Political and Economic Implications of Blockchain Technology in Business and Healthcare

Dário de Oliveira Rodrigues
Instituto Politécnico de Santarém, Portugal

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

A volume in the Advances in Data Mining and Database Management (ADMDM) Book Series

Published in the United States of America by
IGI Global
Business Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Rodrigues, Dario de Oliveira, 1963- editor.
Title: Political and economic implications of blockchain technology in business and healthcare / Dario de Oliveira Rodrigues, editor.
Description: Hershey, PA : Business Science Reference, [2021] | Includes bibliographical references and index. | Summary: "This book provides relevant theoretical frameworks on the political and economic impact of blockchain technology, which is thought to be able to redesign human interactions concerning transactions"-- Provided by publisher.
Identifiers: LCCN 2021005801 (print) | LCCN 2021005802 (ebook) | ISBN 9781799873631 (hardcover) | ISBN 9781799873648 (paperback) | ISBN 9781799873655 (ebook)
Subjects: LCSH: Technological innovations--Economic aspects. | Blockchains (Databases)--Industrial applications. | Blockchains (Databases)--Economic aspects.
Classification: LCC HC79.T4 P649 2021 (print) | LCC HC79.T4 (ebook) | DDC 338/.064--dc23
LC record available at https://lccn.loc.gov/2021005801
LC ebook record available at https://lccn.loc.gov/2021005802

This book is published in the IGI Global book series Advances in Data Mining and Database Management (ADMDM) (ISSN: 2327-1981; eISSN: 2327-199X)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 1
Blockchanging Trust:
Ethical Metamorphosis in Business and Healthcare

Dario de Oliveira Rodrigues
https://orcid.org/0000-0002-2817-5115
Instituto Politécnico de Santarém, Portugal

ABSTRACT

By cutting transaction costs and streamlining agreements' execution via "smart contracts," blockchain technology (BT) turns decentralization into an economic advantage and an antidote against politically harsh decisions that can obliterate privacy, freedom, and democracy. Although BT's ethical bottom line is still uncertain, its use can smooth out the trade-off between privacy and convenience, reconciling both. BT can also help reconfigure the compromise between intellectual property rights and the common good, opening more ethical routes to the diffusion of innovation. BT's data security can be translated into straightforward access to information. On the one hand, this signals new inclusion routes for "identityless" and unbanked people, and on the other, it releases society from biased information and fake news providing access to trusted data. BT guarantees contents precision, distributing a consensual tamper-proof "hyperledger" proving transactions' authenticity and data's integrity. As consensus should be plural, BT's decentralization is thought to be a must in ethical terms.

INTRODUCTION

"Technology is neither good nor bad, nor is it neutral" (Kranzberg, 1986). Kranzberg's First Law

This chapter's main objective is to show why an ethical reform can be expected in a *new normal* (Berwick, 2020; Tam, 2021) time of shaken confidence, perhaps even more shaken than in the last financial crisis (2007-2008). Hence, the ethical impact of Blockchain Technology (BT) on the *Cyberethics-mix* will be considered, entailing four fundamental ethical issues to cope with in the cyberspace: (i) *Privacy*

DOI: 10.4018/978-1-7998-7363-1.ch001

of Personal Data; (ii) *Property Rights on Digital Data*; (iii) *Possibility of Accessing Information*; (iv) *Precision of Digital Content* (Rodrigues, 2012).

BT is a data management technology (Alcazar, 2017, p. 93) for distributed databases, which can be seen as an institutional or social technology for coordination (Davidson et al., 2016; Swan, 2015) that creates a "secure, robust, and transparent distributed ledger able to leverage resources within a global peer-to-peer network by building algorithmic trust" (Narayan, 2020, p. 121442).

Seeking to understand the political-economic implications of a new trust mechanism underlying human transactions that it is thought will profoundly change society, this chapter relates Internet evolution with the referred four ethical issues, especially noting business and healthcare.

First, it should be mentioned that this chapter emphasizes the author's liberal perspective. The chosen investigation method was based on qualitative research, using the literature review research methodology, which is considered adequate to overview several thematic areas on a given topic. Among the literature reviews available, the most used for business studies are systematic review, semi-systematic review, and integrative review (Snyder, 2019). Considering the need to carry out a synthesis to envision the intended ethical repercussions of BT, the author used the integrative literature review, which is indicated to frame a study from new perspectives, especially when it comes to research themes and topics little explored (Torraco, 2005), as is the case as far as the author was able to observe.

This chapter is sequentially organized to accomplish four specific objectives. The first one is to shed light on the evolving trade-off between privacy and convenience, highlighting that BT's protocol makes it possible to overcome secular privacy limitations and emphasizing that its innovative features eventually can be restrained by misinformed or mistaken (to say the least) political decisions. The chapter's second specific objective is to observe the trade-off evolution or the changing compromise between self-controlling personal data and public interest. The chapter's third specific objective is to remark how BT can catalyze access to information and digital inclusion (*e.g.*, access to financial services), assuring information integrity and avoiding a silo mentality usually justified by privacy constraints. It is also discussed why BT is a double-edged sword, which also can reinforce data centralization and the lust for power, pushing society into a worrisome non-democratic path. The chapter's fourth and last specific objective is to highlight the ethical importance of content precision and accurate information in a time of fake news and political distrust, showing that BT can deliver transparency and trust, eventually inspiring the wake of a Truth Age. Finally, the author presents solutions and recommendations, observes some technical limitations, advocates research priorities, and concludes.

BACKGROUND

Business Ethics and Trust

Defining business ethics, Somerville & Wood (2008) pointed out that "[it] focuses on how we use and should use traditional ethical views to evaluate how institutions orchestrate human behavior" (p. 143). It is known that ethics focuses on studying human conduct, but when it has to do with business, it is also essential to assess how institutions impact humans. Hence, it is crucial not losing sight of what is next, considering that Blockchain Technology (BT) allows even strangers to transact without intermediaries.

The blockchain protocol, which is based on a set of cryptographic techniques, ignited a second phase of the Internet, the definitive "Internet of Value" (Twesige, 2015), a decentralized operating system

powered by BT that people can also use to transact value directly with each other and not only to share information as they did so far.

Enabled by blockchain technology, entrepreneurs and innovators have recognized the possibilities of creating an open financial system that has limited or no involvement from financial institutions. (…) Although this movement is still at its early stages, it showcases the potential of blockchain technology in spawning a new set of business models that are centered around decentralization and disintermediation. If this movement continues to gain momentum, it may start to disrupt existing industries and create new opportunities for entrepreneurship and innovation. (Chen & Bellavitis, 2020, p. 152)

It is known that decentralization avoids the vulnerability (*e.g*., hacker attacks) inherent to the "single points of failure" from which trust is often conveyed over a network (Liu et al., 2018). "[There is] no single point of failure [when] records are on many computers and devices that hold identical information" (Kshetri, 2017, p. 70). However, decentralization comes with a problem: the lack of trust resulting from eventual disagreements between parties on every transaction. During millennia, such mistrust has relegated peer-to-peer (P2P) transactions to the reliable but small context of a family or a local group of trusted friends (*e.g*., ancient tribes). Later on, such lack of trust was mitigated by relying upon trusted intermediaries, as will be seen next. Remarkably, this trust limitation was finally solved early this century (Nakamoto, 2008), with the invention of a new kind of trust based on consensus among peers.

As referred by Turkanović et al. (2018), "a blockchain node is any computer that has the core blockchain client installed and operates a full copy of the blockchain ledger" (p. 5115). The output of such ubiquitous data's replication is the so-called *distributed trust* (Bellini et al., 2020), which results from maintaining a unique, unmistakably, immutable, and verifiable timestamp of all transactions in a network, *i.e*., an "hyperledger" (Nakamoto, 2008).

No bonds nor trust between business parties are needed anymore for contractual ties being established and settled between strangers, which the continuous trade of cryptocurrencies has shown for more than a decade. This distributed trust is also of paramount importance when using self-executable contracts ("smart contracts") in blockchain networks such as Ethereum (Hartel et al., 2019). It is essential to understand that BT empowers the Internet both to share information and transact value peer-to-peer. In other words, data can now also represent digital assets on the Internet. Thus, it is thought that such tokenized data will change the world financially, economically, and politically (precisely in this exact order).

[Tokenization] is the process of converting a piece of data into a random string of characters known as a token. Tokenization protects sensitive data by [replacing it with] non-confidential data. The token serves merely as a reference to the original data, but cannot be utilized to determine those values. (...) tokenization in essence allows you to compartmentalize personal data and manage them across different users simply and effectively. That data can therefore only be accessed by an entity who has the correct token. The information is secure and completely portable since the personal data is controlled by the individual and shared with permission, a stark difference to data that are being utilized currently. (Morrow & Zarrebini, 2019, pp. 221-222)

It is not surprising that BT's first application has been a cryptocurrency. Bitcoin has attracted attention and led to financial speculation, eventually distracting people from BT's true meaning, which is no less

than altering the genesis of trust. Hence, the general understanding of what it can represent politically and economically was postponed.

The real promise of BT, then, is not that it could make you a billionaire overnight or give you a way to shield your financial activities from nosy governments. It's that it could drastically reduce the cost of trust by means of a radical, decentralized approach to accounting—and, by extension, create a new way to structure economic organizations. (Casey & Vigna, 2018, p.5)

BT's adoption brings a change in trust's very genesis (Casey & Vigna, 2018). This change is significant because "systems that alter the scope of trust change society" (Werbach, 2018). Before this technology was known, there were only three types of trust available:

1. Trust between peers (Schneier, 2012): held between family and friends, it is a kind of tribal trust only useful among groups with less than 150 individuals (Dunbar, 2010).
2. Confidence in the "rule of law": based on the social contract between the individual and the nation-state, giving the latter the institutional power to enforce agreements (Hobbes, 1914).
3. Trust in intermediaries: based on the dependence on centralized entities, like banks, that manage the trust necessary to ensure the smooth running of transactions (Datta & Chatterjee, 2008).

Nowadays, a fourth type of trust becomes available: *distributed trust.* As stated by Werbach (2018), "Bitcoin's blockchain mechanism just might have launched a revolution in trust." (p. 17). Over more than 30 years, the world witnessed the exponential growth of information shared by Internet users who have emancipated from traditional media thanks to a vibrant social media ecosystem. Social networks, blogs, and other applications (e.g., torrents) enabled social media and P2P sharing information. Drawing a parallel with the onset of the Internet's first economic media (social media), one can consider that humanity is now entering the second phase of the Internet, the moment in time when users started to carry out transactions with each other due to the onset of another economic media: the digital money (Beller, 2020). Thus, conveying both economic media when it encompasses information and money for the first time, the Internet contemplates both types of value (use and exchange value), becoming either ground-breaking or disruptive and entailing several ethical consequences.

Economic thinking has long distinguished "value-of-use" from "value-of-exchange" (Smith, 1937). "[Value is a word that] has two different meanings, and sometimes expresses the value of [using] some object, and sometimes [expresses] the power of purchasing other goods that the possession of that object conveys" (Smith, 1989, p. 47). In its first phase, the Internet's usefulness resulted from sharing information between users at a level never seen in human history. This sharing of information, nowadays mostly done through the services of a few giant multinationals (e.g., Facebook) that concentrate user's data and effectively control the Internet (Lopez et al., 2019), has made the *Internet of Information* an instrument of choice to provide a kind of value that users could not sell but have been using to fulfill human affiliation and self-esteem needs (Maslow, 1943). Significantly, during this process, users' data have been captured and *monetized* by digital media intermediaries who have obtained an enormous economic advantage in capturing the value of data extracted from users (Lopez et al., 2019). So, the product sold by Facebook to third parties has been precisely the same one that users have not been able to monetize themselves. Although this limitation is still endured on the Internet by billions of people, it is already

technically solved, and things will probably be very different in the more or less near future, hopefully for the best if ethics, privacy, and freedom prevail.

Empowered by BT, the Internet entered the second phase of its existence. This second phase is also the last because there are only two types of economic value, and both are now served as economic media on the Internet: social media and digital currencies. Hence, besides sharing information, users can now directly trade digital assets on the Internet, transacting data with each other in the absence of intermediaries. In other words, the Internet is becoming an instrument of choice to decentralize data, democratize trade and let payments be made directly among users (P2P). As stated by Bergeron et al. (2020), "the blockchain is a brilliant concept for democratizing currency exchange and has been fully realized in many cryptocurrency implementations" (p. 51). Thus, according to several authors (Antonopoulos, 2017; Tapscott & Euchner, 2019; Visconti, 2020), this is the beginning of the so-called "Internet of Value" (IoV) where the middleman is not needed anymore.

Just like the internet that was introduced in the 1960s and late 1970s, is a communications protocol that governs the rules and regulations for information exchange over the network of networks, [blockchain] is a protocol that governs the rules and regulations for value exchange. One is the internet of information, while the other is the IoV. Internet is a communications protocol and Blockchain is value exchange protocol. With value being broadly defined. (Twesige, 2015, p. 3)

As the digital *copy-paste* procedure has no marginal costs, sharing data became a no-brain operation. Whoever shares digital information still will keep such's information utility, abdicating nothing. Therefore, digital sharing does not involve trust requirements (because there is no trade involved). On the other side, transacting is entirely different. Unlike sharing, trading implies giving up something and relying on the other parties' ability to respect deals. Transacting requires trust, which is equivalent to social capital, creating *reserves of goodwill* that facilitate business networking and optimize social relationships, thus increasing society's wealth (Werbach, 2018).

In the first phase of the Internet, the FTP-IP and HTTP protocols made it possible to democratize information sharing and bypass traditional media. Hence, the new digital media tycoons disintermediated the mass media sharing information process and re-intermediated it in an entirely new way. More recently, BT industrialized the generation of trust between peers (Berg et al., 2017), inaugurating an "Internet of Money" (Antonopoulos, 2016) and paving the way to democratize transactions, perhaps driving complete disintermediation of both economic media. If it is so, it is thought that this time things can change for good.

[Blockchain] could enable a new era of the Internet usage called the Internet of Value (IoV) in which any types of assets such as intellectual and digital properties, equity and wealth can be digitized and transferred in an automated, secure, and convenient manner. (Truong et al. 2018).

The same reasons that made and still make the internet a success, are the same ones that will make the Block Chain thrive. For example, its fast, public, open to anyone, cheap and easy to utilize, transparent and programmable. Just like how the internet made it possible to transfer information instantaneously from any part of the world, the Block Chain technology lets the users transfer value globally. (Twesige, 2015, p. 3)

It is thought that BT will be ubiquitous, and eventually, the IoV will notoriously impact society. After all, "if you look back at history, every time there was a big expansion in the world's economic activity, it was generally induced by the creation of a new form of trust." (Berg et al., 2019, p.4).

Concerning healthcare, it is thought that patient-centric applications powered by BT will play a decisive role in enabling more ethical healthcare businesses. Patient data is now "big data," and it turns out that BT allows a seamless health data integration without compromising security and confidentiality. Hence, BT can provide trust in real-time, data for predictive modeling and the generation of insights, ultimately improving patient involvement and satisfaction.

BT will reform the relationship with providers by offering solutions that safeguard data's integrity and privacy. Considering the current patients' inconvenience when accessing clinical data and health records, one can anticipate that BT will be highly transformative in healthcare. For example, in clinical trials, guaranteeing data's integrity is a fundamental professional and ethical obligation to protect patients and produce reliable results that can lead to new treatments and save lives. Observing the Estonian pioneer case, Heston (2017) stated that "the success of the Estonian medical record blockchain project will depend upon its ability to keep medical records private while at the same time widely available to medical providers [pharmaceutical companies,] and insurance companies.".

The world is witnessing a global implosion of trust with "public distrust of government, business, media, and NGOs" (Edelman 2017), and it is unlikely that the SARS CoVid-19 pandemic will contribute to reverse such tendency. Thus, trust is needed, and the author considers BT to be a game-changer in altering the rationale that justifies human conduct from an ethical point of view, implying a metamorphosis of the "cyberethics-mix" (Rodrigues, 2012). This ethical evolution will be covered in the following pages, just after a brief explanation of BT.

Blockchain Technology

On October 31, 2008, a white paper showed how to institute a protocol to distribute trust through a digital network (Nakamoto, 2008). This protocol is called *blockchain*, a set of cryptographic techniques that ensures data's authenticity, confidentiality, and integrity. The two former qualities are guaranteed by a digital signature system that uses a public and a private key mechanism called asymmetric encryption. It should be acknowledged that "encryption is said to be asymmetric because the key for encryption is different from the key for decryption (Martins, 2018, p. 24). Both keys only work in pairs: by signing a transaction with his private key, the sender guarantees data's authenticity as the recipient will only be able to decrypt data if he uses the sender's public key. In turn, by signing a transaction with the recipient's public key, the sender guarantees data confidentiality because only the recipient will be able to decrypt that data using his private key.

The digital signature system usually consists of two parts: a signature algorithm and a verification algorithm. The signature algorithm is used to generate a digital signature on the message, the signature is usually controlled by the signature key, the signature algorithm or the signature key is kept secret and is controlled by the signer. The verification algorithm is used to verify the digital signature of the message, and the message can be verified according to the signature effectively. The verification algorithm is usually controlled by the verification key, but the verification algorithm and the verification key are public, so the person who needs to verify the signature can easily verify it. (Zhai et al. 2019, p. 6)

Regarding the third quality of BT's protocol, data integrity, it can be guaranteed thanks to an algorithm called *hash*. The *hash function* transforms any data set, with variable size (there is a theoretical maximum size of 2'091'752 terabytes which in practice is unattainable), into a short sequence of characters with fixed size (a string of 256 bits in the case of bitcoin). Applying the hash function consecutively to a given data set whose integrity persists always results in the same hash string. It is easier to compare small sets of data, which means that comparing *hash values* is a safe way to check the data set's integrity without making exhaustive (perhaps unfeasible) comparisons. The *hash function* is not reversible, and even knowing the *hash value* of a given data set, there is no logical way to reconstitute that data set backward. Hence, the *hash function* allows both to safely check data's integrity and increase privacy concerning sensitive data (Nakamoto, 2008).

The hash algorithm is a function that maps a sequence of messages of any length to a shorter fixed-length value, and is characterized by susceptibility, unidirectionality, collision resistance, and high sensitivity. Hash usually used to ensure data integrity, that is, to verify the data has been illegally tampered with. When the data tested changes, its hash value also changes correspondingly. Therefore, even if the data is in an unsafe environment, the integrity of the data can be detected based on the hash value of the data. (Zhai et al. 2019, p. 3)

Therefore, blockchain cryptographic techniques guarantee data's authenticity, confidentiality, and integrity (Yaga et al., 2019), and blockchain-based decentralized distributed ledgers have shown to be viable (Berg et al., 2017). Hence, such *cryptographic cocktail* can be used for coordinating activity in a distributed economy (Davidson et al., 2016),

CYBERETHICS METAMORPHOSIS

Data Privacy

Privacy risks are associated with the uncontrolled disclosure of personal information (AICPA., 2020). The right to personal and family privacy has been considered one of the most fundamental rights of individuals. For decades it is consecrated as a human right (UN, 1948). The European General Data Protection Regulation also recognizes privacy as a right to which every person is entitled (GDPR, 2018). The philosopher Bertrand Russell (1931) considered that technology consists of a change from the contemplation of nature to its manipulation, and such a change carries risk (Marturano, 2002). Hence, given the extraordinary development of Information and Communication Technologies (ICT) and nowadays digital pervasiveness, it is understandable why privacy violation has become a preoccupying ethical concern.

ICT progress makes it necessary to employ fewer and fewer people in surveillance efforts, and limits to controlling citizens are no longer guaranteed by the numerical need to employ a significant part of the population in doing so, which opens the way for abuses and disproportionality in such monitoring (Brown & Korff, 2009). For this very reason, attacking the privacy of many people or even that of an entire population has never been easier than it is today. As Rodrigues (2012) pointed out, "it is important to mention the loss of some privacy as a tolerable downside of getting and securing a greater convenience [and] one could think that the fundamental ethical objective is to achieve a balance between the "need

to know" and the "right not to divulge" (pp. 329, 330). However, ICT progress aggravated the privacy loss, and it seems reasonable to ask whether the present trade-off is justifiable, for instance in healthcare.

Decades ago, before computers came into widespread use, IMS [(Intercontinental Medical Statistics)] field agents photographed thousands of prescription records at pharmacies for hundreds of clerks to transcribe—a slow and costly process. Nowadays IMS automatically receives petabytes (1015 bytes or more) of data from the computerized records held by pharmacies, insurance companies and other medical organizations—including federal and many state health departments. Three quarters of all retail pharmacies in the U.S. send some portion of their electronic records to IMS. All told, the company says it has assembled half a billion dossiers on individual patients from the U.S. to Australia. (Tanner, 2016, p.26)

Privacy on the Internet of Information

As mentioned above, the first phase of the Internet was characterized by the then-new and disruptive possibility of sharing information between peers. Some companies early recognized the inherent value of this new reality, namely the Internet's potential to increase the marketing benefits of personalized products and services and how new digital resources could facilitate the job (Kotler, 1999; Kotler et al., 2016). As stated by Rodrigues (2012), "the possession of detailed information about customers allows companies to create personal profiles that lead to a better service rendering. This way, companies can provide consumers personalized offers." (p. 330).

Understanding that the exponential progress of ICT has been changing the game rules, tilting the marketing playfield so much that privacy can be overturned, the author mentioned, still in 2012, the disadvantage for privacy resulting from using social networks:

It is crucial the professional commitment of those who are responsible for social networks, which must be governed by its own code of ethics and promote a self-regulation that encourages an ethical participation of all users. After all, without a moral responsibility capable of accepting the sacred nature of the right of individuals to the privacy of their private lives and to the information they wish will remain confidential, the business practice on the Internet will constitute a continuing threat from an ethical point of view, always subsisting the risk of someone invading the privacy of others. (Rodrigues, 2012)

Some years later, taking a notorious example of privacy loss, one can say that the indignation caused by the Cambridge Analytica & Facebook scandal was justified by the unexpected exposure of about 50 million Facebook users' profiles (Cadwalladr et al., 2018), showing how deceptive can be the use of personal data by third parties. After all, even with recent stringent data protection laws in Europe and the USA, namely the General Data Protection Regulation (GPDR) and the California Consumer Privacy Act (CCPA), many companies still feed their business models with personal data to sell advertisements (Lopez et al., 2020).

A documentary shown in 2020 by cable TV operator NETFLIX presented the pungent testimony of former employees of some of the leading ICT multinational companies, increasing the awareness of privacy issues by denouncing that social media users have their data processed by algorithms that feed ethically doubtful business models (O'Neil, 2017). As mentioned by Rodrigues (2020), "[whistle-blowers explained] that these gigantic multinationals use artificial intelligence and sophisticated algorithms to

become very rich, at an unprecedented pace, profiting from the emotions and opinions expressed by social media users."

According to Petrescu & Krishen (2020), such companies monetize personal information following "business models based on algorithms that encourage addiction and privacy breaches as features of social media platforms" (p.187). This encouragement can make sense from a business point of view, as it allows those digital platforms to make a strongly targeted segmentation of their users, increasing their appetite for specific ads. This because better-delineated segments are more valuable and reach higher prices for the advertising space disputed in online auctions. (Rodrigues, 2020).

To make things worse for users, there is a so-called privacy paradox identified by Barnes (2006), "according to which people often state to care about privacy, but at the same time freely relinquishes private information online" (Bleier et al. 2020, p. 26).

Known as the privacy paradox, it is a documented fact that users have a tendency towards privacy-compromising behavior online which eventually results in a dichotomy between privacy attitudes and actual behavior (…) Although users are aware of privacy risks on the internet, they tend to share private information in exchange for retail value and personalized services (Barth & De Jong, 2017, p. 1039)

This psychological vulnerability reaches worrying proportions in social networks. Ubiquitous digital platforms let users satisfy a long-time known hierarchy of needs (Maslow, 1943). Very profitable business models wisely predict that users do not need to be compensated for their loss of privacy other than by obtaining successive opportunities to climb a hierarchy of needs whose top is unreachable (King, 2009).

Instead of working to decrease consumers' privacy concerns, firms might therefore also aim to attenuate the negative effects of such perceptions by providing increased value in exchange, for instance through better service or lower prices - although that is admittedly tough if the price is already zero. (Bleier et al. 2020, p. 26).

For users, the trade-off is losing privacy in exchange for a so-called "better service." However, that service seems to have a never-ending exchange value, namely because users cannot monetize (and so, cannot perceive) the value of the data they give in exchange for losing privacy. Hence, monetizing data has been an extremely profitable business, especially for some ICT multinational companies (*e.g.*, Facebook) that set up an oligopoly or even a monopoly since "they grow very fast and that, in the end, often one winner remains" (Van der Aalst et al. 2019). Also, Taplin (2017) stated that this kind of business model seems to collide with privacy, freedom, and democracy.

As will be seen in the next sections, such an ethically reprehensible business reality can now change and should so. Blockchain Technology (BT) offers new possibilities concerning data ownership and business transactions on the Internet. After all, it may be time for data monetization to start working both ways, reverting as well to users and not only to "the giants of the internet [that] expanding into every corner of the economy, politics and our lives." (Alleman, 2018).

Concerning healthcare, ICT development makes choosing between privacy and convenience more complicated. As referred by Wildman et al. (2019), "Sweeney (2015) was able to match patient names to publicly available anonymized health data. [His studies] show that the claim that anonymized data poses no threat to privacy is dubious at best. (p. 35)

Currently, much of the open data available is spatial (geographic or satellite) data, which is relatively unproblematic to post online as it poses minimal privacy risks. However, for the full benefits of open data to be gained, this spatial data needs to be supplemented with information on welfare payments, hospital admission rates, income tax assessments and other potentially sensitive areas of government policy and administration which could drive innovation. As more and more datasets from these disparate policy areas are posted online, the greater the risk that individuals may be reidentified and their personal details exposed. (Hardy & Maurushat 2017, p.33).

Once upon a time, simply removing a person's name, address, and Social Security number from a medical record may well have protected anonymity. Not so today. Straightforward data-mining tools can rummage through multiple databases containing anonymized and non-anonymized data to reidentify the individuals from their ostensibly private medical records. (Tanner, 2016, p.27)

A particularly threatening tool that menace privacy rights is thought to be applications (apps) for smartphones and other mobile devices. Given the need to deal with an increasing volume of information, it is foreseeable that future apps will be equivalent to "digital prostheses" that will inevitably be part of everyday life. Accordingly, privacy issues will become more worrisome.

The apps that can help, for instance, to avoid humans' physical presence quickly proved to be indispensable in a pandemic. Hence, privacy concerns will probably grow. For example, in monitoring contagious diseases, the mandatory installation of such apps, advocated by certain politicians, has increased the controversy surrounding protecting privacy. As stated by Bengio et al. (2020), "the advent of the coronavirus disease 2019 (COVID-19) pandemic has seen widespread interest in the potential utility of automatic tracing apps, as well as concern over their potential negative effects on individual privacy" (p.1).

Other authors take their concern even further, considering freedom itself threatened. According to Rowe et al. (2020, p.1), "if the app is imposed, individuals will feel they are being surveilled, which raises immediate ethical concerns and may signal authoritarian regimes."

Seeking to obtain a comparative overview of various apps' privacy vulnerabilities, Wen et al. (2020) conducted a study of covid-19 contact tracing apps by performing a cross-platform comparison on 41 apps (26 Android and 15 iOS) "having obtained significant privacy concerning findings, including broadcasting users' fingerprints, tracking a specific individual, and collecting other mobile device information." (p. 14).

After observing some privacy concerns on the *Internet of Information*, the focus on privacy will now be shifted to the new *Internet of Value*.

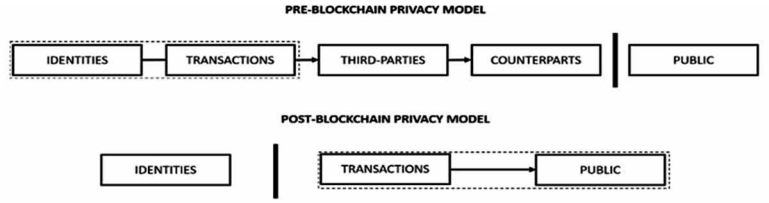
Privacy on the Internet of Value (IoV)

The cryptographic resourceful blockchain technology (BT) both allows keeping the originality of digital information over the Internet (and consequently the value resulting from such exclusivity) and simultaneously overcoming severe limitations concerning privacy.

While the traditional privacy model limits personal data's public visibility, it does not prevent service providers from accessing that same data. However, the privacy model based on the blockchain protocol separates personal data from data owners' identities (see Figure 1). Separating people's identities from their data is now possible, "because metadata [*e.g.*, *hash values*] such as patient identity, visit ID, provider

ID, payer ID, etc. can be kept on a Blockchain, but the current [sensitive] records should be stored in a separate universal health cloud" (Karafiloski & Mishey, 2017, p. 767).

Figure 1. The privacy model metamorphosis overview (pre-blockchain & post-blockchain)



As mentioned in the previous section, digital interactivity facilitates consumers' profiling, and such knowledge allows the adaptation of products and services (Kotler et al., 2016). Meanwhile, most companies want to focus their businesses on distinctive competencies, gladly dispensing the burden of possessing data not relevant to their core business, mainly when this ownership implies liabilities in safeguarding customers' privacy under penalty of not comply with the law. These companies want to streamline their business processes and reduce their transaction costs (Coase, 1993). Therefore, there is a coincidence of interest between most companies and their customers regarding privacy issues, being that personal data control made by customers and data protection laws are no problem at all for most companies.

With the introduction of the General Data Protection Regulation (GDPR), the European Commission has provided a legal framework that aims to empower individuals in taking control of their personal information. Such control is not necessarily a disadvantage to parties processing personal information: when used properly, GDPR can actually facilitate data flows that used to be much more complicated. (Buyle et al., 2019, p.346)

There are not real reasons for personalization and privacy to be antagonists; good governance and regulation are the starting points that will allow the right controls to be in place for data to be collected in a meaningful and ethical way. Privacy, online and offline, is not about sharing information or leaving people alone, but about transparency on the methods used and the purposes sought. It is about each person's right to decide, free from commercial and governmental pressures and interests. (Garcia-Rivadulla, 2016, p.235)

However, although this ethical stance favoring privacy, there are significant exceptions in the ICT sector, as is the case for the largest multinationals responsible for a worrying asymmetry of information in society (Neitz, 2019). Thus, instead of being under citizens' control, information about people's lives is channeled to these powerful companies. Meanwhile, data centralization is probably happening in totalitarian states, as authoritarian political regimes try to collect data and concentrate information about their citizens seeking complete political control.

The reality is bleak: centralization is reigning in the cyberspace, with huge technological corporations controlling our data, and re-intermediation and control are stronger than ever in the so-called" sharing

"economy. The Internet is also fragmented by countries, with many states imposing heavy controls to information and communication services. (Lopez et al., 2020, p. 901)

In this worrying ethical framework, the blockchain protocol may emerge to public eyes as *a trust-distributing formula* that endows the Internet with a functional language to transact value and not just to share information. It turns out that this change can result in both good and evil (Kewell et al., 2017), increasing ethical dilemmas.

Centralizing and controlling the ability to share information about user's preferences in social media raises ethical concerns, but the idea of combining that ability with the new BT features that make it possible to control consumers' digital transactions is even more worrisome. Centralized digital currencies can do this workload easily, either at the state level (Peters et al. 2020) or privately (Gerard, 2020). After all, everyone is a consumer, and it is not only privacy that eventually will be threatened but also the freedom of choice and democracy (see the same book, Chapter 4 - *Blockchanging Politics: Opening a Trustworthy But Hazardous Reforming Era*).

Some say that Central Banks Digital Currency is not cryptocurrency (Insight, 2021). However, it is indeed cryptocurrency, although centralized (Echarte Fernández et al., 2021), and there is a trade-off between privacy and accountability in any traceable digital currency as is the case of CBCD, which is "managed on a permissioned blockchain, i.e., only authorized entities are involved in transactions verification" (Barki & Gouget, p. 1).

A CBDC will also in some way need to address an innate tension between privacy and transparency, protecting user data from abuse while selectively permitting data mining for end-user services, policymakers, and law enforcement investigations and interventions. […] This is typically achieved using advanced cryptographic primitives known as zero-knowledge proofs. […] To reap the benefits of zero-knowledge proofs, participants must be able to generate and validate transactions containing encrypted data. (Allen et al., 2020, p. 2)

CBDC is programmable money, and "regulators and central banks are right to be cautious" (Ali & Narula, 2020, p. 13). However, citizens must be cautious because money is essential and digitally controlling it is not a question of minor importance. One should have in mind that "power corrupts and the absolute power corrupts absolutely" (Dewing, 2021, p. 74). As referred to by Bichler & Nitzan (2021), "the quest for capitalized power - and more and more of it - is the key driving force of modern capitalism." These authors stated the further warning that "U.S. subjects are likely to hear much more about the benefits of [many] processes that, they will be told, require them to accept ever-larger corporations and a much more authoritarian society" (Bichler & Nitzan, 2021). Furthermore, CBDC can also be issued by authoritarian governments, let alone the perils of a *post-Covid-19 new normal* (Berwick, 2020) corset influence even in democratic states.

[Although] programmability seems like a promising avenue (…) enabling privacy and auditability through cryptographic techniques will be necessary to reduce the risk of financial surveillance and misuse of data. [The question is] who will develop this system? Will it be an upstart cryptocurrency-based stable coin, or a coalition led by a large company like Facebook which already connects with billions of users globally? […] In this case, exercising caution means understanding what the technology can and cannot do, whether by staffing up internally or partnering with technical organizations, and preparing for an

uncertain future. The industry is moving fast; the most perilous path of all is inaction. (Ali & Narula, 2020, p. 13)

Considering what is at stake in terms of citizens' privacy and freedom, transparency in handling digital currencies is a new ethical fundamental aspect of democracy. If it is true that such transparency is ensured in the case of data transmitted in *permissionless-blockchains* such as the Bitcoin network, the same cannot be said concerning the *permissioned-blockchains* where CBDC will be processed. Thus, CBDC blockchain protocols must be equipped with "advanced cryptographic primitives known as zero-knowledge proofs" (Allen et al., p. 43) and techniques such as "homomorphic cryptography" (Liu et al., p. 296) that can also have an essential role in securing electronic voting and protecting democracy. It is thought that these and other programming details should be open-sourced to guarantee "a traceable, transferable and divisible digital currency system that protects user's privacy while enabling the retrieval of user's identity in case of suspicious transactions, e.g., suspicion of fraud or money laundering activities" (Barki & Gouget, 2021).

This being said, hopefully decentralization brought about by BT may contribute to defending citizens' privacy rights, reducing the growing threat that hangs over freedom itself. After all, ciphered data can decisively contribute to optimizing the trade-off between "Privacy" and "Convenience," allowing new privacy standards by letting users own and control their data.

The blockchain recognizes the users as the owners of their personal data. Companies, in turn, can focus on utilizing data without being overly concerned about properly securing and compartmentalizing them. (…) [With such a] decentralized platform, making legal and regulatory decisions about collecting, storing and sharing sensitive data should be simpler. Moreover, laws and regulations could be programmed into the blockchain itself, so that they are enforced automatically. (Zyskind & Nathan, 2015)

It should be noted that these privacy guarantees also translate into competitive advantages for companies. As Bleier et al. (2020) pointed out, "consumers are more willing to permit marketers to use their information when the firm treats their information fairly" (p. 30), and "firms catering to consumers' privacy concerns may obtain a favorable market positioning relative to others who pay little attention to such concerns. Privacy can create opportunities." (p. 30). Governments could also benefit from such guarantees. According to Karafilovsky & Mishey (2017), "[blockchain] will help governments and other enterprises be liberated from the liability that data is becoming." (p. 767). For instance, the Estonian government has harness BT's potential In recent years (Meier et al. 2020).

The ethical concern with privacy protection is of paramount importance in healthcare. Data has value, and health data have enormous value. A multi-billion-dollar industry is currently built around data brokers that buy patients' health data from doctors and hospitals, anonymize it, and sell it to other firms to guide their pharma investments or better target their advertising (Tanner, 2016).

The possibilities opened by BT are changing the trade-off between privacy and convenience, making it possible to establish new privacy standards that let patients own and control their data. For instance, BT can be used to manage personal data and identities (Mainelli, 2017), facilitating the process of assessing individuals for enrolment to specific clinical trials (Bergeron et al. 2020) and transacting personal data such as Electronic Medical Records (Liu et al. 2018a, p.6)

[Distributed ledgers] can help you keep relevant health or qualification records at your fingertips. Using "smart" ledgers, you can forward your documentation to people who need to see it, while keeping control of access, including whether another party can forward the information. You can even revoke someone's access to the information in the future. (Mainelli, 2017, p.4)

As stated by Karafiloski & Mishey (2017), "losing control of privacy is what happens when social media networks are constantly collecting users' data, actions and habits" (p. 764), both in the case of social media and in the case of mobile apps. Concerning the so-called "contact tracing applications," it has been noticed that current solutions do not offer absolute privacy guarantees (Dehaye & Reardon, 2020). When using these apps, almost always the only way for a user to revoke access to personal data is to uninstall the application itself. Still, there is no guarantee that personal data will not exist forever on the companies' central servers that own this application or not will be transferred to third parties.

Users lose total control of what happens with the data afterwards and they cannot withdraw the permissions. Usually there is a privacy setting page on most of the social media sites, where users can limit what other people see about them. What they cannot control and configure is what the social media corporation sees. (Karafiloski & Mishev, 2017, p. 764)

One major concern with mobile applications is that users are required to grant a set of permissions upon sign-up. These permissions are granted indefinitely and the only way to alter the agreement is by opting-out. (Zyskind & Nathan, 2015, p.181)

There are also healthcare applications that use pseudo-anonymized data, sometimes presented as a guarantee of privacy. However, several studies point to the fact that this is not a way to ensure privacy, as such data can be combined and end up revealing personal information.

It was recently used to show that individuals in a simply anonymized mobile phone data set are re-identifiable from only four pieces of outside information. Outside information could be a tweet that positions a user at an approximate time for a mobility data set or a publicly available movie review for the Netflix data set. Unicity quantifies how much outside information one would need, on average, to reidentify a specific and known user in a simply anonymized data set. The higher a data set's unicity is, the more re-identifiable it is. It consequently also quantifies the ease with which a simply anonymized data set could be merged with another. (De Montjoye et al. 2015, p. 538)

Some authors mention several encryption techniques to reinforce BT's privacy guarantees. As stated by Hassan et al. (2019), "modern differential privacy algorithms in conjunction with blockchain, can eradicate the issue of privacy loss (p. 762).

Another promising technique is homomorphic encryption. Although it is "still not efficient enough for real-time applications" (Moore et al. 2014, p. 2793), homomorphic encryption "shows that stronger and cost-effective encryption schemes are possible to be added to blockchain technology to make it more suitable to security and privacy-based applications, specifically using artificial intelligence" (Yaji et al. 2018, p.85).

One can use homomorphic encryption techniques to store data over the blockchain with no significant changes in the blockchain properties. This ensures that the data on the blockchain will be encrypted, addressing the privacy concerns associated with public blockchains. The use of homomorphic encryption technique offers privacy protection and allows ready access to encrypted data over public blockchain for auditing and other purposes, such as managing employee expenses. Ethereum smart contracts provide homomorphic encryption on data stored in blockchain for greater control and privacy. (Zhang et al. 2019, p. 28)

Finally, it should be noted that BT has revealed, in practice, sufficiency in assuring privacy because asymmetrical encryption guarantees confidentiality, and the hash algorithm makes it impractical to reverse the encrypted data (Nakamoto, 2008). BT also has revealed to ensure convenience. As stated by Liu et al. (2018), "by implementing [blockchain based privacy-preserving data sharing, [the patients] can have complete control over their EMRs [(electronic medical records)] and the users or institutions can use data conveniently without any risk on patients' privacy." (p. 6)

Thus, it can be said that BT's cryptographic properties open a very promising avenue in terms of privacy protection. Hopefully, it will translate into increased individual autonomy, which can substantially impact politics, the economy, and healthcare.

Data Ownership

The ethical dilemma of choosing between protecting intellectual property rights or defending the public interest has been heightened in the digital age. Technological innovations and the creation of new products and services require substantial effort (time and money), so the desire to obtain some return on investment (ROI) is ethically defensible. On the other hand, considering the public convenience of disseminating innovations (*e.g.*, an essential vaccine), it becomes necessary to optimize the trade-off between intellectual property rights and the public interest.

There is no single answer to determine whether innovative ideas have an owner or whether only the expression of those ideas can be considered as belonging to a particular individual. Some will give more credit to the merit of intellectual creation, while others will judge that those creators did nothing more than use and express society's accumulated knowledge, often counting on others' work before him. If this answer makes a difference in people's lives, then this is an ethical dilemma, indeed. However, if this is not the case, it is just an ideological matter of opinion. To clarify which is the case, one should investigate the Blockchain Technology (BT) enabling role in the upcoming "Augmented Internet" (Dai, 2020).

Until recently, digital data ownership was not like physical ownership. The latter can be held and transferred indefinitely, while the former only works in specific contexts, and moving its value around on the Internet has not been possible without trustable intermediaries.

Indeed, sharing digital information does not require much effort because the marginal cost of doing *copy-paste* on the Internet is practically zero, so digital copies quickly become abundant. As a result of such immediate convenience, original data lose their exchange value as soon as shared on the Internet. Even if shared information keeps its usefulness, price instantly falls to zero (Anderson, 2009). Therefore, it becomes practically impossible to prevent someone (even anonymously) from making unauthorized copies and spreading them over the Internet, diminishing the value of the original pieces of information. As stated by Romer (2002), "technological change has substantially undermined the effective protection offered by copyright" (p. 213)

Although the *pre-blockchain Internet* was still incomplete and unable to endure peer-to-peer trade, its sharing features were competitive enough to create a digital economy that started to change the world right away. Hence, the first phase of the Internet brought difficult times to authors and data ownership. As such, since those days, a few powerful intermediaries took full advantage of the digital *status quo*.

Artists, designers and creative workers can share easily on the Internet, but keeping the right with proper attribution or getting fairly compensated has proven difficult in the digital world that we know. There is not a transparent way to own something that can be so easily copied and fully replicated, with no sign of the original. (…) Once the work is put online, or even sold online, the author loses control. (Karafiloski & Mishev, 2017, p. 766).

Ownership on the Internet of Information

The first stage of the Internet highlighted the competitive importance of networks (Castells, 2011). As referred by Power & Phillips-Wren (2011), "the value of a telecommunications network is proportional to the square of the number of connected users of the system" (p. 254). Success calls for creativity and cross-fertilization of projects and ideas from different minds and owners in such a competitive environment. Therefore, restrictive copyright laws are not flexible enough to allow creators to innovate and be competitive. Unfortunately, for many editors, the *free web content's paradise* became a living hell for many scarcity-based business models. Indeed, the traditional *copyright licenses* seemed to help neither authors nor consumers. Some less restrictive approaches paved their way, as is the case of *Creative Commons Licenses*, a legal framework that pursues competitiveness on behalf of authors by freeing creativity and innovation (Flew, 2005).

[Creative Commons] attempts to build on existing copyright law by offering a set of "some rights reserved" licenses designed primarily for authors and artists. Copyright owners who choose to release their work under a Creative Commons license disclaim some part of the default protection that attaches under statutory law. (…) Essentially, users of these types of licenses are reframing their "property right" protected by federal law into a contract right ordered by the terms of the agreement. (Goss, 2007, p. 964)

On the *Internet of Information*, the great enemy of authors and other digital producers was not piracy as it may seem, but instead obscurity. After all, popularity can be easily monetized on the Internet through advertising (Anderson, 2009). For instance, the Creative Commons type of licenses and the so-called *freemium* business models have been successful in the *pre-blockchain* phase of the Internet (Anderson, 2009; Günzel-Jensen & Holm, 2015).

As will be seen in the following section, Creative Commons Licenses can be articulated with BT, opening avenues for the transaction of digital assets (tokens) and streamlining business through "smart ledgers" (Mainelli, 2017) and "smart contracts" (Hartel et al. 2019).

During the past thirty years, data has become increasingly valuable (Jørgensen, 2020). The advances in ICT made it possible to massify data collection, storage, analysis, and application to the resolution of many problems, including in healthcare:

A growing number of companies specialize in gathering longitudinal information from hundreds of millions of hospitals' and doctors' records, as well as from prescription and insurance claims and

laboratory tests. Pooling all these data turns them into a valuable commodity. Other businesses are willing to pay for the insights that they can glean from such collections to guide their investments in the pharmaceutical industry, for example, or more precisely tailor an advertising campaign promoting a new drug. (Tanner, 2016, p. 26)

The value of the clinical data used for clinical trial development only exceptionally reverts in favor of those who originate that same data. For instance, when such individuals have the chance to benefit as patients in those clinical trials directly and that is it. One cannot doubt that this redistributive system is unfair to those who have been information sources for years or decades without being paid.

For decades researchers have run longitudinal studies to gain new insights into health and illness. By regularly recording information about the same individuals' medical history and care over many years, they have, for example, shown that lead from peeling paint damages children's brains and bodies and have demonstrated that high blood pressure and cholesterol levels contribute to heart disease and stroke. To this day, some of the original (and now at least 95-year-old) participants in the famous Framingham Heart Study, which began in 1948, still provide health information to study investigators. (Tanner, 2016)

Tanner (2017) pointed out that "after a person gets medical care, pharmacies, insurers, labs, electronic record systems, and the middlemen connecting all these entities, automatically transmit patient data directly to what is, in effect, a big health data bazaar" (p. 2). One can notice that the numbers are getting more significant: "the data market in healthcare was estimated $14.25 billion in 2017 and is estimated to grow over $68.75 billion by the end of 2025." (Rooney et al., 2019, p. 19).

There is no doubt that clinical data is most profitable for some healthcare stakeholders that are almost exclusively information intermediaries, and the correspondent value can now be disputed by patients thanks to BT. As will be seen in the next section, BT opens an entirely new digital ownership world and data management permissions. As such, an "Augmented Internet" (Dai, 2020) is fitted to process *smart contract* operations nurturing *peer-to-peer* (P2P) trade among healthcare stakeholders, including patients. Moreover, this new digital reality is reaching and embracing the physical world, like it is happening in the energy sector (Bao et al., 2020).

Some P2P energy trading markets based on blockchain mainly use blockchain to realize market auction mechanism. The work in [Mengelkamp et al., 2018] proposed a decentralized market platform for consumers and prosumers in local energy markets based on the private blockchain. A central intermediary is never needed to manage local energy transactions. (Bao et al., 2020, p.5)

Ownership on the Internet of Value (IoV)

Empowered by BT, the Internet facilitates and makes the transaction of digital tokens ubiquitous. Tokens are units that quantify value, and they can represent digital assets (see Chapters 3 and 4). There are also tokens whose properties allow representing non-fungible assets.

Non-fungible tokens (NFT) are a class of tokens introduced in late 2017 with the ERC-721 standard. While fungibility – the ability to be substituted in place of one another – is an essential feature of any currency, non-fungibility is the opposite as every token is distinguishable and thus also cannot be di-

vided or merged. This also has implications for tracking the ownership of tokens as each NFT needs to be tracked separately. (Regner et al. 2019, p. 4)

[A non-fungible asset] is not equal to its counterparts. The most tangible example of a non-fungible asset is any sort of collectible. A baseball is just a baseball until it is signed by Babe Ruth. Then, it gains additional value and becomes a non-fungible asset, valued differently than all other baseballs out there. Non-fungible assets generally have a greater scarcity than fungible ones, and therefore hold more intrinsic and unique value. With scarcity and value now measurable in the digital realm through blockchain and distributed ledgers, we are just beginning to see the potential of non-fungible digital assets. (Muzzy, 2018)

The distinct properties of NFTs have opened a new type of digital representation of value, namely allowing the tokenization of individualized assets, a function prohibited to fungible tokens, which cannot digitally represent the exclusivity of assets such as physical ones.

According to the ERC-721 standard, each NFT has a unique identification, is transferable, and includes metadata (Entriken et al., 2018).

ERCs [see Key Terms and Definitions] are predefined rules developed using Smart Contracts for implementing token measures in Ethereum Blockchain. ERC-20 can define by providing the contract address and availability of tokens. (…) ERC-721 token standard supports Non Fungible Tokens. It makes these tokens have a unique value and identity. Tokens are attached to digital objects using metadata to help off-chain rendering or storage (Muthe et al. 2020, p. 75)

NFT's specific purpose is to represent the ownership of physical assets, such as houses or works of art, and digital assets such as music or exclusive photos. Therefore ERC-721 tokens cannot be divided because they represent an entire and indivisible asset. These tokens can be used in exchanges, but their value results from each one's uniqueness or singularity. They can also represent *negative value assets*, such as loan debts and other liabilities. This faculty is possible because NFT are distinguishable from each other, and it is possible to trace any of them (Entriken et al., 2018). As happens with so many other aspects related to the democratization of value transfers made possible by *blockchain cryptographic protocols*, it is believed that NFTs will contribute to the political-economic disintermediation making individuals more autonomous in managing their assets without resorting to intermediaries.

NFTs will change the market. The collectibles market has always been centralized. Topps made the money, not the baseball players. The same is happening again, with sports leagues like the NBA minting money on NFT videos. But that's just in the short term. Big companies will always make money, but expect more players and artists to get in on the action. The rise of NFTs holds the power to tear down some of those walled gardens and put power back in the hands of the creators and the athletes. (Jeffries, 2021)

The above-mentioned Creative Commons Licenses can now be fully integrated in a self-executable manner through *smart contracts*. This new operational granularity allows for more resourceful and innovative transactions to be carried out, eventually matching entrepreneurship and sustainable human development. As stated by Helbing (2017), "to benefit from the digital revolution, we need an entirely

new approach. [...] We need to build an ecosystem of socio-economic activities, where each new idea, product, and service creates opportunities for further ideas, products, and services." (p. 316).

Therefore, the Creative Commons' flexible type of property rights license makes sense in the digital era, especially in the light of BT; as was described by Savelyev (2018), "it is possible to combine the simplicity of using open source/creative commons licenses with receipt of a licensee fee by the licensor. It can be facilitated by a set of standardized smart contracts, the terms of which can be described in a comprehensible language ("laymen code")" (p. 6).

Tokenization processes show a digital reality that was understood more than 25 years ago: the digital world has much more *elasticity* than the physical world (Negroponte, 1995), and such versatility is now reaching the financial world. This *digital plasticity* is now cryptographically encoded, conferring additional features to the one-dimensional money of the *pre-blockchain* era. It is believed that this is a historical shifting fact that soon will change, by this order, finance and economy (see the same book, Chapter 3 - *Blockchanging Money: Reengineering the Free World Incentive System*, and Chapter 4).

By allowing its users to trade fungible assets directly with each other and adding unique properties to non-fungible assets (changing the way one relates to these assets), BT increases individual autonomy and commercial dynamics, making it possible for everyone to transact globally in the absence of intermediaries.

When you are the sole owner of your personal data on purchases, online browsing history, or mobile data, you can also choose whether or not to "sell" your own data, with rights and restrictions using smart ledgers. This could shift the power of (and profit from) data management from big, established firms back to individual users. (…) Mutual distributed ledger systems have the potential to provide us with identity and activity management, even permitting us to make a market selling information about ourselves, taking control and cash back from companies (Mainelli, 2017, p.5)

In healthcare, clinical data eventually will contribute to a revenue redistribution, shifting value from shareholders to stakeholders (*e.g.*, patients). When everyone guarantees their health data's absolute ownership, any person can stipulate the conditions for aggregating their health data with other individuals, such as patient organizations and other health-related communities. As such, individuals will release and monetize data in the proportions agreed between themselves. *This type of collective action has nothing to do with collectivism because it is based on the decisive role of individual economic incentives.* Hence, incentives can now work according to community interests, paving the way for more public utility coming from civil society.

BT can be used to level the economic playing field, allowing individuals to gain bargaining power in the face of organizations that usually get patients' data without giving any financial consideration (although clinical data is precious, as seen above). Such bargaining power will come from a consensus on aggregated data's fair value, leading to balanced business agreements.

It must be mentioned that to understand the new "cryptoeconomy" (Buterin, 2017), one should know that collective action results from individual incentives, and that has nothing to do with collectivism (see Chapters 3 and 4).

Blockchains are generally positioned to disrupt processes reliant on centralized mediation or trust-based operations. Blockchains interoperating with end-user applications for managing personal medical data, i.e., medical data vaults, have been envisioned as effective mechanisms for individuals to share their

medical data with researchers and receive tangible rewards, such as cryptocurrency payments, for such data sharing. (Bergeron et al. 2020, p. 45)

While privacy regulation alone can lead to a decrease in planning and operational health information exchanges, when coupled with incentives [cryptocurrencies], privacy regulation with requirements for patient consent can actually have positive effects on the development of health information exchanges efforts. (Bleier et al. 2020, p. 28)

In a blockchain society, public knowledge of transactions no longer has to imply bargaining to keep the underlying information private. So, it increases individual autonomy by allowing individuals to manage and store their digital identities. This way, it is possible to transact personal data in the absence of intermediaries and safely. Hopefully, disintermediation in healthcare will eventually lead to a more ethical distribution of wealth derived from patients' valuable data.

Data Accessibility

The ubiquity of ICT can and must make the world more human. Computers and the Internet are precious resources in the pursuit of individual and organizational goals. Therefore, access to such resources is fundamental, and it is crucial, from an ethical point of view, to observe how they should be distributed in society.

Individuals with access to an instrument as powerful as the Internet, will always be in a better position to achieve their objectives. Indeed, one concern regarding the social effects of computers is the fact that they could increase the cleavage between the more and the less favored individuals, and the gap between "have" and "not to have" may become the abyss between the "knowing" and "not knowing. (Rodrigues, 2012, p. 326)

According to World Bank statistics, there are currently one billion people without legal identity documentation worldwide (Allan & Mortensen, 2020). This exclusion hurts not only those persons but also the economy as a whole. Several authors have described that expeditious access to data is a fundamental condition for individuals' competitiveness. According to Bleier et al. (2020), citing Martin and Murphy (2017), "a competitive advantage may then not only materialize in terms of higher sales or market share but also increased access to consumer data" (p. 30).

Accessibility of data requires trust in whoever accesses it, whereby a way to solve the lack of trust raised on the Internet before the current transition for the *blockchain* era will now be discussed.

Accessibility on the Internet of Information

Even during the first phase of the Internet, the possibility of accessing information has been a controversial issue. The Internet was made technically possible by joining two inventions: the TCP / IP suite protocol, developed almost 50 years ago by the Defense Advanced Research Projects Agency - DARPA (Clark, 1988), thanks to their creators, Vinton Cerf and Robert Kanh (Leiner et al., 2009), and the HTTP protocol, developed more than 20 years later by Sir Tim Berners-Lee (Berners-Lee et al. 1996). The latter provided the Internet with "the lightness and speed necessary for distributed, collaborative, hypermedia

information systems" (Berners-Lee et al. 1996, p. 1). Therefore, it was a joint effort, separated by more than two decades, that gave rise to the Internet.

The controversy about accessing the information on the Internet still exists; while updating or correcting detected data errors seems ethically irreproachable, the need to guarantee the integrity of the information and prevent, for example, the possibility of an individual falsifying his own identity advises to limiting access to information (Rodrigues, 2012).

The limitations due to privacy protection have contributed to maintaining a large volume of data in silos, making it difficult to interconnect and elaborate the ontologies necessary to develop a semantic web that aims to "making web content interpretable" (Euzenat & Rousset, 2020, p. 181). As referred in Sfetcu (2019) an ontology is a description (like a formal specification of a program) of the concepts and relationships that can exist for an agent or a community of agents, and Koufakis et al. (2020), citing Feilmayr and Wöß (2016), refined the definition of ontology stating that "An ontology is a formal, explicit specification of a shared conceptualization that is characterized by high semantic expressiveness required for increased complexity." (p. 3)

Today, there is an appeal for constructing the so-called *linked data*, an effort on a global scale sponsored by the World Wide Web founder, Sir Tim Berners-Lee. Disagreeing with the Internet's centralized path, he is trying to reverse such a situation with its "Solid" project (Buyle et al., 2019). His discomfort with the current data centralization on the Internet is understandable because it goes against the original idea mentioned by Leiner et al. (2009) regarding the creation of the Internet in the early 70s: "The Internet as we now know it embodies a key underlying technical idea, namely that of open-architecture networking" (p. 2).

Thus, not surprisingly, several authors propose to combine the new protocol developed by Berners-Lee for his latest project with the blockchain protocol, allowing users to maintain ownership and control of their data in a truly decentralized environment.

Combining Solid Pods and distributed ledgers in introducing complete decentralisation of data with total user-control, keeping the integrity of the stored information intact through Blockchain-based verification (…) These configurations introduce new dimensions on the Web and mobile applications' data storage that developers can benefit from building Distributed Applications (DApps) in a complete decentralised environment. (Ramachandran et al. 2020, p. 645)

It is thought that by freeing economic agents from the burden of protecting privacy, BT can streamline the data linkage process and the ontology engineering necessary for semantic web development.

As will be seen in the next section, the blockchain protocol optimizes the trade-off between the freedom to access information and the risks that this possibility entails. In healthcare, this risk limits patients' access to their health records and clinical data, but things can be different in the blockchain era.

Accessibility on the Internet of Value (IoV)

In the recently created IoV, which encompasses both *economic media* (social media and digital money), the possibility of accessing information will be more critical than ever before. The transaction costs reduction that BT made possible, especially by avoiding the cost of distrust (Davidson et al., 2018; Berg et al., 2019), should result in more straightforward digital information access. Such efficiency can help to ethically tackle global financial challenges, including those created by more than two billion people

who have a mobile phone but no bank account (Bhyer & Lee, 2019), and at least one billion *identityless* individuals that cannot exercise citizenship. Hopefully, both these large groups of people will significantly benefit from *blockchain-based* proof-of-identity applications.

[Blockchain] allow the almost instantaneous transfer of digital tokens, if not at zero cost then at a significantly cheaper rate than established services. This makes the transfer of small amounts of currency economically viable, enabling new actors to enter the field and new opportunities (…) It might be anticipated, then, that reductions in the cost of financial transactions through DLTs [(Distributed Ledger Technologies)] will result in widening financial inclusion. (Kweel et al. 2017, pp. 19, 20)

By combining the decentralized blockchain principle with identity verification, a digital ID can be created that would act as a digital watermark which can be assigned to every online transaction. The solution can help the organizations to check the identity on every transaction in real time, hence, eliminating rate of fraud. Consumers will be able to login and verify payments without having to enter any of the traditional username and password information. (…) [An app] will store their encrypted identity, allowing them to share their data with companies and manage it on their own terms. (Jacobovitz, 2016, p. 3)

Decentralized apps (Dapps) eventually free many people who depend almost exclusively on social media oligopoly to communicate. Hopefully, they will help to avoid the politically dangerous "polarization, and dehumanization" (Hartel et al. 2020) derived from continuous social media's "fragmentation and polarization of audiences" (Hart et al. 2009; Sunstein, 2009).

Influential selection biases, indicating that citizens do not merely seek for congruence on the content level, but that sources and negativity biases also drive people's motivation to consolidate digital spaces that reassure consistent image of the self and potentially result in distorted and fragmented worldviews on the individual level. (Van der Meer, et. al, 2020, p. 958)

Today, healthcare data goes almost entirely to providers and intermediaries' databases. One of the reasons for this high centralization level is that privacy requirements limit information sharing by stakeholders. Thus, most patients rarely can access their health records directly.

By adopting blockchain networks that interconnect the various players in the health sector, patients will be able to access their own clinical and personal data, ensuring their confidentiality without resorting to intermediaries (Yaeger et al., 2019). This confidence is possible because the blockchain protocol provides an assignment to everyone, which lets patients take total control over access permissions and share their clinical data with complete security. Clinical data is aggregated to the individual and always accessible instead of being transmitted through intermediaries (Goldwater, 2016).

Furthermore, everyone's health data can be collected and added to the blockchain through the so-called *oracles* (see Chapter 3) bridging blockchains and the external world. It is thought that many *oracles* will be integrated into more and more mobile devices and *wearable interfaces,* such as glasses and bracelets equipped with biometric sensors, that will be part of the so-called *Internet of Things* (IoT).

In healthcare, IoT devices have the ability to provide real-time sensory data from patients to be processed and analyzed. Collected IoT data are subjected to centralized computation, processing, and storage. Such centralization can be problematic, as it can be a single point of failure, mistrust, data manipulation and

tampering, and privacy evasion. Blockchain can solve such serious problems by providing decentralized computation and storage for IoT data. (Ray et al., 2020)

Using cryptographic keys, the patient obtains full control over the permissions necessary to share or transact his data with total security. The only necessary mediation will be provided by sensors and *oracles* that will be part of the IoT.

A blockchain oracle is a mechanism that fetches data from the external world to include it in the isolated execution environment of a blockchain. (…) Blockchain oracles are needed to bridge blockchains and the external world because of unique characteristics of blockchain. Some kinds of data in the external world are inherently unable to be independently validated by multiple distributed parties, for example because the data has restricted access, or is transient sensor data. Oracles import this kind of data as transactions into a blockchain. (Lo et al., 2020, p. 10658)

Finally, it should be added that governments can also benefit their social capital by increasing healthcare digital access, namely instituting government transparency and giving patients open access to healthcare information. For example, this openness and transparency already occur in Estonia, where e-health systems have been operational for over 20 years. As Metsallik et al. (2018) refer, "The main success factors for the e-health system in Estonia are clear governance, legal clarity, a mature ecosystem, agreement about access rights, and standardization of medical data and data exchange rules." (p. 1).

For the past decade, the Estonian government has been focusing on BT to increase government transparency and secure citizens' access to information. For example, "the Estonian eHealth Foundation started a new era in securing healthcare data by safeguarding off-chain stored EHRs [(Electronic Health Records)] using a blockchain protocol that logs all data access activities" (Einaste, 2018).

The blockchain ensures that users own and control their personal data. Our system respects the fact that the user owns the data and only gives access to the data to healthcare professionals after approval by the user. The access control is fine-grained, thus strengthening compliance with data privacy and data security. For example, users can revoke access authorizations at any time or grant one-time access only. Moreover, the accesses are logged transparently and traceably. (Meier et al. 2020, p. 2)

It is expected that BT will provide data accessibility and transparency to fulfill the ethical principles of free societies and democratic regimes. One should notice that the opposite direction, towards data centralization, appears to be ethically reprehensible and politically dangerous (Chapter 4).

Precision of Content

The progress of ICT has led to a situation where it has never been easier to access or distribute information. Unfortunately, data sharing on the Internet makes it easier to obtain and disclose false or incorrect information and, also, to manipulate or be manipulated even by correct information if tailored and repeatedly presented.

The author already mentioned the economic interest in signaling well-defined segments of users on social networks. This market segmentation aims to increase advertising performance, thanks to business models tunned to selling ads that become more profitable in case of user's profiles are well outlined.

There are reports that an artificially exacerbated market segmentation (deceptive marketing) and subsequent targeting practices lead to an information bias determined by algorithms that are "telling lies" (O'Neil, 2017. p.7). The ethical implications and practical consequences of such *fake news* and *biased content* are very harmful. The information interactively and iteratively conveyed in social media may persist as an erroneous and surreptitious input on users' decision-making processes on politics, economy, and healthcare.

[Algorithms] are merely "opinions embedded in mathematics" and reflect subjective goals and ideologies (…) Creators of said algorithms, unintentionally (or intentionally) weave "human prejudice, misunderstanding, and bias" into their models (…) The welfare of society depends on the benevolent use of data. (…) Algorithms filter, curate, and dictate the information consumed by the public, profoundly, "shap(ing) lives and outcomes as a consequence" (Berry, 2020, pp. 93, 94)

First, while mistakes may be unintentional, ignoring or even fostering mistakes is unethical. Second, by creating inscrutable algorithms, which are difficult to understand or govern in use, developers may voluntarily take on accountability for the role of the algorithm in a decision (…) algorithms are a less visible part of the decision and often less accessible to question—even being held secret. (Martin, 2019, pp. 129, 136)

Precision of Content on the Internet of Information

In the *pre-blockchain* stage of the Internet, besides critical user thinking, several indicators were already available about the authority, reliability, and credibility of content providers. These indicators came from "trusted third parties" (*e.g.*, Verisign) or the users themselves.

[Surowiecki's "crowd wisdom" (2005)] can quickly show each user the popularity and the level of acceptance of particular web content. This democratic criterion of popular validation is [integrated] in algorithms such as the Google company's PageRank, which uses [attention and reputation indicators] to determine [content] relevance (Rodrigues, 2012).

As stated by Kraft & Donovan (2020), "both people and platforms play roles in disinformation spreading" (p. 196), and there are many humans and sources of information on the Internet. After all, even a reckless child can post information, write a comment, or even make a website. As still pointed out by Kraft & Donovan (2020), "disinformation relates to the fragmentation of conversational contexts across platforms" (p. 196), and despite institutional seals, high levels of disinformation have been diminishing the confidence raised on the Internet.

Moreover, unlike traditional media, Internet sources can be anonymous or have only a virtual identity. Also, most content producers are small in size, not benefiting in any way from the credibility associated with the scale and reputation of traditional mass media, like TV channels, the press, and other gatekeepers of information in the industrial age.

Therefore, each time becomes more difficult for individuals to distinguish the important from the trivial on the Internet. As if all this were not enough, predatory business models and actors who take advantage of new digital possibilities with the deliberate intention of centralizing, compartmentalizing, and manipulating information aggravate the ethical problem of contents' imprecision.

Till now, the Internet was and still is very different from traditional mass media, and digital interactivity is mostly responsible for this difference, shifting power from the emitter to the receptor, from broadcasting to narrowcasting (Hirst, et al., 2014), *i.e*., from antennas and TV cables to the computers, smartphones, and other user's devices. Such interactivity turned consumers into "prosumers," who are not mere information recipients. "Prosumers" are both consumers and producers (Toffler & Alvin, 1980), and it is thought that in the same way that they share data on the Internet of Information today, they will trade every time more tokens on the Internet of Value in the years ahead.

Of course, when it is about business transactions, for instance, in the energy sector, data accuracy and content precision will become even a more critical factor than when it was just about data sharing.

Today, many households and office buildings have solar panels installed on their premises, and this allows them to be producers capable of selling surplus energy to others. This fostered the P2P concept of energy trading, by encouraging consumers to become prosumers (i.e., capable of both producing and selling surplus energy). This means that more energy is available, and consequently reduces overall energy costs. (…) Applying blockchain for energy trading has the potential to increase efficiency and security. (Ali et al., 2020, p. 2)

For all these reasons, it is increasingly important to investigate new ways to increase content's precision on the Internet, considering that the use of new decentralized ways of doing so is likely to provide guarantees of plurality and exemption that are practically impossible to obtain when the legitimacy of the information is centrally dictated.

Here is where Blockchain Technology (BT) comes in, obviating the need to trust intermediaries and central specifications thanks to a new kind of legitimacy defined by consensus. In a blockchain, there is virtually no risk of someone changing previously validated information or delete it. As will be seen in the next section, when distrust and polarization induced by social media content reach unprecedented limits (*e.g*., US Presidential Elections and Washington Riots), it is believed that the precision provided by BT applications will have an essential ethical role in modern society.

Precision of Content on the Internet of Value (IoV)

Blockchain Technology brought value to the Internet and empowered its users. This was possible because blockchains work by widely distributing a consensual ledger on the web, which has proved to be an immutable source of truth, auditable by stakeholders, and capable of guaranteeing the authenticity and integrity of transactions carried out in cyberspace. Thus, this *smart ledger* was soon called an "hiperledger" (Salem et al., 2008)

Traditional secure network design vests trust-relationship management and gatekeeping roles in a central actor with complete authority within the hierarchy of the network. Blockchain removes the requirements for centralized authority by removing the need for the trust management middleman role. (…) Its game-changing design secures and inscribes data, protecting it from tampering and corruption (Alcazar, 2017, pp. 92, 93)

As stated by Kewell et al. (2017), "a blockchain is a ledger of transactions of digital assets: of who owns what, who transacts what, of what is transacted and when" (p. 9), and therefore blockchains are

known as "smart ledgers" which "allow for the storage and future execution of computer programs, so-called smart contracts" (Carter, 2018, p. 8).

Blockchains are ledgers (or databases) and anything that can be coded into a ledger can be recorded on a blockchain. The most obvious data are numbers recording units of account. But strings of numbers can be used to represent identities, or programs, and in this way, ledgers can become units of computation. (…) What blockchains bring to the internet are public ledger protocols. What this does, in effect, is to turn the internet into a 'public computer', or a 'world computer.' (Davidson et al. 2017)

Blockchain Technology (BT) is a powerful "trust machine" (Economist, 2015). It will have profound implications for society, especially by allowing the execution of *smart contracts*, which applications are not limited to the financial sector, going from the detection of *fake news* and *deepfake*, to the creation of a new type of political confidence based on cryptography.

It is crucial to have techniques to detect, fight, and combat "deepfake" digital content that may include fake videos, images, paintings, audios, and so on. Achieving this purpose is not difficult if there is a credible, secure, and trusted way to trace the history of digital content. Users should be given access to a trusted data provenance of the digital content, and be able to track back an item in history to prove its originality and authenticity (Hasan & Salah, 2019, p. 41596)

The application of the blockchain protocol to ensure data's accuracy is a mark to the economy. As mentioned above, BT makes it possible to create tokens that certify fungible assets (*e.g.*, guaranteeing their provenance) or prove non-fungible ones' genuineness (*e.g.*, artwork uniqueness). Not least, tokens will streamline transactions. For example, the fungible tokens can perform speedy transactions with no middleman (Grover et al., 2019), and the non-fungible ones can allow partial ownership of expensive items that are yet illiquid because of their price tag so that many more individuals can own them and transact them (Dai, 2020).

Blockchain is like a register that stores transactions in an accruable, safe, transparent, and traceable way. As a secure and distributed register of transactions, blockchain is being explored as a means of reliably certifying the origins and history of particular products: whether in terms of securing food supply chains, or in recording the many linked acts of creation and ownership that define the provenance of an artwork. In the future, we may adopt the same solution wherever there is a need to ensure (or establish) the originality and authenticity of some artefact, be it a written document, a photo, a video or a painting. (Floridi, 2018, p. 321)

Smart-contracts can specify business terms, including those necessary to assure content precision. In a few words, *smart-contracts* remove distrust not only from business equations but also from digital interactions in general. For instance, they can be used to authenticate a video and avoid *deep fakes*, *i.e.*, "hyper-realistic videos that apply artificial intelligence (AI) to depict someone say and do things that never happened" (Westerlund, 2019, p. 39). In this case, the *smart-contract* may include attributes and variables to register the video's details and its owner's data.

Smart contracts typically codify the business logic of a blockchain application. For example, a lottery contract contains logic that decides when the player wins the jackpot, and what percentage of each bet will go to the owner of the lottery. (…) Millions of smart contracts have already been deployed on Ethereum. Consistent with all human endeavour, the developers of smart contracts are striving for success. (Hartel et al. 2019, p. 177539)

Smart contracts can also have parameters that include the editing and distribution permissions of a video according to contractual clauses. This convenient integration is done through code and math, and the entire execution of the contract is immediately registered, being that the *hash* of the video will forever seal its authenticity. Therefore, if a user wants to track a video to its source, he can easily do that. This blockchain's method is a remarkable way to verify *contents' pedigree*, and it works well with data stored in any digital format, as is the case of decentralized files storing systems:

We provide a solution [using] smart contracts to trace and track the provenance and history of digital content to its original source even if the digital content is copied multiple times. The smart contract utilizes the hashes of the Inter-Planetary File System (IPFS) used to store digital content and its metadata. (…) IPFS generates a unique hash which is the address of a bundle of files containing the video content and its metadata. The hash address is used to locate and access the bundle of files stored on the IPFS network. (Hasan & Salah, 2019, pp. 41596, 41598)

Stored files can also be bundled with property rights agreements and deployed in "smart-contracts, and "[that] bundle can include a file containing the terms and conditions agreement of copying and editing in case the video [or any other data format] to be copied to create [or remix] different content by other authors or artists." (Hasan & Salah, 2019, p. 41598)

It is thought that *smart-contracts* will be very relevant in healthcare. For example, they can determine which specific health data will be shared with researchers accredited by the university A or instead by paying the amount X. They also can be executed on a specific date or if blood test results have a particular value. In the first case, the smart-contract would be executed by unblocking a payment when calendar date Y arrived, while in the second case, the *smart-contract* would be fulfilled by sending a medical prescription when the blood test reached a Z level. In yet another example, a researcher can hire N participants for clinical trials, doing so based on a quantification of a given variable, for instance, genetic (Gn), therapeutic (Tn), or demographic criteria (Dn). It should be noted that researchers must be able to stipulate contractual conditions without having access to the patients' identity. On the contrary, as long as patient data belong to intermediaries, clinical trial participants will continue not to be *hired* but instead recruited. This usual terminology can be quite revealing of the interests at hand, namely showing the absence of financial compensation for the *recruited* ones. In summary, *smart-contracts* guarantee precision to clinical research while ensuring that patients themselves will control their clinical data (Srinivasan, 2017).

Finally, BT also makes it possible to eliminate counterfeit medicines, ensure knowledge of provenance, and track the pharmaceutical industry's supply chain. This provenance checking is essential, directly impacting a patient's health and augmenting consumer trust. Among many other applications, BT can be used to check medical records (*e.g.*, vaccination bulletins) or manage safe transactions with stakeholders, for example, insurance companies (IEEE, 2018).

SOLUTIONS AND RECOMMENDATIONS

As stated by Kranzberg (1986), "technology is neither good nor bad; nor is it neutral" (p. 545), and it is the way technology is used that dictates the respective outcomes, both for good and evil. Thus, technological innovations dispense *a priori* ethical justifications. As referred by Keweel et al. (2017), "innovations are morally and ethically instantiated" (p. 429). Nonetheless, although it does not make sense from an ethical point of view to evaluate a technology innovation by itself, it is worth evaluating it in terms of its effectiveness and transformative potential. In the case of Blockchain Technology (BT), "study shows that there are huge potentials to use blockchain technology" (Lorne et al. 2018, p. 107), and this is a potentially disruptive technology (Frizzo-Barker et al. 2020).

Data's centralization is being promoted by "tech giants as data-driven intellectual monopolies" (Rikapp & Lundvall, 2020, p. 2). Sure, these colossal data silos organize their innovation activities but can delay data sharing and compromise privacy and complicate data linkage, preventing ontologies from being made to create a fully semantic web. As those data silos are too big, it also can perish competition and the free market. Only when information is securely shared, cross-fertilization of ideas can occur, and innovation can thrive. Therefore, openness is considered an ethical solution, which is why BT, "as a data management technology" (Alcazar, 2017, p.93), should be recommended.

As it is known, the electronic health records (EHR) repository is fragmented across healthcare providers and other stakeholders. Decentralized tamper-proof data repositories can be combined with a data management system to avoid patient data leakage and arbitrary modifications on personal clinical data. Such modifications should not be done by anyone other than the patients themselves or whoever delegated by them (*e.g.*, clinicians). Therefore BT-based data management solutions can be the right choice aiming at safety and convenience.

Sharing and transacting health data is crucial to improving healthcare service (including self-service) and reducing medical costs. Hence, distributed BT-based networks can facilitate patient data collection by creating a reliable environment for a secure data exchange and eliminating the privacy problem. This environment can solve, for example, ethical-legal problems in running clinical trials. BT also should be considered to create supply chain traceability solutions, letting patients have access to information about the provenance and validity of medicines, increasing consumer confidence and safety.

Finally, by implementing secure blockchain networks in healthcare services, patients regain ownership of their health data. Being in control of own data is required to share or transact it safely to satisfy patients 'needs and their communities' healthcare goals. Finally, it is thought that this rationale generally applies to other sectors of society.

LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

There are limitations inherent to the Internet itself that can prevent Blockchain Technology (BT) from ethically fulfilling its democratizing potential. Internet basic functionalities depend on very few service providers, and the Internet is controlled by only a few multinational companies (Jensen, 2020). As stated by Lopez et al. (2019), "Even though the Internet design is inherently decentralized, in practice, key functionalities rely on a very few service providers, who support and thus may effectively control the Internet." (p. 1901). Hopefully, BT will decentralize the political-economic playing field, mostly when user-friendly decentralized apps (dApps) become available, reducing the costs of trust and empower-

ing users with the cryptographic resources needed to use blockchains without losing their privacy (see Chapter 4). Therefore, the investigation of such dApps is crucial for ethical reasons, allowing building more competitive solutions to lower transaction costs, which most economic agents will appreciate.

There are also technical limitations in the blockchains themselves. According to Qin & Gervais (2018), *the scaling trilemma* dictates that blockchains can have at most two of the following three properties: *decentralization*, *scalability*, and *security*. This technical trade-off is related to performance aspects, such as the slow rate of transactions featured on *public-permissionless blockchains*, which are freely accessible. These blockchains have no hierarchical constraints to work, and although such absence of authoritative parts eventually makes them function too slow as more computation tasks are required, that is the price to pay for having a *trustless* system just based on sophisticated math, namely a *cocktail* of cryptographic functions.

The governance of *public-permissionless blockchains* is entirely decentralized, which can be advantageous, but their programming and maintenance, in charge of the so-called *core developers*, is complex. Without getting into technical specifications, which are out of this chapter's scope, there are reasons to believe that more agile and versatile solutions will arise from using better algorithms and *hybrid blockchain*s. There are at least two hybrid solutions to optimize the trade-off mentioned above: *private-permissionless blockchains*, which allow more privacy by restricting transactions log viewers and more security by extending consensus participants, as well as *public-permissioned blockchains*, which allow gaining speed by restricting consensus participants, and more transparency by extending log viewers. The latter combines transparency and scalability gains with the privacy and security limitations inherent to centralization, sacrificing the *non-censorship resistance* as authoritative nodes can override/delete any commands. The former combines privacy and security gains with the scalability limitations of consensus (Neitz, 2019). It is thought that these and other BT technical limitations (some inflated as is the case of alleged electricity excessive consumption dealt with in the homonymous section of Chapter 4) will be overcome because its protocols are evolutionary and are being improved since its creation. This improvement effort has already produced alternative consensus protocols (*e.g.*, *proof-of-stake*), which can validate and record transactions more efficiently (Irresberger et al., 2020). As such, BT's Research and Development (R&D) should focus on the trade-off between network speed, scalability, and privacy on the one hand and the consensuses' transparency and security on the other.

Finally, one should notice that if more than half of the blockchain networks' computer nodes accept incorrect information as legit, this information will become the network accepted truth. Such a problem is called *the 51% attack*, and "adversaries controlling more than half of the total hashing power of a [blockchain] network can perform this attack" (Sayeed & Marco-Gisbert, 2019, p. 1788). Hence, the R&D of trustable consensus mechanisms is crucial to reducing transaction costs by improving BT's efficiency and safety. Thus, this is a top research priority, and the referred *cyberethics-mix* will benefit from improved blockchain governance (see Chapter 4). Hopefully, such governance will be decentralized to safeguard citizens' privacy, property accessing rights, content precision, transparency, plurality, and democracy.

CONCLUSION

On the one hand, blockchain technology (BT) allows democratizing several political-economic prerogatives once exclusively used by public and private intermediaries. On the other hand, BT grants centralizing

governance even further, and Central Bank Digital Currency (CBDC) is a good example of that. Such ambivalence raises ethical dilemmas as a new confidence-building mechanism unleashes distributed trust on the new Internet of Value decisively changing the political power dynamics.

Thanks to blockchain protocols, Internet users can share and transact *zero-knowledge proofs* (see *Key Terms and Definitions*) about which data is valid and who stands for that validity without revealing the data itself. In this way, identity owners do not need to store private data or personal information on a blockchain network to use and transact that same data. What is stored is just cryptographic code that represents the data but hides sensitive information. This way, for the first time, people can have the best of two worlds: privacy and convenience.

Enabling data interoperability without compromising its security and confidentiality, BT is changing the data management paradigm. Blockchain-powered *decentralized apps* (see *Key Terms and Definitions*) will make it possible to store the consumers' encrypted identities, solving personal data management's ethical constraints hampering the stipulation of business terms, especially for privacy reasons.

Data accuracy can be used to prove data genuineness. Such precision allows creating *smart contracts*, which are self-executable and can be used to automate business transactions, making them irrevocable, assuring transparency, and guaranteeing accountability. Smart contracts can also ensure privacy and data ownership rights, being widely applicable in many situations. For example, they can be used to prove data authenticity (*e.g.,* clearing fake news) and guarantee government accountability, for instance, binding political promises to electoral results. This blind trust is possible because smart contracts deliver immutable budget allocation (see Chapter 4).

BT also reduces complexity and costs in healthcare, making it possible for patients to become the sole owners of their data. Once released from privacy constraints, patient communities will be able, for example, to aggregate and monetize individual health records according to their collective interests, such as participating or not in specific clinical trials.

Supposing that free-market prevails, one can expect that user-friendly decentralized applications (*dApps*) will change healthcare, including pharmaceutical research and development (R&D). Aggregated data increases the bargaining power of patients' communities facing healthcare intermediaries. Thus, blockchain-enabled business networks can induce a redistribution of value, transferring it from shareholders to stakeholders. BT will also make it possible to eliminate counterfeit medicines, safely check medical records (*e.g*., vaccination certificates) and guarantee safe transactions with other stakeholders (*e.g.,* insurance companies), among many other applications.

BT can change the data management paradigm decentralizing transactions and redistributing wealth by democratizing value transfer prerogatives, paving the way to a more ethical society. In 2012, the author figuratively referred to the need for an ethical computer engineer to apply the appropriate digital technologies to safeguard people's rights in the digital era. Hopefully, there will be political discernment in the present decade to unleash the new distributed trust so that people themselves can play the role of that ethical engineer.

REFERENCES

AICPA. (2020). *Privacy Risk Management*. Available online at: https://www.aicpa.org/interestareas/informationtechnology/resources/privacy-risk-management.html

Alcazar, C. V. (2017). Data you can trust. *Air and Space Power Journal*, *31*(2), 91–101.

Ali, F., Aloqaily, M., Alfandi, O., & Ozkasap, O. (2020). *Peer-to-Peer Blockchain based Energy Trading*. arXiv preprint arXiv:2001.00746.

Ali, R., & Narula, N. (2020). *Redesigning digital money: What can we learn from a decade of crypto-currencies. Digital Currency Iniative (DCI)*. MIT Media Lab.

Allan, K., & Mortensen, J. (2020). Legal Identity Documenting in Disasters: Perpetuating Systems of Injustice. In Natural Hazards and Disaster Justice (pp. 261-278). Palgrave Macmillan.

Alleman, J. (2018). Threat of Internet Platforms: Facebook, Google, etc. In *29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?"*. Trento, Italy: International Telecommunications Society (ITS).

Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., & Zhang, F. (2020). *Design Choices for Central Bank Digital Currency: Policy and Technical Considerations (No. w27634)*. National Bureau of Economic Research. doi:10.3386/w27634

Anderson, C. (2009). *Free: The future of a radical price*. Random House.

Antonopoulos, A. M. (2016). *The internet of money* (Vol. 1). Merkle Bloom LLC.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain*. O'Reilly Media, Inc.

Bao, J., He, D., Luo, M., & Choo, K. K. R. (2020). A survey of blockchain applications in the energy sector. *IEEE Systems Journal*, 1–12. doi:10.1109/JSYST.2020.2998791

Barki, A., & Gouget, A. (2020). *Achieving privacy and accountability in traceable digital currency*. Cryptology ePrint Archive, Report 2020/1565.

Barnes, S. B. (2006). A privacy paradox: Social networking in the united states. *First Monday*, *11*(9). Advance online publication. doi:10.5210/fm.v11i9.1394

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. doi:10.1016/j.tele.2017.04.013

Beller, J. (2020). Economic Media: Crypto and the Myth of Total Liquidity. *Australian Humanities Review*, *66*, 215–225.

Bellini, E., Iraqi, Y., & Damiani, E. (2020). Blockchain-based distributed trust and reputation management systems: A survey. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 21127–21151. doi:10.1109/ACCESS.2020.2969820

Bengio, Y., Ippolito, D., Janda, R., Jarvie, M., Prud'homme, B., Rousseau, J. F., ... Yu, Y. W. (2020). Inherent privacy limitations of decentralized contact tracing apps. *Journal of the American Medical Informatics Association: JAMIA*. Advance online publication. doi:10.1093/jamia/ocaa153 PMID:32584990

BergC.DavidsonS.PottsJ. (2017). Blockchains industrialise trust. Available at SSRN 3074070.

Berg, C., Davidson, S., & Potts, J. (2019). BT as economic infrastructure: Revisiting the electronic markets hypothesis. *Frontiers in Blockchain*, *2*, 22. doi:10.3389/fbloc.2019.00022

Bergeron, J., Nguyen, A., Alt, C., Brewster, N., Krohn, T., Luong, V., ... Moss-Pultz, S. (2020). Simulating patient matching to clinical trials using a property rights blockchain. *Digital Medicine*, *6*(1), 44. doi:10.4103/digm.digm_30_19

Berners-Lee, T. Fielding, R. & Frystyk, H. (1996). *Hypertext transfer protocol--HTTP/1.0*. Academic Press.

Berry, P. (2020). Troubleshooting algorithms: A book review of Weapons of Math Destruction by Cathy O'Neil. *The McMaster Journal of Communication*, *12*(2), 91–96. doi:10.15173/mjc.v12i2.2450

Berwick, D. M. (2020). Choices for the "new normal". *Journal of the American Medical Association*, *323*(21), 2125–2126. doi:10.1001/jama.2020.6949 PMID:32364589

Bichler, S., & Nitzan, J. (2021). *Corporate Power and the Future of US Capitalism*. Real-World Economics Review Blog.

Bleier, A., Goldfarb, A., & Tuckerc, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466–480. doi:10.1016/j.ijresmar.2020.03.006

Brown, I., & Korff, D. (2009). Terrorism and the proportionality of internet surveillance. *European Journal of Criminology*, *6*(2), 119–134. doi:10.1177/1477370808100541

Buterin, V. (2017). *Introduction to Cryptoeconomics*. Paper presented to Ethereum Foundation.

Buyle, R., Taelman, R., Mostaert, K., Joris, G., Mannens, E., Verborgh, R., & Berners-Lee, T. (2019, November). Streamlining governmental processes by putting citizens in control of their personal data. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia* (pp. 346-359). Springer.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian, 17*, 22.

Carter, S. (2018). *Timestamping Smart Ledgers: Comparable, Universal, Traceable, Immune*. Timestamping Smart Ledgers-Long Finance.

Casey, M. J., & Vigna, P. (2018). In blockchain we trust. *MIT's Technology Review*, *121*(3), 10–16.

Castells, M. (2011). *The rise of the network society* (Vol. 12). John Wiley & Sons.

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, *13*, e00151. doi:10.1016/j.jbvi.2019.e00151

Clark, D. (1988, August). The design philosophy of the DARPA Internet protocols. In *Symposium proceedings on Communications architectures and protocols* (pp. 106-114) 10.1145/52324.52336

Coase, R. H. (1993). *The nature of the firm: origins, evolution, and development*. Oxford University Press.

Dai, C. (2020). DEX: A DApp for the Decentralized Marketplace. In *Blockchain and Crypt Currency* (pp. 95–106). Springer. doi:10.1007/978-981-15-3376-1_6

Datta, P., & Chatterjee, S. (2008). The economics and psychology of consumer trust in intermediaries in electronic markets: The EM-Trust Framework. *European Journal of Information Systems*, *17*(1), 12–28. doi:10.1057/palgrave.ejis.3000729

DavidsonS.De FilippiP.PottsJ. (2016). Disrupting governance: The new institutional economics of distributed ledger technology. Available at SSRN 2811995. doi:10.2139srn.2811995

Davidson, S., De Filippi, P., & Potts, J. (2017). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, *14*(4), 639–658. doi:10.1017/S1744137417000200

DavidsonS.NovakM.PottsJ. (2018). The cost of trust: a pilot study. Available at SSRN 3218761.

De Montjoye, Y. A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536–539. doi:10.1126cience.1256297 PMID:25635097

Dehaye, P. O., & Reardon, J. (2020, November). Proximity Tracing in an Ecosystem of Surveillance Capitalism. In *Proceedings of the 19th Workshop on Privacy in the Electronic Society* (pp. 191-203). 10.1145/3411497.3420219

Dewing, M. (2021). Combining Social & Legal Constructions: Constitutional Reformations for the Future. *FAU Undergraduate Law Journal*, 57-79.

Dunbar, R. (2010). *How many friends does one person need? Dunbar's number and other evolutionary quirks*. Faber & Faber.

Echarte Fernández, M. Á., Náñez Alonso, S. L., Jorge-Vázquez, J., & Reier Forradellas, R. F. (2021). Central Banks' Monetary Policy in the Face of the COVID-19 Economic Crisis: Monetary Stimulus and the Emergence of CBDCs. *Sustainability*, *13*(8), 4242. doi:10.3390u13084242

Economist. (2015). The promise of the blockchain: The trust machine'. *The Economist, 31*, 27.

Einaste, T. (2018). *Blockchain and healthcare: the Estonian experience—e-Estonia*. https://eestonia.com/blockchain-healthcare-estonian-experience/

Entriken, Evans, & Sachs. (2018). *ERC-721 Non-Fungible Token Standard*. Retrieved from https://eips.ethereum.org/EIPS/eip-721

Euzenat, J., & Rousset, M. C. (2020). Semantic web. In *A Guided Tour of Artificial Intelligence Research* (pp. 181–207). Springer. doi:10.1007/978-3-030-06170-8_6

Feilmayr, C., & Wolfram, W. (2016). An Analysis of Ontologies and Their Success Factors for Application to Business. *Data & Knowledge Engineering*, *101*, 1–23. doi:10.1016/j.datak.2015.11.003

Flew, T. (2005). Creative Commons and the creative industries. *Media and Arts Law Review*, *10*(4), 257–264.

Floridi, L. (2018). Artificial intelligence, deepfakes and a future of ectypes. *Philosophy & Technology*, *31*(3), 317–321. doi:10.100713347-018-0325-3

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, *51*, 102029. doi:10.1016/j.ijinfomgt.2019.10.014

Garcia-Rivadulla, S. (2016). Personalization vs. privacy: An inevitable trade-off? *IFLA Journal*, *42*(3), 227–238. doi:10.1177/0340035216662890

GDPR. (2018). *General data protection regulation (GDPR).* Intersoft Consulting.

Gerard, D. (2020). *Libra Shrugged: How Facebook Tried to Take Over the Money*. David Gerard.

Goldwater, J. (2016). The use of a blockchain to foster the development of patient-reported outcome measures. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, MD: ONC/NIST.

Goss, A. K. (2007). Codifying a commons: Copyright, copyleft, and the Creative Commons project. Chi.-. *Kent L. Rev.*, *82*, 963.

Grover, P., Kar, A. K., Janssen, M., & Ilavarasan, P. V. (2019). Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions–insights from user-generated content on Twitter. *Enterprise Information Systems*, *13*(6), 771–800. doi:10.1080/17517575.2019.1599446

Günzel-Jensen, F. & Holm, A. B. (2015). Freemium Business Models as the Foundation for Growing an E-Business Venture: A Multiple Case Study of Industry Leaders. *Journal of Entrepreneurship, Management and Innovation, 10*.

Hardy, K., & Maurushat, A. (2017). Opening up government data for Big Data analysis and public benefit. *Computer Law & Security Review*, *33*(1), 30–37. doi:10.1016/j.clsr.2016.11.003

Harel, T. O., Jameson, J. K., & Maoz, I. (2020). The Normalization of Hatred: Identity, Affective Polarization, and Dehumanization on Facebook in the Context of Intractable Political Conflict. *Social Media + Society*, *6*(2). doi:10.1177/2056305120913983

Hart, W., Albarracín, D., Eagly, A. H., Brechan, I., Lindberg, M. J., & Merrill, L. (2009). Feeling validated versus being correct: A meta-analysis of selective exposure to information. *Psychological Bulletin*, *135*(4), 555–588. doi:10.1037/a0015701 PMID:19586162

Hartel, P., Homoliak, I., & Reijsbergen, D. (2019). An Empirical Study Into the Success of Listed Smart Contracts in Ethereum. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 177539–177555. doi:10.1109/ACCESS.2019.2957284

Hasan, H. R., & Salah, K. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 41596–41606. doi:10.1109/ACCESS.2019.2905689

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Differential privacy techniques for cyber physical systems: A survey. *IEEE Communications Surveys and Tutorials*, *22*(1), 746–789. doi:10.1109/COMST.2019.2944748

Helbing, D. (2017). From remote-controlled to self-controlled citizens. *The European Physical Journal. Special Topics*, *226*(2), 313–320. doi:10.1140/epjst/e2016-60372-1

Heston, T. (2017). *A case study in blockchain healthcare innovation*. Academic Press.

Hirst, M., Harrison, J., & Mazepa, P. (2014). *Communication and new media: From broadcast to narrowcast*. Oxford University Press.

Hobbes, T. (1914). *Leviathan*. Dent.

IEEE SA Beyond Standards. (2018). *Leveraging Blockchain for Clinical Trials/Research*. Available at: https://beyondstandards.ieee.org/leveraging-blockchain-clinical-trials-research/

Insight, A. (2021, May 30). *Digital Currency v/s Cryptocurrency: Brief Overview for Beginners.* Retrieved May 30, 2021, from https://www.analyticsinsight.net/digital-currency-v-s-cryptocurrency-brief-overview-for-beginners/

IrresbergerF.JohnK.SalehF. (2020). The Public Blockchain Ecosystem: An Empirical Analysis. Available at SSRN. doi:10.2139srn.3592849

Jacobovitz, O. (2016). *Blockchain for identity management*. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University.

Jeffries, D. (2021, May 21). *Dan Jeffries: It's 2031. This Is the World That Crypto Created*. Retrieved May 22, 2021, from https://www.coindesk.com/its-2031-this-is-the-world-that-crypto-created

Jensen, J. L. (2020). *The Medieval Internet: Power, politics and participation in the digital age*. Emerald Group Publishing.

Jørgensen, R. F. (2020). The right to privacy under pressure. *Nordicom Review*, *37*(s1), 165–170. doi:10.1515/nor-2016-0030

Karafiloski, E., & Mishev, A. (2017, July). Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017-17th International Conference on Smart Technologies* (pp. 763-768). IEEE. 10.1109/EUROCON.2017.8011213

Kewell, B., Adams, R., & Parry, G. (2017). Blockchain for good? *Strategic Change*, *26*(5), 429–437. doi:10.1002/jsc.2143

King, P. W. (2009). *Climbing Maslow's pyramid*. Troubador Publishing Ltd.

Kotler, P. (1999). *Marketing management: The millennium edition* (Vol. 199). Prentice Hall.

Kotler, P., Kartajaya, H., & Setiawan, I. (2016). *Marketing 4.0: Moving from traditional to digital*. John Wiley & Sons.

Koufakis, A., Chatzakou, D., Meditskos, G., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2020). *Invited keynote on IOT4SAFE 2020: Semantic Web Technologies in Fighting Crime and Terrorism: The CONNEXIONs Approach*. Academic Press.

Krafft, P. M., & Donovan, J. (2020). Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign. *Political Communication*, *37*(2), 194–214. doi:10.1080/10584609.2019.1686094

Kranzberg, M. (1986). Technology and History:" Kranzberg's Laws. *Technology and Culture*, *27*(3), 544–560. doi:10.2307/3105385

Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional*, *19*(4), 68–72. doi:10.1109/MITP.2017.3051335

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... Wolff, S. (2009). A brief history of the Internet. *Computer Communication Review*, *39*(5), 22–31.

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018a, December). BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE.

Liu, J., Li, B., Chen, L., Hou, M., Xiang, F., & Wang, P. (2018, June). A data storage method based on blockchain for decentralization DNS. In *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)* (pp. 189-196). IEEE.

Liu, T., Cui, Z., Du, H., & Wu, Z. (2021). Privacy-Preserving and Verifiable Electronic Voting Scheme Based on Smart Contract of Blockchain. *International Journal of Network Security*, *23*(2), 296–304.

Lo, S. K., Xu, X., Staples, M., & Yao, L. (2020). Reliability analysis for blockchain oracles R. *Computers & Electrical Engineering*, *83*(10658), 2.

Lopez, P. G., Montresor, A., & Datta, A. (2019, July). Please, do not decentralize the Internet with (permissionless) blockchains! In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1901-1911). IEEE.

Lorne, F. T., Daram, S., Frantz, R., Kumar, N., Mohammed, A., & Muley, A. (2018). Blockchain Economics and Marketing. *Journal of Computer and Communications*, *6*(12), 107–117.

Magyar, G. (2017, November). Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In *2017 IEEE 30th Neumann Colloquium (NC)* (pp. 135-140). IEEE.

Mainelli, M. (2017). Blockchain could help us reclaim control of our personal data. *Harvard Business Review Digital Articles*, 2-5.

Martin & Murphy. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135-155.

Martin, K. (2019). Designing Ethical Algorithms. *MIS Quarterly Executive*, *18*(2).

Martins, P. (2018). *Introdução à Blockchain*. FCA-Editora de Informática, Lda.

Marturano, A. (2002). The role of metaethics and the future of computer ethics. *Ethics and Information Technology*, *4*(1), 71–78.

Maslow, A. H. (1943). A Theory of Human Motivation. *Psychological Review*, *50*, 370–396.

Meier, P., Beinke, J. H., Fitte, C., & Teuteberg, F. (2020). Generating design knowledge for blockchain-based access control to personal health records. *Information Systems and e-Business Management*, •••, 1–29.

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., & Weinhardt, C. (2018). "A blockchain-based smart grid: Towards sustainable local energy markets," Comput. Sci.-. *Research for Development*, *33*(1-2), 207–214.

Metcalfe, B. (1995). Metcalfe's law: A network becomes more valuable as it reaches more users. *Info-World*, *17*(40), 53–54.

Metsallik, J., Ross, P., Draheim, D., & Piho, G. (2018). Ten Years of the e-Health System in Estonia. CEUR Workshop Proceedings.

Monkiewicz, J. (2020). New Finance: In Search for Analytical Framework. Academic Press.

Moore, C., O'Neill, M., O'Sullivan, E., Doröz, Y., & Sunar, B. (2014, June). Practical homomorphic encryption: A survey. In *2014 IEEE International Symposium on Circuits and Systems (ISCAS)* (pp. 2792-2795). IEEE.

Morrow, M. J., & Zarrebini, M. (2019). Blockchain and the Tokenization of the Individual: Societal Implications. *Future Internet*, *11*(10), 220.

Muthe, K. B., Sharma, K., & Sri, K. E. N. (2020, November). A Blockchain Based Decentralized Computing And NFT Infrastructure For Game Networks. In *2020 Second International Conference on Blockchain Computing and Applications (BCCA)* (pp. 73-77). IEEE.

Muzzy, E. (2018). *CryptoKitties Isn't About the Cats*. Retrieved from https://medium.com/@everett.muzzy/cryptokitties-isnt-about-the-cats-aef47bcde92d

Nakamoto, S. (2008). *A peer-to-peer electronic cash system*. Bitcoin. https://bitcoin.org/bitcoin.pdf

Nakamura, Y., Zhang, Y., Sasabe, M., & Kasahara, S. (2020). Exploiting smart contracts for capability-based access control in the Internet of Things. *Sensors (Basel)*, *20*(6), 1793.

Narayan, R., & Tidström, A. (2020). Tokenizing coopetition in a blockchain for a transition to circular economy. *Journal of Cleaner Production*, *263*, 121437.

Negroponte, N. (1995). *Being Digital–A Book (P) review*. Wired.com, 3.

Neitz, M. B. (2019). The Influencers: Facebook's Libra, Public Blockchains, and the Ethical Considerations of Centralization. *NCJL & Tech.*, *21*, 41.

O'Neil, C. (2017). How can we stop algorithms telling lies? *The Guardian*, 7-16.

Peters, M. A. Green, B. & Yang, H. (2020). *Cryptocurrencies, China's sovereign digital currency (DCEP) and the US dollar system*. Academic Press.

Petrescu, M., & Krishen, A. S. (2020). The dilemma of social media algorithms and analytics. *J Market Anal*, *8*, 187–188. https://doi.org/10.1057/s41270-020-00094-4

Power, D. J., & Phillips-Wren, G. (2011). Impact of social media and Web 2.0 on decision-making. *Journal of Decision Systems*, *20*(3), 249–261.

Ramachandran, M., Chowdhury, N., Third, A., Domingue, J., Quick, K., & Bachler, M. (2020, April). Towards Complete Decentralised Verification of Data with Confidentiality: Different ways to connect Solid Pods and Blockchain. In *Companion Proceedings of the Web Conference 2020* (pp. 645-649). Academic Press.

Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2020). Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Systems Journal*.

Regner, F. Urbach, N. & Schweizer, A. (2019). *NFTs in Practice–Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application*. Academic Press.

Rikap, C., & Lundvall, B. Å. (2020). Big tech, knowledge predation and the implications for development. *Innovation and Development*, 1-28.

Rodrigues, D. (2012). Cyberethics of Business Social Networking. In E-Marketing: Concepts, Methodologies, Tools, and Applications (pp. 756-780). IGI Global.

Rodrigues, D. (2020, October 29). *The Dangerous Business Model of Social Networks*. Observador. https://observador.pt/opiniao/o-perigoso-modelo-de-negocio-das-redes-sociais/

Romer, P. (2002). When should we use intellectual property rights? *The American Economic Review*, *92*(2), 213–216.

Rooney, L., Rimpiläinen, S., Morrison, C., & Nielsen, S. L. (2019). *Review of emerging trends in digital health and care*. A report by the Digital Health and Care Institute.

Rowe, F., Ngwenyama, O., & Richet, J. L. (2020). Contact-tracing apps and alienation in the age of COVID-19. *European Journal of Information Systems*, 1–18.

Salem, A. O., Safeia, M. T. A., & Siam, S. M. (2008). *Report of Blockchain Techniques and Applications*. Academic Press.

Savelyev, A. (2018). Copyright in the blockchain era: Promises and challenges. *Computer Law & Security Review*, *34*(3), 550–561.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences (Basel, Switzerland)*, *9*(9), 1788.

Schneier, B. (2012). *Liars and outliers: enabling the trust that society needs to thrive*. John Wiley & Sons.

Sfetcu, N. (2019, February 17). *Blockchain Design and Modelling*. SetThings. https://www.setthings.com/en/blockchain-design-and-modelling/

Smith, A. (1937). *The wealth of nations*. Academic Press. (Original publication 1776)

Smith, A. (1989). Of the Origin and Use of Money. In General Equilibrium Models of Monetary Economies (pp. 47-53). Academic Press.

Somerville, I., & Wood, E. (2008). Business ethics, public relations and corporate social responsibility. In *The public relations handbook* (pp. 143–160). Routledge.

Srinivasan, P. (2017, November 9). *Healthcare Blockchain: How smart contracts could revolutionize care delivery*. Prolifics.

Sunstein, C. R. (2009). *Going to extremes: How like minds unite and divide*. Oxford University Press.

Surowiecki, J. (2005). *The wisdom of crowds*. Anchor.

Sweeney, L. (2015). Only you, your doctor, and many others may know. *Technology Science*, *2015092903*(9), 29.

Szabo, N. (2002). *The Origins of Money (No. 0211005)*. University Library of Munich.

Tam, K. P. (2021). The new normal of social psychology in the face of the COVID-19 pandemic: Insights and advice from leaders in the field. *Asian Journal of Social Psychology*, *24*(1), 8.

Tanner, A. (2016). For Sale: Your Medical Records. *Scientific American*, *314*(2), 26–27. Retrieved November 30, 2020, from https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/

Tanner, A. (2017). *Strengthening protection of patient medical data*. The Century Foundation.

Taplin, J. (2017). *Move fast and break things: How Facebook, Google, and Amazon have cornered culture and what it means for all of us*. Pan Macmillan.

Tapscott, D., & Euchner, J. (2019). Blockchain and the IoV: An Interview with Don Tapscott Don Tapscott talks with Jim Euchner about blockchain, the IoV, and the next Internet revolution. *Research Technology Management*, *62*(1), 12–19.

Toffler, A., & Alvin, T. (1980). *The third wave* (Vol. 484). Bantam books.

Truong, N. B., Um, T. W., Zhou, B., & Lee, G. M. (2018, May). Strengthening the blockchain-based IoV with trust. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 5112–5127.

Twesige, R. (2015). *A simple explanation of Bitcoin and Block Chain technology*. https://www.researchgate.net/profile/Richard-Twesige 2/publication/270287317_Bitcoin_A_simple_explanation_of_Bitcoin_and_Block_Chain_technology_JANUARY_2015_RICHARD_LEE_TWESIGE/links/54a7836f0cf267bdb90a0ee6/Bitcoin-A-simple-explanation-of-Bitcoin-and-Block-Chain-technology-JANUARY-2015-RICHARD-LEE-TWESIGE.pdf

United Nations General Assembly. (1948). Universal declaration of human rights. United Nations.

Van der Aalst, W., Hinz, O., & Weinhardt, C. (2019). *Big digital platforms*. Academic Press.

Van der Meer, T. G., Hameleers, M., & Kroon, A. C. (2020). Crafting our own biased media diets: The effects of confirmation, source, and negativity bias on selective attendance to online news. *Mass Communication & Society*, *23*(6), 937–967.

Visconti, R. M. (2020). Blockchain Valuation: IoV and Smart Transactions. In The Valuation of Digital Intangibles (pp. 401-422). Palgrave Macmillan.

Wen, H. (2020). A study of the privacy of covid-19 contact tracing apps. *International Conference on Security and Privacy in Communication Networks*.

Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11).

Wildman, N., Archer, A., Brouwer, H. M., & Cawston, A. (2019). *The ethics of data acquisition: Protecting Privacy and Autonomy While Harnessing the Potential of Big Data*. Academic Press.

Yaeger, K., Martini, M., Rasouli, J., & Costa, A. (2019). Emerging BT solutions for modern healthcare infrastructure. *Journal of Scientific Innovation in Medicine*, *2*(1).

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview.* arXiv preprint arXiv:1906.11078.

Yaji, S., Bangera, K., & Neelima, B. (2018). Privacy Preserving in Blockchain Based on Partial Homomorphic Encryption System for Ai Applications. *IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)*, 81-85. doi: 10.1109/HiPCW.2018.8634280

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019). Research on the Application of Cryptography on the Blockchain. *Journal of Physics: Conference Series*, *1168*, 032077.

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3), 1–34.

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180-184). IEEE.

KEY TERMS AND DEFINITIONS

Consensus: A group decision-making process in which group members develop and agree to support a decision in the best interest of the whole.

Decentralized Apps (DAPPS): Digital applications or programs that exist and run on a blockchain or P2P network of computers (instead of a single computer) and are outside the purview and control of a single authority.

Ethereum Request for Comments (ERC): A token standard that implements an Application Programming Interface (API) for tokens within *smart contracts*. It provides functionalities like transferring tokens from one account to another, to get the current token balance of an account, and the total supply of the token available on the network.

Smart Contract: A smart contract is a piece of code implementing arbitrary rules on a computer with distributed consensus (a blockchain), such that when the code is live it cannot be changed. Smart contracts are business logic that runs on a code that no one party controls or can turn off.

Token: A unit of value secured by cryptography that represents an asset or a specific use or functionality. It is created on top of a blockchain by using *smart contracts*.

Zero-Knowledge Proof: A cryptographic way of proofing that a statement is true without revealing anything beyond the veracity of that statement.