DIFFERENT TYPES OF GOVERNMENT AND GOVERNANCE IN THE BLOCKCHAIN

Jersain Zadamig Llamas Covarrubias *,
Irving Norehem Llamas Covarrubias **

* *Corresponding author*, Lawyer, Independent Researcher, Mexico
Contact details: Av. Juárez No. 976, Colonia Centro, Guadalajara Jalisco, 44100, México
** Computer Engineer, Independent Researcher, Mexico

OPEN ACCESS

How to cite this paper: Llamas Covarrubias, J. Z., & Llamas Covarrubias, I. N. (2021). Different types of government and governance in the blockchain. *Journal of Governance & Regulation, 10*(1), 8-21. https://doi.org/10.22495/jgrv10i1art1

ISSN Print: 2220-9352
ISSN Online: 2306-6784

Received: 19.10.2020
Accepted: 21.01.2021

JEL Classification: G30, G38, K24, L22, M15
DOI: 10.22495/jgrv10i1art1

Abstract

This research work, a study was carried out on blockchain technology and its types, as well as the creation of new models of government and governance from the scope of an organization, infrastructure and platform. Governance and commercial models were addressed, based on standardization of data and legal frameworks. On the other hand, it showed how operational governance causes consequences in business models, whether with transactions, multi-signature, forks, consensus mechanism, smart contracts, tokenization, online dispute resolution and decentralized application (World Economic Forum, 2020, pp. 97-196). It was discovered that at least in current business models, private blockchain networks are more useful than public networks because they have greater operational flexibility and data governance, without exempting that public networks must also have mechanisms of governance since sometimes a human consensus must be reached to make updates to protocols and technical rules (The Law Society, 2020, pp. 24-61). This paper shows the basic principles that must be observed about governance and regulation in the implementation of blockchain technologies in systems created by governments, corporations and/or organized civil societies.

Keywords: Blockchain, Government, Governance, Decentralized Autonomous Organization

Authors' individual contribution: Conceptualization – I.N.L.C.; Methodology – J.Z.L.C. and I.N.L.C.; Writing – Original Draft – J.Z.L.C.; Writing – Review & Editing – J.Z.L.C. and I.N.L.C.; Supervision – J.Z.L.C. and I.N.L.C.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

1. INTRODUCTION

The devastating effects caused by the global financial crisis of 2008 resulted in society losing confidence in society's systems, that is, in the fundamental institutions of the economy that were deposited in banks, regulators and government. Therefore, the year 2008 marked a significant point of inflexion in public opinion, losing confidence in financial institutions and traditional governments and transmuting a new legitimacy towards large technology firms (Brown & Whittle, 2020, p. 82). As a result of this financial collapse, the Bitcoin white paper emerged in 2008 and was formally implemented in January 2009, this disruptive technology emerged, with the main idea of creating a form of electronic money of person to person, which allows the sending of online payments, directly between the parties and without passing through financial institutions, supplying some trusted third parties through cryptographic technology.

Another important factor to take into consideration is the interruption of administrative, legal and corporate processes caused by the pandemic known as COVID-19, forced governments, companies and society in general to re-evaluate the acceleration and construction of new models of services, goods and businesses, which would allow the evolution or the extinction of contemporary institutions. After this problem, entities have begun to organize new models in digital ecosystems, where government and governance are critical factors since blockchain is too useful for automating work between entities, which lead to creating business and business processes in an agile way.

Blockchain technology was conceived to be disruptive to the central authority and the uneven traditional organization, where the defenders argue that the idea behind distributed technologies and blockchain protocols should be the way to favour the constitution of a new form of social organization managed only by the rules promulgated within a computer source code in the blockchain network (Cappiello, 2020, pp. 23-24). Given this, it is necessary to ask whether each blockchain corresponds to an autonomous legal order, in addition to whether these systems can self-regulate without the need for a central (public) authority (Cappiello & Carullo, 2020, p. 2).

Currently, blockchain is a potential solution that allows a better implementation in most of the processes of any entity, allowing transparency, trust and ease of use in corporate voting systems. Even turn these systems into more inclusive corporate governments, by facilitating the inclusion of the voice of employees and customers (EU Blockchain Observatory and Forum, 2020, p. 25). But the debate continues to build, as the applications of blockchain technology represent an extremely fast-changing field, also with little theory established by recognized experts and no easy answers. The academic debate regarding this issue is still in a basic stage, as it focuses on cryptocurrencies such as Bitcoin and not so much on the major accounting record per se as technology. Therefore, at this time, a comprehensive and enunciative analysis of the impact of blockchain technology on political governance and democracy (Atzori, 2017, p. 46).

Blockchain networks promise to safeguard the confidentiality, integrity and availability of the information in such a tangible way as to share the data in a peer to peer networks (P2P), since the validation of the blocks, ensure that the network has a global state that is valid and accepted by all, without the existence of a central authority that governs it. Although blockchain technology had an essential role in the decentralization of applications and could be the representation of the total rejection of a central entity, this network has faced various challenges regarding its application in environments of analogous reality.

Key questions of governance often remain unaddressed in this literature, such as how and where exactly are decisions made and discontent voiced in blockchain-based activities? Do blockchains overcome the flaws of existing decision-making processes? Do blockchains give rise to new governance problems and pathologies? Is 'blockchain-based governance' desirable for all actors in the global political economy? (Campbell-Verduyn, 2018, p. 4). Before launching a blockchain project, you should also ensure that all stakeholders are aligned and that strong governance is in place, that is defining the roles and responsibilities of everyone in the network so that you can properly design the infrastructure (Tormen, 2019, p. 143).

From the different types of blockchain networks, being public and private (distributed ledger technology (DLT)), the consensus to upgrade the blockchain network without a trusted environment, creating smart contracts that communicate without the exchange of any intermediary, until the invention of decentralized autonomous organizations (DAO), where the members can decide the rules for self-governance before their existence, leads to the creation of crucial challenges in decision-making in conflicts of great importance.

It might sound contradictory to address governance in blockchain because *prima facie*, decentralized networks are protected as opposed to the control of an entity. Although this is true from a technological perspective, the reality is that we are human. For a blockchain network of a business level to be successful, some decisions need to be made throughout the life cycle of the system. Even on public networks like Bitcoin, the most famous, decentralized, pseudonymous and permissionless network, in the past, it had to deal with big and difficult decisions like the block size controversy known as SegWit implementation. Therefore, it is necessary that there is a basic agreement on the essential processes that must be followed in a network.

Considering the fact that blockchain technology is new and that it is still in the development phase, it is important to study the impact and the challenges of implementing decentralized blockchain-based applications and governance on the targeted society (Morabito, 2017, p. 43). Blockchain governance has tremendous transformative potential for our societies. However, the risks and benefits associated with its practical applications must be cautiously evaluated. There are hence reasons to investigate the role of the blockchain-based governance as a large catalyst of individual power, in a complete sense (Morabito, 2017, p. 56).

Governance is the most critical and compulsory requirement for a blockchain project's success because it maintains a decentralized property with self-executable business and legal contracts that are embodied in the transactions as smart contracts. The primary challenges for a blockchain project's success are specific to the scope, motivation, and governance rather than to the technology (Arun, Cuomo, & Gaur, 2019, pp. 45-47).

This research work will address the meaning and operation of blockchain technology, as well as its different types of networks, to begin later a study regarding the commercial, governmental and operational governance models, involving all the layers that make up this technology. This paper will talk about transactions, smart contracts, decentralized applications (DApps), forks, consensus mechanisms, online dispute resolution, computational infrastructure and data standardization according to practical legal frameworks.

As a warning, this research work aims to address in its greatest content the implementation of governance of private networks or DLT and its implementation in government entities and corporations, solving some questions, about the legal and corporate structure of a blockchain network, as well as property rights and the role of participants in the network. Likewise, the minimum foundations of the de facto and normatively applicable rules for the implementation of decentralized and distributed systems will be described, in harmony with the rights and obligations of the members of the consortium and participants.

This paper is structured as follows. First, in Section 2 we talk about different ideas related to governance in the blockchain technology and mention the different types of blockchains that exist to understand the nature of each of them. Once this is explained, Section 3 analyses the difference between government and governance, from the business perspective where we explore the different legal agreements between the parties involved in the blockchain networks and also present the different infrastructure implications by the option chosen where private blockchains show to have better mechanisms that enforce governance. After talking about this governance from the business perspective, the paper shows the operational governance is managed without any central authority and is used to control the governance over a group of people. In the discussion part (Section 4) some point of view related to the concerns of blockchain governance and their possible risks are analyzed. Finally, Section 5 concludes by presenting some advantages to choose a DLT over a public blockchain to enforce that system complies with regulations and governance.

2. LITERATURE REVIEW

In 1997 Szabo published a paper entitled *The God Protocols* (1997), which opens a milestone in the debate regarding trusted entities, because he says that if we imagine an ideal protocol, we would have the most reliable third party that one can imagine because God is on the side of all, it specifies that with a reliable protocol, with a protocol from God, all parties will send their contributions to God. God would reliably determine the results and return them. Moreover, Lessig (1999) wrote his work *Code: And Other Laws of Cyberspace*, which deals with the structure and nature of Internet regulation, making an analysis of the source code and the law, exploring the relationship of the programming source code as an instrument of social control, synthesizing that the code is the law.

According to previous information, is it possible that a source code and mathematical algorithms can substitute a set of representatives and that the governed control this code? This technological representative could require the consensus of thousands of the governed who sign with their key (asymmetric system), their consent for a specific action. But this libertarian breath is not new either, because in the rise of the Internet, movements and scientists in favour of protection in cyberspace were expressed, such as Clark (1992, p. 19), who was even more radical and said that we reject kings, presidents and voting, we believe in consensus and code execution.

With blockchains, people can create their systems of rules or smart contracts, enforced by the underlying protocol of a blockchain-based network. Creating systems without law and implementing private regulatory frameworks what refer to *lex cryptographica*. Blockchain enables a system that is enforced automatically by the blockchain itself reducing the necessity of intermediaries (De Filippi & Wright, 2018, pp. 5-6). *Lex cryptographica* blockchain-based systems could operate autonomously without creating tensions with existing laws and regulations, the system operates driven just by the protocol and the smart contracts (De Filippi & Wright, 2018, pp. 49-50).

However, blockchain technology should not be seen as a solution that tries to eliminate representation, but rather to reinforce the necessary order executions when scheduled, creating immutability and strict compliance. Admittedly, in misuse, DAO could be designed to bypass existing laws and regulations, for example, the operations of a DAO ultimately depend on the operations of the underlying blockchain-based network. As long as the DAO collects enough funds to operate, it will continue to work to advance its mission, without paying attention to the implications this could have on society (De Filippi & Wright, 2018, pp. 153-154), but the reality is that technology is not bad, perhaps the use that is given to it, but that does not mean it will be necessary to stop the progress of society.

On the other hand, Grabowski (2019, p. 84) mentions that in blockchain governance, each cryptocurrency also has its own set of self-regulation, this means, each blockchain has a team that constantly makes decisions and, as such, these projects must be governed. And just as there are various forms of government, also in the blockchain, specifically in cryptocurrencies; some cryptocurrencies operate like an oligarchy with the founders or a small group of influencers having the final decision. Other cryptocurrencies are more democratic and allow those who own the coin to vote on decisions. In any company or community, strong and competent governance is necessary for success. Bad decisions and power struggles can lead to a crisis and the same holds for cryptocurrency. When investing in a cryptocurrency, it is worth considering how it is governed, this aspect of blockchain is perhaps the greatest predictor of a particular chain's success or failure states.

Similarly, Holbrook (2020, pp. 257-258) shows that blockchain technology brings new challenges but also new opportunities to enterprises around compliance. Not all blockchains could meet all compliance requirements, for example, permissioned blockchains enable compliance whereas permissionless generally do not enable it. And no matter which business is being analyzed compliance should be addressed. Blockchain is not a one-size-fits-all solution and challenges may vary and this will have an impact on governance, risk, and compliance. That is the reason some projects understand the importance of permissioned blockchains and some of them have an organization that helps to provide governance, that is the example of Hyperledger where Linux foundation understands this and build a technical community

and an ecosystem for blockchain development, with legal and brand support (Dhillon, Metcalf, & Hooper, 2017, pp. 140-141).

Furthermore, Parkin (2020, p. 117) expresses that blockchain networks are created by humans. People enrol machines to maintain and run their networks. That is when it is clear that human actors operate the networks, not the machines and the codified rules of the protocol. The idea of decentralisation is to promote systems that are not easily coerced, but as the decisions have to be made in centralised channels this makes it harder to allow this effect. The limits for algorithmic decentralisation are related to people because they have the final word on how these systems are deployed.

Specifically, the present work will guide you to understand why permissioned blockchains should be used in commercial applications to ensure easy data governance and legal compliance. We will cover different agreements that exist in both permissioned and permissionless blockchains, and explain some issues that could arise in smart contracts, tokenization and online dispute resolution. We will provide legal and technical foundations on blockchain to implement governance inside and outside of the chain.

2.1. Blockchain definition

A pseudonymous entity called Satoshi Nakamoto (2008) published a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*. In 2009 Satoshi revealed the open-source software, and the network went live. From its emergence to the present, the term blockchain, which is the technology that was born by cryptocurrencies, has been perfected, revolutionizing all sectors and systems in this world.

Without conflicting about what blockchain means, two definitions are shared below by Bashir (2020), a simple definition and another technical:

"Layman's definition: *Blockchain is an ever-growing, secure, shared recordkeeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.*

Technical definition: *Blockchain is a peer-to-peer, distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers*" (p. 12).

2.2. Types of blockchain

With the excellent blockchain disruption and its impact on all sectors, this technology has a broad application in various use cases. In this section, we will talk about the need to create different models of blockchain networks.

It should be noted that there is a solid legal framework that protects specific legal assets, resulting in the need to select a type of blockchain network before starting a project. As Werbach (2018, pp. 133-134) mentions, the legal system will shape the blockchain economy, but the real success of systems based on this technology will depend on the internal capacity to create new forms of governance.

2.2.1. Public (permissionless)

The initial blockchain model was the product of the Bitcoin network, being completely open and without permission, where all nodes are treated impartially. This network works perfectly on untrusted networks due to the immutable nature of the registry. Bitcoin, Ethereum, and various projects that share the Proof of Work (PoW) consensus mechanism ensure that recorded transactions are not editable, so these networks are ideal for records that should not be changed. However, these types of networks can frequently face scalability problems at some point if the necessary changes are not implemented (Raj, 2019, p. 15).

In short, in public networks or also known as permissionless, there are no restrictions to read transactions, since anyone can download the updated blockchain ledger with the node client and participate.

2.2.2. Private (permissioned)

This type of network was introduced to expand the reach of blockchain technology. This permissioned blockchain, as the name implies, uses an approach opposite to that of the public blockchain, since they introduce access control to provide specific access to participants in a network, having an administrator who assigns the roles to the participants in the network. It is imperative to point out that in these networks it must be guaranteed that no attacker or unknown entity forms part of the network nor in the processes of validation or creation of the blocks and thus avoid any possible attack on the network. Likewise, these types of networks are suitable for organizations in which a ledger is only shared internally. It should also be clear that these types of networks are often not completely immutable. Their transactions can be modified with some effort, for what this is in contrast to public blockchains, where it is almost impossible to alter them (Raj, 2019, p. 16).

Also, private blockchain networks, also known as DLT, tend to be smaller and do not use a cryptocurrency, and their membership is tightly controlled. This type of blockchain is favoured by consortia that have trusted members and exchange confidential information (Laurence, 2019, p. 8).

In practice, companies are likely to be drawn to private blockchains rather than public blockchains for several reasons, including because there is greater certainty of the rules governing how these blockchain networks operate. In this regard, there are two important models in DLT, which are the *distributed ledger model*: the trusted intermediary runs all the nodes and participants access the nodes on a software-as-a-service basis; and the *shared ledger model*: the trusted intermediary runs a node that hosts a full copy of the database. Participants can also run their own nodes that download a partial copy of the database (this copy only includes data to which the relevant participant is a counterparty) (The Law Society, 2020, pp. 26-28).

One very famous DLT is Hyperledger, which is an open-source project that was created to help advance blockchain technologies between industries. In this DLT five mainframes are contemplated, being Hyperledger Iroha, Hyperledger Sawtooth,

Hyperledger Burrow, Hyperledger Fabri, and Hyperledger Indy. It should be noted that there are various private or DLT networks such as Quorum, Ripple, R3 Corda, MultiChain, Symbiont, and OpenChain.

2.2.3. Hybrid

The consortium blockchain is a hybrid blockchain that is semi-decentralized. It combines the best characteristics of blockchain networks without permission and with permission. Instead of assigning most tasks to a single organization, a consortium blockchain assigns the same functions to nodes maintained by multiple organizations (Raj, 2019, p. 17).

In these types of networks, also known as semi-private networks, one part of the blockchain is private, and another is public. The private part is controlled by a group of people, while the public part is open to anyone. This hybrid model can be used in scenarios where the private part of the blockchain remains internal and is shared among known participants. In contrast, anyone can still use the public part of the blockchain, optionally allowing the mining to secure the network. In this way, the blockchain can be protected by PoW, which provides consistency and validity for both the private and the public part (Bashir, 2020, p. 26).

3. GOVERNANCE AND GOVERNANCE IN BLOCKCHAIN NETWORKS

It is imperative to point out the difference between government and governance because although in practice, they are used interchangeably as synonyms, in the strict sense, they have different meanings. In a specific way, the government is "the group of people who officially control a country", that is, the government is an element of the state, made up of people called rulers who direct the administrative, political function of territory.

Continuing with the analysis, governance "is a neutral concept referring to the complex mechanisms, processes, relationships and institutions through which citizens and groups articulate their interests, exercise their rights and obligations and mediate their differences" (UN, 2008, p. 23). At the data level, governance is "a set of processes that ensures that data assets are formally managed throughout the enterprise. A data governance model establishes authority and management and decision making parameters related to the data produced or managed by the enterprise" (NIST, n.d.).

With these caveats made, the intersection between blockchain and the government can be interpreted as the application of this technology for government actions. At the same time, blockchain governance refers to the mechanisms through which decentralized node networks adapt and change over time, including decisions such as changes to block size, storage format, execution protocol in smart contracts, consensus mechanisms and more.

If control over decisions is not required, then the public blockchain grants a good reputation, as they are superior as they are less prone to drastic changes in governance. However, in cases where an entity requires more control over network governance or business processes and transactions, a private network would be the best option. Although it should be clear that even in private networks, the members could experience challenges with governance because even if the members of the network know each other, decisions can also be made contrary to the interests of the participants (World Economic Forum, 2020, pp. 115-119).

Governance can also be defined as entities whose sole responsibility is to establish the set of rules and laws in which a given system makes binding decisions. While blockchain started with permissionless networks like Bitcoin that relied on systemic governance based on technologies through incentives and coordination, this isn't easy to implement when the business world tries to apply blockchain principles in their business and legal models, since that the business world is highly regulated and, therefore, most business use cases are based on private blockchain models with checks and balances that influence from the design of operations to the growth model of the organization models (Gaur et al., 2018, p. 69).

In general, governance in blockchain networks is a complicated problem, so finding a balance between centralized and decentralized controls is key to maintaining correct development and application. Some critical governance issues that have been dealt with in practice are solving scalability problems without weakening the network; changing incentives for the community; improvements in decentralized standards; and decisions that perfect robust infrastructures.

Government and governance are essential elements for participation, ownership, rights and obligations. In blockchain networks, the role of each participant must be well defined and contribute something to the network, since regardless of the role played, as a leader, executive or central group, participant or member of the project, end-user and/or provider as the third party, their contributions make the network a sustainable ecosystem. While the consortium group may be interested in network legal and budgetary issues, end-users will only be interested in information security or consensus rules; however, this does not excuse lack of participation.

Public blockchain networks, specifically Bitcoin, lack a formal governance structure; however, their developers and the community, in general, can manipulate and create changes of a technical nature in the network voluntarily and compatible with the consent of the majority. That's the reason that Bitcoin Improvement Proposal (BIPs) was born, some important BIPs have been BIP-11: M-of-N Standard Transactions, BIP-16: Pay to Script Hash and BIP-141: SegWit.

Next, two crucial governance models will be defined for private blockchain networks or DLT, being business and operational governance, which are divided into two separate models but with consequences that could affect one another, for example, the legal and operational aspects. Business decisions could influence the operational way in which blockchain networks work. On the other hand, operational governance could cause problems at its intersection with analogous reality, which could transcend and impact corporate governance.

3.1. Business governance

This model includes the formation of a legal person or an agreement between various members, where a form of government is established between legal entities as well as a budget for the creation of business models and the allocation of profits, allowing the selection of new lines of business, marketing strategy and standards for the incorporation of new members to the company (World Economic Forum, 2020, p. 54).

In this model, the governing body belonging to corporate governance will have ultimate responsibility for all aspects of the consortium's business governance, such as collections, funds, vendor selection, services, and software. It could also have authority over operational policies, such as the information security requirements that participants must meet.

It is crucial to verify before building a model of this type, to know what the purpose of the consortium is and what the organizational structure will be like, the ownership of intellectual property, ensure competition and inclusion, define the management of responsibility and risks, as well as count with a business and economic strategy.

Finally, a pivotal decision to form this model in the entities is to know a priori, if they want to create a new legal entity or enter into a formal contractual agreement between the members of a consortium, for which they will be explained below, various basic principles to build governance models in harmony with the blockchain network.

3.1.1. Governance and commercial models, data standardization, legal framework

When two or more people or entities exchange data with each other, the governance models that maintain this relationship must be compatible with each other, with well-defined legal frameworks and commercial agreements. The government model must guarantee trust between the participants, as well as a standardization of data to improve the reliability of the records on a blockchain platform and that the parties can understand these.

Regarding standardization, there may be organizations that create international standards such as The Institute of Electrical and Electronics Engineers (IEEE) and The International Organization for Standardization (ISO) (World Economic Forum, 2020, pp. 101-102).

An example is the ISO that has a Technical Committee (ISO/TC 307 Blockchain and distributed ledger technologies[1]) that is developing a standard for the implementation of blockchains and distributed ledger technologies, they are working in ISO/DTS 23635 Blockchain and distributed ledger technologies — Guidelines for governance[2].

Likewise, establishing the legal framework is necessary and challenging to determine who is the owner of the network and the data, as well as who is the processor and responsible for the information, besides, to which jurisdiction the disputes are applied, who controls the information. Another aspect is the business model that is a fundamental piece for the success of consortia (World Economic Forum, 2020, p. 103).

The importance of all these elements applied to governance, and commercial organization model, data standardization and correct application of a legal framework will lead to creating advantages, such as being able to save lower operating costs, or that risks are limited to specific actions of the entities, reducing the risk of exposure and limited liability. Although also certain disadvantages such as control problems between digital assets and participants, as well as being considered as a legal partnership and not a legally formal agreement, attributing more rights and obligations. With that said, we will explore business models for blockchain networks below.

Contractual Consortium Model

In this model, all the members of the consortium (including the developer of the blockchain platform) establish governance structures with clearly defined levels. The members of the consortium can be end-users, but there can also be such users who are not members of the consortium, governed by end-user licenses. These users will have a lower level of influence on the development of the platform. In a strict sense, they will receive it as a service, while the new members that join the consortium would be above this since they can contribute to the development of the platform with more rights and influence (The Law Society, 2020, p. 50).

Corporate Joint Venture (JV) Model

This model implies the creation and incorporation of an independent corporate entity responsible for the platform. The members of the consortium will be the parts of the JV, so if a technology company participates in the consortium union or participates in another way, it may be part of the joint venture or a service provider to it. The entity will be responsible for creating the terms of the platform or participation agreements that apply to all participants and end-users. Each member of the JV must invest in the development of the platform, which can range from financing the product itself, providing intellectual property or essential technical or industry knowledge (The Law Society, 2020, p. 51).

Participant Agreement Model

It is not a consortium agreement as such, but rather contractual agreements established between individual parties. In this model, the network operator will create a standard set of platform terms that would then be offered to a variety of participants as a one-to-many solution (The Law Society, 2020, p. 53).

Developer Agreement Model

Like the Participant Agreement Model, it is not a consortium agreement as such, but rather a contractual agreement established between individual parties. In this agreement, some participants will enter into a multi-party agreement between themselves and the network operator with a common purpose. Still, the network operator would retain the decision-making power of the platform (The Law Society, 2020, p. 53).

[1] https://www.iso.org/committee/6266604.html
[2] https://www.iso.org/standard/76480.html

3.1.2. Infrastructure

Once addressing the organizational model of governance, it is essential to note that the board of directors or members of the consortium decide the infrastructure layer, so it is part of the corporate governance model. In contrast, the platform layer is part of the model of operational governance that will be discussed later. Having made this clarification, the infrastructure layer is responsible for enabling the services of the blockchain platform, being computing, storage, networks, virtualization, which is often complicated to carry out due to the great legal difficulty in reaching agreements with third parties or making organizational decisions.

It should be clear that decentralized and distributed are not synonymous, the difference between these two concepts is that distributed means that the calculation is spread across multiple nodes instead of just one and decentralized means that no node is instructing any other node about what to do, this can be adopted in an internally distributed architecture to accelerate data latency and computational power (Raval, 2016, p. 4).

From the above, distributed means that not all processing is done in the same place, so we can find systems that are centralized and distributed at the same time. About decentralization that all control of processing does not fall to a single entity, Buterin (2017), creator of Ethereum, has classified three types of decentralization, being the architectural, political and logical, which are expressed below:

- *Architectural (de)centralization*: how many physical computers is a system made up of? How many of those computers can it tolerate breaking down at any single time?
- *Political (de)centralization*: how many individuals or organizations ultimately control the computers that the system is made up of?
- *Logical (de)centralization*: does the interface and data structures that the system presents and maintains look more like a single monolithic object, or an amorphous swarm? One simple heuristic is: if you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?

In cloud computing, there are several models, being Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) (Barry, 2013, pp. 41-43), Function as a Service (FaaS) (Jägare, 2019, pp. 188-189), until reaching blockchain as a Service (BaaS), where with a level of maturity in the platforms it is expected that entities can migrate the next few years to this model, a practical example of this latest BaaS model is Microsoft's Azure, in which the Ethereum blockchain is provided as a service, and the platform on the IBM Cloud, which provides the IBM blockchain as a service. One step in this BaaS is to become an Electronic Government as a Service (eGaaS), giving specific blockchains for governance functions applications such as http://egaas.org, which aims to organize and control activities without circulation of documents and bureaucratic expenses (Bashir, 2020, p. 752).

Public, private or hybrid networks can also be used to protect intellectual property and the protection of personal data. In the case of blockchain, we would have; as a result of a possible collision between rights and technologies, on the one hand, immutability and transparency, while on the other hand, confidential personal information, suppression or erasure, coupled with complications in the transmission of information and identification of the subjects and those responsible for the treatment. Hence, a possible solution to this uncertainty would be the implementation of private blockchains to comply with the rights enshrined in special data protection laws, without leaving out that this could go against the blockchain nature as they are not fully distributed networks and decentralized, or even another hybrid solution, would be to store the data in a private network, but at the same time the hash of the data in a public network to protect the integrity of the information.

3.2. Operational governance

This model includes establishing information security and other standards using blockchain technology. It grants permissions to new network participants when they comply with applicable rules and determines when participants must update new versions of software and dispute resolution (World Economic Forum, 2020, p. 54).

In this model, it is essential to verify how the members join the network, as well as who is responsible for approving them if it is necessary to know the users and in what circumstances a user can leave the network. Is also important to define how the data, exchange and storage standards, based on whether the data goes inside or outside the blockchain and separating the data depending on the category and nature of the same according to the special laws on intellectual property and the protection of personal data.

In the case of public networks, it is necessary to know how the operational governance of the computer source code of the blockchain network works to achieve consensus and decision-making from technical aspects, which have repercussions in actions of analogous life. To understand better this, we will explain governance at a platform level below.

In this layer, it is imperative to select what type of network should be implemented, depending on the business model and needs. Once knowing the kind of model to be implemented, it is necessary to define the consensus mechanisms that are a fundamental pillar of blockchain networks so that they can have interoperability. Smart contracts will also allow the creation of programs on blockchain platforms, encoded in various programming languages to move to automated contract execution. Lastly, regarding authentication & authorization, different blockchain platforms can support multi-signature transactions, thus allowing multiple participants to sign in the same transaction digitally.

3.2.1. Transactions

As mentioned above, blockchain eliminates the need for intermediaries, establishing trust and avoiding fraud in transactions and property, since as the information is authenticated and validated throughout the network, the property and origin of all data can be known and transactions. Thus, each participant of the network (called a node) has a copy of the ledger that contains the details of all

chronologically validated transactions that have occurred on the network. It is necessary to mention that each transaction is authenticated and validated through a cryptographic key guaranteeing that the owner of a specific entity of value makes the transaction and avoids double-spending.

The steps of a transaction are simple: first, the sender transfers an entity of value to the receiver and begins a transaction, this includes the public address of the receiver, the value of the transaction and a cryptographic digital signature; second, the transaction is authenticated, where the participants called nodes in the network receive the transaction information and authenticate the validity, when it is validated it is placed in a group of transactions; third, a block is created with a group of transactions and an updated version of the ledger by one of the participating nodes, so that in a specific interval depending on the network, the block is transmitted to the entire network for validation; fourth, the block is validated, since the participating nodes start the validation process upon receipt of the block of transactions, so it is required for its completion that the consensus rules are met (for example, 51% validity); fifth, the block is added to the existing blockchain, and the updated blockchain ledger is transmitted to the entire network, this process has the duration according to the network protocol (Upadhyay, 2019, pp. 13-15).

Multisignature

These types of scripts establish a condition in which '*N*' public keys are registered in the script and at least '*M*' of them must provide signatures to unlock the funds. This scheme is also known as *M-of-N*, where *N* is the total number of keys, and *M* is the threshold of signatures required for validation. For example, a 2 of 3 multiple signatures is one in which three public keys are listed as potential signers, and at least 2 of them must be used to create signatures for a valid transaction to spend the funds (Antonopoulos, 2017, p. 149). Multisignature refers to requiring more than one key to authorize a transaction; this is an implementation in the Bitcoin network that will help in decision-making for entities.

Multisig is vital for governance, especially when there are large amounts of funds (Bitcoin), as these scripts ensure that for the transfer of funds more than one signature must be required to make a payment, but these signatures must be in different locations or managed by different people, for example in a company can be divided into several executive firms so as not to compromise funds.

3.2.2. Forks

A fork is said to have occurred when there is a conflict between the nodes regarding the validity of the blockchain, that is, more than one blockchain is on the network. A soft fork, is any change in the blockchain protocol that is backwards compatible, let's say that instead of 2 MB blocks, it is possible that a new rule only allows 1 MB blocks, so outdated nodes will follow viewing the new transactions as valid (1 MB is less than 2 MB in this example). However, if the non-updated nodes continue to create blocks, the blocks they create will be rejected by the updated nodes. Therefore, if the minority of nodes in the network is updated, the chain they will form will be less accurate and will be overridden by the blockchain created by the non-updated nodes. The soft forks are resolved when the majority of the nodes on the network update their node software (Prusty, 2018, p. 30).

Likewise, a hard fork is a software update that introduces a new rule on the network that is not with the previous software. More simply, the hard fork is an expansion of the rules, for example, a new rule allowing the block size to be 2 MB instead of 1 MB would require a hard fork. Nodes that continue to run the previous version of the software will see the new transactions as invalid. Therefore, the fork can only be resolved when all nodes on the network update their node software. Until then, there will be two different blockchains on the network (Prusty, 2018, p. 30).

Broadly speaking, if enough miners choose to run different software, the network forks and there will be two blockchain networks that diverge over time. In some ways, forks are a beneficial feature of blockchain networks, as they demonstrate that no group that somehow achieves a majority of voting rights (in the form of mining 'hash power') can force a minority to accept their decisions. The two parties will go their ways, and users will decide which blockchain they value and trust. Forking is a well-accepted practice in the open-source world (Werbach, 2018, p. 145).

3.2.3. Consensus mechanism

The consensus is a fundamental aspect of human societies, as it is a way of specifying that a diverse group agrees to something without any conflict. This antecedent is an essential element as it is part of operational governance, that is, of how blockchain networks will work. Even Ludwin (2017) said that cryptocurrencies don't *have* governance mechanisms, they *are* governance mechanisms.

The best-known consensus mechanisms are the PoW, which is based on the proof that adequate computational resources have been spent before proposing a value for the acceptance of the network, this scheme is used in Bitcoin, Litecoin and other cryptocurrency blockchains. Currently, it is the only algorithm that has proven to be astonishingly successful against any attack on a blockchain network, such as the Sybil attack. Another is Proof of Stake (PoS), which works on the idea that a node or user has an appropriate stake in the system; that is, the user has invested enough in the system that any malicious attempts by that user outweigh the benefits of making such an acknowledgement on the network. Another critical concept in PoS is the age of the coins, which is a criterion derived from the amount of time and the number of coins that have not been spent. In this model, the chances of proposing and signing the next block increase with the age of the coin (Bashir, 2020, p. 32).

Other consensus mechanisms are Delegated Proof of Stake (DPoS), Proof of Elapsed Time (PoET), Proof of Deposit (PoD), Proof of Importance (PoI), Federated consensus or federated Byzantine consensus, Reputation-based mechanisms, Practical Byzantine Fault Tolerance (PBFT), Proof of Activity (PoA), Proof of Capacity (PoC), Proof of Storage & Proof of Authority (PoA).

However, consensus mechanisms and their rules only serve for the operational layer where pre-programmed functions are followed, so it is necessary to specify that blockchain technology should not depend solely on consensus rules to solve real disputes and problems that go further from a transaction validation by miners.

Likewise, despite being neither a platform nor operational decision, it is necessary to mention that the future and possible change of the consensus mechanism in the Ethereum network will be a governance decision in blockchain. In this case, Ethereum currently uses the consensus mechanism known as Proof of Work, but due to some scalability problems they have repeatedly announced their change to the consensus mechanism called Proof of Stake, so the community of Ethereum will have excellent governance and decision-making challenge in architecture changes that allow fragmentation of the proposed network to solve scalability.

3.2.4. Smart contracts

A smart contract is a secure and unstoppable computer program that represents an automatically self-executing agreement. Also, it is written in a programming language that a machine can understand and runs automatically when certain conditions are met. They are based on the principle that the code is the law, which means that a third party doesn't need to control or influence the execution of the smart contract (Bashir, 2020, p. 290). In this case, intangible or digital assets could be easy to transfer, using a computer program that runs on the blockchain network, where the circumstances are defined, their occurrence is verified and executed (transfer or transmission of digital assets).

It should also be mentioned that smart contracts are divided into two types: deterministic and nondeterministic. Given this, the white paper of the JUR project (2019, pp. 20-21), states that non-deterministic do not contain all the elements necessary to conclude, so they are not entirely self-executing, by not being able to automatically trigger transactions without data that are not directly accessible to the contract. On the contrary, determinists contain all the elements that allow automated analysis of the data available to trigger the execution of the contract.

However, some problems in the implementation of smart contracts are their lack of auditing that could lead to an incorrect execution according to the original legal objectives, because more than automated computer programs that run on blockchain networks, their implementation must be even deeper in the hands of digital identity, to reach a level of governance of smart contracts, where it is possible to identify the signature of the entities responsible for the contracts.

Other types of contracts are smart legal contracts, or also known as Ricardian contracts, invented by Ian Grigg in 1996 and allow legal contracts to be translated into digital counterparts with the original traditional prose that remains intact. This approach enables a contract to move from legal paper documents to a world of cryptography and the world of accounting. Smart contracts can contain traditional prose, to become smart legal contracts (in reference to Ricardian contracts) (Mohanty, 2019, p. 51).

Grigg (2004) called these contracts Ricardian because they were developed for the Ricardo system. Ricardo defined his contracts with three components: legal code (the human-readable standard text), computer code (the executable steps of a smart contract) and parameters (the variables that influence how computer code is executed). The legal code included the cryptographic hash chain of the computer code, to guarantee that it was referring to a smart contract and in parallel, the smart contract included the cryptographic hash chain of the text of the legal contract. Therefore, the two were linked, and if there was a problem with the smart contract, one could resort to the legal contract for resolution (Werbach, 2018, p. 212).

The Ricardian contract solves the problems of a smart contract, as it takes the legal prose, incorporates the signature and then copies the agreed document, this last copy step is the magic because it uses a secure hash. With this method, an algorithm is produced that results in a unique number that is entirely related to the document and only this document can reveal that hash and with the security that refers to a certain document. The main subject of Ricardian contracts is not the name, extract or terms and conditions; it is the hash since it forces the developer to maintain a complete repository and contract. In short, a Ricardian contract incorporates smart code and negotiation (prose, code and parameters), where the Ricardian contract becomes a digital document that captures the contract between the parties, ensuring by its hash that the correct contract is identified and is also always present, and includes all the necessary components to keep up to date the trade that users wish to apply.

In conclusion, in smart contracts and smart legal contracts, it must be ensured that there should exist an adequate data governance framework with any data variable relevant to them. It is a formalization of authority, control, and decision-making regarding these data variables. This implementation is unlikely to be under the complete control of the parties to a smart contract; however, there should be a meeting of minds as to the acceptance of data governance (The Law Society, 2020, p. 45).

Tokenization

A token is a unit of value that an organization creates to self-govern its business model and empower its users to interact with its product while facilitating the distribution and exchange of rewards and benefits to all its stakeholders. Likewise, with the ability to tokenize anything, whether tangible or intangible, we achieve an unlocking of liquidity of assets, we understand liquidity as a new easy or fast way to access the capital stored in each asset. Therefore, with tokens, the value of a property is represented, and they can be negotiated much more efficiently, allowing new economic models such as fractional ownership where investors can own a certain percentage of a particular asset as if they were shares. However, some issues such as digital identity, money laundering and tax matters must be met and present challenges for various financial market regulators (Au & Power, 2018, pp. 19-20).

Tokens are fungible when we can substitute any unit of the token for another without any difference in its value or function, on the other hand, non-fungible tokens are tokens that each represent a unique tangible or intangible element and, therefore, are not interchangeable. For example, a token representing ownership of a specific Van Gogh painting is not equivalent to another token representing Picasso, even though they may be part of the same art ownership token system, as each token is non-fungible. It is associated with a unique identifier, such as a serial number (Antonopoulos & Wood, 2018, p. 223).

An example is the decentralized virtual reality world called Decentraland, where participants can own and trade pieces of virtual land in the game, as well as build, develop, or trade other assets within the game. It is important to note that when a token is fungible, it obtains a characteristic of a non-rival good, which is when the use of this by a consumer does not prevent others from enjoying the good, for example, fiat currencies are fungible because each unit is interchangeable with any other equivalent individual unit. While a non-fungible token, it obtains the categorization of a rival good, whereby exclusion the consumption process is exhausted, in such a way that a consumer prevents others from enjoying the good, therefore, each property represented in Decentraland is a type cryptographic token of a blockchain that represents a single asset.

Online dispute resolution (ODR)

When knowing some possibilities of dispute resolution, we will find that with traditional justice, a centralized and possibly necessary system is still used as a starting point. Nevertheless, paying homage to blockchain and decentralized and distributed systems, it is decided to develop a new model of a decentralized court of justice or a new alternative dispute resolution on blockchain. Currently, there are two approaches; the first is that smart contracts can operate within the contract and legal framework, coupled with the fact that they can be judged by traditional courts, as we saw in the case of Ricardian contracts, which are also known as smart legal contracts, and as a second point, a decentralized dispute resolution procedure. Most jurisdictions recognize the arbitration clauses of the New York Convention, specifically in foreign arbitration awards, where the courts accept and enforce the sentence in this way in the appropriate circumstances.

Nobody likes to think about disputes more than they would about the exit process; however, it is essential to define a strategy to address these disputes. In this context, governance should cover areas such as the following:

- *Raising complaints*: Where should these issues arise? What if you are working on a truly decentralized model? Do you have a forum to raise this?
- *Investigation*: How will the facts be collected? How will the problem be documented? If the outcome of a smart contract transaction is disputed, will it (and its corresponding customer) be pulled from the ledger? Likewise, disputes will not always arrive happily, but what is the process to resolve them? Is there a subset of participants who should decide on the issue? Should this become a legal process? (Gaur et al., 2018, p. 380).

Some decentralized court projects are Kleros, Aragón, JUR, Mattereum, LTO Network, Blockchain Arbitration Forum, Enigma, Sagewise, Agrello, Oath Protocol and OpenLaw.

3.2.5. Decentralized application (DApps)

Swan (2015, pp. 22-25) defines DApps as genus and DAO, DAC and DAS as species, being a trajectory to build increasingly autonomous smart contracts. These are shorthand terms for decentralized applications (DApps), decentralized autonomous organizations (DAO), decentralized autonomous corporations (DAC), and decentralized autonomous societies (DAS). Essentially, this group connotes a potential progression to increasingly complex and automated smart contracts that look more like self-contained entities, performing pre-programmed and eventually self-programmed operations tied to a blockchain, and this creates a scenario of decentralized applications that work without a central entity, to offer and manage goods or services, with more direct interaction, achieving that users are directly related to smart contracts and the blockchain.

DAO is not artificial intelligence (AI) since an AI system has the ability of an unnatural entity to make decisions through an evaluation process (Turner, 2019, p. 16). In the same vein, the power of a system to interpret external data correctly, learn from said data, and use those learnings to achieve specific goals and tasks through flexible adaptation (Kaplan & Haenlein, 2019), while in DAO, the orders are scheduled to be fulfilled and voted on by consensus.

It is not about eliminating representation, but rather about reinforcing the execution of orders necessary when programmed, creating immutability and strict compliance. It is true that in misuse, DAOs could be designed to avoid or bypass existing laws and regulations; for example, the operations of a DAO ultimately depend on the functions of the underlying blockchain-based network. As long as the DAO collects enough funds to operate, it will continue to work to advance its mission, paying no attention to the implications this could have on society (De Filippi & Wright, 2018, pp. 153-154). Decentralized autonomous organizations represent the most advanced state of automation, where a blockchain-based organization is not run by humans or by group consensus but rather by smart contracts, algorithms and deterministic code (De Filippi & Wright, 2018, p. 146).

That said, let's imagine a democratic algorithm that set of steps that can be used to solve problems or help us make decisions. Now imagine that this algorithm is running in a shared way between multiple devices, recording each movement in blocks with a cryptographic chain and a consensus mechanism. However, for it to be framed in legal fictions, this would have to be something more than an algorithm, which is why a DAO is a viable option because it is executed without human intervention (autonomous plus non-sovereign) and operates through various rules, impossible to modify by a single person, since the consensus is necessary.

With this organization, we would have a self-referential, self-organizing, autonomous (not sovereign) and possibly autopoietic system (Luhmann, 1998, p. 73), constituted by its elements

produced by the system itself, until the determination of which is decided in the code, however, this could have continuation or irruption of reproduction of parts, strictly speaking not reproducing, but maintaining itself.

It is essential to point out the difference between autonomy and sovereignty since for the purposes of this research we are referring to autonomy as the capacity of a system to decide on its actions without the participation of another system or operator. In contrast, sovereignty is the freedom to choose with your thoughts and actions, to control resources without the coercion of other entities.

Moving on to another topic, it should be mentioned briefly, the case of the saga known as *The DAO*, wherein a few weeks in mid-2016, some 11,000 people around the world committed cryptocurrencies worth approximately 150 million dollars to a virtual company with no employees, management or legal existence. It all started when a group of Ethereum developers from slock.it created a distributed crowdfunding system called DAO, in which governance and corporate operations were carried out automatically using smart contracts. In this DAO, users paid ether (the native currency of the Ethereum network) in exchange for tokens that gave them the authority to vote on projects to be financed and organizations that were seeking financing registered through another interface to receive votes. However, something went wrong, as, within weeks of launch, a cybercriminal took advantage of an error in the DAO's computer source code to divert more than a third of the cryptocurrencies deposited. And although this was a robbery, from a technological perspective, it was valid since it followed the rules of smart contracts and the rules of the system (Werbach, 2018, pp. 67-69).

At the end of this case, the Ethereum project leaders had to convince most of the nodes to implement an update, to recover the stolen funds; clearly, this divided the entire community and of course undermined the trust of the Ethereum project. In the end, the Ethereum foundation provided an update to the software where the DAO hack never happened, and thus the blocks did not recognize the transfers made by the cybercriminal. And while most miners updated the software without complication, other users claimed that Ethereum was not truly immune to centralized interference, raising concerns for the future and public networks. In the end, a small group of miners continued to run the old software under the name Ethereum Classic (ETC), creating a hard fork where two utterly different blockchain networks now exist. In conclusion, this DAO incident showed us that a blockchain does not eliminate the need for trust, as there are problems that will need to be solved through real governance.

Lastly, with the constant growth of the blockchain, several ideas have emerged that use decentralized ownership of the blockchain to provide more user-focused and fully decentralized services. Some of the key ideas in this space are the Decentralized Web, Decentralized Identity, and Decentralized Finance (DeFi) (Bashir, 2020, p. 57).

4. DISCUSSION

With all these exceptions made, by correctly understanding the various models and interests of each party, we can create a logical process for all network participants, understanding that governance is an essential factor for decision-making in the commercial, operational and technical. It was proven how organizations should consider new models and governance schemes to support technological and social solutions.

Some government and governance challenges in blockchain networks will lie in philosophical, social and economic problems, which will be constant and different on each occasion, revolving around updating the computer source code of the network to be able to face the issues and solve them. Probably in the future, there will be the talk of global governance, where protocol updates will be for all participants in automated blockchain systems.

Blockchain risks and uncertainties should also be considered, such as operational security issues that have yet to be fully explored. Besides, the lack of interoperability and communication between blockchain networks, their scalability and infrastructure limits, should be examined. From a legal approach, governance, infrastructure, anonymity and data protection problems that could generate various concerns (Giambelluca, 2020, p. 100). It is known that even blockchain and DLT systems have been used to carry out illegal activities, and consequently, illicit applications called dark boxes, which show the need for urgent regulatory development with truly global standards to detect and prosecute this type of systems that allow to illicit actions (Cappiello, 2020, pp. 26-27).

Observing the intersection between existing legal systems and new systems based on computer source code, the maximalist conception of blockchain arises, which means defending complete governance into the network whenever possible. However, it would be incorrect to consider that blockchain technology is an island without people, and consequently, governance outside the system is essential for governance systems (Lai, 2020, p. 291). It is important to establish the rules, governance mechanisms to elaborate, modify and maintain these rules, besides, the creation of a mechanism to make the rules enforceable to the participants. The business rules must define the roles, duties and responsibility, then the legal rules establish the compliance requirements, assigning risks and losses, for example, through guarantees and limitations of liability, and finally, establish the technical rules regarding the structuring, communication, protection and verification of the data in the technical processes that will be used (Lai, 2020, p. 297).

Governance is concerned with rules of engagement for greater good and fairness in any system. Governance is also about rules and choice-making in any system. Reasonably not surprisingly, if there are rules, there are also exceptions to those precepts. Thus, governance is about coordinated decision making, and it manifests itself in different ways. For instance, consensus requires governance (equitable participation) by introducing economic incentives in trust systems, and in some cases, the combination of a reputation

system with consensus ensures integrity in participation (Arun, Cuomo, & Gaur, 2019, p. 105).

Although blockchain technology can sometimes be considered as a technology that looks for problems and not that it solves, a practical solution was the port of Valencia called GESPORT 4.0, which aimed to digitize the documentation, increase the efficiency of the process and facilitate communication. The port experimented with public and private chains and recently developed a licensed private container management solution that is based on Hyperledger Fabric. The organization selected a licensed private blockchain solution for several reasons, including the existence of sensitive data, the need for governance through a community of stakeholders, the ability to store data, and bypassing complicated consensus mechanisms. Additionally, decision-makers looked at performance, transaction volume, system scalability, and security before committing to Hyperledger Fabric (World Economic Forum, 2020, p. 119).

In a strict sense, a governed blockchain network is not decentralized, and for the same reason, a truly decentralized blockchain network will not be governed. But in practice, Ethereum Foundation's solution on The DAO demonstrates the importance of governance in blockchain networks. However, private networks or DLTs are most useful in systems with more need to make decisions, comply with regulations and exercise governance. In public networks, it is a mistake to think that blockchain, specifically Bitcoin as the first cryptocurrency, eliminated the need for trust since in reality it only eliminated the need for validation of trusted third-party transactions that is only part of trust in a broad sense.

5. CONCLUSION

Governance and commercial models were addressed, based on standardization of data and legal frameworks. It showed how operational governance causes consequences in business models, whether with transactions, multi-signature, forks, consensus mechanism, smart contracts, tokenization, online dispute resolution and decentralized application (World Economic Forum, 2020, pp. 97-196). It was discovered that at least in current business models, private blockchain networks are more useful than public networks because they have greater operational flexibility and data governance, without exempting that public networks must also have mechanisms of governance since sometimes a human consensus must be reached to make updates to protocols and technical rules (The Law Society, 2020, pp. 24-61).

In the same way, possibly blockchain is not the solution for all kinds of problems, since in some cases it will be better to implement a public network and in others a private network, being useful depending on the capacities and needs. However, having a reliable central authority is not a bad thing. It can sometimes be a good option since if there are severe losses in amount, it is trusted that the responsible authority will compensate for any losses due to errors and omissions.

Rules and governance must emerge from the bottom up for decisions to be legitimate and for distribution and decentralization to be correctly carried out. The debate over the scalability of Bitcoin and the post-DAO Ethereum hard fork are great examples and teachings that governance in blockchains is a sine qua non for building harmony between technology and information societies.

The decentralized model poses difficulties when you need to change the rules because those changes need to be agreed upon and accepted by all members to function consistently. A governance framework will be needed to achieve and operate blockchain as a legal application and needs to take into account oversight and monitoring functions, rule setting, and acceptance and change control management. Governance in general will be a necessity not only for legal but for all technologies that manage information. This transmutation to some common rules for information governance is not only critical to blockchain but to other pursuits like e-discovery and cybersecurity (Bambara et al., 2018, p. 85).

Just as Bitcoin brought banking for the unbanked, the decentralized dispute resolution systems, process and mechanism has the potential to bring justice for the unjusticed (Lesaege, Ast, & George, 2019, pp. 14-15). And just as cryptocurrencies have banked those who did not have bank accounts, and they have granted justice to the world in general, from a governance perspective in the blockchain it is expected that all entities and corporations are decentralized, so that people around the world have access to goods and services without restriction, agility and with fewer costs.

Finally, the intersection between the government, governance and blockchain networks is a fundamental pillar in the regulatory list of the countries, since their importance is so much in the present, that on September 24, 2020, the European Commission (2020) published the *Proposal for a Regulation of the European Parliament and the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, in which it establishes uniform transparency and disclosure requirements about the issuance, operation, organization and governance of crypto-asset service providers, including the duty of token issuers regarding assets to have robust governance arrangements, including a clear organizational structure with well-defined, transparent, consistent lines of responsibility and effective processes to identify, manage, monitor and report the risks to which they are or could be exposed. Besides, the description in the white paper of the crypto asset must contain a detailed description of the issuer's governance mechanisms and establish on-time special and illustrative governance provisions that must be followed.

In conclusion, law and technology can influence each other; they interact through a complex system of dependencies and interdependencies. DLT technologies in general and public blockchains in particular, are about to lead (and have largely led), our society to a paradigm shift, because thanks to these technologies people are experiencing a new way of trust, that is, trust without parts, where they do not trust each other, do not even know each other, but trust technology. In addition to this, even though blockchain technology is creating new forms of rule governance, both inside and outside the chain, this does not mean that sovereign national states will fall, on the contrary, the latter are only

obliged to modify their operation and, if necessary, its regulatory provisions to adapt to new technologies (Cappiello, 2020, pp. 36-37).

Some technical and non-technical limitations must be considered for blockchain adoption in real-world applications. In the paper, we analyzed public and private blockchains. However, the ones that facilitate the governance of the information are the private blockchains and probably could exist some hybrid model where public blockchains could enforce in some way the regulations of the governance. Also, some topics that could arise new interrogators will be the application of blockchain in artificial intelligence or the Internet of Things (IoT), because these future systems will interact with a high amount of data and even will generate huge information in the process. This will clearly show the necessity of making agreements to the interaction between the blockchain, society and their legal regulations. Because somehow these mechanisms of gathering, processing and storing data should be discussed.

Finally, this research is only the beginning of a set of topics in blockchain technologies. Once the government and governance in blockchain networks are established, new debates will arise such as who owns the intellectual property of virtual assets produced? And who will be responsible for the personal data being processed? And decide who will be responsible, both administratively and criminally for illegal acts that occur in the blockchain networks.

This will demonstrate the importance to find answers for some interrogates like: How will records on a blockchain network be catalogued as evidence? Is it possible that traditional justice can solve the problems in Blockchain networks, or will it have to resort to online dispute resolutions (ODR)? What will its intersection with the money laundering laws be? What will taxation be like in blockchain networks? The society should decide the future of this technology with a new series of debates to solve this new type of issues.

REFERENCES

1. Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain* (2nd ed.). Sebastopol, CA: O'Reilly Media, Inc.
2. Antonopoulos, A. M., & Wood, G. (2018). *Mastering Ethereum: Building smart contracts and DApps.* Sebastopol, CA: O'Reilly Media, Inc.
3. Arun, J. S., Cuomo, J., & Gaur, N. (2019). *Blockchain for business.* Boston, MA: Addison-Wesley Professional.
4. Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation, 6*(1), 45-62. https://doi.org/10.22495/jgr_v6_i1_p5
5. Au, S., & Power, T. (2018). *Tokenomics: The crypto shift of blockchains, ICOs, and tokens.* Birmingham, the UK: Packt Publishing Ltd.
6. Bambara, J., Allen, P., Iyer, K., Madsen, R., Lederer, S., & Wuehler, M. (2018). *Blockchain: A practical guide to developing business, law, and technology solutions.* New York, NY: McGraw-Hill Education.
7. Barry, D. K. (2013). *Web services, service-oriented architectures, and cloud computing* (2nd ed.). San Francisco, CA: Morgan Kaufmann Elsevier.
8. Bashir, I. (2020). *Mastering blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more* (3rd ed.). Birmingham, the UK: Packt Publishing Ltd.
9. Brown, G., & Whittle, R. (2020). *Algorithms, blockchain & cryptocurrency: Implications for the future of the workplace.* https://doi.org/10.1108/9781838674953
10. Buterin, V. (2017, February 6). *The meaning of decentralization.* Retrieved from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
11. Campbell-Verduyn, M. (2018). Introduction: What are blockchains and how are they relevant to governance in the global political economy? In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance* (pp. 1-24). https://doi.org/10.4324/9781315211909-1
12. Cappiello, B. (2020). Blockchain based organizations and the governance of on-chain and off-chain rules: Towards autonomous (legal) orders? In B. Cappiello, & G. Carullo (Eds.), *Blockchain, law and governance* (pp. 13-42). https://doi.org/10.1007/978-3-030-52722-8_2
13. Cappiello, B., & Carullo, G. (2020). Introduction: The challenges and opportunities of blockchain technologies. In B. Cappiello, & G. Carullo (Eds.), *Blockchain, law and governance* (pp. 1-12). https://doi.org/10.1007/978-3-030-52722-8_1
14. Clark, D. D. (1992). *A cloudy crystal ball: Visions of the future.* Retrieved from https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf
15. De Filippi P., & Wright, A. (2018). *Blockchain and the law: The rule of code.* https://doi.org/10.2307/j.ctv2867sp
16. Dhillon, V., Metcalf, D., & Hooper, M. (2017). *Blockchain enabled applications: Understand the blockchain ecosystem and how to make it work for you.* https://doi.org/10.1007/978-1-4842-3081-7
17. EU Blockchain Observatory and Forum. (2020). *Governance of and with blockchains* (EU Blockchain Observatory and Forum Report). Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/report_governance_v1.0_0.pdf
18. European Commission. (2020*). Proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593
19. Gaur, N., Desrosiers, L., Novotny, P., Ramakrishna, V., O'Dowd, A., & Baset, S. A. (2018). *Hands-on blockchain with Hyperledger: Building decentralized applications with Hyperledger fabric and composer.* Birmingham, the UK: Packt Publishing Ltd.
20. Giambelluca, G. (2020). Blockchain: The regulatory challenges for central banks and financial sector. In B. Cappiello, & G. Carullo (Eds.), *Blockchain, law and governance* (pp. 99-102). https://doi.org/10.1007/978-3-030-52722-8_7
21. Grabowski, M. (2019). *Cryptocurrencies: A primer on digital money.* https://doi.org/10.4324/9780429201479
22. Grigg, I. (2004). The Ricardian contract. In *Proceedings of the First IEEE International Workshop on Electronic Contracting.* https://doi.org/10.1109/WEC.2004.1319505
23. Holbrook, J. (2020). *Architecting enterprise blockchain solutions.* https://doi.org/10.1002/9781119557722

24. Jägare, U. (2019). *Data science strategy for dummies*. Hoboken, NJ: John Wiley & Sons.
25. JUR. (2019). *Whitepaper V.2.0.2 July 2019*. Retrieved from https://jur.io/wp-content/uploads/2019/05/jur-whitepaper-v.2.0.2.pdf
26. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62*(1), 15-25. https://doi.org/10.1016/j.bushor.2018.08.004
27. Lai, T. (2020). Blockchain, law and governance: General conclusion. In B. Cappiello, & G. Carullo (Eds.), *Blockchain, law and governance* (pp. 289-304). https://doi.org/10.1007/978-3-030-52722-8_21
28. Laurence, T. (2019). *Blockchain for dummies* (2nd ed.). Hoboken, NJ: John Wiley & Sons.
29. Lesaege, C., Ast, F., & George, W. (2019). *Kleros short paper v1.0.7*. Retrieved from https://kleros.io/whitepaper.pdf
30. Lessig, L. (1999). *Code: And other laws of cyberspace*. New York, NY: Basic Books.
31. Ludwin, A. [@adamludwin]. (2017, July 26). 1/Cryptocurrencies don't *have* governance mechanisms, they *are* governance mechanisms [Tweet]. Retrieved from https://twitter.com/adamludwin/status/890314573760184320
32. Luhmann, N. (1998). *Sistemas sociales: Lineamientos para una teoría general*. Barcelona, Spain: Anthropos Editorial.
33. Mohanty, D. (2019). *R3 Corda for architects and developers: With case studies in finance, insurance, healthcare, travel, telecom, and agriculture*. https://doi.org/10.1007/978-1-4842-4529-3
34. Morabito, V. (2017). *Business innovation through Blockchain: The B3 perspective*. New York, NY: Springer International Publishing.
35. Nakamoto, S. (2008) *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf
36. National Institute of Standards and Technology (NIST). (n.d.). *Data governance*. Retrieved from https://csrc.nist.gov/glossary/term/data_governance
37. Parkin, J. (2020). *Money code space: Hidden power in Bitcoin, blockchain, and decentralisation*. https://doi.org/10.1093/oso/9780197515075.001.0001
38. Prusty, N. (2018). *Blockchain for enterprise: Build scalable blockchain applications with privacy, interoperability, and permissioned features*. Birmingham, the UK: Packt Publishing Ltd.
39. Raj, K. (2019). *Foundations of Blockchain: The pathway to cryptocurrencies and decentralized blockchain applications*. Birmingham, the UK: Packt Publishing Ltd.
40. Raval, S. (2016). *Decentralized applications: Harnessing Bitcoin's blockchain technology*. Sebastopol, CA: O'Reilly Media, Inc.
41. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media, Inc.
42. Szabo, N. (1997). *The God protocols*. Retrieved from https://nakamotoinstitute.org/the-god-protocols
43. The Law Society. (2020, September 7). *Blockchain: Legal and regulatory guidance report*. Retrieved from https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report
44. Tormen, R. (2019). *Blockchain for decision makers: A systematic guide to using blockchain for improving your business*. Birmingham, the UK: Packt Publishing Ltd.
45. Turner, J. (2019). *Robot rules: Regulating artificial intelligence*. https://doi.org/10.1007/978-3-319-96235-1
46. United Nations (UN). (2008). *Compendium of basic United Nations terminology in governance and public administration* (Committee of Experts on Public Administration Session). Retrieved from https://digitallibrary.un.org/record/619419/files/E_C.16_2008_3-EN.pdf
47. Upadhyay, N. (2019). *UnBlock the blockchain*. https://doi.org/10.1007/978-981-15-0177-7
48. Werbach, K. (2018). *The blockchain and the new architecture of trust*. https://doi.org/10.7551/mitpress/11449.001.0001
49. World Economic Forum. (2020). *Redesigning trust: Blockchain deployment toolkit: Supply chain focus*. Retrieved from https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf