Guide For Beginners’ (*Blockgeeks,* 1 March 2019) <https://blockgeeks.com/guides/what-is-blockchain-technology/> accessed 17 May 2019

– – ‘What is Ethereum? [The Most Comprehensive Guide Ever!]’ (*Blockgeeks*, 2016) <https://blockgeeks.com/guides/ethereum/> accessed 17 May 2019

Sagar J, ‘Confideal: Smart Contracts Made Simple’ (*News BTC,* 2017) <https://www.newsbtc.com/2017/10/23/confideal-smart-contracts-made-simple/> accessed 28 May 2019

Schiller V, ‘The Civil Constitution’ (*Civil*) <https://civil.co/constitution/> accessed 24 May 2019

Schouterden S, ‘Bitcoin and Encryption are Protected by Freedom of Speech’ (*Bitcoin.com,* 11 June 2015) <https://news.bitcoin.com/bitcoin-and-encryption-are-protected-by/> accessed 27 May 2019

Scott-Railton J and others, Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague’ (*The Citizen Lab,* 27 November 2017) <https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/> accessed 15 May 2019

Shukla S, ‘Get to Know Berkman Klein Fellow Dragana Kaurin’ (*Berkman Klein Center for Internet & Society at Harvard University,* 5 February 2019) <https://cyber.harvard.edu/story/2019-02/get-know-berkman-klein-fellow-dragana-kaurin> accessed 20 June 2019

Singh A, Answer ‘Are there any Altcoins I can invest in 2019 and why? There are too many scams and it’s hard to find a good one for a long-term investment’ (*Quora*, 14 March 2018) <https://www.quora.com/How-would-I-store-digital-documents-on-the-blockchain-rather-than-just-record-transactions> accessed 17 May 2019

SocialFlow <http://www.socialflow.com/> accessed 25 May 2019

Spiegel Online, ‘The End of Financial Times Deutschland Germany Hit by Wave of Newspaper Bankruptcies’ (23 November 2012) <https://www.spiegel.de/international/business/media-woes-hit-germany-as-financial-times-deutschland-goes-under-a-869001.html> accessed 24 May 2019

STORJ <https://storj.io/> accessed 21 June 2019

The Writers Bureau, ‘What is Freelance Journalism?’ <https://www.writersbureau.com/writing/what-is-freelance-journalism.htm> accessed 16 May 2019

Tiwari A, ‘Don’t Use This “Fake TOR Browser” — Scammers Are Fooling People’ (*Fossbytes,* 13 July 2017) <https://fossbytes.com/fake-tor-browser-rodeo-scan/> accessed 14 May 2019

Tordesillas ET, ‘OPINION: Lila Shahani, Maguindanao massacre and impunity’ (*ABS CBN News*, 26 November 2018) <https://news.abs-cbn.com/blogs/opinions/11/26/18/opinion-lila-shahani-maguindanao-massacre-and-impunity> accessed 31 May 2019

UN Blockchain <https://un-blockchain.org/> accessed 18 May 2019

UNESCO, ‘#TruthNeverDies: Journalists are killed everyday to silence the truth. Share their stories to Keep them alive? (*Exposure*, 26 October 2018) <https://unesco.exposure.co/truth-never-dies> accessed 27 May 2019

UNESCO, ‘International Programme for the Development of Communication’ <https://en.unesco.org/programme/ipdc> accessed 23 June 2019

U.S. Press Freedom Tracker, ‘All Incidents’ (2019) <https://pressfreedomtracker.us/all-incidents/?search=protes> accessed 13 May 2019

Wang T, ‘Energy consumption of Google from 2011 to 2017 (in gigawatt hours)’ (*Statista*, 31 May 2019) <https://www.statista.com/statistics/788540/energy-consumption-of-google/> accessed 21 June 2019

Wall E, ‘Privacy and Cryptocurrency, Part I: How Private is Bitcoin?’ (*Medium*, 7 March 2019) <https://medium.com/human-rights-foundation-hrf/privacy-and-cryptocurrency-part-i-how-private-is-bitcoin-e3a4071f8fff> accessed 28 May 2019

Washington Post, ‘Jamal Khashoggi’ (2018) <https://www.washingtonpost.com/people/jamal-khashoggi/?utm_term=.c7d57fafb6a1> accessed 16 May 2019

Whitepaper Database, ‘Po.et (POE)-Whitepaper’ (15 March 2018) <https://whitepaperdatabase.com/po-et-poe-whitepaper/> accessed 24 May 2019

Whittle B, ‘Storing Documents on the Blockchain: Why, How, and Where’ (*Coin Central*, 23 December 2018) <https://coincentral.com/storing-documents-on-the-blockchain-why-how-and-where/> accessed 19 May 2019

Williams AT, ‘The growing pay gap between journalism and public relations’ (*Pew Research Center*, 11 August 2014) <https://www.pewresearch.org/fact-tank/2014/08/11/the-growing-pay-gap-between-journalism-and-public-relations/> accessed 23 May 2019

Woolf N, ‘What Could Blockchain Do for Journalism?’ (*Medium*, 13 February 2018) <https://medium.com/s/welcome-to-blockchain/what-could-blockchain-do-for-journalism-dfd054beb197> accessed 20 May 2019

Yazici D, ‘Impunity for crimes against journalists in Russia is serious threat to media freedom, OSCE Representative says on anniversary of Anna Politkovskaya’s killing’ (*OSCE*, 7 October 2017) <https://www.osce.org/fom/348441> accessed 31 May 2019

Zmudzinski A, ‘CEO of Blockchain Media Company Po.et Leaves for Washington Post’ (*Cointelegraph*, 25 January 2019) <https://cointelegraph.com/news/ceo-of-blockchain-media-company-poet-leaves-for-washington-post> accessed 25 May 2019

VIDEOS

Capgemini, ‘Capgemini Smart Container using Blockchain’ (9 February 2018) <https://www.youtube.com/watch?v=6A0FMv-JXQE> accessed 23 June 2019

CNN, ‘Saudi's use social media to hunt down dissenters’ (*Quest Means Business*, 22 October 2018) <https://www.youtube.com/watch?v=A1xgYWxl6fQ&feature=youtu.be> accessed 15 May 2019

Huntley S and Marquis-Boire M, ‘Tomorrow’s News is Today’s Intel: Journalists as Targets and Compromise Vectors by Shane Huntley’ (*Black Hat,* 3 August 2014) <https://www.youtube.com/watch?v=7mI-qCRohWU> accessed 14 May 2019

Ivan on Tech, ‘Difference between DAPPS and Smart Contracts? Programmer explains’ (9 March 2018) <https://www.youtube.com/watch?v=4rczD8xKPJc> accessed 27 May 2019

Oliver J, ‘Journalism: Last Week Tonight with John Oliver (HBO)’ (LastWeekTonight, 7 August 2016) <https://www.youtube.com/watch?v=bq2_wSsDwkQ> accessed 25 May 2019

Protocol Labs, ‘Introducing Filecoin, a decentralized storage network’ (19 July 2017) <https://www.youtube.com/watch?v=EClPAFPeXIQ> accessed 22 June 2019

Simply Explained - Savjee, ‘Smart contracts - Simply Explained’ (20 November 2017) <https://www.youtube.com/watch?v=ZE2HxTmxfrI&list=PLX_38LSoURa9lUR2VvacK763AWSQoA7hP> accessed 27 May 2019

SocialFlow, ‘What is the UAT Ecosystem?’ (Facebook 29 August 2018) <https://www.facebook.com/socialflow/videos/1790864651028711/?v=1790864651028711> accessed 24 May 2019

SPEECHES

Levine O, Director of innovation for the International Center for Journalists (Speech at RightsCon, 12 June 2019)

TREATIES

OHCHR, ‘International Covenant on Civil and Political Rights’ (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> accessed 15 May 2019

United Nations, ‘Universal Declaration of Human Rights’ (2015 adopted 10 December 1948) <https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf> accessed 19 May 2019

ANNEX 1: LIST OF SOFTWARE, APPS AND ADD-ONS

Password managers:

- KeePass
- Password Safe

Email providers:

- Hushmail
- ProtonMail
- RiseUp
- Tutanota

Security software:

- Avast! (Protects against viruses)
- CCleaner (Deletes your data)
- Comodo (Network firewall)
- Eraser for Windows (Deletes your data)
- Malwarebytes (Removes malware)
- Spybot (Removes malware)
- Veracrypt (Encrypts your computer files)

Encrypted instant messaging and Voice over Internet Protocol (VOIP):

- Cryptocat
- Jitsi
- Pidgin
- Signal

Web browser add-ons:

- Adblock Plus
- DoNotTrackPlus
- Ghostery
- HTTPS Everywhere
- NoScript Security Suite
- Privacy Badger
- uBlock Origin

Private search engines:

- DuckDuckGo
- F-Secure Safe Search

Web browsers:

- Brave
- Dragon Internet Browser
- Epic Privacy Browser
- FreeBrowser
- Lantern
- Tor Browser

Virtual private network (VPN) providers:

- NordVPN
- OpenVPN
- Psiphon
- TunnelBear

Public key encryption for email:

- Thunderbird + Enigmail + OpenPGP
- GPG4USB for Windows
- Mailvelope

Apps on Android:

- Android Privacy Guard
- Obscuracam: Secure Smart Camera
- Orbot: Proxy with Tor
- Umbrella: Security made easy

Note: This list was developed by Canadian Journalists for Free Expression (CJFE),[255] which is one of many guides explaining all of the technological applications journalists should consider using.

[255] Canadian Journalists for Free Expression (n. 86).