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 4
Blockchanging Politics: Opening a Trustworthy but Hazardous Reforming Era

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

Pedro Santana Lopes
GlobalLawyers, Portugal

ABSTRACT

There has been a fundamental change in the genesis of political-economic trust, with the arrival of a decentralized but structured way to reach consensuses and automatically implementing decisions through self-executable contracts. Blockchain technology (BT) is a distributed, consensus-based, and secure way for individuals to make enforceable censorship-resistant quantifiable agreements. Every vote is a transaction, and BT is paving the way for decentralizing politics, defending privacy, and streamlining voting procedures. It has the potential to provide much more granular governance that hopefully will preserve freedom and defend democracy. However, especially in an embarrassing post-COVID-19 world, BT's centralization can, instead, pave the way for citizens' control, turning cryptographic protocols into an authoritarian digital corset tightened by some to menace the privacy and freedom of many.

INTRODUCTION

"Invention is the mother of necessity." (Kranzberg, 1986) Kranzberg's Second Law

To change the world is the dream of some. Blockchain Technology (BT) empowers humankind with the potential to fulfill that dream or make it a nightmare. In this chapter it will be discussed why BT can make-or-break democracy in a "post-Covid uncertain future" (Leach et al., 2020, p.1), being uncertain who will benefit the most now that confidence is embedded on the Internet "through a distributed consensus protocol" (Faber et al., 2020, p. 6857).

DOI: 10.4018/978-1-7998-7363-1.ch004

A permanent record of all transactions is set in "cryptographic stone" on the ledger, which means no one can rewrite or deny history. In other words, it is impossible to cheat with blockchain because everything is in the open to those involved and authorized to see. Risk is minimized in a system in which governance is truly shared. I can't think of a better definition of trust. (Dwyer, 2017, p. 12)

As argued by Young (2018), BT's *distributed-trust* makes it possible to dream about a political transformation that includes a never seen democratic authenticity where granular decisions will be made by citizens holding governments directly accountable thanks to decentralized blockchain-based transactions and a "smart social contract" (Young, 2018, p. 61).

Blockchain technology has the potential to reshape the organizational landscape, rendering traditional, hierarchical ways of organizing obsolete. Its distributed nature enables organizing in nonhierarchical ways. […] nonhierarchical ways of organizing the structures needed to build new social contracts [(smart social contracts)] for sustainability and further shape the transition to a sustainable development. (Faber & Hadders, 2016, p. 17)

It is thought that BT can be used to enhance or disrupt democracy, and this chapter highlights what is believed to be a historic opportunity to guarantee political transparency to build trust. Such trust has never been as necessary as today to preserve privacy and freedom aiming for a digital responsive democracy that leads to a sustainable and fair society.

The authors approached BT's political implications from a liberal democratic perspective. They opted for an investigation method based on qualitative research. The research methodology chosen was the literature review, which is considered adequate to overview several thematic areas on a given topic. Among the literature review, 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 of social sciences knowledge, which is required to make the intended political-economic analysis, the authors used an 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 far as the authors were able to observe, this lack of research still characterizes the study of BT's political implications.

This chapter is organized as follows: BT and decentralization will be considered first before discussing why the Internet is entering a new stage to change society again, this time with an even more significant political-economic impact. The opposite effects of using two very different digital currencies will illustrate how BT can serve two contrasting political regimes. After discussing such political implications, strategic solutions will be recommended advocating BT's resourceful use to face a challenging *new normal* (Berwick, 2020) where *post-Covid-19* physical reality and *blockchain* digital reality will inevitably merge, creating a new political era whose outlines are still open.

BACKGROUND

Blockchain: A Civilizational Milestone

It is thought that blockchain's political best novelty is the prompt execution of people's will. Intermediaries usually establish trust, but they can also break it (which is not an exception in politics). The authors

consider that the new guarantee of trust provided by Blockchain Technology (BT) represents an inflection point in human development. As everybody can rely on the blockchain-based distributed trust (Bellini et al., 2020, p.1127), thanks to the auditability of the blockchain protocol (Zheng, 2018), even strangers can now blindly trust each other. Hence, individuals do not need to walk alone anymore depending on institutional third parties to establish reliable political-economic ties between themselves. Hopefully, BT will help remove the considerable agency costs due to many tempting but empty promises sometimes used by politicians, which, at least in democratic regimes, are supposed to be honest intermediaries.

It is argued that digital technologies offer "particular benefits to authoritarian and illiberal regimes" (Feldstein, 2019, p.42). Indeed, information is an instrument of power (Heitman & User, 2018), and new digital technologies combined with centralized data can make life too easy for governments that eventually want to control and manipulate their citizens. However, BT's decentralizing properties make this digital technology ambivalent, being that "theoretical and empirical studies have identified that decentralization is strongly associated with democracy" (Busygina et al., 2018, p. 61). As stated by Sir Tim Berners-Lee, the creator of the *World Wide Web*, "blockchain is a way for different parties that do not know each other to reach an agreement without the need for a referee or a trusted third party" (Buyle et al. 2019, p.2). According to Alcazar (2017), "concisely stated, blockchain is a technology that stores data in a way that makes it incorruptible, doing so via its integrated data ledgers [(*hyperledger*)]." (p. 91).

Digital systems develop faster than analogic ones, and systems distributed over a network appear to be more competitive. Gordon Moore, a founder, and CEO of Intel (Mack, 2011), accurately predicted in 1965 that "the speed of computers, as measured by the number of transistors that can be placed on a single chip, will double every year or two" (Mollick, 2006, p. 62). In the '80s, Robert Metcalfe, the inventor of Ethernet (the connection architecture for local area networks - LAN- most used globally), referred that a network's value is proportional to the square of its size. This statement was later named Metcalfe's "law" (Metcalfe, 2013).

Several decades after these statements were made, it turns out that, in the case of the two most prominent social networks in the world, Facebook and WeChat (Chen, 2017), data fit Metcalfe's "law" quite well, and significantly their costs are inversely proportional to the square of network size (Zhang et al., 2015). So, it seems to be true that digital networks' competitive advantage can be inferred from their size (the number of network nodes).

The cost of the computing and communication used to create connectivity is halved every two years according to the Moore's Law. Combining Moore's and Metcalfe's Laws together, the number of users at which a network's value exceeds its cost halves every two years. In the same time, the value of connectivity has been going up. (Li, 2008, p. 23)

In the last years, information and communication technologies (ICT) have diminished social media sharing costs. However, that reduction had no parallel in terms of *transaction costs*: "The Internet vastly improved the flow of data within and between organizations, but the effect on how we do business has been more limited. The Internet was designed to move information - not value - from person to person "(Tapscott & Tapscott, 2017).

However, the Internet changed. In the *blockchain era*, the *Internet of Information* is replaced by the *Internet of Value*, and regarding transaction costs (Coase, 1993), some authors consider that a much more significant reduction is expected (Davidson et al., 2018; Berg et al., 2019).

Such a critical cost reduction anticipates the economic success and the pervasiveness of this technological innovation, which justifies introducing the expression *Information and Transaction Technologies* (ITT) herein proposed by the authors. It is thought that this new designation attends to both economic media shared and transacted on today's Internet, respectively, social media and digital tokens.

As stated by Jain (2020), "digitization pushed verification prices for various types of transactions close to zero [and] Blockchain technology completes this method by providing free verification." (p. 5). According to Chen (2018), "blockchain technology is one of the most revolutionary general-purpose technologies, and it may have far-reaching implications for entrepreneurship and innovation" (p. 573).

Blockchain technology allows the creation of platforms where the exchange and provision of digital assets does not have need/rely on an intermediary. On these platforms, trust in a platform operator is replaced by trust in the underlying incentives, code, and consensus rules. This is possible because blockchain technology decreases the cost of networking. (…) In the case of blockchain, by reducing the market power of intermediaries, the technology conjointly permits platforms to work with lower barriers to entry and innovation. (Jain, 2020, p. 5,6).

As published in the "The Economist" cover page, BT is a powerful "trust machine" (2015) based on cryptography and mathematical certainty, making it possible to carry out secure transactions even in the absence of intermediaries. As it will be seen, BT's transaction features encompass electoral tokens ("cryptovotes"), which can be a game-changer in politics.

The fascination with the blockchain derives from the fact that it establishes the truth of an event without recourse to a trusted third party in an adversarial environment where no-one can be trusted. The truth of an event, i.e., the creation and/or transfer of tokens, is established by means of "distributed consensus," i.e. the confirmation by a majority of nodes in a decentralized network that a given block has [been validated]. Consequently, the blockchain itself is "trustless" because it creates and confirms a certain state of affairs and replaces the need to trust third parties with the ability to trust the technology itself. (Mik, 2017, p. 7)

A Blockchain is just a database that works as a distributed ledger, verifying and validating sequential blocks containing transaction data. This ledger replication is called a *hyperledger*.

There are different types of blockchains configured in two main dimensions. According to Dumas et al. (2021), those are the *permission dimension* (which sets limitations concerning the user's right to write and amend the ledger) and the private dimension (which sets limitations concerning the users' right to access and submit data into the ledger). These dimensions are represented in the axis of Table 1.

Most transactions carried out by citizens throughout their lives involve third parties on whom it is impossible to place complete trust. It is believed that such transactions will tend to be carried out on blockchain networks, which involve lower transaction costs than traditional solutions.

Landermore (2012) defines *democracy* as "a procedure for collective choice decisions" (p. 10), and the authors consider that, in the *Blockchain Era*, it will not be possible to live in a democracy without the kind of transparency achieved by *public blockchains*. An exhaustive explanation of blockchain technicalities goes beyond this chapter's scope, but it is politically essential to understand *public blockchains* and *private blockchains*. There are also two types of *public blockchains,* which are *public-permissionless* blockchain and *public-permissioned* blockchains. The other types of blockchains are privately or state-

owned, resulting in user's data centralization, with the consequent loss of privacy. Although *private blockchains* have usefulness (plenty of use cases already exist, and many others will arise), they should not resume the alternatives that must be available in a blockchain democracy since "contractual terms can be manifested in a computer code, what is not generally prohibited based on the *freedom of contract* principle." (Savelyev, 2017, p. 10).

Table 1. Blockchain types

Editability	**Openness**		
	Public (open access: all can read/join)	**Private (restricted access)**	
Permissionless (free validation rights)	Public-Permissionless Blockchain (reading & mining rights)	Hybrid Blockchains: Private-Permissionless (publicly mineable only)	
Permissioned (restricted validation rights)	Hybrid Blockchains: Public-Permissioned (publicly readable only)	Consortium Blockchains	Private Blockchains

Source: Authors' work.

Personal rights on the Internet can be guaranteed by using private cryptographic keys to access *public blockchains*, while transactions carried out on *private blockchains* stay dependent on third parties. In other words, some blockchains decentralize power, and others do the opposite.

Some ideas and critical elements about decentralization will be seen in the following section, whose understanding is considered fundamental before addressing BT's political-economic implications, blockchain governance issues, and the authors' solutions and recommendations.

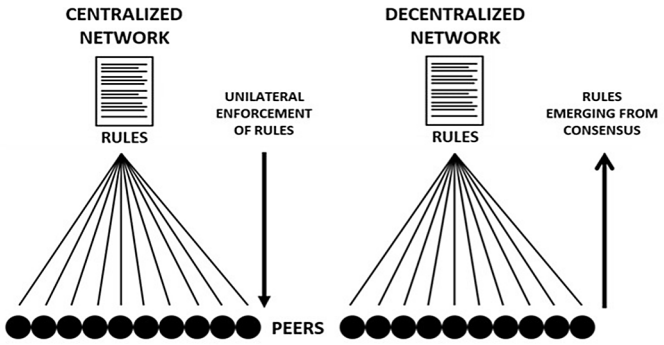
Decentralization

In the *blockchain era*, *decentralization* should be understood "as a property similar to redundancy and no single point of control" (Vergne, 2020, pp. 3,4). To investigate the decentralizing potential of Blockchain Technology (BT) applied to communities' ecosystems, one should start to see the role that *tokens*, *smart contracts*, and *decentralized autonomous organizations* (DAO) will likely play perhaps sooner than expected. Some of these concepts are not of intuitive or easy apprehension to *non-digitally born* mindsets (as is the authors' case), but one should give it a try because they are fundamental pieces to understand the reasons behind the predictable expansion of the blockchain universe.

DAOs are one of the most notorious results of the new type of structured digital decentralization made possible by BT. According to several authors (Zwitter & Hazenberg, 2020); Dwyer, 2017; Young, 2018, 2018a), although DAOs having started to strictly care about the creation of economic value, they may extend to public administration and the direction of the state. BT's structured decentralization may lead to the third sector's emancipation and the self-organization of civil society in ways that have not been thought possible until recently (see Figure 1).

In this sense, Dwyer (2017) points that "a key aspect of the DAO is that it takes traditional aspects of governance that were previously enacted by the state and implements these through software-defined processes with an underlying liberal free-market ideology." (p. 14)

Figure 1. Rules flows in centralized and decentralized networks.
(Adapted from [Fliphodl, 2018])



As self-sufficient social structures, DAOs can make and implement decisions. Despite not being hierarchical, they can generate consensus among their constituents about managing socio-economic resources (see the same book, Chapter 5 – *The Real Blockchain Game Changer: Protocols and DAOs for Coordinating Work to Provide Goods and Services*).

With the concept of decentralized autonomous organizations (DAOs), blockchain technology can not only cure all sorts of blown-up bureaucratic structures, by coordinating people, resources, and processes in more transparent and efficient ways. It will even allow one to build a new form of socio-ecological, liberal, efficient and democratic kind of capitalism. This will consider externalities of everyone's activities on their environment and others by combining blockchain technology with the Internet of Things, creating a socio-ecological finance system. In such a way, it is possible to boost a sustainable circular and sharing economy, with a variety of incentives, i.e. new socio-economic feedbacks. (van den Hoven et al., 2019, p. 166)

It is thought that in a free-market system and once technically optimized, DAOs will be unstoppable infrastructures. Relying on *smart contracts* to trigger a *collective action* that can be encouraged by tokens' transactions, DAOs can manage resources in a decentralized way. Such decentralization of value is possible due to the tokens' programmability accomplished by BT.

Tokens are objects or symbols that represent and quantify physical or digital assets. Thanks to *smart contracts*, tokens can be programmed to perform precise functions. They can integrate *social capital* and *social work* to manage consensus among DAOs' users. Thus, besides being valuable to trade, tokens can also perform concrete tasks to reach specific objectives and accomplish certain missions. Hence, hopefully, tokens can be used as individual incentives to manage communities' sustainability through collective action.

In turn, *smart contracts* allow to move, lock or unlock digital tokens (*e.g.*, cryptocurrencies) in a decentralized way through the Internet, which is only possible thanks to Blockchain Technology (BT). For example, smart contracts developed on the Ethereum blockchain make it possible to go beyond mere monetary transactions, adding rules and logic to transactions. This new feature is the great novelty and evolution of the blockchain protocol paving the way to a digital decentralization spreading from the strictly monetary sphere to the economic, social, and political sphere, eventually in this order.

While Blockchain was born with Bitcoin, its applications have gone far beyond Bitcoin or digital currency. Many people believe that blockchain could revolutionize many fields, such as finance, accounting, management, and law leading to three generations of blockchains, namely, Blockchain 1.0 for digital currency, Blockchain 2.0 for digital finance, and Blockchain 3.0 for digital society (Zhao et al., 2016)

Whenever it is financed with the required tokens to comply with its clauses, a smart contract will self-execute like and when stipulated. For instance, considering political elections, a smart contract can link the electoral choices (results = x votes) with quantifiable commitments made by the winning party (budgets = y dollars/euros/bitcoins). Such a smart contract may be triggered to transfer funds automatically, on specific dates, to adjudicate public services or finance any mensurable electoral proposal (y = f (x)). Such sequences of aggregated automatisms are possible because each vote is a single token's transaction.

It is thought that a substantial reduction in transaction costs (*e.g.*, agency costs) is achievable probable in the next few years due to falling costs of trust mediation, which should have a profound political-economic impact. The auto-enforceable code under a blockchain and smart contracts can substitute the middlemen and lower bureaucracy (Shermin, 2017), diminishing transaction costs and allowing a more efficient economic organization and better governance (Davidson et al., 2016).

The political way to generate trust is very compelling. It is the key to the state's power, the "Leviathan" of Thomas Hobbes (Gibbons, 2001), giving rise to the ability to collect taxes and other dividends. However, BT introduced a new kind of trust, built and distributed in a decentralized way (powerful even among strangers), coming from everywhere through the Internet instead of centrally issued as before, which one can think makes sense:

Everything is in the edge: not only the humans that use the services, but also the activities that put them in contact in the first place. Control must be at the edge, because both the information needed to take decisions and the effects that the decisions may have are located there (Lopez et al. 2019, p. 1909).

The migration from centralized to decentralized organizations characterizes the evolution of complex systems (Kauffman, 1993). It occurs in several domains, such as the spontaneous institution of the order in free markets (Hayek, 1976), in computer systems (open-source and peer-to-peer networks), communication systems (digital social media), and political systems (democracy). All these systems show an evolution towards decentralization, which is also natural in politics because, over time, centralization is vulnerable to exploitation in the form of inflation, corruption, and rent-seeking. The authors agree with Kim & Lee (2011), who stated that "the centralization of government is the fundamental source of corruption" (p. 523). On the contrary, the costs of decentralization fall over time, often due to technological progress and computers, as in blockchain (Davidson et al., 2016).

The lesson is that when you compare centralized and decentralized systems you need to consider them dynamically, as processes, instead of statically, as rigid products. Centralized systems often start out fully baked, but only get better at the rate at which employees at the sponsoring company improve them. Decentralized systems start out half-baked but, under the right conditions, grow exponentially as they attract new contributors. (Dixon, 2018)

However, even though decentralized systems are more competitive due to their low transaction costs, governments (*i.e*., politicians and bureaucrats) have themselves rents to protect, which is easier to do with a monopoly over governance. It is thought that in the *post-Covid-19 new normal* (Berwick, 2020), such monopolies, unfortunately, can be more than a politicians' megalomaniac dream. Hence, threats for *blockchain governance* acceptance can be expected to rise in proportion to the politicians' rents at risk (Lessig 2015, Hendrickson et al. 2015).

Entrepreneur-driven technological competition is often met with political response (…) So we should expect that while centralized ledgers may not always be able to compete on cost, they can still compete through co-option of force, through enacting legislation or regulation to artificially drive up the cost of decentralized technologies—including by rendering them illegal (Davidson et al., 2016, p. 4).

Therefore, even in democratic regimes, the path of decentralization is not open, which puts democracy and freedom at risk, given the digitally enhanced political power of centralized data. As stated by Kranzberg (1986), "technology is neither good nor bad, nor is it neutral." (p. 545), and it is thought that BT will in no way be neutral or innocuous to society. Thus, it is convenient to look at the concept of decentralization and understand BT's political implications to make sufficiently informed choices in the light of a challenging global technological framework.

According to Khare (2003), *centralized* means "drawn toward a center or brought under the control of a central authority" (p. 20), and *decentralized* means "withdrawn from a center or place of concentration; especially having power or function dispersed from a central to local authorities" (p.27). In this last case, the control is not vertically exerted directly anymore but instead emerges organically through the collaboration and aggregation of peers.

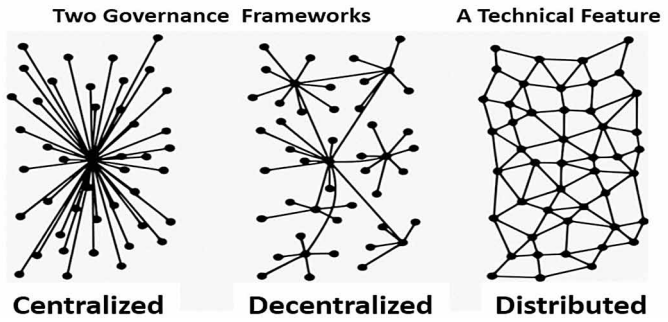
[In a] decentralized database multiple databases are distributed over a network (…) with no central authority managing the database. (…) [BT] is a system of recording information in a way that makes it difficult or impossible to change (…) hundreds and thousands of computers working together so they can verify data by reaching a "consensus". The consensus illustrates that the uploaded data is valid. (Rajapashe, 2020, p. 50)

Baran (1964) differentiated networks based on the number of nodes that needed to fail to break down communications, ranging from a single node in centralized networks to a few in decentralized networks and a majority in distributed networks. (Vergne, 2020, p. 5)

In a distributed network, data is replicated across multiple storage devices (nodes) with equal rights (see Figure 2). Resources like data storage or processing power are spread among peers and network nodes to accomplish a particular job or task, for instance, increasing processing power or creating a global ledger (*hyperledger*). In turn, a decentralized system can also be geographically distributed, but it will always rely upon the control of the node operators (*e.g*., Bitcoin). Therefore, building a decentralized system is all about distributing trust locations across all participants of the system.

Decentralized systems provide the benefit of being distributed and authority agnostic [(censorship resistant)]. On the contrary, a distributed system might span geographical boundaries but [still be] owned and controlled by a single entity (with the advent of cloud computing this is a very common scenario). Trust in such a system is still centralized (District0x, 2020)

Figure 2. Baran's typology of communication networks
(Adapted from [Baran, 1964])



Cloud storage services like Dropbox, Box or Google Drive are definitely centralized: these companies control how the information flows on their respective client-server architecture. However, their networks most probably have a distributed component in order to provide a sufficiently fast and secure service around the world. (SMA, 2018)

Components of a decentralized system operate on local information to accomplish goals rather than under the influence of a central ordering (see Figure 1). In turn, when it refers to distribution is all about communication and messaging. A distributed system computation is shared across components that communicate and coordinate their actions by sending messages. In other words, the components interact to achieve a common goal.

Therefore, these are two very different concepts. While distributed network designs configure a technical feature, a (de)centralized network sets a *governance framework* (see Figure 2).

Having observed valuable introductory concepts about blockchain and decentralization is time to move on to BT's political-economic implications, starting by distinguishing two very different types of digital currencies to envision their profound impact on society.

POLITICAL-ECONOMIC IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Cryptocurrencies Impact: The Good, the Bad, and the Ugly

For better or worse, digital currencies are here to stay for political and economic reasons. Programmability is a decisive competitive advantage, bringing with it the possibility of stipulating the features of each currency on a case-by-case basis. Such a profound change should lead society to think twice about what is really at stake. However, unfortunately, blockchain's theme is not readily acknowledged by ordinary people, especially when the pandemic crisis is a severe problem enough to fill people's minds and keep them concerned.

Considering both economic media, digital money, and social media (Beller, 2020), the authors think that the most significant matter that people have to deal with is protecting privacy. The privacy lost on social media should not also happen on the primary economic media because consequences to society will probably worsen. A story of The Economist (2017) was titled "The world's most valuable resource

is no longer oil, but data," and as argued by Lopez (2020), "if data is like oil, then the owner is the first one who drills [...] This is what is precisely happening now on the Internet, where data brokers and tech companies benefit from personal data drilled from users. "(p. 3).

The reality is that there is a wide range of technologies (hardware, software, biological) that can help companies or governments to drill our data without our permission. Accessing, trading, or making money using our personal data without our consent is unethical, and basically a theft of our privacy rights. Governments should protect individuals of abuses to their privacy by third parties. But either they are weak in front of big multinational companies or authoritarian states themselves are interested in this information (Lopez, 2020, p.3)

Such a loss of privacy is not a good thing, but a latent move against citizens can be even worse: after drilling the oil of peoples' social data, corporatocracy and authoritarian states can mine the gold of peoples' money data, supremely crowning their financial and political power. Unfortunately, funding such a mission will not be hard with centralized digital currencies in those hands.

Perhaps the most extraordinary impact of digital money, which is programmable and thus entirely different from current electronic money, will result from its pioneering capacity to diversify human incentives systems (see the same book, Chapter 3 - *Blockchanging Money: Reengineering the Free World Incentive System*). Obviously, such programming should be done ethically and wisely. If this will not be the case, digital money's features can be gloomy. Hence, programmable money can be *good*, *bad*, or *ugly*, according to the elected (hopefully not dictated) policies. Great opportunities come with significant risks, which is the case with blockchain technology (BT), especially when combined with artificial intelligence (AI) and Big Data. Blockchains and trusted data will reinforce the ability of computers to learn, rationalize, and take actions to achieve specific goals (Rath, 2019). However, it is up to politicians to set the right goals.

As stated by Fenwick & Vermeulen (2019), "one reason to believe that the economic, cultural and social impact of *new* digital technologies will be much greater than we have experienced before is that new technologies increasingly *amplify* each other" (p. 13). Numerical data is programmable and infinitely variable. As such, digital media is always "subject to algorithmic manipulation" (Dush, 2015; Manovich, 2002, 2013: O'Neill, 2017). Thus, *algorithmic manipulation* can now affect not just one but two economic media. Social media manipulation has been happening with notorius ethical repercussions: monetizing techniques adopted by ubiquitous digital platforms (*e.g*., Facebook) which "puts the expressive (attentional, cognitive, affective) power of people to work [while] platform owners reap the spoils and externalize the costs [(*e.g.,* the Washington riots)]." (Beller, 2020, p. 216):

The values we project and create in media factories are abstracted by means of new sets of metrics (of which 'like' is only the most primitive), and, in the processes of monetisation are converted and collapsed into the value-form priced by the code of money. They are, in short, liquidated and placed on the market. After being sold to attention brokers, this value, realised as money, flows upwards to platform owners. (Beller, 2020, p. 216)

In a *post-Covid-19* world, programmable money will probably defeat traditional money due to allowing an inexorable reduction of *transaction costs* (Coase, 1937). It is thought that in a financial scenario of digital money ubiquitously, defending democracy requires "decoding the protocols of money already

operating today in semiotic media to make it possible for users to redesign them more in accord with their interests." (Beller, 2020, p. 216).

Money's good old days probably will be gone. Perhaps soon one will say that traditional money was bad enough coming from "a speculative financial system with a life of its own" (Mertes, 2002), or something even worse will be spoken if the inflation reach levels such where "it can quickly become an ugly beast" (Darlington III, 2014, p. 7). State-sponsored digital currencies are coming, and private cryptocurrencies are entering the financial mainstream. The authors agree with Dumas et al. (2021), who stated that cryptocurrencies "[not being backed by any government], could serve well, especially during moments of turmoil, when countries with vulnerable economy might consider crypto assets an interesting tool, less exposed to monetary risks (*e.g*., hyperinflation, an issue affecting the national currencies)" (p. 16). One way or the other, digital currencies are coming. As referred to by Naudet (2021), "in this conception, [of cryptocurrency,] we could realistically consider the emergence of a resolutely reliable and egalitarian international monetary system, at the origin of a consecration of social peace by the energetic mutation of the currency." (p. 7).

It should be noticed that the first strategic choice when evaluating a future digital currency should consider two opposite political scenarios:

1. Centralization - resulting from a prohibition or severe constraint (*e.g.,* fiscal) of all cryptocurrencies except those based on *private blockchains* (*state-sponsored*, *fully private*, or *consortia* blockchains);
2. Decentralization – resulting from free use of private cryptographic keys by any law-abiding citizen to operate cryptocurrencies on *public blockchains* (*public-permissionless,* or in a somehow minor degree *public-permissioned* blockchains).

According to several authors (Antonopoulos, 2016, 2017; Tapscott, 2016, 2017; Young, 2018; Lopez et al., 2019), programmable money should not be "captured by the state," staying available to be freely used and traded on open networks, where each citizen can use *private keys* to move it around without constraints in and out their communities. Hence, it is thought that *private and state-sponsored digital currencies must freely compete in decentralized markets*.

Also, regarding the desirable nature of digital money, one should notice Congressman Tom Emmer' words in the US Congress, outlining his vision of a *digital dollar* open to all:

It is American values like freedom, privacy, openness and permissionless entrepreneurship that have led [the USA] to dominate global commerce and innovation. We should have the courage of our convictions to build these values into a digital dollar and not to emulate systems like China's new digital yuan, which is closed, centralized, surveilled and permissioned so that access can be denied and payments blocked by those in power. (…) The same rules that apply to physical cash should apply to the digital dollar. While this may not go far enough for some, the only way to go farther would be to create a permissioned closed and surveilled system like China. (…) Technologies like this can empower individuals and make their governments more accountable directly to them. We can't cede this power to the government at the expense of the individual. (Ledger Insights, 2020)

This speech made clear that the USA (and implicitly also the rest of the free world) must follow an open model to create *good* digital currencies to stimulate innovation and entrepreneurship. Choosing a closed model would originate a *bad* centralized digital dollar that can be engineered to feed certain powers

and eventually become *ugly* enough to obliterate the US founding fathers' checks and balances system in *the land of the free* (Blaustein, 1987). The authors could not agree more with this Congressman's words.

It is judged that centralized opaque versions of state-sponsored digital currencies can induce citizens' submission to non-auditable political power, allowing governments to monitor consumption, raising the bar of state surveillance and citizens' control. Therefore, digital currencies are a challenging type of money that can increase the government's control over citizens who are also consumers. It is thought that voters understand the long-lasting need to withdraw the money from politics, but, unfortunately, it is doubtful that the urgent need to separate politics from digital money can be timely and sufficiently understood given the population's lack of knowledge about BT. Moreover, people's attention is being disputed by sanitarian and economic concerns. Thus, this chapter aims to contribute to filling that gap.

The pioneering example of such global threat to privacy and freedom is the so-called *Digital Yuan*, China's central bank digital currency - the Digital Currency / Electronic Payment (DCEP) which marked "the first launch by a major economy of a sovereign digital currency [technically enabling] the merger of the monetary and payment systems." (Didenko et al., 2020).

Digital Yuan's network access is controlled, and all transactions are subject to central validation. The use of this digital currency requires the consent of the network's master keys holder because such keys are hidden in an opaque computer code. In other words, the computer system administrator (in this case, an authoritarian political regime) can discretionarily prevent payments made by any individual, thus being able to condition each user's consumption behavior, perhaps not only in China when Digital Yuan becomes global. As stated by Slawotsky (2020), "a blockchain powered digital Yuan — the currency of the world's second biggest economy (already digitalized to a far greater extent than the United States) might serve as an intriguing pathway towards a Chinese alternative to the USD. "(p. 39). According to Hoxtell & Nonhoff (2019), "authoritarian states are not only restricting the flow of information within their own countries and using the Internet as a tool to repress their citizens, but they are also exporting this model of Internet governance to other countries" (p .13).

The Internet is now "a global ledger" (Tapscott & Euchner, 2019), which empowers those who have the right keys to use it freely. It should be emphasized that the owner of the master keys of a centralized digital network also controls the respective data flows, being able to validate or change all network's transactions. Thus, privacy and private property depend on each individual ability to protect his data by using secure cryptographic keys. Only the possession of those digital secret keys will guarantee citizens' rights to privacy, private property, and even free will. Thus, in the authors' perspective, all law-abiding citizens should have the right to use private cryptographic keys. Moreover, it is thought that this is the most crucial safe conduct of every democratic system in the *blockchain era.*

As the story goes, when people are afraid and feel insecure, as in the face of the pandemic crisis of COVID-19, they are predisposed to compromise in matters of freedom to achieve the desired security. This *syndrome*, of an anxious nature, can lead people to accept restrictive measures that would otherwise be unlikely to see the light of day. Moreover, these measures are not just a reality in undemocratic countries with authoritarian regimes.

In China, the outbreak has strengthened and advanced a pre-existing authoritarian project that relied on emerging technologies and data to implement Xi Jinping's "prevention and control" doctrine with respect to Chinese society. But similar tools have been employed by democracies, including several that have become international models for their successful handling of the public health crisis introduced by the coronavirus (Greitens, 2020, p. 18).

As stated by Degeling et al. (2020), "many individuals are likely to accept limits on personal autonomy in pursuit of population health benefits at times when members of the public are being told to prepare for a major health emergency" (p. 7), and there are concerns about privacy risks due to pandemics, including mass surveillance in a *post-Covid-19* world (Wang, 2021). Information means power, and having too much data about citizens' lives can be tempting for some governments. Much personal information is being collected (*e.g.,* in apps and social networks), aimed at favoring governments and companies. Henceforth, due to digital currencies' properties, regimes may go even further, compromising people's privacy and ruining democracy.

Digital Yuan is quite different from *Bitcoin*. The latter is based on an open-sourced public blockchain, and no single entity can shut it down or even change its network protocols. Every user has its private secret keys, and changing blockchain's governance protocol requires most of its members' consensus (Nakamoto, 2008). On the contrary, the former is a digital currency native from a state-sponsored *permissioned blockchain* with its access requisites stipulated at a central level by the political regime (Buckley et al., 2021). The same happens with the Chinese social network WeChat, a platform whose use has become an authentic lifestyle for the Chinese citizens. Indeed, the Chinese government has emphasized WeChat, which began as a messaging app like WhatsApp, but was later described as a *super-app* (Chen et al. 2018).

WeChat users can send free messages with text, image, video, and/or audio to individual contacts and groups of contacts. However, WeChat functionality vastly exceeds interpersonal communication because it integrates internal apps that enable users to conduct a wide array of activities—make mobile payments, hail taxis, order food, book hotels, give to charity, play games—from within the WeChat app environment. This integration of utilities creates new gratifications that may increase the "stickiness" of WeChat and increase time spent on WeChat. (Lu & Pan, 2020, p.12)

Despite the usual secrecy that prevails in China, there are reports that BT has been tested on WeChat social networks (Iwamoto, 2021). As mentioned above, this technology allows registering and executing peer-to-peer (P2P) transactions with units representing value (tokens), and the WeChat network accounts for *social value* and *financial value.* Furthermore, it is possible to convert everyday personal experiences into computable transaction rules by indexing those values. The criteria followed to balance individual accounts, increasing or decreasing the social capital displayed by each individual in the WeChat network, will be established by the Chinese regime. Later on, Digital Yuan may function as *ration coupons*, aligning (or suppressing) individual rights to make payments according to each one's *social credit*.

Bitcoin and Digital Yuan clearly define the boundaries of digital currencies' political and economic role. Unlike traditional money, digital currencies work not only as exchange units but also as utility units, storing a political-economic value that stems from their specific features. Bitcoin was openly programmed to be an autonomous reserve of value due to its limited supply (Nakamoto, 2008), while Digital Yuan programming is not known nor auditable. Hopefully, other cryptocurrencies, instead of being economically used as *digital gold* (Bitcoin) or serve as a political instrument (Digital Yuan), will be used as "qualified money" (Helbing, 2014) to diversify financial incentives. The new multidimensionality of money is globally possible by dealing in hyper ledgers with units of value that cryptographically merge *labor* and *capital.* For the first time in history, these two productive factors can be integrated into the same unit of value, allowing to deal with value in a richer way (see Chapter 3).

"We are inventing a type of trust that can grease the wheels of business and facilitate person-to-person relationships [and DAOs] in the age of distributed networks and collaborative marketplaces." (Ebner, 2017, p. 132).

Given that there are different ways of building a blockchain-based society, we must avoid to fall into the trap of a totalitarian post-privacy world, in which people might be restricted—and unnecessarily restrained in unfolding their knowledge, ideas, and talents. If we want to see a world with a level playing field for everyone, we need to insist on responsible blockchain innovations and on using distributed ledger mechanisms for the greater good, rather than allowing them to be usurped and harnessed by a very limited group of people for private interests. (van den Hoven et al., 2019, p. 166)

If freedom prevails, which needs to be proactively guaranteed in the face of a *new normal* (Berwick, 2020) triggered by the confluence of the pandemic crisis and the *blockchain paradigm*, programmable money will not be centralized and used as a corset to control citizens. On the contrary, it will be used to promote collective action, which is very different from collectivism. One should not ignore the harsh reality of central state planning experienced in the 20th century behind eastern Europe's "iron curtain" (Applebaum, 2012) and be aware of BT's disruptive *dark side* of centralization. It is believed that it is crucial to enlighten citizens about the upsurge risks of totalitarianism, from the left and the right, given that technologies such as AI or BT can change the world quickly. Suppose there is room to preserve democracy and freedom. In that case, digital currencies may serve *to expand the pie before dividing it*, taking advantage of the new multidimensionality of money to induce a *collective action* based on individual merit and creativity, innovation, and ethical entrepreneurship focused on a sustainable human development.

Blockchanging Governance

Governance can be defined as the process whereby power is exercised, decisions are made, citizens or stakeholders are given a voice, and account is rendered on important issues (Plumptre, 2006). Blockchain Technology (BT) can be used to perform such processes. Although BT started with the purpose of ensuring bitcoin transactions (blockchain 1.0), it now is used to act proactively in rendering many other accounts, securing and verifying diverse assets and contracts (blockchain 2.0 and 3.0) (Xu et al., 2019).

The notion of *power* is linked to the notion of *hierarchy*, but decentralized networks are changing this notion. The Internet is the Information Age's decisive technology (Castells, 2014), and BT has empowered the Internet even more. As in any hierarchical system, the governance of a network is a prerogative of those who rule. However, the same does not happen in a completely decentralized system, as is the case of *public-permissionless blockchains*, which rely only on open code and public scrutiny. Hence, BT creates a new *distributed trust* whose impact on citizens' behavior will be framed only by the cryptographic rules chosen and political rules allowing or forbidden accessing different blockchains.

Open-source code guarantees transparency and auditing, which is essential to build citizens' trust and grant free access to blockchain networks. On the contrary, closed source-code and centralized protocols can restrain access on an individual basis, obviously limiting citizen's choices. These are two substantially different processes of letting transactions be carried out on blockchains. While the latter requires trust in specific persons or organizations, *i.e*., trust on *private blockchains* (either privately, governmental, or consortium owned), the former is censorship-resistant, depending only on trusting a large community-

based consensus (*public-permissionless* blockchains) or, alternatively, a consensus emerging of a smaller group of *delegated witnesses* trusted by such communities (*public-permissioned* blockchains).

All these protocols to reach a consensus about what should be trusted entails unavoidable trade-offs. 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 scaling trilemma is the reason why *hybrid blockchains* try to combine the best of three worlds, aiming for *security* pursuing the right trade-offs between the *scalability* advantage of *private-permissioned* blockchains and the *decentralization* feature of *public-permissionless* blockchains, which does not arise without a considerable burden:

In a permissionless blockchain, all the transactions and blocks are broadcast, verified and recorded among all participants in a decentralized peer-to-peer network. This process ensures that the whole system is immutable, stable and resistant as long as more than half of the computing resources remain honest. Honest majority is required for an appropriate security property, which however is very costly on the scalability side as all participants need to be informed and to implicitly agree [to reach the consensus]. (Qin & Gervais, 2018, pp. 3, 4)

Hopefully, BT will evolve and adapt to overcoming technical limitations and complying with regulations that will be flexible enough to satisfy the transaction needs of the so-called free world. However, powerful interests can mislead BT's public perception disproportionally connoting Bitcoin with negative factors, such as excessive energy consumption and criminality (see the Limitations and Future Research section). Thus, the lousy reputation can harm the credibility of all BT's applications, eventually diverting blockchain's evolution to protect the status quo. In other words, it can happen the same that happens every time a technological innovation reveals itself as a threat to someone's business (Antonopoulos, 2017). Nevertheless, it is considered that a decentralized approach might provide the most reliable alternative to deal with political and financial affairs, especially at times of institutional distrust. As stated by Atzori (2015), "while the State bases its action on coercion, the blockchain can provide governance services in a more efficient and decentralized way, without having to rely on force. This approach allows a more horizontal and distributed diffusion of authority, in which the source of legitimacy are the individuals themselves." (p. 7)

The collective relationship between individuals and the State can be fully or partially automated by "a series of instant atomic interactions […] Instead of a hierarchical structure managed by a set of humans interacting in person…via the legal system, a decentralized organization involves a set of humans interacting with each other according to a protocol specified in code, and enforced on the blockchain. (Buterin, 2014)

As it goes in Estonia for almost a decade, governments can benefit from BT by instituting digital transparency and secure open access to information, a fact that should be especially appreciated in an area so sensitive to voters' eyes as healthcare.

Estonia is at the forefront, securing more than one million citizens' records in a [blockchain].

The system has proven that interoperability is an achievable goal and demonstrated that the ability to analyze data has helped the government become aware of and more easily track health epidemics. (Vazirani et al. 2020, p. 3)

This Baltic republic is an excellent example of how transparency and openness can benefit a country and improve citizens' lives (Adeodato & Pournouri, 2020). One should remark that such *openness* may not always be followed in the physical world (*e.g*., for security reasons), but in the digital world, it can make sense, as in the case of the successful Estonian e-residency program (e-resident.gov.ee) (Blue, 2020).

BT allows storing proofs of data's authenticity for reference instead of the data itself (Nakamoto, 2008), guaranteeing privacy and convenience. This feature presents the best of two worlds and can be called a "win-win situation" (Fisher et al., 2011), benefiting all players of the blockchain-based identity management ecosystem (Kuperberg, 2019). For instance, opting for decentralized identity management solutions will increase people´s access to online services, contributing to protecting citizens' privacy and solving many unbanked and identityless people's problems (Keweel et al., 2017). More than two billion people with no bank account but with a mobile phone (Ardo & Zamani, 2019) can benefit from low-cost BT solutions to prove their identities and immediately start accessing financial services to make micro-transfers or small remittances of currency (cryptocurrency).

On the other hand, new decentralized media apps (*dapps*) will provide censorship-resistant access to the entire spectrum of information and opinions expressed by social media users. This kind of information can release citizens from the biased content available in today´s social networks, which is managed by machine learning algorithms that feed predatory business models (O'Neill, 2017). The same goes for the biggest state-controlled social network (WeChat) which contents are also being managed by machine learning algorithms, this time to feed an authoritarian regime (Lu & Pan, 2020).

In the *blockchain era*, to expose democracy worldwide to *virulent* ideologies, it is enough to prohibit people from achieving the *group immunity* conferred by private cryptographic keys (*the masks*) and open-sourced code programming (*the vaccines*). Without digital decentralization and transparency, privacy and freedom will not be *immunized against* malignant software *backdoors* (see Key Terms and Definitions) eventually hosted in non-auditable close-sourced programming codes of *private blockchains*. Moreover, both economic media (digital money and social media) will be ideal propagation vectors for *enforcing ideological memes* and *tailoring money rules* cleverly dictated by statistical bias algorithms "that are telling lies" (O'Neill, 2017. p.7).

A Trustworthy Digital Democracy

Electronic Voting

Democracy needs reliable data and citizens' privacy to function effectively. Thus, transparency is a fundamental element of democracy. For instance, without the secret vote, there can be no freedom of choice or independent decisions. If constructive criticism can be stopped by the fear of reprisals and witnesses' anonymity is not guaranteed, fight corruption and organized crime cannot be properly enduring, compromising the rule of law (Helbing, 2014). On the other hand, transparency promotes accountability, which may induce ethical and responsible behavior. Thus, there is an urgent need to find an ethically recommended balance between privacy and transparency (see the same book, Chapter 1 - *Blockchanging Trust: Ethical Metamorphosis in Business & Healthcare*).

A *digital democracy* requires electronic voting (e-voting), and it is thought that e-voting systems must be decentralized. By considering a vote as a transaction, citizens can vote on the blockchain (Barnes et al., 2016). The same process can be used for rapid voting on relevant issues and not just voting for officials (Young, 2018). According to Atzori (2015), "democracy can become more effective through the direct participation of citizens in the decision-making process [and] blockchain technology can implement new models of participation" (p. 9).

Once technical issues have been solved (Specter et al., 2020; Waldron, 2019), whose description would go beyond the scope of this book, Blockchain Technology (BT) eventually will allow coding the electoral decision process directly in *smart contracts*, using open, transparent, and auditable code-source to make the electoral system verifiable and incorruptible. For this reason, it is considered that the electoral process will eventually be reformed by using BT. After all, the same mathematical precision that made Bitcoin's hyperledger secure, tamper-proofing its accounts for more than ten years now, also can be used to certify and audit electronic voting systems. As stated by Wright & De Filippi (2015), "[BT offers] a distributed, irreversible and encrypted public paper trail that can be easily audited."

The technology already exists to have a voting system on the blockchain. "With the cost of voting drastically reduced, politicians hampered by scandal, corruption, or incompetence could easily be removed from their offices, making governance more efficient and decreasing the impact of politicians who have lost the confidence of their constituency. (Young, 2018, p. 9)

E-voting is among the key public sectors that can be disrupted by blockchain technology. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital-currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline. (Kshetri, 2018, p. 95)

Robust voting systems, either traditional or digital, should satisfy obligatory requirements. Barański et al. (2020) reviewed several of such conditions mentioned in the literature (Qadah, 2005; Schneier, 2007; Ayed, 2017; Hjálmarsson et al., 2018; Sadia et al., 2019; Vo-Cao-Thuy et al., 2019) and proposed the following seven mandatory conditions for having a secure and effective e-voting system:

- *Immutability*: No one can change the vote after it was made.
- *Verifiability*: Everyone should be able to verify if his or her vote has been counted correctly.
- *Scalability*: The system should be able to handle large-scale elections, both in terms of votes per second and voting costs.
- *Authorization*: Only authorized voters can vote, and no one can vote more than once.
- *Privacy*: Relation between voter and his vote must be kept in secret. Each voter must be sure about his vote privacy.
- *Coercion resistance*: It should be illegal to sell or exchange votes.
- *Fairness*: No partial results are available until the end of the election.

An extended review of the literature showed that another condition must be added (Takabatake et al., 2016, p. 127):

- *Completeness*: The administrator always accepts an eligible voter, and all valid votes are counted correctly.

Heiberg et al. (2020) consider that "the search for a better balance is on-going" (p. 95), identifying several threat actors that can compromise an *Internet Voting System*: (i) Civil hacktivist seeking publicity; (ii) Single candidate trying to get more votes; (iii) Political party trying to increase the number of seats; (iv) Organization aiming at influencing policy decisions, and (v) Foreign state-level actor trying to gain more control over the country.

Thus, considering so many restrictive conditions of effectiveness, and the possible attack angles, assembling a secure and effective e-voting system seems to be a complex issue. As stated by Çabuk et al. (2020), "security term includes integrity, verifiability, and non-repudiation of votes; authentication and singularity of voter accounts; immutability and trackability of all the records." (p. 132). However, despite these and other requirements, this author adds that "using blockchain mechanisms that support smart contracts (or similar), such as Ethereum, can be a good fit since it would natively support distributed applications on the chain." (p. 132).

The blockchain technology offers a decentralized storage and computation mechanism for e-voting systems, where the voting records are transparent to all the voters and independent observers. (…) It offers a system, in which everyone can trust. This trust is not just about the perception, but rather the mathematical, analytical, and logical means of security, provided by the blockchain technology. (Çabuk et al. 2020, p. 132)

However, "privacy and confidentiality of votes is rather an implementation-dependent, and it is possible to find the relation between a voter and his / her vote, by digging into the chain" (Çabuk et al. 2020, p. 132), being that BT still presents vulnerabilities. These are not good news when a solution with total robustness in all parameters is desired. Therefore, the various electronic voting systems using BT (Benítez-Martínez et al., 2021; Dhinakaran, et al., 2021: Yang et al., 2020) should be viewed with moderate optimism. Some of these systems propose to increase the granularity of public scrutiny even in times of pandemic (Wattegama, et al., 2021), including using remote validation of votes with biometric parameters (Priyadharshini et al., 2021).

Given the complexity and the degree of demand for entirely satisfactory electronic voting solutions, it will be practically mandatory to give up something to obtain the desired convenience. Thus, trade-offs will become necessary. As stated by Çabuk et al. (2020), "any voting protocol suite is a complex set of mechanisms balancing between conflicting requirements. Improving one component may decrease the overall security level of the whole system. Thus (...) a holistic study of the whole suite needs to be conducted. (p. 132). The same rationale is patent in the following quotation of the political philanthropist Bradley Tusk, a Voatz backer speaking to the Harvard Business Review:

It's not that the cybersecurity people are bad people per se. I think it's that they are solving for one situation, and I am solving for another. They want zero technology risk in any way, shape, or form [...] But in my view, then you can't resolve the issues on guns, on climate, on immigration, because the middle 70% doesn't participate in primaries [...] I am solving for the problem of turnout. (Specter et al, 2020, p. 14)

The authors' opinion on BT-based electronic voting systems coincides with that expressed by Waldron (2019), which states that "it is a useful tool, but it is not a solution that address all of the concerns (...) solution not bad but rather incomplete "(p. 4). Simply put, a blockchain is an authenticity tool, not a privacy tool (MX Technologies Inc., 2016). Even so, despite understanding the existing reservations, one should be pragmatic when factors such as the abstention rate and democratic representativeness of national elections are at stake. As such, giving up electronic voting is not a solution.

These are turbulent times, and the pace is one of accelerated change. The future will no longer be a reissue of the past, requiring the capacity for innovation under penalty of obtaining diminishing returns (Hamel, 2000) that can culminate in a resounding civilizational failure. Thus, future elections must include not only "the middle 70%" above mentioned by Tusk (Specter et al, 2020, p. 14), but also the younger voters, the *generation y*, or *millennials*, which *grown-up digital* unlike their parents (the *baby boomers*) and are a tech-savvy group of users instead of mere viewers (Tapscott, 1997; Almeida, 2017).

Weighing the respective pros and cons, the authors consider that electronic voting is highly recommended, and BT's systems are in the pole position to win the challenging race to find a bulletproof system. Meanwhile, Voatz, a BT-based system, was used with its results officially approved in the 2020 US Presidential Elections, although contested by some and including fights in courts (this was the first time people cast votes via smartphone in a Presidental Election). Nevertheless, BT-based electronic voting systems should be improved and eventually combined with other technologies (e.g., homomorphic cryptography) to deal with privacy issues. Still, it can be said that BT is an auspicious solution for using electronic voting systems over the Internet.

Algorithmic Governance

Any dream of making the world better must include political transparency and digital openness as fundamental requisites for protecting democracy and freedom in the *blockchain era.* Otherwise, powerful computing resources, eventually including state-sponsored digital currencies, will put at the mercy of powerful interests, not only personal data, as happening so far in social media, but also citizen's consumption prerogatives. One can think this is wrong, as the government must be scrutinized and conditioned by the citizens, not the other way around. The menace of such an unethical future state-of-affairs is one of the main reasons digital decentralization is considered crucial to keeping the free world on a democratic path.

If people do not preserve the dignity of their data and do not defend privacy, every citizen will be subject to the power of digital centralization. The states and other third parties will take control of even the slightest detail of everyone's life. This level of control is not only possible but highly probable, as partially shown on the *pre-blockchain* version of the Internet (see Chapter 1).

The research about *algorithmic governance* has been mentioned the risks of *datafication* (see Key Terms and Definitions) and mass surveillance. Monitoring entire populations and citizens' profiling create ample opportunities for social sorting, discrimination, state oppression, and manipulating consumers and citizens (Gandy, 2010; Lyon, 2014). However, in the cryptographic *blockchain era*, the digital tools go both ways, also letting citizens protect themselves. Hence, *algorithmic governance* highlights that digital technologies can produce social ordering in a specific way (Katzenbach & Ulbricht, 2019). In the new *Internet of Value*, debauching privacy can easily include consumer behavior monitoring and restraint because the prerogatives of digital currencies can be automated according to each payer political

profile. Nevertheless, the authors hope that in the so-called free world things could happen transparently and democratically.

The inherent consensus-seeking, scalability, and decentralization make blockchain computing the next step in evolution for public governance. Controlling a government's institutions by connecting them to a blockchain system will create greater oversight of the government and will prevent government actors from acting beyond their mandate. (…) When attached to government property, blockchain computing allows for potentially unlimited checks and balances on a government. (Young 2018, pp. 33,34)

BT's auditability and irreversibility can give a decisive contribution to governments' accountability. As stated by Young (2018a), "the future regulatory structure that can be built with blockchain technology has been called "*Lex Cryptographia*" (…) This, like *lex mercatoria*, is executed outside the government control, and independent from the state" (p. 15). "Centralization refers to the degree to which authority and decision-making is concentrated at the top" (Matseshe et al., p. 383), and it is known that for many centuries and still today " "decision power is concentrated at the top of the hierarchy" (Alexandru, 2018, p. 9). However, in the new *Internet of Value* (Tapscott & Euchner, 2019), blockchain computing allows "the decision-making process of a decentralized organization [to be] encoded directly into source code [to] distribute authority throughout without the need for any trusted centralized party" (Wright & De Filippi, 2015).

Several government initiatives are underway (Clavin et al., 2020; Amend et al., 2021). Such pioneering efforts demonstrate that BT foreshadows a new level in governance and human development models. As referred in Atzori (2015), "decentralization through the blockchain technology represents a "natural progression of humanity"(Andreas Antonopoulos, 2014) and a "natural efficiency process "(Swan 2015, p. 31)" (p. 11).

Thanks to smart contracts, the integrity, and fairness of government commitments can directly migrate from the winning party's political proposals, and be precisely executed, with no scope for unattended electoral promises or tricky subjective interpretations. As referred by Young (2018), "In addition to being an ideal tool for scaling democracy, blockchains are also an ideal tool for ensuring a party does not act outside of its mandate because parties cannot act outside of the encoded powers granted to them" (p. 66). This same author proposed a *social smart contract* and two kinds of *blockchain governmental tokens*, which are presented in Table 2, to be used by individuals in their relationship both with the government and is fellow citizens:

Table 2. "Blockchain governmental tokens"

GovernmentCoins (Credits Given to the Government)	**CitizenCoins (Credits Given to the Citizens)**
It provides power within or over the government	It provides access to the government institutions
When a government's blockchain is established, each citizen would vote and do all the things its government ID empowers him to do. The citizens would exercise oversight into the Government's blockchain, see every transaction, and verify that the source-code has not changed.	When a citizens' blockchain is established, citizens would receive a unique cryptographic token as an ID that would identify them to take advantage of government-distributed benefits, enabling each citizen to work (vote) within the government system, and also with other citizens.

Source: Adapted from Young (2018), and Barnes et al. (2016).

As stated by Young (2018), "the code of the Smart Social Contract will determine what abilities the holder of each GovernmentCoin has." (p. 28).

When voters elect someone to a leadership or a bureaucratic role, that person's GovernmentCoin will receive greater privileges, and then have access to the government infrastructure (computers, vehicles, intelligence, military) assigned to the function to which they were elected. This way something for which the individual is responsible [or voted for] can be tracked to the exact individual. Additionally, an individual could be prevented from acting ultra vires, [(see Key Terms and Definitions)] because the government's checks and balances are built into the system. (Young, 2018)

The proposed new type of blockchain-based governance may determine mayors and government officials' direct election. As each vote is a transaction, citizens can command algorithms on the blockchain, treating the political affairs like business deals, which can be called "algorithm governance" (Dwyer, 2017).

Through smart contracts, it is possible to stipulate the scope of political scrutiny, determining the transactions of GovernmentCoins and their practical consequences. In turn, CitizenCoins can manage the entire relationship between the citizen and the state, guaranteeing access to public services and directly influencing everything open to voting. The CitizenCoins can even encourage collective action, which is very different from collectivism as seen below.

Liberal democracy is often associated with an ethical model where consensus results from reason and rational debate between peers (Habermas & Rehg, 1997). This deliberative model, which "claims that collective public deliberation is the definitive democratic experience" (Gabardi, 2001), was replaced by another one, advocated by the neo-liberal policy initiated in the middle of the last century (Schumpeter, 1942). According to neoliberals, consensus should not result from the debate between equals, morally based on a common good's notion, which is always debatable, but instead on the aggregation of individual preferences and interests. This aggregative model of democracy, assuming an economic subject motivated by self-interest, considers that political institutions' organization must result from a sum of individual preferences and interests (Cunningham, 2010).

If these two modes of governmentality, one imagining a mode of politics arising from free reasoning among equals and the other a politics of consensus founded on self-interest are in competition in liberal governmentality, algorithmic governmentality is the total succession of this aggregative model of democracy. It does away with claims towards a rational, discursive public sphere in favour of a bland social unanimity. It replaces politics with economics (Dwyer, 2017, p. 5)

It is thought that a new evidence-based policy is mandatory, where words cannot be broken, and deeds cannot be lacking. In a time of uncertainty and few reliable indicators, it is believed that authenticity, transparency, and mathematical certainty are necessary political assets.

Both liberal and algorithmic approaches make use of quantitative techniques. Numericity was and still is seen as a kind of disinterested politics, where techniques of calculation are understood to be less biased or politically motivated than the excesses of rhetoric or theoretical disputes. […] Here, liberal knowledge provides a historic precedent for viewing numbers as self-evident, for the universal belief that the numbers don't lie. (Dwyer, 2019)

In the following section, the authors will present solutions and political recommendations to place BT's "truth machine" (Economist, 2015) at the service of liberal democracy.

SOLUTIONS AND RECOMMENDATIONS

Fulfilling electoral promises is one of the most ethical commandments of democracy. It is thought that Blockchain Technology (BT) can translate political party programs into immutable computer protocols, scrutinized, and validated on blockchain networks. Thus, BT can bring a new era of confidence in translating political promises into deeds.

In the *blockchain era*, data's legitimacy and transactions' authenticity can be verified in a decentralized way through consensuses, which may be automatically established among citizens instead of relying on third parties' validation mechanisms. BT's political implications will emphasize the need for a much more often voters' involvement in public policies and decisions that concern them, congregating the younger generations presently dismissed from the public cause. Thus, the authors think it will be convenient to adopt transparent proximity mechanisms to guarantee citizens' participation through open, collaborative platforms.

It is understood that the power to control citizens' lives must reside on the periphery of traditional centers of power, i.e., with the citizens themselves, because that is where is the information needed to make decisions and the effects that result from these same decisions (Lopez, 2019). Thus, it is believed that the decentralization of entities and services will promote social justice and transparency through equal opportunities while increasing government accountability and citizen's autonomy by using private keys in controlling their own personal and procedural data.

The blockchain protocol should also change the paradigm of trust in justice (Zaprutin et al., 2020), democratizing access and guaranteeing equality. It is not possible, for example, *losing* documents or lawsuits issued and registered through a *blockchain protocol*. This censorship resistance is because blockchain documents are replicated in a vast as-needed computer network, becoming immutable and practically incorruptible, unlike what happens with documents issued by centralized systems. Thus, the authors think that adopting the blockchain protocol will undoubtedly reform areas where the issue of corruption is more sensitive and harmful to society, as is the case with politics and justice (Aarvik, 2020).

A new digital reality triggered by BT and synergistically pushed by two other powerful technologies, Artificial Intelligence and Big Data, increases the effectiveness of information systems opening business possibilities that all can enjoy in a decentralized free market scenario.

The new-fangled Business world requires better treatment of enormous information and better use with more knowledge incorporated in all business processes. Fundamentally, block chain is apprehensive with keeping correct records, verification, and implementation while AI helps in conducting assessment, examining, and coming to conclusion of certain patterns and datasets, eventually engendering selfdirected interaction. […] Artificial Intelligence and Block Chain needs sharing of data. The decentralized approach of database focuses the significance of data sharing among various clients on a meticulous network. In the same way, AI depends very much on Big Data, exclusively, for data distribution. Including more provisions of data analysis, the future trends prediction and assessments of machines are measured more correctly, and the algorithms developed are more consistent. (Rath, 2019, p. 1031)

It is judged that these new possibilities can be used by the third sector to reinforce its political, economic importance. Hence, civil society must be allowed to be responsible for its future, believing that the private sector's role will be key to innovate and create decentralized markets using DAOs (see Key Terms and Definitions), which may benefit from a substantial reduction of *transaction costs* and tax burden. The authors consider that it will be very difficult or even impossible to continue to raise taxes on wealth creation in the new digital paradigm and keep democracy on track. Given the new horizons opened by technological advances in information systems (Sadowski, 2020), it is thought that such a fiscal ambition makes no sense, and further insistence on taxation would bring the shadow of the totalitarian regimes where market laws are suppressed. Unfortunately, the non-democratic path of authoritarianism cannot be excluded, especially in the light of the crisis triggered by the SARS-CoV-2 virus (Cawthorn et al., 2020), and considering digital surveillance and citizens' control procedures that are being tested in the East (Qiang, 2019).

In the authors' opinion, well-known political options aimed at centralization and ideological uniformization, historically positioned against democracy and freedom, may postpone or even make lose the historical opportunity of using BT to benefit humankind. Hopefully, free world democracies will show enough resilience to adapt to the double edge sword of digital pragmatism. For the first time in human history, it is possible to distinguish collectivism from collective action (Tapscot, 2016). While collectivism implies state planning and coercive central control, collective action is based on the freedom of choice, with the *public-blockchain protocols* ensuring access to transacting freely and ensuring data's ownership (Nakamoto, 2008). Digital money can quantify public and individual benefits simultaneously since digital tokens and cryptocurrencies may have a *multidimensional value*, which is not the case with traditional money. Cryptocurrencies and other digital tokens should be programmed to integrate *labor* and *capital* into single units of account creatively (see Chapter 3). This *financial socio-economic chimera* is strategically recommended in the *blockchain era*. Hopefully, it will constitute a political choice to benefit both individuals and their community ecosystems, promoting unity between community members but respecting individual differences without falling into the old trap of collectivistic single-minded ideologies.

The *blockchain protocol* allows individuals to organize their transactions without traditional organizations, creating decentralized and secure digital infrastructures to produce wealth (see Chapters 4 and 5). It is highly recommended that everyone has free access to *public-blockchain* networks openly promoted by governments, businesses, and civil society. This openness is the generic solution proposed by the authors to democratize and disintermediate transactions, pursuing a transparent reform of the state in the *blockchain era*.

LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

Bitcoin is the most visible face of Blockchain Technology (BT). As stated by Rath (2019), "Bitcoin popularized Blockchain Technology" (p. 1033). Two limitations pointed out to Bitcoin are (i) its volatility allegedly due to its lack of intrinsic value (as stated by Alan Greenspan, referring himself to Bitcoin, "It's a bubble. It has to have intrinsic value." (Ametrano, 2016, p. 11), and (ii) the high energy consumption required to carry out the Proof-of-Work (PoW) mechanism used to establish blockchain network consensus, which demands considerable computing effort. Regarding specifically the first of these two criticisms, the argument of Bitcoin's excessive volatility due to lacking intrinsic value, the authors recommend reading in the same book the homonymous section on Chapter 3, where it is pre-

sented a scientifically positive correlation between cryptocurrencies production costs and their respective prices. Considering the argument of Bitcoin's excessive energy consumption, although further research to increase BT's efficiency is recommended, it seems evident that, as observed by Hayes (2017), "a cryptocurrency with no acceptance or usage will have neither value nor computational power directed at it "(p. 1312). Thus, low price will mean low production costs, and it is judged as a paradox arguing about Bitcoin's unacceptance due to excessive volatility and lack of intrinsic value and, simultaneously, fearing that it provokes an excessive energy consumption.

The decision to mine for bitcoin comes down to its profitability given its relative cost of production (…) a rational agent would not undertake production of bitcoins if they incurred a real ongoing loss in doing so. Bitcoin mining employs computational effort which requires the consumption of electricity to function, which must be paid for. This computational effort is directed at mining bitcoin, in competition with many other miners who presumably are also motivated by profit, on average. (Hayes, 2017, p. 1315)

Production costs drive cryptocurrency acceptance, and energy costs will only be paramount if Bitcoin reveals itself successful (Hayes, 2017), but in this case energy consumption will be avoided at other significant levels, so this issue must be considered in a broader perspective. For example, according to Sedlmeir et al. (2020), "by enabling the digitization of supply-chain processes, blockchain can substantially reduce the amount of paperwork and transport, including air-freight (Jensen et al. 2019), or allow for more targeted recalls, leveraging many opportunities to reduce carbon emissions" (p. 607).

As stated by Sedlmeir et al. (2020) about the energetic waste argument, "this perception inevitably raises concerns about the further adoption of blockchain technology, a fact that inhibits rapid uptake of what is widely considered to be a ground-breaking and disruptive innovation." (p. 599). One can agree about the political impact of such criticism considering that sustainability is a central issue on many agendas. Nevertheless, it is judged that this critique should be rejected for several reasons. In the first place, "participation in the mining process is only profitable as long as the expected revenue from mining is higher than the associated costs [(*e.g.*, electricity)] (Sedlmeir, 2020, p. 601). In the second place, although being true that the redundant ledger's replication over the Bitcoin network nodes increases energy consumption, especially compared to other conventional solutions that are not redundant and less secure (involving centralized databases and single servers), it is also true that trust has a price, and it turns out that the increased security, provided by BT, also avoids energy consumption at other important levels, so the issue of energy consumption must be considered in a broader perspective. For instance, cryptocurrencies may contribute to managing communitarian ecosystems through collective action (Dapp, 2019), which potential ecological effects will probably surpass Bitcoin's energetic consumption globally, eventually resulting in a better entropy balance (Leonard & Treiblmaier, 2019), especially considering renewable energy:

As electric power systems around the world rely more heavily on intermittent renewable energy, distributed energy resources, and sophisticated digital technologies, the industry will need to cope with rising complexity. Blockchain technology has the potential to help manage that complexity. (…) blockchain can be used to underpin a vast, distributed network that records transactions swiftly, immutably, and transparently. Now, substantial investment is flowing toward ventures that apply blockchain technology to the electric power sector. (Livingstone et al., 2018, p. 19)

The authors think it is essential to overview the environmental impact of cryptocurrencies considering other factors relevant for sustainability, such as the gold mining industry. As argued by McCook (2018), some critics have labelled Bitcoin as an environmental disaster. However, it has been demonstrated that Bitcoin is dramatically less harmful to the environment than the gold mining industry (p. 28). The energy consumption of the banking system is even greater.

The Bitcoin network consumes an estimated ~113.89 TWh/yr in total. (…) The gold industry utilizes roughly 240.61 TWh/yr. (…) With the publicly available information that we could find, we estimate the banking system uses 263.72 TWh of energy each year. Deriving a comprehensive number for this sector's energy consumption would require individual banks to self-report. (…) To have an honest conversation about Bitcoin's energy use, a comparison to the most analogous incumbents—the gold industry and the banking system—is appropriate. (Rybarczyk et al., 2021, pp. 4-13)

Finally, there are alternatives to BT's consensus mechanisms besides Proof-of-Work (PoW).

Huge energy consumption is by no means necessary for the creation of a block from a technical perspective and alternative ways for finding consensus are currently being discussed in various communities (e.g., proof of stake, proof of burn, proof of elapsed time, Byzantine fault tolerance and variations thereof, Federated Byzantine agreement) (Leonard & Treiblmaier, 2019, p. 202)

Among these alternatives, the second most consensus mechanism is the so-called Proof-of-Stake (PoS), a planned future improvement of Ethereum which involves much less energy consumption than Bitcoin's PoW (Alfieri, 2019).

Furthermore, new cryptographic protocols are being discovered, some of them presenting already greater energy efficiency, solving scalability issues and maintaining or even increasing the level of decentralization, as seems to be is the case of Holochain, an open-source framework for developing microservices (and micropayments) that run *peer-to-peer* applications entirely on end-user devices without central servers (Holochain, 2020). As stated by Zaman et al. (2021), "in contrast to blockchain, holochain liberates the communicating agents from any form of centralized control by running the applications (hApps) entirely at the user side." (p. 14).

Another criticism made to BT is that cryptocurrencies serve, above all, to illegal purposes, facilitating criminal activities such as *money laundering*, tax evasion, terrorism, among others. As stated by Turner et al. (2020), "illicit bitcoin transactions could take the form of money laundering, terrorism financing or the movement of proceeds from other crimes such as ransomware attacks." (p. 53). However, this criticism is based on a misconception because the very design of a blockchain implies immutable records tracking the history of transactions. This feature improves traceability and facilitates the detection of eventual police cases. Nothing can be deleted from a blockchain, as the records inserted in it are immutable (Nakamoto, 2008).

Unlike fungible traditional currencies, the different units of the same cryptocurrency may be distinguished between themselves. They are made unique because each one of them carries the digital history of its prior transactions. If compared to physical money, *pseudo-anonymous* cryptocurrencies are more traceable (Antonopoulos, 2017). This traceability is a feature of Bitcoin, which does not oblige its users to register or reveal their real-world identity explicitly, although the patterns of user's behavior might themselves be identifying (Nath, 2020).

Ultimately, the literature shows that there is no lack of available data on the Bitcoin blockchain. By providing open data this allows the community to flag certain behavior or orientation of Bitcoin addresses and transactions. (…) The emergence of machine learning and its application to graphs is providing a powerful analysis capability for disrupting Bitcoin related criminal activity. (Turner et al., 2020, p. 63)

Meanwhile, the so-called privacy coins such as Monero and Zcash use complex cryptography to hide special anonymity features, and it seems reasonable to admit a need for some regulation in this regard. Nevertheless, anonymity still has essential roles to play, and digital money's programmability can be used in such regulatory efforts. For instance, Helbing (2014) pointed out that building in the anonymous cryptocurrency's protocol an obligation to spend it quickly (by programming a devaluation timeline) can be a market solution to benefit traceability and still keeping some degree of freedom:

Most of us don't want anybody to know, which toys someone buys in a sex shop. For such and many better reasons, we still need sufficient amounts of cash besides traceable electronic money, even though it should lose its value quickly enough to make traceable transactions sufficiently attractive. (p. 14)

It is advisable not to confuse the tree with the forest by labeling all cryptocurrencies equally. Cryptocurrencies should be classified by authorities, and ethically rated by communities according to the benefits and inconveniences determined by the computer programs that designed them (see Chapter 3). To facilitate such an assessment is another reason why open-source code is highly recommended in a blockchain. The privacy cryptocurrencies case shows the importance of researching how to optimize the trade-off between privacy and security.

Electronic voting is another area where undoubtedly more research is needed, as mentioned above. A general-purpose electronic voting system is a complex problem. Both privacy (votes have to be anonymous to prevent coercion) and public verifiability are required (otherwise, the provider of the e-voting solution, or someone who managed to compromise it, can change the votes), and trade-offs are unavoidable (Wüst & Gervais, 2018). Unlike Young (2018), the authors are unsure if there is yet a "robust voting system" (p. 9) on a blockchain. Observing the current state of electronic voting in "the most digital country in the world" (Butt et al., 2020), this is not precisely so. As referred to by Heiberg et al. (2020), "the Estonian Internet voting scheme does not provide full end-to-end verifiability" (p. 95), relying heavily on the electronic identity infrastructure, which can be problematic as these same authors "consider the user's personal computing environment to be the weakest point in the e-ID ecosystem." (p. 84)

The most serious implication of this threat is an attacker submitting a vote using a compromised e-ID environment without the voter noticing. This is a problem both in the scenario when the attacker changes the originally submitted vote by re-voting, and also when the voter did not intend to vote at all (which is her legal right in Estonia). (Heiberg et al, 2020, p. 20)

Thus, more research is needed on electronic voting systems, because fraud risks are very high and because democratic representativeness is very much at stake due to abstentionism.

Finally, one should keep in mind that BT goes, perhaps decisively, against the *status quo* and the interest of powerful intermediaries, which will certainly try to resist change. Although no one can de-invent BT, nor the Internet will go back to its previous stage, some will probably try to halt or delay the thrive of *public-permissionless* blockchains. Surprisingly enough, BT makes it possible for civil society to use

digital prerogatives usually only used by large organizations. Thus, BT may change power dynamics in politics and economy favoring the third sector.

The authors think that few things in politics and the economy will remain the same in the *blockchain era*, and it is thought that more research into BT is required to educate politicians and citizens better to protect privacy, freedom, and democracy.

CONCLUSION

Networked organizations and distributed systems are unbeatable. For decades, the Internet has allowed sharing of information between people. Due to Blockchain Technology (BT), transactions can also be carried out directly from one person to another without intermediaries. In the *Blockchain Era*, the Internet will be more impactful to society because transacting is even more vital to humankind than sharing. BT was firstly used to execute secure financial transactions *peer-to-peer* (*e.g.*, Bitcoin), but with *smart contracts*, it is possible to automate other transaction agreements, which are being done, including those of a political nature.

There is a natural evolution from centralized to decentralized organizations, in the markets, in computer governance, in digital communication, and in the political system itself (democracy). Nevertheless, the political path of decentralization will not be easy to follow. Dealing only with private and opaque blockchains can be a dangerous option to democracy, and such closed alleys must be avoided. Instead, citizens must enter the brighter avenue recently opened by public and transparent blockchains. Otherwise, people can lose freedom, that is, lose practically everything. The authors think that the *open & decentralized vs. closed & centralized* dichotomy will become the most prominent political dispute of the 21st century. Anywhere freedom triumphs, citizens will be allowed to use *public and transparent open access blockchains*, whose transactions can be executed and verified by everyone. If law-abiding citizens can use *private cryptographic keys*, to freely transact in *public blockchains,* there will be freedom of choice among many *easy-to-use decentralized applications* (*dApps*), which is the case of *cryptocurrencies*.

Not only state-sponsored digital currencies but many private cryptocurrencies should be free to compete in the market. In this scenario, a paradigm of transparency will probably emerge. Thus, *private cryptographic keys* are a pre-requisite of democracy and the only way to deal with the severe risks of losing privacy and freedom in the *Blockchain Era*. People will have more power over information, reinforcing individual autonomy and government officials' accountability. Of course, crimes and police cases will continue to be increasingly sophisticated, as has been the case since the beginning. However, supposing public blockchains' transparency can thrive, the criminal investigation will be strengthened by combining powerful technologies (*e.g.*, Big Data and Artificial Intelligence) to a great extent, thanks to the immutable and auditable character of transactions once registered in a blockchain. However, ICTT availability (see Key Terms and Definitions) demands full transparency, under penalty of losing freedom and democracy, because once that centralization and closed-source computing dominate the Internet, the state and corporatocracy will cross-reference both *economic media* (social media and digital currencies). This is not considered a very auspicious thing because data extracted from digital money users becomes a database with semiotic value (see Chapter 1), and if each digital coin can have a different cryptographic *color*, some governments can be tempted to *paint* them according to each consumer's political vests. In this scenario, such *colored money* will condition consumer behavior and citizens' freedom. So, instead of being confronted with police cases, citizens would be harassed by the policing of all cases. Such a

level of citizens' control is typical in authoritarian states. For instance, in China, the state is sponsoring both the social network "WeChat" and Digital Yuan, eventually combining data handy for the regime. As for the rest of the world, it is known that worse news travels quickly.

Hopefully, political choices will protect democracy and freedom. Then, the *Internet of Value* will serve human ingenuity to foster innovation and entrepreneurship, letting the free world take advantage of the *Blockchain Era*, surpassing any political pitfalls created by the status quo.

REFERENCES

R3. (2020a, September 16). *How "public-permissioned" blockchains are not an oxymoron*. https://www.r3.com/blog/how-public-permissioned-blockchains-are-not-an-oxymoron-2/

R3. (2020b, October 30). *Should we already be using blockchain as a voting system for elections?* Corda. https://www.corda.net/blog/should-we-already-be-using-blockchain-as-a-voting-system-for-elections/

Aarvik, P. (2020). *Blockchain as an anti-corruption tool. Case examples and introduction.* Academic Press.

Adeodato, R., & Pournouri, S. (2020). Secure Implementation of E-Governance: A Case Study About Estonia. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity* (pp. 397–429). Springer. doi:10.1007/978-3-030-35746-7_18

Ahluwalia, S., Mahto, R. V., & Guerrero, M. (2020). Blockchain technology and startup financing: A transaction cost economics perspective. *Technological Forecasting and Social Change*, *151*, 119854. doi:10.1016/j.techfore.2019.119854

Alexandru, I. (2018). *Comparative administrative law issues regarding central and local government*. Societatea de Stiinte Juridice si Administrative.

Alfieri, E. (2019). *Cryptocurrencies and market efficiency. Business administration*. Université Grenoble Alpes.

Almeida, R. J. F. D. (2017). *Generation Y: an analysis of millennials' skills, perceptions, values and expectations against the promise (s) of the Gen-Y City project* (Doctoral dissertation). Universidade de Coimbra.

Amend, J., Kaiser, J., Uhlig, L., Urbach, N., & Völter, F. (2021). *What Do We Really Need? A Systematic Literature Review of the Requirements for Blockchain-based E-government Services*. Academic Press.

AmetranoF. M. (2016). *Hayek money: The cryptocurrency price stability solution*. Available at SSRN 2425270.

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

Antonopoulos Andreas, M. (2017). *The Internet of Money: Volume Two*. Merkle Bloom LLC.

Applebaum, A. (2012). Iron curtain: the crushing of Eastern Europe 1944-56. Penguin UK.

Ardo, A. A., & Zamani, E. D. (2019, April). Mobile phone for financial inclusiveness and empowerment: a case study of anchor borrowers programme. In *Proceedings of 2019 UK Academy for Information Systems International Conference.* AIS.

AtzoriM. (2015). Blockchain technology and decentralized governance: Is the state still necessary? Available at SSRN 2709713. doi:10.2139srn.2709713

Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *Int. J. Netw. Secur. Its Appl.*, *9*, 1–9.

Baran, P. (1964). On distributed communications networks. *IEEE Transactions on Communications Systems*, *12*(1), 1–9. doi:10.1109/TCOM.1964.1088883

Barański, S., Szymański, J., Sobecki, A., Gil, D., & Mora, H. (2020). Practical I-Voting on Stellar Blockchain. *Applied Sciences (Basel, Switzerland)*, *10*(21), 7606. doi:10.3390/app10217606

Barnes, A., Brake, C., & Perry, T. (2016). *Digital Voting with the use of Blockchain Technology*. Team Plymouth Pioneers – Plymouth University.

Baudier, P., Kondrateva, G., Ammi, C., & Seulliet, E. (2021). Peace engineering: The contribution of blockchain systems to the e-voting process. *Technological Forecasting and Social Change*, *162*, 120397. doi:10.1016/j.techfore.2020.120397 PMID:33071364

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

Benhabib, S. (1997). Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy. *The American Political Science Review*, *91*(3), 725–726. doi:10.2307/2952099

Beniiche, A. (2020). *A study of blockchain oracles.* arXiv preprint arXiv:2004.07140.

Benítez-Martínez, F. L., Hurtado-Torres, M. V., & Romero-Frías, E. (2021). A neural blockchain for a tokenizable e-Participation model. *Neurocomputing*, *423*, 703–712. doi:10.1016/j.neucom.2020.03.116

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

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for Blockchain: Review and challenges. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 164908–164940. doi:10.1109/ACCESS.2019.2950872

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

Blaustein, A. P. (1987). Our Most Important Export: The Influence of the United States Constitution Abroad. *Conn. J. Int'l L.*, *3*, 15.

Blue, A. (2020). Evaluating Estonian E-residency as a tool of soft power. *Place Branding and Public Diplomacy*, 1–9. doi:10.105741254-020-00182-3

Brinks, V. (2019). 'And Since I Knew About the Possibilities There…': The Role of Open Creative Labs in User Innovation Processes. *Tijdschrift voor Economische en Sociale Geografie*, *110*(4), 381–394. doi:10.1111/tesg.12353

Buckley, R. P., Arner, D. W., Zetzsche, D. A., Didenko, A. N., & Van Romburg, L. J. (2021). Sovereign digital currencies: Reshaping the design of money and payments systems. *Journal of Payments Strategy & Systems*, *15*(1), 7–22.

Busygina, I., Filippov, M., & Taukebaeva, E. (2018). To decentralize or to continue on the centralization track: The cases of authoritarian regimes in Russia and Kazakhstan. *Journal of Eurasian Studies, 9*(1), 61-71.

Buterin, V. (2014). DAOs, DACs, DAs and more: An incomplete terminology guide. *Ethereum Blog*, *6*, 2014.

Butt, S. A., Pappel, I., & Õunapuu, E. (2020, November). Potential for Increasing the ICT Adaption and Identifying Technology Readiness in the Silver Economy: Case of Estonia. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia* (pp. 139-155). Springer.

Buyle, R., Taelman, R., Mostaert, K., Joris, G., Mannens, E., Verborgh, R., & Berners-Lee, T. (2019). *Streamlining governmental processes by putting citizens in control of their personal data*. Academic Press.

Çabuk, U. C., Adiguzel, E., & Karaarslan, E. (2020). *A survey on feasibility and suitability of blockchain techniques for the e-voting systems.* arXiv preprint arXiv:2002.07175.

Castells, M. (2014). The impact of the internet on society: A global perspective. *Change*, *19*, 127–148.

Cawthorn, D. M., Kennaugh, A., & Ferreira, S. M. (2020). The future of sustainability in the context of COVID-19. *Ambio*, 1–10. PMID:33289053

Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 90225–90265. doi:10.1109/ACCESS.2020.2992341

Chen, J. (2017). Can online social networks foster young adults' civic engagement? *Telematics and Informatics*, *34*(5), 487–497. doi:10.1016/j.tele.2016.09.013

Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business Horizons*, *61*(4), 567–575. doi:10.1016/j.bushor.2018.03.006

Chen, Y., Mao, Z., & Qiu, J. L. (2018). *Super-Sticky Design and Everyday Cultures', Super-Sticky Wechat and Chinese Society*. Emerald Publishing Limited. doi:10.1108/9781787430914

Choi, M. K., Yeun, C. Y., & Seong, P. H. (2020). A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 118732–118740. doi:10.1109/ACCESS.2020.3005134

Clavin, J., Duan, S., Zhang, H., Janeja, V. P., Joshi, K. P., Yesha, Y., Erickson, L. C., & Li, J. D. (2020). Blockchains for Government: Use Cases and Challenges. *Digital Government: Research and Practice*, *1*(3), 1–21. doi:10.1145/3427097

Coase, R. H. (1991). *The nature of the firm (1937). The Nature of the Firm*. Origins, Evolution, and Development.

Conway, D., & Garimella, K. (2020). Enhancing Trust in Business Ecosystems With Blockchain Technology. *IEEE Engineering Management Review*, *48*(1), 24–30. doi:10.1109/EMR.2020.2970387

Cunningham, S. (2010). Joseph A. Schumpeter, Capitalism, socialism, and democracy. *International Journal of Cultural Policy*, *16*(1), 20–22. doi:10.1080/10286630902807278

Dalton, G. (1982). Barter. *Journal of Economic Issues*, *16*(1), 181–190. doi:10.1080/00213624.1982.11503968

Dapp, M. M. (2019). Toward a Sustainable Circular Economy Powered by Community-Based Incentive Systems. In *Business Transformation through Blockchain* (pp. 153–181). Palgrave Macmillan. doi:10.1007/978-3-319-99058-3_6

Darlington III, J. K. (2014). *The future of Bitcoin: mapping the global adoption of world's largest cryptocurrency through benefit analysis*. Academic Press.

DavidsonS.De FilippiP.PottsJ. (2016). *Economics of blockchain*. Available at SSRN 2744751.

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, *14*(4), 639–658. doi:10.1017/S1744137417000200

De Beauclair, I. (1963). The Stone Money of Yap Island. *Bulletin of the Institute of Ethnology, Academia Sinica*, *16*, 147–160.

De Beauclair, I. (1971). Studies on Botel Tobago, and Yap. In *Asian Folklore and Social Life Monographs, edited by Lou Tsu-k'uang* (pp. 183–203). Orient Cultural Service.

Degeling, C., Chen, G., Gilbert, G. L., Brookes, V., Thai, T., Wilson, A., & Johnson, J. (2020). Changes in public preferences for technologically enhanced surveillance following the COVID-19 pandemic: A discrete choice experiment. *BMJ Open*, *10*(11), e041592. doi:10.1136/bmjopen-2020-041592 PMID:33208337

Dhinakaran, K., Raj, P. B. H., & Vinod, D. (2021). A Secure Electronic Voting System Using Blockchain Technology. In *Proceedings of the Second International Conference on Information Management and Machine Intelligence* (pp. 307-313). Springer. 10.1007/978-981-15-9689-6_34

Didenko, A. N., Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). *After Libra, Digital Yuan and COVID-19: Central Bank Digital Currencies and the New World of Money and Payment Systems*. Academic Press.

District0x. (2020). *An Introduction To Decentralization*. District0x Education Portal. https://education.district0x.io/general-topics/what-is-decentralization/introduction/

Dixon, C. (2018). *Why Decentralization Matters*. https://medium.com/s/story/why-decentralization-matters-5e3f79f7638e

Dumas, J. G., Jimenez-Garcès, S., & Șoiman, F. (2021, March). Blockchain technology and crypto-assets market analysis: vulnerabilities and risk assessment. The 12th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2021.

Dush, L. (2015). When writing becomes content. *College Composition and Communication*, 173–196.

Dwyer, R. (2017). *Code! = Law: Explorations of the Blockchain as a Mode of Algorithmic Governance*. Retrieved from https://www.academia.edu/34734732/Code_Law_Explorations_of_the_Blockchain_as_a_Mode_of_Algo rithmic_Governance

Dzieduszycka-Suinat, S., Murray, J., Kiniry, J., Zimmerman, D., Wagner, D., Robinson, P., Foltzer, A., & Morina, S. (2015). *The Future of Voting End-to-End – Verifiable Internet Voting. Specification and Feasibility Assessment Study*. U.S. Vote Foundation. https://usvotefoundation-drupal.s3.amazonaws.com/prod/E2EVIV_full_report.pdf

Ebner, N. (2017). Negotiation is changing. *J. Disp. Resol., 99*.

Eikmanns, B. C. (2018). *Blockchain: Proposition of a new and sustainable macroeconomic system*. Frankfurt School, Blockchain Center.

Faber, B., Michelet, G. C., Weidmann, N., Mukkamala, R. R., & Vatrapu, R. (2019, January). BPDIMS: a blockchain-based personal data and identity management system. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 10.24251/HICSS.2019.821

Faber, N. R., & Hadders, H. (2016, June). Towards a blockchain enabled social contract for sustainability, Creating a fair and just operating system for humanity. In *Proceedings of the First International Conference on New Business Models*, *Toulouse, France* (pp. 16-17). Academic Press.

Feldstein, S. (2019). The road to digital unfreedom: How artificial intelligence is reshaping repression. *Journal of Democracy*, *30*(1), 40–52. doi:10.1353/jod.2019.0003

Fenwick, M., & Vermeulen, E. P. (2019). Technology and corporate governance: Blockchain, crypto, and artificial intelligence. *Tex. J. Bus. L.*, *48*, 1.

Fisher, R., Ury, W. L., & Patton, B. (2011). *Getting to yes: Negotiating agreement without giving in*. Penguin.

Fitzpatrick, S. M., & Diveley, B. D. (2004). Interisland Exchange in Micronesia: A Case of Monumental Proportions. In S. M. Fitzpatrick (Ed.), *Voyages of Discovery: The Archaeology of Islands* (pp. 129–146). Praeger.

Fitzpatrick, S. M., & McKeon, S. (2020). Banking on Stone Money: Ancient Antecedents to Bitcoin. *Economic Anthropology*, *7*(1), 7–21. doi:10.1002ea2.12154

Fliphodl, F. (2018, November 22). *Social Media Alternatives Series, EP. 1: What You NEED to Know.* Fliphodl. https://www.fliphodl.com/social-media-alternatives-series-ep-1-what-you-need-to-know/

Friedman, M. (1991). *The Island of Stone Money*. Hoover Institution, Stanford University.

Furness, W. H. (1910). *The Island of Stone Money, Uap of the Carolines*. J. B. Lippincott.

Gabardi, W. (2001). Contemporary models of democracy. *Polity*, *33*(4), 547–568. doi:10.2307/3235516

Gandy, O. H. Jr. (2010). Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems. *Ethics and Information Technology*, *12*(1), 29–42. doi:10.100710676-009-9198-6

Gibbons, R. (2001). Trust in social structures: Hobbes and Coase meet repeated games. *Trust in Society, 2*, 332-353.

Greitens, S. C. (2020). Surveillance, Security, & Democracy in a Post-COVID World. *International Organization*, *74*(S1), E169–E190. doi:10.1017/S0020818320000417

Gurguc, Z., & Knottenbelt, W. (2018). *Cryptocurrencies: overcoming barriers to trust and adoption*. eToro.

Habermas, J., & Rehg, W. (1997). *Contributions to a discourse theory of law and democracy*. Polity Press.

Hamel, G. (2000). *Leading the revolution*. Harvard Business School Press.

Haneem, F., Bakar, H. A., Kama, N., Mat, N. Z. N., Ghazali, R., & Mahmood, Y. (2020). *Recent Progress of Blockchain Initiatives in Government*. Academic Press.

Harari. (2020). *The world after coronavirus*. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Harrison, M. (2018). *Decentralizing the International Monetary System: An Assessment of Regulatory Structures for Cryptocurrencies in the Age of Digital Finance*. Academic Press.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, *134*, 104040. doi:10.1016/j.ijmedinf.2019.104040 PMID:31865055

Hayek, F. A. (1976). *Denationalisation of money*. Ludwig von Mises Institute.

Heiberg, S., Krips, K., & Willemson, J. (2020). Planning the next steps for Estonian Internet voting. *E-Vote-ID*, *2020*, 82.

Heiss, J., Eberhardt, J., & Tai, S. (2019, July). From oracles to trustworthy data on-chaining systems. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 496-503). IEEE. 10.1109/Blockchain.2019.00075

HelbingD. (2014). *Qualified money-a better financial system for the future*. Available at SSRN 2526022 doi:10.2139srn.2526022

HendricksonJ.HoganT.LutherW. (2015). The political economy of bitcoin. SSRN.

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmt'ysson, G. (2018). Blockchain-based e-voting system. *Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 983–986. 10.1109/CLOUD.2018.00151

Holochain.org. (2020). *What is Holochain?* https://developer.holochain.org/docs/what-is-holochain/

Hoxtell, W., & Nonhoff, D. (2019). *Internet Governance: Past, Present and Future*. Konrad Adenauer Stiftung. https://www.gppi.net/media/Internet-Governance-Past-Present-and-Future.pdf

Humphrey, C. (1985). Barter and Economic Disintegration. *Man*, *20*(1), 48–72. doi:10.2307/2802221

Ingham, G. (2013). *The nature of money*. John Wiley & Sons.

Insights, L. (2020, June 12). *Congressman argues for permissionless digital dollar to demonstrate U.S. values.* Ledger Insights - Enterprise Blockchain. https://www.ledgerinsights.com/digital-dollar-congress-permissionless/

Iwamoto, K. (2021, February 15). *China's New Year digital yuan tests hasten Asia e-currency race*. Nikkei Asia. https://asia.nikkei.com/Spotlight/Asia-Insight/China-s-New-Year-digital-yuan-tests-hasten-Asia-e-currency-race

JaccardG. (2018). Smart contracts and the role of law. Available at SSRN 3099885. doi:10.2139srn.3099885

JainD. (2020). The Economics of Cryptocurrencies-Why Does It Work? Available at SSRN 3644159.

Jensen, T., Hedman, J., & Henningsson, S. (2019). How tradelens delivers business value with blockchain technology. *MIS Quarterly Executive*, *18*(4), 221–243. doi:10.17705/2msqe.00018

Katzenbach, C., & Ulbricht, L. (2019). Algorithmic Governance. *Internet Policy Review*, *8*(4), 1–18. doi:10.14763/2019.4.1424

Kauffman, S. A. (1993). *The origins of order: Self-organization and selection in evolution*. Oxford University Press.

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

Keynes, J. M. (1915). The Island of Stone Money. *Economic Journal (London)*, *25*(98), 281–283.

Khare, R. (2003). *Extending the REpresentational State Transfer REST Architectural Style for Decentralized Systems* (Doctoral dissertation). University of California, Irvine.

Khare, R., & Taylor, R. N. (2004, May). Extending the representational state transfer (rest) architectural style for decentralized systems. In *Proceedings. 26th International Conference on Software Engineering* (pp. 428-437). IEEE.

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences (Basel, Switzerland)*, *9*(9), 1736. doi:10.3390/app9091736

Kim, S. (2020). *Fractional Ownership*. Democratization and Bubble Formation - The Impact of Blockchain Enabled Asset Tokenization.

Kim, Y. S., & Lee, J. W. (2011). Corruption and Government Roles: Causes, Economic Effects, and Scope. *Korea and the World Economy*, *12*(3), 513–553.

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

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, *35*(4), 95–99. doi:10.1109/MS.2018.2801546

Kuperberg, M. (2019). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management*, *67*(4), 1008–1027. doi:10.1109/TEM.2019.2926471

Landemore, H. (2012). *Democratic reason: Politics, collective intelligence, and the rule of the many*. Princeton University Press.

Lannoye, V. (2020). *The History of Money for Understanding Economics*. Vincent Lannoye.

Leach, M., MacGregor, H., Scoones, I., & Wilkinson, A. (2020). Post-pandemic transformations: How and why COVID-19 requires us to rethink development. *World Development*, *138*, 105233. doi:10.1016/j.worlddev.2020.105233 PMID:33100478

Leonard, D., & Treiblmaier, H. (2019). Can cryptocurrencies help to pave the way to a more sustainable economy? Questioning the economic growth paradigm. In *Business transformation through Blockchain* (pp. 183–205). Palgrave Macmillan. doi:10.1007/978-3-319-99058-3_7

Lessig, L. (2015). *De ja vu all over again*. Talk given at Sydney Blockchain workshop.

Lewis, A. (2015). *A Gentle Introduction to Digital Tokens*. Bits on Blocks. https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens

Li, G. (2008). *Economic sense of Metcalfe's Law*. Academic Press.

Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018, December). BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-6). IEEE. 10.1109/GLOCOM.2018.8647713

Livingston, D., Sivaram, V., Freeman, M., & Fiege, M. (2018). *Applying blockchain technology to electric power systems*. Academic Press.

Lopes, J., Pereira, J. L., & Varajão, J. (2019). *Blockchain based E-voting system: a proposal*. Academic Press.

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.

Lotti, L. (2019). The Art of Tokenization: Blockchain Affordances and the Invention of Future Milieus. *Media Theory*, *3*(1), 287–320.

Lu, Y., & Pan, J. (2020). Capturing Clicks: How the Chinese Government Uses Clickbait to Compete for Visibility. *Political Communication*, 1–32.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2). Advance online publication. doi:10.1177/2053951714541861

Mack, C. A. (2011). Fifty years of Moore's law. *IEEE Transactions on Semiconductor Manufacturing*, *24*(2), 202–207. doi:10.1109/TSM.2010.2096437

Manovich, L. (2002). *The Language of New Media*. MIT Print.

Manovich, L. (2013). *Software Takes Command*. Bloomsbury Academic Print.

Massey, R., Dalal, D., & Dakshinamoorthy, A. (2017). *Initial coin offering: A new paradigm.* Deloitte. Available at https:// www2.deloitte.com/content/dam/Deloitte/us/Documents/ process-and-operations/ us-cons-new-paradigm.pdf

Matseshe, L. K., Arasa, R., & Yohannes, T. H. (2017). *The Moderating Effect Of Decision-Maker On The Relationship Between Strategy And Organizational Structure*. Academic Press.

Mattke, J., Maier, C., & Reis, L. (2020, June). Is cryptocurrency money? Three empirical studies analyzing medium of exchange, store of value and unit of account. In *Proceedings of the 2020 on Computers and People Research Conference* (pp. 26-35). 10.1145/3378539.3393859

Mertes, T. (2002). Wall Street. *Amass*, *12*(2), 80.

Metcalfe, B. (2013). Metcalfe's law after 40 years of Ethernet. *IEEE Computer*, *46*(12), 26–31. doi:10.1109/MC.2013.374

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, *9*(2), 269–300. doi:10.1080/17579961.2017.1378468

Mollick, E. (2006). Establishing Moore's law. *IEEE Annals of the History of Computing*, *28*(3), 62–75. doi:10.1109/MAHC.2006.45

Monroe, A. E. (1923). *Monetary Theory before Adam Smith* (Vol. 25). Harvard University Press. doi:10.4159/harvard.9780674183438

Möser, M., Böhme, R., & Breuker, D. (2014, March). Towards risk scoring of Bitcoin transactions. In *International Conference on Financial Cryptography and Data Security* (pp. 16-32). Springer.

Mouial-Bassilana, E., Restrepo, D., & Colombani, L. (2018). Le déséquilibre significatif dans les contrats commerciaux: nouvel outil de lutte contre les GAFA. *Actualité juridique. Contrat, 471.*

Mueller, L., Glarner, A., Linder, T., Meyer, S. D., Furrer, A., Gschwend, C., & Henschel, P. (2018). *Conceptual Framework for Legal and Risk Assessment of Crypto Tokens*. Academic Press.

MX Technologies Inc. (2016). *Checks, Balances, and Bitcoin: The Genius of the Blockchain*. Retrieved from https://www.mx.com/moneysummit/checks-balances-and-bitcoin-the-genius-of-the-blockchain/

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

NathG. V. (2020). *Cryptocurrency and Privacy-An Introduction to the Interface*. Available at SSRN 3658459. doi:10.2139srn.3658459

Naudet, L. B. (2021). *Regard sur les conséquences des mutations organiques de la monnaie dans la manifestation des conflits armés depuis l'éclatement du système de Bretton-Woods*. Academic Press.

Norta, A. (2016, November). Designing a smart-contract application layer for transacting decentralized autonomous organizations. In *International Conference on Advances in Computing and Data Sciences* (pp. 595-604). Springer.

Noyen, K., Volland, D., Wörner, D., & Fleisch, E. (2014). *When money learns to fly: Towards sensing as a service applications using bitcoin.* arXiv preprint arXiv:1409.5841

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

Pasuthip, P., & Yang, S. (2020). *Central Bank Digital Currency: Promises and Risks.*

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond banks and money* (pp. 239–278). Springer. doi:10.1007/978-3-319-42448-4_13

Plumptre, T. (2006). *"How Good is our Board?" How Board Evaluations Can*. Policy.

Pocher, N. (2019). The Internet of Money between Anonymity and Publicity: Legal Challenges of Distributed Ledger Technologies in the Crypto Financial Landscape. In *JURIX*. Doctoral Consortium.

Poovey, M. (1998). *A history of the modern fact: Problems of knowledge in the sciences of wealth and society*. University of Chicago Press. doi:10.7208/chicago/9780226675183.001.0001

Prinz, A. (1999). Money in the real and the virtual world: E-money, c-money and the demand for cb-money. *NETNOMICS: Economic Research and Electronic Networking*, *1*(1), 11–35. doi:10.1023/A:1011441519577

Priyadharshini, A., Prasad, M., Raj, R. J. S., & Geetha, S. (2021). An Authenticated E-Voting System Using Biometrics and Blockchain. In *Intelligence in Big Data Technologies—Beyond the Hype* (pp. 535–542). Springer. doi:10.1007/978-981-15-5285-4_53

Qadah, G. Z. (2005). Requirements, design and implementation of an e-voting system. *Proceedings of the IADIS International Conference on Applied Computing*, 405–409.

Qiang, X. (2019). The road to digital unfreedom: President xi's surveillance state. *Journal of Democracy*, *30*(1), 53–67. doi:10.1353/jod.2019.0004

Qin, K., & Gervais, A. (2018). *An overview of blockchain scalability, interoperability and sustainability*. Hochschule Luzern Imperial College London Liquidity Network.

Rajapashe, M., Adnan, M., Dissanayaka, A., Guneratne, D., & Abeywardena, K. (2020). Multi-Format Document Verification System. *American Scientific Research Journal for Engineering, Technology, and Sciences*, *74*(2), 48–60.

Rath, M. (2019, November). A review of Artificial Intelligence Emerging technologies and challenges in Block Chain Technology. In *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 1031-1035). IEEE. 10.1109/ICSSIT46314.2019.8987807

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.

ReinersL. (2020). *Cryptocurrency and the State: An Unholy Alliance*. Available at SSRN 3682724.

Reisenwitz, C. (2014). Smart contracts promise for the Poor. *Bitcoin Mag*. https://bitcoinmagazine.com/articles/smart-propertys-promise-poor-1390852097/

Rooney, D., & Chavan, M. (2017). Globalization/internationalization. The International Encyclopedia of Organizational Communication, 1-15.

Rybarczyk, R., Armstrong, D., & Fabiano, A. (2021, May). *20210513 Galaxy Digital Mining - On Bitcoin Energy Consumption.* Retrieved June 1, 2021, from https://docsend.com/view/adwmdeeyfvqwecj2

Sadia, K., Masuduzzaman, M., Paul, R. K., & Islam, A. (2019). *Blockchain Based Secured E-voting by Using the Assistance of Smart Contract*. arXiv:1910.13635.

Sadowski, J. (2020). *Too smart: How digital capitalism is extracting data, controlling our lives, and taking over the world*. MIT Press. doi:10.7551/mitpress/12240.001.0001

Safko, L. (2010). *The social media bible: tactics, tools, and strategies for business success*. John Wiley & Sons.

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. doi:10.1080/13600834.2017.1301036

Schaller, R. R. (1997). Moore's law: Past, present and future. *IEEE Spectrum*, *34*(6), 52–59. doi:10.1109/6.591665

Schneier, B. (2007). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). John Wiley & Sons, Inc.

Schumpeter, J. A. (1942). *Capitalism, socialism and democracy*. Routledge.

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, *62*(6), 599–608. doi:10.100712599-020-00656-x

Sharma, P., Jindal, R., & Borah, M. D. (2020). Blockchain technology for cloud storage: A systematic literature review. *ACM Computing Surveys*, *53*(4), 1–32. doi:10.1145/3403954

Shermin, V. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, *26*(5), 499–509. doi:10.1002/jsc.2150

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. Penguin.

Slawotsky, J. (2020). US Financial Hegemony: The Digital Yuan and Risks of Dollar De-Weaponization. *Fordham Int'l LJ*, *44*, 39.

SMA. (2018, November). *FLIPHODL.* https://www.fliphodl.com/social-media-alternatives-series-ep-1-what-you-need-to-know/

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. doi:10.1016/j.jbusres.2019.07.039

Specter, M. A., Koppel, J., & Weitzner, D. (2020). *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections.* Available online: https: //www.usenix.org/system/files/sec20-specter.pdf

Srivastava, A., Jain, P., Hazela, B., Asthana, P., & Rizvi, S. W. A. (2021). Application of Fog Computing, Internet of Things, and Blockchain Technology in Healthcare Industry. In *Fog Computing for Healthcare 4.0 Environments* (pp. 563–591). Springer. doi:10.1007/978-3-030-46197-3_22

Starr, R. M. (1989). The structure of exchange in barter and monetary economies. In *General Equilibrium Models of Monetary Economies* (pp. 129–143). Academic Press. doi:10.1016/B978-0-12-663970-4.50014-1

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

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

Takabatake, Y., Kotani, D., & Okabe, Y. (2016). An anonymous distributed electronic voting system using Zerocoin. *IEICE Technical Report*, *116*(282), 127–131.

Tapscott, D. (1997). *Growing Up Digital: The Rise of the Net Generation*. Harvard Business Press.

Tapscott, D., & Euchner, J. (2019). Blockchain and the Internet of Value: An Interview with Don Tapscott Don Tapscott talks with Jim Euchner about blockchain, the Internet of value, and the next Internet revolution. *Research Technology Management*, *62*(1), 12–19. doi:10.1080/08956308.2019.1541711

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

Thagapsov, A., & Kozlovskiy, M. (2020). Bitcoin as Money. *Economic Analysis*.

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, *4*(3), 356–367. doi:10.1177/1534484305278283

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Analysis techniques for illicit Bitcoin transactions. *Frontiers of Computer Science*, *2*, 53.

Urgo, A. K., Lestan, M., & Khoriaty, A. (2017, September 17). *A cooperative of decentralized marketplaces and communities. Powered by Ethereum, Aragon, and IPFS*. District0x. https://district0x.io/docs/district0x-whitepaper.pdf

van den Hoven, J., Pouwelse, J., Helbing, D., & Klauser, S. (2019). The blockchain age: Awareness, empowerment and coordination. In *Towards digital enlightenment* (pp. 163–166). Springer. doi:10.1007/978-3-319-90869-4_13

Vassiliadis, S., Papadopoulos, P., Rangoussi, M., Konieczny, T., & Gralewski, J. (2017). Bitcoin value analysis based on cross-correlations. *Journal of Internet Banking and Commerce*, *22*(S7), 1.

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2020). Blockchain vehicles for efficient medical record management. *NPJ Digital Medicine*, *3*(1), 1–5. doi:10.103841746-019-0211-0 PMID:31934645

Vergne, J. P. (2020). *Decentralized vs. Distributed Organization: A Framework for the Future of Blockchain and Machine Learning and for Avoiding Digital Platform Dystopia*. Academic Press.

Vo-Cao-Thuy, L., Cao-Minh, K., Dang-Le-Bao, C., & Nguyen, T. A. (2019). Votereum: An Ethereum-Based E-Voting System. *Proceedings of the 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*, 1–6.

Voatz. (2021, February 4). *Voatz Response to Researchers' Flawed Report*. Voatz. https://voatz.com/2020/02/13/voatz-response-to-researchers-flawed-report/

Waldron, C. (2019). *Viability of the Usage of Blockchain Technology in Electronic Voting*. Academic Press.

Wang, J. (2021). *An In-depth Review of Privacy Concerns Raised by the COVID-19 Pandemic.* arXiv preprint arXiv:2101.10868.

Wattegama, D., Silva, P. S., Jayathilake, C. R., Elapatha, K., Abeywardena, K., & Kuruwitaarachchi, N. (2021). *"iSAY": Blockchain-based Intelligent Polling System for Legislative Assistance*. Academic Press.

Weatherford, J. (2009). *The history of money*. Currency.

Wright. De Filippi, Primavera. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia, SSRN 1, 16 (Mar. 20, 2015)

Wüst, K., & Gervais, A. (2018, June). Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE. 10.1109/CVCBT.2018.00011

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, *5*(1), 1–14. doi:10.118640854-019-0147-z

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016, April). The blockchain as a software connector. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182-191). IEEE. 10.1109/WICSA.2016.21

Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. *Future Generation Computer Systems*, *112*, 859–874. doi:10.1016/j.future.2020.06.051

Young, S. (2018). Changing governance models by applying blockchain computing. *Catholic University Journal of Law and Technology*, *26*(2), 87–128.

Young, S. (2018a). Enforcing constitutional rights through computer code. *Cath. UJL & Tech*, *26*, 52.

Zaman, S., Khandaker, M. R., Khan, R. T., Tariq, F., & Wong, K. K. (2021). *Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare.* arXiv preprint arXiv:2103.01322.

Zaprutin, D. G., Nikiporets-Takigawa, G., Goncharov, V. V., Sekerin, V. D., & Gorokhova, A. E. (2020). Legal Practice in the Blockchain era. *Revista Gênero e Interdisciplinaridade, 1*(1).

Zelmanovitz, L. (2011). Money: Origin and essence. *Criterio Libre*, *9*(14), 65–90. doi:10.18041/1900-0642/criteriolibre.2011v9n14.1232

Zhang, X. Z., Liu, J. J., & Xu, Z. W. (2015). Tencent and Facebook data validate Metcalfe's law. *Journal of Computer Science and Technology*, *30*(2), 246–251. doi:10.100711390-015-1518-1

Zhao, J. L., Fan, S., & Yan, J. (2016). *Overview of business innovations and research opportunities in blockchain and introduction to the special issue*. Academic Press.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4), 352–375. doi:10.1504/IJWGS.2018.095647

Zwitter, A., & Hazenberg, J. (2020). Decentralized Network Governance: Blockchain Technology and the Future of Regulation. *Frontiers in Blockchain-Blockchain for Good*, *3*, 12. doi:10.3389/fbloc.2020.00012

KEY TERMS AND DEFINITIONS

Agency Costs: Are the costs associated with the differences between the intentions of an agent and a principal, where the principal does not have complete control over the situation.

Backdoor: A hidden part of a computer program that may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information within networks without consent.

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

Cryptocurrencies: A digital or virtual currency that is secured by cryptography. It is a special case of a digital token which has its own blockchain.

Datafication: A modern technological tendency to transform different aspects of our life into data that are later transformed into information perceived as a new form of value.

Decentralized Autonomous Organization (DAO): A group of people with no central management that coordinate over the internet around a shared set of rules to achieve a common mission. It relies on a system created by a group of developers to automate decision-making, including assigning voting rights.

E2E-VIV: End-to-End Verifiable Internet.

ICTT: Information, Communication, and Transaction Technologies (an original expression proposed by the authors).

Meme: It is for memory just as the gene is for biology. It is the minimum unit of information that multiplies from brain to brain or between places where information is stored.

Proof of Stake: A type of consensus mechanism used by blockchain networks to achieve distributed consensus. It requires users to stake their tokens to become a validator in the network.

Proof of Work: The pioneer consensus mechanism. A proof of work is a piece of data which was difficult (costly, time-consuming) to produce to satisfy certain requirements. It must be trivial to check whether data satisfies said requirements.

Smart Contract: An auto-executable piece of code implementing arbitrary rules on a computer with distributed consensus (a blockchain), such that when the code is live it cannot be censored or shut down. Smart contracts are analogous to the business logic instantiated in code in businesses and organisations around the world, the difference being that here the code 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. It can be created on top of a blockchain by using smart contracts.

Transaction Costs: The costs incurred in making any economic trade when participating in a market. They are costs that do not accrue to any participant of the transaction.

Ultra Vires: (Latin - "Beyond the Powers") A Latin phrase used in law to describe an act which requires legal authority but is done without it.