ARTICLE 19

Blockchain and freedom of expression

2019

ARTICLE 19
Free Word Centre
60 Farringdon Road
London
EC1R 3GA
United Kingdom
T: +44 20 7324 2500
F: +44 20 7490 0566
E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org

Contents

Executive summary

In this report, ARTICLE 19 examines the impact and implications of blockchain technology for the right to freedom of expression.

Blockchains can be generally thought of as a technology to securely store data, using unique properties of cryptography. Unlike traditional forms of record-keeping, they do not rely on a central source to store records, instead distributing data across a network. Blockchains are the technical foundation of digital cryptocurrencies such as Bitcoin. Blockchains, both private and public, have a multitude of current and proposed applications beyond transactions – they can be used to authenticate persons and data, as well as serve as a basis for file systems and content distribution.

Blockchain technology is a topic of much interest and curiosity across many sectors. Due to its characteristics, which generally include immutability, transparency, pseudonymity, and decentralisation, some proponents of blockchain technology suggest that it has the potential to power censorship-resistant platforms and protect freedom of expression.

ARTICLE 19 monitors emerging technologies for their potential impact on freedom of expression, and analyses those impacts; we have done so in recent years for a variety of digital technologies including encryption and anonymity tools. In this report, we examine some key freedom of expression issues implicated by blockchain technology; and also analyse four use cases which have significant freedom of expression implications - content dissemination, content authentication, data storage, and cryptocurrency transactions.

Our findings and observations can be summarised as follows:

- **Technology is never the only solution** to protecting and promoting freedom of expression. It is a powerful tool in enabling freedom of expression, but in the wrong hands, technology can also become an instrument of repression. Even where states or other actors promote or permit access to technology (such as blockchain technology), this does not absolve them from meeting their obligations under international human rights law.

- Since blockchains are tools through which individuals can exercise their right to freedom of expression, this confers obligations on state and private actors under international law to **respect freedom of expression in their implementation.**
- **Censorship-resistance alone does not guarantee that the implementation or governance of blockchain technologies adheres to international standards.** While the immutability of blockchains is often presented as a net benefit for freedom of expression, ARTICLE 19 finds that there are instances where it may be necessary to limit free expression where the purposes are legitimate under international law and respecting the rule of law, i.e. where platforms are used for the storage or dissemination of content that can be legitimately restricted under international law. In this respect, blockchain technology may pose challenges for the ability of states to exercise their international legal obligations.
- Blockchains impose a **shifting of trust to technology and private actors** who design, implement, mediate, and govern that technology. The promise of distributed' and 'decentralised' systems is not entirely true in practice. Usage of these technologies is not necessarily trustless but involves placing significant trust in software, those vetting the software, the tools used in accessing that technology, and key players implementing and operating elements of decentralised networks.
- Blockchain technology may introduce **security risks**. While promoted as 'secure,' most users - unless they possess considerable technological sophistication - are likely to use some intermediary in order to access the technologies, whether mobile applications, browser extensions, or third party actors. These points of access introduce vulnerabilities: phones and computers can be hacked or stolen, and third parties can be compromised.
- **Civil society should have a voice in the oversight of technical and economic standardisation.** The implementation of blockchain technology introduces questions of governance, including how and by whom these technologies are governed, particularly where technologies are designed by core groups of developers who may be relatively homogenous in terms of gender, ethnicity, and nationality and therefore not representative of the plurality of stakeholder voices.

Summary of recommendations

To states

- States' obligations to respect, protect, and fulfil human rights, including online, extends to the public's right of access to blockchain technology. Hence, any restrictions on blockchain platforms, or intermediaries that provide blockchain access, must be necessary, proportionate, and subject to independent judicial review.
- States should ensure that providers, coders, and implementers of blockchain platforms are in principle immune from liability for third party data stored on those platforms when they have not been involved in storing the content in question.
- States should refrain from measures such as shutdowns on Internet access or restrictions on the encryption technologies that underpin blockchains, particularly through the inclusion of encryption 'backdoors,' as these measures represent disproportionate interferences with the right to freedom of expression.
- To the extent that states use blockchains to store data of citizens or public records, states should ensure that they adhere to international human rights principles on access to information and data protection.
- When coordinating among stakeholders to standardise and implement blockchain technologies, states should ensure that human rights norms are among the key considerations in these partnerships, and that civil society is included in any strategic planning.

To private actors in the digital sector

- Companies, coders and implementers of technologies should ensure that their technologies are designed in a way that takes into consideration the rights to freedom of expression and privacy.
- Companies should ensure that deployment of blockchains is done after careful considerations of all risks, including security and impact on users, and match between blockchain specific benefits and use cases that enable realisation of these benefits.

- As crucial intermediaries, companies that provide private blockchain platforms for dissemination or storing of content should be transparent about any internal guidelines for the removal of content in blockchains, where content removal is feasible, as well as the appointment of moderators or validators with authority to flag or censor content. Companies should also provide notice and access to a remedy for individuals who have had their content removed.
- Coders and implementers of technologies should ensure that their governance includes a diverse array of voices, including members of civil society, and that non-private platforms are accessible to a plurality of audiences.

To all stakeholders

- States, private sector and all other stakeholders, should carefully consider the implementation of blockchain technology; in particular:
    - Whether the issues they are seeking to address do in fact require a technological solution, whether these issues could not be better remedied through a social solution or whether other existing technologies could suffice; and more specifically, whether they specifically need an immutable database distributed across multiple servers;
    - Where is trust being placed: whether it is in the coders, the developers, those who design and govern mobile devices or apps; and whether trust is in fact being shifted from social institutions to private actors. All stakeholders should consider what implications does this have and how are these actors accountable to human rights standards;
    - Operational issues, such as what happens if individuals lose passwords or the means of access;
    - Whether the new technology will be practically accessible and subject to governance that respects human rights norms, or whether its implementation will be concentrated among a core group of developers or third parties;
    - Whether the adoption of technologies exposes them to legal

liability if malicious actors misuse the technology for objectionable purposes;

- Whether there is potential that an individual may - at some point in the future - require recourse or redress with respect to the information immutably encoded in the blockchains, and how this redress will be realised.

- Civil society should strive to engage with private actors, coders of blockchain technologies, and states, to ensure that international human rights norms are considered and incorporated in the development and implementation of new technologies and consider the impact of these technologies on human rights of beneficiaries in their projects.

Introduction

In the last decade, blockchains have garnered significant attention, mainly due to their role as the foundation of cryptocurrencies such as Bitcoin. The underlying methods behind cryptocurrencies has since been expanded to create decentralised networks of various forms with applications in many different sectors. Some of these applications, both actual and contemplated, have significant implications for freedom of expression.

While blockchains elude simple definition, they are best conceptualised as a secure method of storing information due to their special qualities by design.[1] Blockchains are ledgers with several copies in existence at the same time; if one copy is taken down or tampered with, the other copies will still exist. Data in the ledger is stored in a chronological sequence, or 'chain.' Each individual data container in the chain is called a 'block,' from which the term 'blockchain' derives. The blocks in a blockchain are interconnected by cryptography to ensure their validity. Blockchains can be both private and public, and both are examined as part of this analysis.

One helpful analogy to understand the role that blockchains serve is the revision history of a page on Wikipedia. Every article on Wikipedia stores a 'revision history' where anyone can view any edit that was ever made to the article. If someone decides to make a change or revert an article to a prior state, that change will be recorded in the 'revision history' so that any future person can tell what was modified. Blockchains can provide a form of revision history for a range of transactions. But there is an important distinction: Wikipedia is a centralised entity, so if Wikipedia were to be shut down, those activity records would vanish. But if Wikipedia were to somehow exist on a blockchain there would be no single version to censor, because the data would be distributed throughout a network.[2]

Proponents of blockchain technology advocate that their distributed nature can be used to protect human rights and can be a technological solution to the increased centralisation of the Internet.[3] They argue that the control exerted today by Internet intermediaries has a *negative effect* on freedom of expression and the realisation of human rights online. Hence, the practical immutability of blockchains make them censorship-resistant and eliminates

reliance on intermediaries. Proponents point to potential applications including the dissemination of unpopular opinions and other at-risk content. Further, they argue that blockchains may provide other benefits, including the ability to authenticate individuals and information if explicitly designed to do so.

Blockchain technology is supported across many industries and associations, and companies are eagerly investing in blockchain sectors ranging from banking to healthcare. Some states are implementing blockchains as well, in particular for identification and record-keeping; which makes an analysis of the human rights implications of these technologies critical. Civil society organisations are also exploring the potential applications of blockchains ranging from content dissemination, source protection, identification and authentication. Some media organisations, such as Civil,[4] are proposing other uses for blockchains as an economic model for sustaining journalism, self-regulation, and license management.[5]

A number of international and regional bodies have also highlighted the importance of blockchains and called for the development of new standards in this area.[6] For example:

- The 2018 Resolution of the European Parliament, *Blockchain: a forward-looking trade policy*, highlighted the ability of blockchains to provide "permanent real-time access to an immutable, time-stamped database holding documents pertaining to transactions, thus helping to build confidence, avoid compliance issues and tackle the use of counterfeited goods or fake documents." The Resolution encouraged the European Commission to follow developments in the area of blockchains, to assess their "judicial and governance aspects" and "develop a set of guiding principles for [their] application to international trade."[7] It also called on the European Union (EU) and EU member states to "play a leading role in the process of standardisation and security of blockchains, and to work with international partners and all relevant stakeholders and industries to develop blockchain standards."[8]
- The UN Office for Project Services (UNOPS) and the UN Office of Information and Communications Technology launched a call for proposals for blockchain companies to present blockchain-based identity solutions to combat child trafficking in Moldova.

- The UN ECOSOC's Economic Commission for Europe (UNECE) has advocated for the creation of international and regional platforms on blockchains to engage "all key actors and potential beneficiaries" particularly to see if blockchains can help achieve the Sustainable Development Goals.[9]
- At the 2018 General Assembly, the UN Secretary-General convened a meeting of twenty figures from across industry, civil society, and academia regarding new technologies including blockchains.[10] The EU has created a "Blockchain Roundtable" and is working on a comprehensive strategy across Europe.[11]

However, in this report, ARTICLE 19 argues that blockchains' quality of censorship-resistance does not necessarily mean that its implementation or governance[12] adhere to international freedom of expression standards. These standards do not merely grant a right of censorship-resistance, but also require restrictions on freedom of expression to be clearly defined in law and to be necessary and proportionate to specifically enumerated legitimate aims. At a more fundamental level, where law is nuanced, technology is rigid and in some cases the implementation of blockchains precludes the co-existence of both *technological* and *social* solutions. As with many technologies, blockchains could be dual-use and have the potential to promote harm as well as good.

ARTICLE 19 believes that the underlying qualities and assumptions behind blockchains should be carefully examined from a human rights perspective. This report outlines the features of blockchains which, in their implementation, should be reviewed for their compliance with freedom of expression; and the responsibilities of states and private actors to protect and promote the right to freedom of expression in relation to blockchains. ARTICLE 19 hopes that this report and our recommendations can be used by all stakeholders in their work in this area.

Background to blockchains

Blockchains' story began in 2009, when the pseudonymous Satoshi Nakamoto released Bitcoin, the world's first digital and decentralised currency, or cryptocurrency. Blockchain technology is the basis for recording Bitcoin transactions.[13] This means that Bitcoin did not require banks to transfer assets because the blockchain code keeps track of the transfers itself. Instead of having banks verify transactions of Bitcoin, the transaction record is completely public and the task of verifying transactions is crowdsourced. It is possible to go online and view every Bitcoin transaction going back to its origin, since the whole ledger is verified and replicated across nodes worldwide.

Key terminology

A blockchain is a type of digital ledger that is copied in multiple locations simultaneously on a peer-to-peer network to securely store data. Blockchains are a more specific form of a **distributed ledger technology (DLT)**, which describes any database that is simultaneously maintained in several locations.[14]

New information in a blockchain is added in chronological order to a series (chain) of containers of data (blocks). The data is authenticated by crowdsourcing via a method called *consensus* where individuals in the network continuously and independently verify the information in the blockchains using cryptographic methods: new data that is added in a blockchain also validates the data before.[15] Information can only be added to the ledger, and once recorded, it cannot practically be deleted without the network noticing. The purpose of these features is to ensure the integrity of the record, not necessarily the information itself, and to protect the record from being tampered with. Tampering with a block would require changing not only that block but every single block that follows it in a domino effect. Doing so throughout the whole distributed network, depending on the size of the network and specific method of consensus, can range from difficult to practically impossible.

Some blockchains can be used to record information such as dates, numbers, or messages as part of blocks. Information stored in the blockchains can also be encrypted, such that the text is technically 'public' but is unintelligible except to authorised individuals that possess an encryption password or key to read it.

Blockchains can be public or private. **A public blockchain** is a transparent blockchain where any member of the public with the right software applications can view and participate in recording and verifying transactions in the ledger. Bitcoin is based on public blockchains because any person can access and verify any transaction ever conducted using Bitcoin. This method of ultra-transparency serves as a way to generate trust in the network even with anonymous or untrustworthy participants.

A private or permissioned blockchain is a blockchain where some participants may be given more power to verify transactions as well as dictate the structure and function of the network.[16] Permissioned blockchains are usually more centralised and often require permission for access. These forms of blockchains are appealing to private companies that maintain a shared trusted environment, such as financial institutions, and that may seek to retain some level of control over the players in the network.[17] Indeed, many companies are developing implementations of permissioned blockchains in a variety of sectors.

One final element introduced by blockchains is the smart contract, a computer protocol that can facilitate the performance of a transaction without a third party, similar to a digital escrow. If certain programmed conditions are met, the contract will automatically execute; however, this requires the contract to be programmed properly and shifts trust away from a third party to the proper coding of the contract. Bugs, or exploitable flaws, in smart contracts are especially problematic because the blockchains are such a rigid technology: by design, contracts cannot be modified upon execution. This rigidity, combined with software exploits, has already led to the freezing or hacking of millions in assets.[18]

Key characteristics of blockchains

Some key characteristics of blockchains[19] include the following:

- **Immutability**: This means that information cannot be changed or removed. An analogy to Wikipedia and its revision history feature is relevant here; even if a Wikipedia article is edited, the transaction of editing that article is logged for anyone to see and that change is recorded as the most recent edit. Blockchains' immutability is challenged by some proposals to use encryption so that access to data stored on the blockchains can be limited to whoever has the key, or even effectively 'deleted' if the encryption keys are deleted.
- **Transparency**: Transactions on the blockchain ledger are recorded for the network to see. This feature promotes authentication of transactions under the assumption that parties are untrusted. It is still possible to store encrypted data within transactions on some blockchains, meaning that the encrypted data is viewable but that only parties with access to decryption keys can access the data.
- **Pseudonymity**: While transactions or activities recorded in a blockchain contain data referencing a sender and receiver (such as the sender and recipient of Bitcoin), that data is most often referenced as a digital address that may not necessarily be tied to a particular individual. That address is, however, an identifying piece of information that can still be hypothetically traced to users. Hence users on most blockchains are pseudonymous – requiring extra steps of investigation, often practically unfeasible – in order to connect a digital coin wallet address to a real person. To the extent that intermediaries and third parties serve as access points to blockchains, those parties may retain records such as access by IP addresses and other metadata about users that can help trace user activity on the blockchains to real individuals. Some blockchains provide more privacy than others.
- **Disintermediation**: Blockchains are peer-to-peer networks, and do not rely on a central authority or intermediary to authenticate transactions (this may be less so in the case of permissioned blockchains). However, in reality, individuals may likely end up using access points to interact with blockchains, and those access points may serve as gatekeepers to undermine the decentralised nature of the technology.

- **Lack of scalability**: This is considered a disadvantage of blockchain technologies such as Bitcoin, which typically process 3-20 transactions per second globally as part of the verification and consensus procedure for transactions.[20] These transaction times multiply significantly to serious processing times if large numbers of transactions are undertaken.
- **Data limitations**: Because blockchains are extremely resource intensive, the amount of data individual blocks contain is extremely limited, usually limited to a small number of characters. Hence, with current technology, it would not be feasible to store multimedia content in a block. However, blocks could store *links* to data that is stored elsewhere.

Despite the limitations created by the issues of scalability and data storage capacity, some existing and anticipated applications have already implemented, or intend to implement, ways of using blockchains to distribute messages and content. Some applications such as Ethereum allow blockchain technology to be used and accessed through web browser extensions. These applications are still developing at present and undoubtedly many new implementations will come with time.

International human rights standards and blockchains

Right to freedom of expression

The right to freedom of expression is protected by a number of international human rights instruments, in particular Article 19 of the Universal Declaration of Human Rights (UDHR)[21] and Article 19 of the International Covenant on Civil and Political Rights (ICCPR),[22] and regional human right treaties.[23]

In General Comment No 34,[24] the UN Human Rights Committee (HR Committee) - charged with interpreting the ICCPR - explicitly recognised that Article 19 of the ICCPR also applies to all forms of electronic and Internet-based modes of expression.[25] State parties to the ICCPR are required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[26] Additionally, in his 2011 report, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FoE) noted that access to the "infrastructure and information communication technologies, such as cables, modems, computers and software, to access the internet in the first place" implicate freedom of expression.[27]

Importantly the right to freedom of expression includes the right to anonymity and 'pseudonymity.'[28] Anonymity protects the freedom of individuals to communicate information and ideas that they would otherwise be inhibited from expressing; it also protects the freedom of individuals to live their lives privately. Technology tools such as encryption that enable meaningful exercise of the right to freedom of expression in the digital age must be strongly protected and promoted.[29]

Under international standards, restrictions on the right to freedom of expression must meet the conditions of the so-called "three-part test" which mandates that restrictions must be:

- **Provided for by law**; any law or regulation must be formulated with sufficient precision to enable individuals to regulate their conduct accordingly;
- **In pursuit of a legitimate aim,** listed exhaustively as: respect of the rights or reputations of others; or the protection of national security or of public order (ordre public), or of public health or morals;
- **Necessary and proportionate in a democratic society**, i.e. if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.[30]

Additionally, Article 20(2) of the ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law.

Right to privacy

The right to privacy, protected in international law through Article 17 of the ICCPR, complements and reinforces the right to freedom of expression as it is essential for ensuring that individuals are able to freely express themselves, including anonymously,[31] should they so choose. The mass surveillance of online communications therefore poses significant concerns for both rights.

The right to privacy has evolved to address issues relating to the collection, use, and dissemination of personal information held by governments and private bodies in information systems. Starting in the 1960s, principles governing the collection and handling of this information known as "fair information practices" were developed and adopted by international bodies and national governments,[32] including the UN General Assembly[33], the Commonwealth[34] and the Economic Community of West African States (ECOWAS).[35] In Europe, both the Council of Europe[36] and the European Union have incorporated these principles into data protection treaties. Specifically, the EU maintains a General Data Protection Regulation (GDPR) which imposes obligations on private companies that host personal data, and allows customers to withdraw consent and request that data be deleted. The GDPR defines personal data as "any information relating to an identified or identifiable natural person."[37] It is noted that the immutability features of blockchain technologies pose regulatory challenges in their compliance, or lack thereof, with GDPR.[38]

Internet governance

The Internet governance principles, including on application of human rights principles to decentralised technologies, originated at the first World Summit on the Information Society (WSIS) in 2003 in Geneva. WSIS led to the defining of 'Internet Governance' and produced the Geneva Principles that provide a detailed account of the concept of the information society and the underlying principles.[39] The Second WSIS, held in Tunis in November 2005, provided a working definition for Internet governance:

> [T]he development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the internet.[40]

In 2011, the Council of Europe adopted Ten Internet Governance Principles.[41] The principles, inter alia, endorse the universality, openness, and integrity of the Internet, the multi-stakeholder approach to Internet governance, and the decentralised management and interoperability of the Internet.

It is most noteworthy that, along with public actors, private actors are called upon to respect human rights and fundamental freedoms when developing, offering and operating their services and applications.[42]

So far, various Internet governance forums hosted sessions about blockchains, exploring new decentralized governance frameworks enabled by this technology.[43] However, it is unclear to what extent Internet governance bodies will provide leadership, coordination and organisation in this area.

Intermediary liability

International bodies have also commented on liability regimes for intermediaries, which also applies in the case of intermediaries providing access to blockchain technologies. While international human rights law puts obligations on states to protect, promote and respect human rights, it is widely recognised that business enterprises also have a responsibility to respect human rights.[44]

Importantly, the Special Rapporteur on FoE has long held that censorship obligations should never be delegated to private entities.[45] In his June 2016 report to the HRC,[46] the Special Rapporteur on FOE stipulated that states should not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extra-legal means. He further recognised that "private intermediaries are typically ill-equipped to make determinations of content illegality,"[47] and reiterated criticism of notice and takedown frameworks for "incentivising questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation," i.e. underlining the danger of "self- or over-removal" in these situations.[48] The FOE recommended that any demands, requests and other measures to take down digital content must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under Article 19 (3) of the ICCPR.[49]

Similar recommendations were raised by four special rapporteurs in their 2011 Joint Declaration on Freedom of Expression and the Internet.[50]

With respect to the obligations of intermediaries not to censor peer-to-peer content, the Court of Justice of the European Union (CJEU), held that blanket web filtering systems installed by Internet Service Providers (ISPs) to prevent illegal file-sharing on peer-to-peer networks was incompatible with fundamental rights.[51]

Blockchains and freedom of expression

International human rights norms apply in the context of decentralised and disintermediated platforms, particularly in the case of the Internet. As the right to freedom of expression is not designed to fit any particular medium or technology, in this section, ARTICLE 19 reviews how these standards are relevant for consideration with blockchain technologies. We first make some general observations in this area, followed by four blockchain use cases: content dissemination, content authentication, platform creation, data storage, and cryptocurrency transaction; examining both the positive and negative effects of the implementations of these use cases.

Decentralisation, disintermediation and freedom of expression

The appeal and primary feature of blockchains are their decentralisation and disintermediation. ARTICLE 19 believes that decentralised platforms promise benefits for the freedom of the press, because it makes it harder for governments to censor content.[52] However, blockchains' aspiration of removing intermediaries risks negative impacts on freedom of expression (see below for more information). Further, states still maintain responsibilities to protect and promote freedom of expression that cannot be abdicated by delegating those responsibilities to technology.

Blockchains still retain centralised features. Permissioned blockchains tend to be, by design, more 'closed' in who can access then and the creator may even appoint who runs the nodes responsible for authenticating transactions. In the case of public blockchains, most users still require intermediary services and software to connect to and interact with blockchains. The presence of these third parties to access blockchain services, whether they be software, websites, or browser extensions, means that users are placing trust in entities that may or may not be trustworthy.

Digital access and literacy

The structure of blockchains often makes it infeasible to host or download them on mobile phones, which can serve as a barrier of access in areas where Internet connectivity primarily occurs via mobile devices. Because every full node (host of the blockchains) stores a copy of the entire transaction log, blockchains only grow longer and larger with time, and thus can be extremely resource-intensive to download on a mobile device. For instance, over the span of a few years the blockchains underlying Bitcoin grew from several gigabytes to several hundred. Hence, it is generally infeasible to access blockchains or operate full nodes on mobile devices. In regions of the world where most Internet access occurs through mobile devices, this has implications for accessibility and can serve as a way of excluding access to blockchains. One implementer of blockchain-based identity technologies admits:

> Unstable governance can make establishing a technology-centric economy difficult. Most developing nations within Africa and the Middle East have very low smartphone consumer penetration. Millions of citizens across these regions depend on the flip-phone economy and are unable to participate in the self-sovereign identity revolution.[53]

It follows that there are some communities that are underrepresented in the operations of blockchain networks, and are not involved in validating content that could nevertheless impact them. Stakeholders must always ask how various groups who are economically, socially, or physically marginalised can effectively access new technologies.

Further, these technologies are inherently complex, and outside the atypical case where individuals do possess the technical sophistication and means to install blockchain software and set up nodes; the question remains as to how the majority of individuals can effectively access them. This is especially true of individuals who may have added difficulty interfacing with technologies due to disability, literacy or age.[54] Ill-equipped users are at increased risk of their investments or information being exposed to hacking and theft. In the event that interaction with technology is mediated by third party providers, then the same question arises as to how those interfaces with the technology are necessarily trustworthy or accountable.

Finally, the extent to which access to blockchains store personal data and may require personal passwords, encryption keys, or other identifiers to access that data presents a potential issue for privacy and data protection. In reality, individuals often forget passwords; if they lose the encryption password to their data stored in a blockchain implemented for important state-based benefits or identification, this might mean that a person is foreclosed from ever accessing their data. One private company that works with regulators worldwide proposed that "the most likely method for reclaiming a private key would be to physically go to a secure facility where the key's owner would have to pass a number of security measures before the key is restored."[55] However, if this is the case, the system effectively has 'backdoors' built in and undermines the point of having the system in the first place.

Security and vulnerability of access points

Blockchains require placing significant trust in the technologies and the tools used to access them, and these forms of access may have vulnerabilities no matter how secure the underlying blockchain may be. In reality most individuals accessing blockchains will do so using applications provided by third party sources, often mobile devices for authentication purposes. Or they may use browsers: the Ethereum platform can be accessed using a browser-based plugin. Unfortunately, phones and browsers can be and often are compromised.

Access to a blockchain still requires access to a network (generally speaking, the Internet). While access to blockchains can be hampered in the event of hacking of the user interface, other risks are restrictions on access and Internet shutdowns. One potential catch-22 is that states that may be most in need of censorship-resistant platforms may also be the ones most likely to resort to measures such as Internet shutdowns or restrictions on connectivity to curb freedom of expression. ARTICLE 19 believes that restrictions on the modes of access to blockchains should be analysed under the existing framework for access to Internet intermediaries, and thus restrictions on access must be satisfy the three-part test under international law.

Blockchains promise of anonymity, or at least pseudonymity, because limited information regarding individuals is stored in transaction logs. However, this does not make the underlying access platforms resistant to protecting

anonymity. For instance, the central internet regulator in China proposed regulations that would require local blockchain companies to register users with their real names and national identification card numbers.[56] ARTICLE 19 notes that mandatory online registration schemes in the context of blockchain are a disproportionate interference with the right to be anonymous online, and that states still maintain an obligation to respect this in the context of blockchains.

Governance

The policies and assumptions that guide blockchain technologies impact both the dissemination of content and the way in which individuals access information. Truly decentralised and distributed public blockchain initiatives pose a novel challenge from an Internet governance perspective because public blockchains primarily rely on core developers of open-source software. Permissioned blockchains, on the other hand, are often driven by private actors pursuing these technologies for primarily commercial purposes; states may implement these technologies as well. Some Internet governance bodies have begun to recognise blockchains already, including the Institute of Electrical and Electronics Engineers (IEEE), which develops many international standards driving telecommunications and ICT hardware.[57] It is important that civil society groups have a voice in the oversight of technical and economic standardisation.

It is a myth that blockchain transactions are trustless - they rely greatly on trust in the software, their developers, those vetting the software, and key players implementing and operating nodes. There is concern regarding the homogeneity of the developers and stakeholders of blockchain technologies, which disproportionately underrepresent women and persons from the Global South.[58] This is particularly important given the private sector's obligation to promote human rights. A majority of start-ups proposing blockchain-based solutions are U.S.-based, which raises questions regarding the plurality of governance and the relative power of certain stakeholders in networks.

With respect to state interferences, there may be instances where states wish to exercise their duty under international law to regulate certain forms of objectionable content, but are prevented from doing so due to the immutable nature of blockchain. ARTICLE 19's position is that the measures taken by

states in this situation must be the least restrictive means necessary; i.e. the presence of objectionable content on a permissioned blockchain or in the metadata of a blockchain transaction should not be used as pretext for a blanket ban on access to these technologies. Any restrictions should be ordered by an independent court or adjudicatory body and be subject to review. Further, because regulations, including export controls, on blockchains could risk restricting encryption and other technologies that promote freedom of expression, special care must be taken that any regulations do not have the effect of limiting speech-protecting technologies.

Use case: content dissemination

At present there is an ongoing and intense debate about limits to freedom of expression, a debate which has only intensified in discussions over the use of blockchain technology for content dissemination. Immutability (which the proponents argue makes blockchains censorship-resistant), also raises the greatest degree of concern from an international human rights framework. This use case separately examines three types of content that are implicated by these technologies: text content, media content and the 'permanent web,' and blockchain-based social networks.

Dissemination of text

Blocks in a blockchain can carry a very limited amount of data. In the blockchain record for a cryptocurrency like Bitcoin, this data usually just includes sender, recipient, amount of transaction, and a cryptographic hash of the previous block to validate its spot in the chain. However, transactions can also carry a limited amount of metadata; in the case of Bitcoin, metadata can contain up to 80 bytes (80 characters).[59] Other blockchains may have greater limits, although the quantity of storable data will generally be small. The capacity to store metadata can serve as a brief 'memo' field in a block.

The possibility of using blockchains to share text became prominent in the 2018 Peking University case,[60] involving a student who in the past had reported a sexual assault and subsequently committed suicide. When her friends shared their stories of the university's alleged role in covering up the sexual assault, their accounts were quickly censored. One student then wrote a letter detailing the intimidation and coercion she faced from the university and authorities. She disseminated the letter via blockchain by posting the letter in the metadata of a transaction for Ethereum. While the text was technically immutable, the lack of widespread use or understanding of blockchain prevented it from reaching the same level of virality it could have on social media. Furthermore, Chinese platforms such as WeChat responded by blocking access to all Ethereum transaction pages. This early case raises questions as to the scalability of metadata implants as a censorship-circumvention tool. It also highlights the concern of shutdowns or blockages utilised to prevent individuals from accessing information on blockchains.

While the small byte limits of metadata in transactions make it difficult to embed large amounts of text, it is possible to post hyperlinks as text. Researchers in Germany found examples of hyperlinks to objectionable materials embedded in Bitcoin transactions, including links to child pornography websites. This raises significant legal concerns to the extent that the links to this content cannot be practically taken down, for instance, following an order by an independent judicial body. Furthermore, because the transaction log of blockchains replicates itself across computers, individuals who copy the Bitcoin chain are forced to host links to objectionable content on their systems, potentially exposing them to legal liability based on the laws of their country.

ARTICLE 19's assessment:

- **Positive aspects**: The ability to circumvent censorship is an important objective for the realisation of human rights, and it is positive that the private sector is attempting to answer the problem of content controls. But while the storage of text in blockchains may be a potentially beneficial use case, it must be applied in a manner that is consistent with the full scope of rights to freedom of expression and permissible restrictions on those rights under international law.

- **Negative aspects**: Immutability on a public blockchain potentially allows any person to permanently embed content as metadata in the chain; this goes too far and would prevent states from imposing certain legitimate restrictions that are necessary and provided for by law. The inability for an independent judicial authority to be able to effectively order the takedown of links to objectionable content, such as images of child sexual abuse, is highly problematic. ARTICLE 19 notes that while the effective limitation of metadata embedding of hyperlinks means that the actual offending content exists elsewhere and could be taken down, this does not limit postings of text that harm the rights or reputations of others.

Dissemination of multimedia and the 'permanent web'

As noted earlier, data storage limitations of blockchains and the multiplication of chains across nodes make them ill-suited to the distribution of large files like multimedia.

However, there are some proposed work-arounds to this issue under development. One such method is the **Inter-Planetary File System (IPFS)**, a file-sharing protocol where the same set of files are hosted across node computers throughout a network.[61] Node computers serve as individual libraries, but must opt-in whether to access and host files, which mitigates the risk that operators inadvertently wind up with objectionable and unintended content. Every file uploaded to IPFS has an associated cryptographic hash which is a unique alphanumeric identifier. In order to access a file, the user must know the hash associated with a file. If a user wishes to secure a file so it is not accessible to just anyone with the hash, then the user can take further steps such as encrypting the file. This can be used to effectively 'take down' a file.

How IPFS is executed is fundamentally different to the way the Internet normally works. Typically, to access a file online, a user must input a specific web address. If that web address is no longer functioning or has been taken down, the user is out of luck. With IPFS, the requested file rather than a specific web site is searched for. This is called content addressing, and the paradigm this creates has been referred to as the 'permanent web.' The difference is one between visiting a physical library location to find a record, versus being able to search a global catalogue to find the nearest location of the record directly.

When this system is implemented with the text metadata storage properties discussed in the preceding section, it becomes possible to store references to IPFS files in in blocks in a blockchain. These references are the unique hashes associated with each IPFS file, like a unique library call number. The actual storage of files through IPFS is more centralised since the network is comprised of a core group of users who maintain node computers, which possess and serve files.

For example, during the Catalan independence referendum in 2017, the Spanish government blocked many websites related to the referendum,

following a ruling by the Constitutional Court of Spain. The Catalan Pirate Party then placed a site online using the IPFS protocol. However, the Spanish government managed to block the domain gateway.ipfs.io, which was used to store referendum information across many servers.[62]

IPFS was also used to make copies of Wikipedia pages where Wikipedia is censored, such as a Turkish read-only mirror of the site created following the restriction of access to Wikipedia in Turkey.[63] In response to the censorship, IPFS issued the following statement:

> A main goal of the IPFS Project is improving humanity's access to information. We strongly oppose the censorship of history, of news, of free thought, of discourse, and of compendiums of vital information such as Wikipedia. Free access to information is key to modern human life, to a free society, and to a flourishing culture. We're alarmed by the erosion of civil liberties wherever it occurs, and we want to help people like the citizens of Turkey preserve freedom of information, even in the face of a tightening iron fist.

However, in response to the question "who controls the information," the IPFS project noted that the Wikipedia project was executed in haste in response to the censorship, and that over time it aims to establish a clear chain of custody. Thus, there is a degree of centralisation and trust involved in whatever parties are generating copies of the content on IPFS, and a majority of actors on a network could theoretically utilise this for malicious purposes.

A critical consideration is the capability of IPFS to host harmful content that cannot be taken down. The development of IPFS has attempted to address this to some degree, suggesting *blocklists* that are operated by consensus that prevent the hashes of certain forms of illegal or objectionable content from being recorded into the blockchain. However, to the extent that the system allows this form of regulation, it means that an actor that obtains control of the majority of a network required to establish consensus can impose censorship over content for malicious reasons (i.e. to restrict freedom of expression).

ARTICLE 19's assessment:

- **Positive aspects**: The ability to use IPFS to copy web sites in response to blocking, as in the case of Wikipedia, is a potentially powerful tool to circumvent censorship and promote access to information.

- **Negative aspects**: It is unclear how protocols such as IPFS properly address the hosting and dissemination of harmful content. Some proposals include blocklisting content but it is unclear how this addresses the case of content that is already disseminated across the IPFS network, or where content is maintained by a majority of malicious actors within a network. While content can hypothetically be completely removed if all holders agree to remove it (which is unlikely to occur in practice), the hash of the content would still exist on the blockchain. Therefore the inability to block content on nodes in certain jurisdictions could lead to legal liabilities, problems adhering to GDPR compliance, or worse. Governments still can block access points to IPFS gateways, preventing any access to the network, which undermines the censorship-resistance in practice.

Further, it is unclear whether the characteristics of IPFS are necessary given current censorship-circumvention tools. Individuals who wish to avoid censorship have ways to disseminate that content in manners that are not necessarily immutable. For instance, individuals can store local copies of the media and have them uploaded in different jurisdictions or via virtual private networks (VPNs) or TOR. At a fundamental level, the utility of IPFS is unclear whereas the objective of technologies like VPNs and TOR are protecting the *privacy* of the individual user, IPFS is not inherently designed to protect user rights but instead protect the content itself.

Ultimately, under international legal frameworks the decision of whether content is forced to be taken down through legitimate government action is a question of *policy* and it is not clear why this policy question should be shifted in favour of a technological solution that is not easily subject to international legal protections.

Blockchain-based social networks

Related to the use of blockchains as a method of disseminating content is their use as distributed platforms that provide a means for individuals to exercise expression. Internet intermediaries, such as search engines and social media platforms, play a crucial role in enabling people around the world to communicate with one another. ARTICLE 19 believes that access using blockchain platforms should be subject to the same protections as other intermediaries.

Some existing use cases for blockchain social platforms include the SocialX and Steemit:

- **SocialX** ecosystem[64] proposes an elaborate structure which includes both the ability to interact on a platform via content and multimedia via the IPFS filesystem as well as engaging in microtransactions with a license management system. In order to moderate content, the SocialX system "will automatically decide which users are active enough to become moderators" to make them community managers and be able to judge content and issue warnings and ultimately ban users.[65] The platform incorporates a community-based voting system with rewards, although some users have greater voting weight than others based on whether they provide 'good' content (although it is not defined what 'good' content means).[66]

- **Steemit**,[67] on the other hand, rewards users who receive votes on their posts with an added rewards system. Steemit features a video platform, DTube, which runs using IPFS on the Steem blockchain database.[68] DTube advertises that "because of the decentralised nature of IPFS and the STEEM blockchain, DTube is not able to censor videos, nor enforce guidelines. Only the community can moderate content, through the power of their upvotes and downvotes."[69] However, downvotes only make content less visible, they do not actually remove the stored content. One of its founders claims that their policy is to 'downvote' posts of copyrighted or objectionable content, and that the procedure to block content on its site in response to orders would be to "disallow certain IPFS hashes from being played in [DTube's] player."[70] In practice, this may mean that the biggest file-hosting nodes on DTube would exercise power to block or censor content.

ARTICLE 19 has previously raised concerns that digital companies can often exercise undue discretion in content regulation.[71] For example, some actors might maintain 'blocklists'[72] of images, or rely on the requests of 'trusted flaggers' who are community members granted an elevated level of trust by the platform. The subjective nature of these lists and the appointment of individuals are also incorporated into blockchain-based platforms such as the aforementioned examples. As such, ARTICLE 19 recommends that

blockchain-based companies be transparent about their internal guidelines for the removal of content, and offer access to remedies for individuals who have content removed.

Another type of platform is the creation of secure communication systems over blockchain; one such project is Mainframe, which attempts to set up a method of secure communication, not unlike the mobile app Signal.[73] However, platforms like these, even though they are open-source, still require trust in the underlying codebase and platform.

ARTICLE 19's assessment:

- **Positive aspects**: Distributed social media actors endeavour to address some of the concerns of censorship that are present with traditional platforms and Internet intermediaries.

- **Negative aspects**: It is not clear that current proposed platforms are actually decentralised in practice. They still are designed by core groups that are deciding the governance of their platforms, and certain users in the platforms are elevated over others based on decisions and algorithms implemented by the platform. Hence, the issues of centralisation present with traditional platform intermediaries seem to simply be shifted to a different third party. To the extent that platforms use IPFS as a file-sharing protocol, they introduce the same challenges and risks associated with use of the protocol, including legal liabilities for objectionable content stored on the platforms.

Use case: authentication

Since blockchain is a means of validating data, one of its natural implementations is the authentication of various forms of information. These use cases are examined below.

Authentication of individuals

One proposed use for blockchain is for the authentication of individuals through the use of 'ID tokens' which assign unique identifiers to individuals through which they can verify their identities. Identity is vital to participate fully in digital society. However, designed and implemented unchecked, digital identity technologies could have adverse consequences for the most vulnerable populations, particularly in terms of surveillance.

State identification

The importance of legal identity has been recognised by international bodies.[74] "Legal invisibility" is a major problem for various groups, placing them at risk of discrimination and exploitation, such as migrants often given fake ID documents for transport across borders, or people without proof of identity.

Some argue that the decentralised nature of blockchain can provide a remedy to this by granting individuals with "self-sovereign identity" where they are the ones to create and register identity and the only ones to control what to do with it and with whom to share it.[75]

One use case of identity blockchains in the humanitarian context is the implementation by the World Food Programme (WFP) of "Building Blocks" which helps WFP distribute cash-for-food aid to over 100,000 Syrian refugees in Jordan.[76] Individuals scan their irises to pay for goods at a supermarket, and those records are compared against a UN database. However, the database is a permissioned one, such that WFP still acts as a central intermediary and "the project's scope and impact are narrow . . . [s]o narrow that some critics say it's a gimmick and the WFP could just as easily use a traditional database." [77]

The pervasive problem of child trafficking in Moldova led UNOPS, in conjunction with the World Identity Network (WIN), to launch a call for proposals, "Blockchain for Humanity", with the aim of implementing a pilot initiative to use blockchain technology to combat child trafficking in the country.[78] ConsenSys, a US-based company, won the contract, and Moldova plans to launch a pilot of a digital identity project which would require children attempting to cross the border to scan their eyes or fingerprints, automatically notifying their legal guardians via phone.[79] The proposed benefit of blockchain is that the immutability of entries will make it impossible to change entries using bribes, and that biometric data cannot be lost or guessed. At the same time, it is unclear how the data of the children will be secured 'off-chain' or how access rights will be managed. Additionally, the interfaces used to connect to the blockchain world are also vulnerable to hacks or code flaws.[80] Anti-trafficking groups are sceptical whether plans like this will actually help the majority of victims, largely due to accessibility issues. Even ConsenSys, the company implementing the Moldova project, speaks with caution about the potential of these systems to be used for surveillance.[81]

At the same time, self-sovereign identity isn't a silver bullet, and if we don't build it carefully, malicious actors could still capitalize on it as an element of control. Blockchain identities have, for the most part, remained pseudo-anonymous, from which real-life identities could be extracted given the transactional behavior of the agent under investigation. If blockchain architects aren't careful in the way they align transaction permissions and public/private state variables, governments could use state-sponsored machine learning algorithms to monitor public blockchain activity and gain insight into the lower level activity of their citizens.

In the field of "know-your-customer" and fraud prevention, one project, Civic, endeavours to use blockchain to "secure and protect personal information transfer" in order to create a "decentralised identity ecosystem."[82] On this platform, users create virtual identities and store it on a device, so that the identity can be verified in later transactions and mitigate the problem of identity fraud. However, it is unclear what platforms such as these do in the event that individuals lose access to their device, or if another individual gains access to their device.

In the event that identification information is stored or referenced on the blockchain, then it is critical which methods are used to protect that identification information. Presumably blockchain-based identities will not be public, which would introduce privacy and surveillance risks if a database of individual IDs (particularly children) were completely available in the clear online.

ARTICLE 19 also notes that hacks and leaks of sensitive personal data happen daily. So the next alternative is that the information is encrypted, or that a digital fingerprint or 'hash' serves as a link to content stored in the blockchain. However, there are questions such as who maintains access to that data; or what happens if individuals lose their password or other means of accessing the data, and hence cannot associate their real self with their digital identity. Similarly, it is not clear what would happen if, due to a data breach, these vulnerable populations have now lost the privacy. It is not clear if some third party or the state would retain a backup mode of access; and if data is stored off-chain, how this is different to a decentralised system.

ARTICLE 19's assessment:

- **Positive aspects:** Verification of identities is an important objective for the realisation of many rights, and empowering individuals to assert control of their own data is a legitimate end. It is positive that entities in the private sector are incentivised to attempt to address some of the problems created by "legal invisibility".

- **Negative aspects**: The objective of creating verifiable legal identities is a practical response to the problem of "legal invisibility", although it is unclear whether this problem requires a technological solution. For one, proposing registering individuals in a blockchain database necessarily assumes those individuals are a) known to whatever registering body and b) have access to the technology to be registered. But where individuals are unknown, the problem of how they become registered in the first place remains.

The immutability of blockchain presents a unique problem with ID tokens in that once individuals input data in the blockchain, it is unclear how that data is changed; for instance, in the case of transgender individuals who may not wish for an immutable copy of the incorrect gender to be stored in the blockchain. Or, there could be an error in inputting data, such as an incorrect birth date or other biographical information. This raises a question, as an initial issue, whether it is a *good thing* for identification data to be immutable. Finally, in the event that individuals lose or forget their means of access to these databases, there should be fail-safes to ensure that those individuals are not prejudiced. Once these fail-safes are introduced, however, it is unclear how blockchain-based systems offer any unique benefit.

Voting and democratic participation platforms

The right of every citizen to participate in government through free and fair elections is well established under international human rights law. Free and fair elections are a crucial component of civil and political rights. Indeed, it is impossible to conceive of people exercising their democratic aspirations without effective participation in the electoral process. Respect for human rights, including the freedoms of expression, is central to an effective electoral exercise.

The identity verification applications of blockchain have been proposed to issue tokens for voting purposes and were even recently used in a number of countries.[83] Many attempts are being made to introduce blockchain-based voting around the world, using systems such as Votem, Democracy Earth, and Smartmatic, attracting interest from governments.[84]

However, critics point to problems with this approach, arguing that the application of blockchain is unnecessary and only introduces new possibilities for disenfranchisement and security risks, particularly with respect to vulnerabilities in the mobile devices used to access the blockchain.[85] The security concerns surrounding client software further include ghost clicking, malware, and 'man-in-the-middle' attacks; hence there is no implementation that satisfies all the criteria of free and fair elections any more effectively than existing methods.[86]

In the case of decentralised voting, the introduction of blockchains may bring additional vulnerabilities into the process that did not exist before. The main issue with blockchain-based voting models is that the interface between the user and the blockchain is vulnerable to interference — in the case of the Voatz system, it "isn't so much a blockchain-based app as it is a mobile app with a blockchain attached," and hence the information still travels over the Internet making it vulnerable to interference.[87] Matt Blaze, a cryptography and security expert at the University of Pennsylvania, offered strong words:

> So seriously, stop this crap. Elections matter. The requirements for elections have literally evolved over centuries of democracy. Voting is not a testbed application for your too-clever-by-half startup idea.[88]

In the case of voting, the basic assumption of blockchain - lack of trust between parties - could mean that fundamental social institutions have failed, namely because elections do require trust in a central authority such as an election commission.[89] Further, as with the case of digital identities, there are risks that a voter could become disenfranchised simply by losing a digital voting key through a damaged hard drive. The existing blockchain "solutions," are partially centralised in order to guard against malicious interference, naming a consortium of bodies such as universities, NGOs, and government bodies to serve as validators, making the platforms look more like a permissioned blockchain.

Blockchain-supported voting only shifts existing problems with voting to different layers. In particular, the transparency characteristic of blockchain poses problems in that individuals should not be able to view votes counted in real-time during an election, which would put different voters on unequal playing fields depending on what time of day they voted; however, if it is required that votes are counted transparently in real time, then this relies on a central body to do so, which negates the reason for having a blockchain system in the first place.

ARTICLE 19's assessment:

- **Positive aspects:** Potentially, blockchain technologies could offer solutions to certain problems in the current forms in which election take place, such as security breaches, corruption or fraud.

- **Negative aspects**: These systems raise numerous problems at a fundamental level: they propose to shift trust from the state to the third parties implementing these systems. This could invariably have the effect of undermining trust in institutions. Furthermore, there may be instances where there is value in a centralised actor retaining some form of backup access, i.e. in the event where individuals lose their credentials, pass away or are injured and cannot input biometrics and the like. However, such measures defeat the purpose of a blockchain-based approach.

Therefore, it is unclear how these proposals represent a shift to a 'trustless' system. They appear rather to re-shift responsibility from institutions accountable under international law to actors that may not be trustworthy at all.

Authentication of content (digital notarisation)

Blockchains have important uses for authentication of content. Due to their immutability, blockchains can be used to create a contemporaneous record of an event or of the production or acquisition of information. The OpenTimestamps project attempts to serve as a 'digital notary,' using the blockchain to prove that data existed prior to some point in time.[90] This system has many potential applications.

For example, the Guardian Project, a non-profit which creates secure apps for activists, journalists, and humanitarian organisations, has a project called ProofMode for smartphones which cryptographically signs photos and videos taken at the time of capture, and is compatible with digital notarisation.[91] This feature allows the authenticity of the media for evidentiary value, and various characteristics (such as time and location of capture) to be later verified. By analogy, it would be similar to posting a photo immediately to Twitter to be able to later show that the photo existed on that date, although the distinction is that Twitter (and any search engine which takes a snapshot of Twitter) are intermediaries which are theoretically subject to censorship or takedown.

Systems such as these can be used to establish ownership of content for copyright purposes, whereby individuals could create timestamps to prove creation at a certain date and potentially limit the need for intermediation. This could hypothetically reduce the need for notice-and-takedown procedures.

There are some systems proposed for management of digital rights which could maintain chain of title and help track and administer IP.[92] ARTICLE 19 previously noted that notice-and-takedown procedures are vulnerable to abuse and can lead to censorship by intermediaries as the burden often shifts to users who may have limited resources to prove that they have the right to disseminate content.[93]

ARTICLE 19's assessment:

- **Positive aspects**: The use of authentication tools for human rights investigators and defenders could be a valuable resource in documenting and disseminating evidence of rights abuses. States do have an obligation to provide access to accurate, reliable and understandable information, including on matters of public interest, such as in cases of natural disasters or in early warning systems. Digital notarisation could be a method for verifying that information is indeed coming from a state actor.

- **Negative aspects:** While digital notarisation promises a form of authentication with significant evidentiary value, this potentially raises the bar too high in attempting to standardise a burden of proof that may not be practically accessible to individuals in many situations. The issue of verification of content should not be expanded to a bigger issue than it is, and it is unclear whether technical solutions will be acknowledged and accepted by judicial bodies. Furthermore, digital notarisation may be subject to abuse, in that malicious actors could attempt to authenticate false content in an attempt to increase its legitimacy. Although online misinformation tends to have little impact on the public, the push by states and private companies to regulate 'fake news' and disinformation has deleterious consequences for freedom of expression.[94] Similarly, private actors or states must not limit the dissemination of digital content simply based on it not being digitally notarised.[95]

Use case: personal data and storage of identity-linked information

Since blockchain is in essence a way to securely store data, some applications have proposed to use blockchains to store records about individuals in a secure manner where the dissemination of those records can be kept in the control of the user. This application is related to the use case of authentication of individuals in the identification context. However, some current proposed uses for data storage include using blockchain to store medical records, which introduces challenges of its own, including, as one researcher notes:[96]

> The lack of boundaries within this schema is also reason for concern with regards to confidential information. Despite robust encryption and other security measures, we have witnessed the proliferation of data breaches that would never occur if the information was simply collected by the one entity that needs it and stored in one locked cabinet, or on an offline hard drive.

Indeed, keeping data on the blockchain presents many risks, including the possibility that future technological advancements, like quantum cryptography, may later be able to decipher information that is considered cryptographically secure today.[97] This could, in the future, jeopardise the security of information that is trusted to be safely stored at present.

ARTICLE 19's assessment:

- **Positive aspects:** ARTICLE 19 believes that keeping control of personal data in the hands of individuals, including the disposition and permissible recipients of that data, is an important goal.

- **Negative aspects:** The immutable nature of blockchain means that once data is stored on-chain, it cannot practically be deleted or modified. Perhaps an encryption access permission could be revoked, but that does not remove the possibility that at some point the information could be hacked should technology become more sophisticated.

To the extent that personal data is not stored on the blockchain (i.e. 'off-chain') but just a digital signature used to reference content elsewhere, this raises questions as to the security and centralisation of the data stored, who is accountable for it, and what remedies an individual possesses with respect to that data.

Use case: cryptocurrencies

Blockchain technologies provide a method of remittance that allows for pseudonymous transactions. This can implicate abuses of freedom of expression, particularly where these technologies are used as a tool for government control.[98]

Although there is a growing number of use cases for implementation of state-backed cryptocurrencies or blockchains used for remittance,[99] generally, government attempts to block crypto exchanges are associated with attempts to seize control over the Internet and the activities of individuals online.

While this is a relatively new phenomenon, ARTICLE 19 has studied it in the case of Iran which banned Telegram and its associated cryptocurrency.[100] Telegram app long posed a threat to the government's control over Iran's communications and information. With the announcement of Telegram's cryptocurrency authorities saw it as a further disruption for Iran's banking sector. In April 2018, the secretary of Iran's Supreme Council of Cyberspace declared Telegram's cryptocurrency would "ruin Iran's economy," and would be "blocked at any moment."[101] The government's sensitivity towards cryptocurrencies surfaced with the continued deterioration of the economy and currency crisis. In May 2018, following the announcement of the withdrawal of the United States from the nuclear deal, and the reintroduction of sanction, drastic depletion of financial transactions from the state controlled national currency was met with censorship of all cryptocurrency exchanges. On 27 August 2018, the Central Bank of Iran confirmed they are developing a Rial-backed national cryptocurrency; the Supreme Council of Cyberspace confirmed this decision by announcing that they would likely lift the ban on cryptocurrencies, such as Bitcoin, by the end of September 2018.[102] The national cryptocurrency has already been likened to Venezuela's project Petro, which was also used to counter massive inflation in the country, though it has been largely seen as a failure.[103]

It seems government policies to allow access to cryptocurrencies are very much tied to the control they can exert over the space, which might serve to undermine their stated project of aiding the economy, and ultimately merely keep track of the nation's monetary traffic rather than strengthen it.

ARTICLE 19's assessment:

- **Positive aspects**: The ability to transfer currency pseudonymously provides a means for individuals to engage in transactions outside of the sphere of government monitoring or interference, particularly if those transactions involve expressing political support. In particular, the possibility of micro-transactions may allow individuals to more easily access copyright or other goods that may have been less accessible previously.

- **Negative aspects**: Anonymous transfers of currency could be associated with content that can be legitimately restricted under freedom of expression standards.

Conclusions and recommendations

The potential use cases for blockchains that impact freedom of expression are already diverse. Time will likely reveal more. Because blockchains are tools through which individuals can exercise the right to freedom of expression and other human rights, these technologies are subject to and must be examined through the lens of human rights law.

To the extent that blockchain involves connectivity to the Internet and the use of encryption technologies, ARTICLE 19 reiterates that states have obligations to protect and promote the right to freedom of expression. Therefore, any restrictions on those technologies must conform to international law. Similarly, private actors that serve as intermediaries to access blockchains, whether they serve as developers, implementers or node operators, have obligations to promote freedom of expression. By extension, the duties of intermediaries in the Internet context apply in the blockchain context. Coders and implementers of technologies should ensure that their technologies are designed in a way that takes into consideration human rights.

The enthusiasm and economic investment directed at blockchain presents exciting opportunities for civil society actors. However, it is important to be mindful of the additional risks that introducing technological solutions may impose, and whether technological solutions are necessary in the first place.

Blockchain requires a shift in trust from traditional institutions to code and the private actors that are providing technologies. The individuals expected to place trust in code and their implementers generally may not have the sophisticated technical background necessary to properly understand or scrutinise them. In the case of public blockchains, individuals still need services to connect to and interact with blockchains unless they setup nodes and run software themselves, the bar for which is excessively high. The presence of these third parties to access blockchain services - whether they be software, websites, or browser extensions - means that users are placing trust in entities that may or may not be trustworthy. This raises significant questions with respect to security and governance; in particular questions such as how these actors are made accountable, how these actors are made to respect international norms, and how user interfaces like mobile phones are

properly secured. Furthermore, the shift in trust may erode the role of existing structures for trust-assurance, such as states and international bodies, which play vital roles in international governance. These proposals must be deeply and critically examined.

Accessing blockchains may introduce security risks. Most users - unless they possess technological sophistication - are likely to use some intermediary in order to access the technologies, whether these are mobile applications, browser extensions, or third party actors. These points of access introduce vulnerabilities: phones and computers can be hacked or stolen, and third parties can be compromised.

From the perspective of digital literacy and access, in some parts of the world where it is more difficult to operate nodes due to by virtue of Internet connectivity occurring primarily via mobile devices, then it follows that there would be some communities that are underrepresented in the overall operation of the network, and who are not involved in the validation of content that could nevertheless impact them.

Finally, the characteristic of immutability of public blockchains is a dual-use quality with both positive and negative implications. While many proponents of these technologies point to the immutability of blockchain as a net benefit for freedom of expression, we note that there are instances where it may be necessary to limit expression where the purposes are legitimate under international law and done pursuant to independent courts or adjudicatory bodies. Notably, this would be in cases where platforms are used for the storage or dissemination of content that violates international law. In this respect, blockchain technologies may pose challenges for the ability of states to exercise their international legal obligations. Censorship-resistance on its own does not guarantee the protection of freedom of expression and compliance with international standards.

Recommendations

In light of the foregoing, ARTICLE 19 suggests that stakeholders should adopt a human rights-based approach to blockchain technologies. In particular, we make the following recommendations.

To states

- States' obligations to respect, protect, and fulfil human rights, including online, extends to the public's right of access to blockchain technology. Hence, any restrictions on blockchain platforms, or intermediaries that provide blockchain access, must be necessary, proportionate, and subject to independent judicial review.
- States should ensure that providers, coders, and implementers of blockchain platforms are in principle immune from liability for third party data stored on those platforms when they have not been involved in in storing the content in question.
- States should refrain from measures such as shutdowns on Internet access or restrictions on the encryption technologies that underpin blockchains, particularly through the inclusion of encryption 'backdoors,' as these measures represent disproportionate interferences with the right to freedom of expression.
- To the extent that states use blockchains to store data of citizens or public records, states should ensure that they adhere to international human rights principles on access to information and data protection.
- When coordinating among stakeholders to standardise and implement blockchain technologies, states should ensure that human rights norms are among the key considerations in these partnerships, and that civil society is included in any strategic planning.

To private actors in the digital sector

- Companies, coders and implementers of technologies should ensure that their technologies are designed in a way that takes into consideration the rights to freedom of expression and privacy.
- Companies should ensure that deployment of blockchains is done after careful considerations of all risks, including security and impact on users, and match between blockchains' specific benefits and use cases that enable realisation of these benefits.
- As crucial intermediaries, companies that provide private blockchain platforms for dissemination or storing of content should be transparent

about any internal guidelines for the removal of content in blockchains, where content removal is feasible, as well as the appointment of moderators or validators with authority to flag or censor content. Companies should also provide notice and access to a remedy for individuals who have had their content removed.

- Coders and implementers of technologies should ensure that their governance includes a diverse array of voices, including members of civil society, and that non-private platforms are accessible to a plurality of audiences.

To all stakeholders

- States, private sector and all other stakeholders, should carefully consider the implementation of blockchain technology; in particular:
    - Whether the issues they are seeking to address do in fact require a technological solution, whether these issues could not be better remedied through a social solution or whether other existing technologies could suffice; and more specifically, whether they specifically need an immutable database distributed across multiple servers;
    - Where is trust being placed: whether it is in the coders, the developers, those who design and govern mobile devices or apps; and whether trust is in fact being shifted from social institutions to private actors. All stakeholders should consider what implications does this have and how are these actors accountable to human rights standards;
    - Operational issues, such as what happens if individuals lose passwords or the means of access;
    - Whether the new technology will be practically accessible and subject to governance that respects human rights norms, or whether its implementation will be concentrated among a core group of developers or third parties;
    - Whether the adoption of technologies exposes them to legal liability if malicious actors misuse the technology for objectionable purposes;

- Whether there is potential that an individual may - at some point in the future - require recourse or redress with respect to the information immutably encoded in the blockchains, and how this redress will be realised.

- Civil society should strive to engage with private actors, coders of blockchain technologies, and states, to ensure that international human rights norms are considered and incorporated in the development and implementation of new technologies and consider the impact of these technologies on human rights of beneficiaries in their projects.

About ARTICLE 19

ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19), is an independent human rights organisation that works around the world to protect and promote the rights to freedom of expression and information. It takes its name and mandate from Article 19 of the Universal Declaration of Human Rights which guarantees the right to freedom of expression.

ARTICLE 19 has produced a number of standard-setting documents and policy briefs based on international and comparative law and best practice on issues concerning the right to freedom of expression. Increasingly, ARTICLE 19 is also examining the role of international Internet technical standard-setting bodies and Internet governance bodies in protecting and promoting freedom of expression.

If you would like to discuss this report further, or if you have a matter you would like to bring to the attention of ARTICLE 19, you can contact us by e-mail at digital@article19.org.

Endnotes

1. B. Ivancsics, Blockchain in Journalism, Columbia Journalism Review, 25 January 2019.
2. Please note that this simplistic analogy does not consider the way that Wikipedia itself is also decentralised through content delivery networks and mirroring.
3. C.f., e.g. W. Al-Saqaf & N. Seidler, Blockchain technology for social impact: opportunities and challenges ahead, Södertörn University, November 2017.
4. For more information about Civil, see https://civil.co/.
5. Economic models for sustaining journalism are not examined as part of this report.
6. Blockchain standards are currently being developed by ISO and standardisation is being considered by the European Union ITU-T (see ITU Blockchain standards) as well as by the IEEE.
7. European Parliament, Resolution Blockchain: a forward-looking trade policy, 2018/2085(INI), 13 December 2018.
8. Ibid.
9. UNECE Executive Committee, Briefing note on Blockchain for the UN Sustainable Development Goals, ECE/TRADE/C/CEFACT/2018/25, 20 April 2018.
10. UN News, UN chief pushes for greater benefits from new technology, as he launches digital experts panel, 12 July 2018.
11. European Commission, EU Blockchain Roundtable paves the way for Europe to lead in blockchain technologies, 20 November 2018.
12. V. Lehdonvirta, The blockchain paradox: Why distributed ledger technologies may do little to transform the economy, Oxford Internet Institute, 21 November 2016.
13. Like traditional hard currency, a cryptocurrency is finite because each "coin" is created out of the same chain. So while the coins are distributed assets they are all connected.
14. While DLTs generally are receiving significant attention for their potential applications in various sectors, this report primarily focuses on blockchains as their unique qualities raises novel questions relevant for freedom of expression.
15. UK Government Office for Science, Distributed Ledger Technologies: beyond blockchain, 2016.
16. World Bank, Brief, Blockchain & Distributed Ledger Technology (DLT), 12 April 2018.
17. Google, Building a better cloud with our partners at Next '18, 23 July 2018.
18. S. Lee, Blockchain Smart Contracts: More Trouble Than They Are Worth?, Forbes, 10 July 2018.

19. In the case of private blockchains, some of these characteristics may be modified depending on the restrictions of implementation and access placed by the underlying network operators.

20. V. Buterin, Privacy on the Blockchain, Ethereum Blog, 15 January 2016.

21. UN General Assembly Resolution 217A(III), adopted 10 December 1948.

22. GA Resolution 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.

23. See, Article 10 of the European Convention on Human Rights, Article 9 of the African Charter on Human and Peoples' and Article 13 of the American Convention on Human Rights.

24. Human Rights Committee (HR Committee), CCPR/C/GC/3, adopted on 12 September 2011.

25. Ibid, para 12.

26. Ibid, para 17.

27. 2011 Report of the UN Special Rapporteur, A/HRC/17/27, 16 May 2011, para 3.

28. See ARTICLE 19, Policy Brief, Right to Online Anonymity, June 2015, p. 10.

29. C.f., e.g., Report of the Special Rapporteur on FoE, David Kaye, A/HRC/29/32, 22 May 2015, paras 12,16 and 56; or Special Rapporteur on FOE for the OAS, Freedom of Expression and the Internet, 31 December 2003.

30. HR Committee, Velichkin v. Belarus, Comm. No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

31. HR Committee, General Comment 16, 1988, UN. Doc. HRI/GEN/1/Rev.1 at 21 (1994), para 84.

32. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

33. Guidelines for the Regulation of Computerized Personal Data Files, G.A. Res. 45/95, 14 December 1990.

34. Commonwealth Secretariat, Model Data Protection Act, 2002.

35. ECOWAS, ECOWAS Telecommunications Ministers Adopt Texts on Cyber Crime, Personal Data Protection, Press Release No 100/2008, 16 October 2008; or Organisation of Eastern Caribbean States Privacy Bill (Proposed draft), April 2004.

36. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, ETS 108, 1981.

37. For more information, see EU General Data Protection Regulation

38. See, e.g. European Union Blockchain Observatory & Forum, Blockchain and the GDPR, November 2018.

39. WSIS, Declaration of Principles, Building the Information Society: a global challenge in the new Millennium, WSIS-03/GENEVA/DOC/4-E, 12 December 2003.

40. WSIS, Tunis Agenda For the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005, para 34.

41. Committee of Ministers of the Council of Europe, Declaration by the Committee of Ministers on internet governance principles, 21 September 2011.

42. See, e.g. Report of the Special Rapporteur on FoE, 11 May 2016, A/HRC/32/38.

43. For example, the W3C has made web payments a priority, see, W3C, Web Payments at W3C; https://www.intgovforum.org/multilingual/content/igf-2018-ws-256-is-blockchain-the-right-technology-for-you

44. Guiding Principles on Business and Human RightsGuiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex, in particular Principle 15.

45. Report of the Special Rapporteur on FoE 16 May 2011, A/HRC/17/27, paras 75-76.

46. The May 2016 Report of the Special Rapporteur on FoE, op.cit., paras 40 – 44.

47. Ibid.

48. Ibid., para 43.

49. Ibid.

50. UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and ACHPR Special Rapporteur on Freedom of Expression and Access to Information (four FoE mandates), Joint declaration on freedom of expression and the Internet, 1 June 2011.

51. CJEU, Scarlet Extended SA v Societe belge des auteurs compositeurs et editeurs (SABAM), Case C-70/10, 24 November 2011.

52. C. Cath, N. ten Oever & D. O'Maley, Media Development in the Digital Age: Five Ways to Engage in Internet Governance, March 2017.

53. Consensys, Blockchain Identities for Lost Citizens, 19 January 2018.

54. C.f. consumer vulnerability has emerged as one of the key areas of focus for regulators and consumer protection in financial sector.

55. L. Mearian, Solving a blockchain conundrum: Biometrics could recover lost encryption keys, Computerworld, 17 May 2018.

56. D. Babayan, Real Reason Why China Doesn't Want Blockchain: Strict Censorship, News BTC, 22 October 2018.

57. C. Cath, N. ten Oever & D. O'Maley, op.cit.

58. N. Roubini, Blockchain isn't about democracy and decentralization - it's about greed, The Guardian, 15 October 2018.

59. M. Bartoletti & L. Pompianu, An analysis of Bitcoin OP_RETURN metadata, February 2017.

60. S. Singh, Blockchain Is Helping to Circumvent Censorship in ChinaBlockchain Is Helping to Circumvent Censorship in China, Slate, 18 July 2018.

61. For more information, see Protocol Labs, IPFSIPFS.IPFS

62. S. Armstrong, Catalonia plots digital government in exile in bid for independence, Wired, 9 October 2017.

63. IPFS, Uncensorable Wikipedia on IPFS, 4 May 2017.

64. For more information see SocialX. Steemit

65. SocialX, Whitepaper, Draft 1.0, p. 34.

66. Ibid. p. 36.

67. For more information see SocialXSteemitSocialXSteemit. Steemit

68. J. Alexander, Controversial YouTubers head to alternative platforms in wake of 'purge', Polygon, 7 March 2018.

69. For more information about D.Tube, see About DTubeAbout DTube.About DTube

70. Reddit, Comments: How will this deal with copyright? or About dTube?.

71. ARTICLE 19, Submission to the UN Special Rapporteur's consultation on online content regulationSubmission to the UN Special Rapporteur's consultation on online content regulation, December 2017.

72. These are also often referred to as 'blacklists' but ARTICLE 19 chooses to use the neutral term 'blocklist.'

73. For more information, see Protocol, Mainframe

74. See, e.g. the UN Sustainable Development Goals, Article 16.9.

75. See, e.g. WIN, UNOPS, Blockchain for Humanity Global Challenge, Turning Invisible Children into Invincible Ones 2018; or L. Orgad, Cloud Communities: The Dawn of Global Citizenship?, European University Institute, Working Papers, 2018/19.

76. R. Juskalian, Inside the Jordan refugee camp that runs on blockchain MIT Technology Review, 12 April 2018.

77. Ibid.

78. Results, Blockchain for Humanity Global Challenge, 2018.

79. U. Bacchi, Scan on exit: can blockchain save Moldova's children from traffickers?, Reuters, 18 June 2018.

80. C.f.Turning Invisible Children into Invincible Ones, op.cit., p. 19.

81. Consensys, Blockchain Identities for Lost Citizens, 19 January 2018.

82. For more information, see Civic, Decentralized KYC ServicesDecentralized KYC Services. Decentralized KYC Services

83. For example, a blockchain-based e-voting system for corporate shareholders was tested in Estonia in 2016 (and now the country has nationalised digital identities); see Is Blockchain the answer to e-voting? Nasdaq believes so, Market Insider, 23 January 2017. Local votes were counted in the Zug municipality Switzerland over blockchain in June 2018, see D. Meyer, Blockchain Voting Notches Another Success - This Time in Switzerland, Fortune, 3 July 2018. In the USA, West Virginia utilised limited blockchain absentee voting in November, 2018 elections, using a 'Voatz' system which collected 144 votes from overseas military personnel; see A, Wood, West Virginia Secretary of State Reports Successful Blockchain Voting in 2018 Midterm Elections, Coin Telegraph, 16 November 2018.

84. J. Dunietz, Are Blockchains the Answer for Secure Elections? Probably Not, Scientific American, 16 August 2018.

85. See, e.g. S. Hirst, Blockchain Based Elections? Security Researchers Say It's Too Soon, 3 October 2018.

86. G. van de Water, Blockchain Ballot: Electoral Enhancement or Danger to Democracy?, December 2017.

87. M. Orcutt, Why security experts hate that "blockchain voting" will be used in the midterm elections, MIT Technology Review, 9 August 2018.

88. Matt Blaze, Tweet, 2 June 2018.

89. R. Chirgwin, Australia Post says use blockchain for voting. Expert: you're kidding, The Register, 22 August 2016.

90. For more information, see Open Timestamps: a timestamping proof standard.

91. The Guardian Project, Combating "Fake News" With a Smartphone "Proof Mode", 24 February 2017.

92. J. Neuburger, Blockchain as a Content Distribution Technology: Copyright Issues Abound, 14 May 2018.

93. ARTICLE 19, Internet intermediaries: Dilemma of Liability, 2013.

94. ARTICLE 19, Free speech concerns amid the "fake news" fad, 18 January 2018.

95. Four Special mandates on FoE, Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, 3 March 2017.

96. J. Berger, Blockchain—Chock full of problems for medical data privacyBlockchain—Chock full of problems for medical data privacy, SJSU Blockchain Project Blog, 4 June 2018.

97. P. Domek, Digital Identity on Blockchain—Reinventing the Web of TrustDigital Identity on Blockchain—Reinventing the Web of Trust, 20 July 2018.

98. While we observe that cryptocurrencies may raise a number of issues, this analysis is focused on their freedom of expression implications.

99. For instance, the World Bank has supported Kenya in the development of a mobile-based bond issuance project called 'M-Akiba', which will assess the use of Blockchain technology to simplify the platforms used for the issuance and sale of bonds; see, e.g. FSDAFrica, The Story of Kenya's M-Akiba: Selling Treasury Bonds via Mobile, 11 May, 2018.

100. News circulated that Telegram would offer its own cryptocurrency, known as Telegram Open Network (TON), through its chat functionality and in Iran, this currency could potentially find a user base of over 40 million people who had integrated the platform into their daily lives. Some were using Telegram for financial matters already.

101. ARTICLE 19, Tightening the net: The internet in the time of currency crisis, October 2018.

102. The secretary of Supreme Council of Cyberspace: cyberspace must be nationalized by the year 1398/Telegram is a bandit, Arz Digital, 3 April 2018.

103. K. Moskovitch, Inside the bluster and lies of Petro, Venezuela's cryptocurrency scam, Wire, 22 August 2018.

DEFENDING FREEDOM OF EXPRESSION AND INFORMATION

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA
T +44 20 7324 2500 F +44 20 7490 0566
E info@article19.org W www.article19.org Tw @article19org Fb facebook.com/article19org