Cryptoregulation in a Nutshell

The Basics of Blockchain and Blockchain Regulation

Pablo García Mexía
José Morales Barroso

LA LEY

Wolters Kluwer

■ LA LEY

Cryptoregulation in a Nutshell

The Basics of Blockchain and Blockchain Regulation

Pablo García Mexía
José Morales Barroso

Wolters Kluwer

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 – Fax: 902 250 502
e-mail: clientes@wolterskluwer.com
http://www.wolterskluwer.es

Edition: April 2020

Legal Deposit: In process (First quarter 2020)
ISBN print version: 978-84-9020-984-4
ISBN electronic version: 978-84-9020-985-1

Design, Prepress and Printing: Wolters Kluwer España, S.A.
Printed in Spain

No responsibility for any possible consequences caused to any individual or organization acting on or refraining from action as a result of any material contained in this publication will be accepted by Wolters Kluwer España, S.A or the author.

business models in order to improve cost efficiency and trust. This makes it possible to transform existing models with new distributed platforms in which the figure of trusted intermediaries or third parties loses validity in favor of consensus and distributed trust.

The concept of the blockchain is in itself very simple, but it quickly becomes complicated when you want to understand how this technology works in more detail and delve deeper into it. This new paradigm consists of a specific set of protocols, which are the ones that define the rules that control communication between the entities that form a network, which we call *nodes*. In the blockchain model, nodes are responsible for storing the record on a decentralized basis, and user applications communicate with them through the network. Data is retained by replicating the blockchain, transmission is end-to-end via peer networks, and data is confirmed by a consensus process among the nodes participating in the network.

Although it is not necessary to know how the blockchain works in order to use it, it is very important to have some basic notions of the main aspects of this new technology, which is not easy to understand in all its details, in order to know what is happening at every moment, in order to get the most out of it and avoid the problems that can arise from incorrect use. That is the purpose of this introductory chapter.

2. THE BLOCKCHAIN: ELEMENTS THAT MAKE IT UP

To know the basics of Blockchain technology (Preukschat, 2017) it is necessary to have notions of algorithms and cryptography, how the network reaches consensus, what are the *tokens*, and other aspects that we will discuss below.

Blockchain technology uses a set of protocols and cryptographic techniques, thanks to which application data and operating records are constituted as a blockchain of information linked together in a decentralized and public way, stored in computers interconnected through a network of distributed computers, the *nodes*, to avoid any central point of failure. Nodes work collaboratively to store, share, and preserve the distributed record, using a *consensus algorithm* to check and guarantee the validity of each block. See Figure 1 below. compares a conventional system, with a centralized server, and the distributed network with the blockchain in each node.

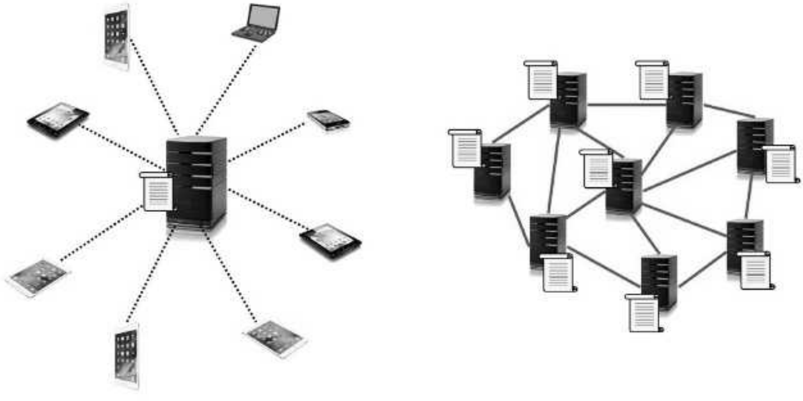


Figure 1. Comparison of a conventional system, with a centralized server, and the distributed network with the blockchain in each node.

Due to the structure of the chain of linked data blocks, once published they cannot be modified by any network member or administrator, which makes the system immutable. These blocks are stored and distributed on a decentralized basis by users, who can add new data and view, but not modify, existing data. It is a paradigm of collaboration with well-defined rules that are easy to adopt among the members of the trust network, based on consensus among the participants, without the figure of a third party, in which transactions are recorded with a modulable level of transparency, from anonymous use schemes to levels of traceability as high as necessary.

The decentralized applications are published in a technical document that describes the protocol, its characteristics and its implementation, and there are several alternatives:

- Use your own blockchain and protocol.
- Use your own protocol with another application's blockchain.
- Use both the protocol and the blockchain from other applications.

2.1. The P2P Network

The network of the blockchain is of the type P2P (*Peer to Peer*), or network between pairs, because it is formed by a set of computers, the *nodes*, that behave as equals to each other. We can consider three basic levels in the network structure, as shown in Figure 2 in a very schematic way.

The inner core is made up of the *communications network*: Internet with TCP/IP protocols. The *nodes*, which are at the next higher level or Blockchain, communicate over the Internet using the common blockchain protocol, which they use to validate and store each of them a copy of the same information. As they all comply with the same rules, they can keep the state of the network up to date in a coordinated way thanks to the ability to communicate with everyone (P2P) offered by the Internet. And on these two layers operate the *applications* of the end users.

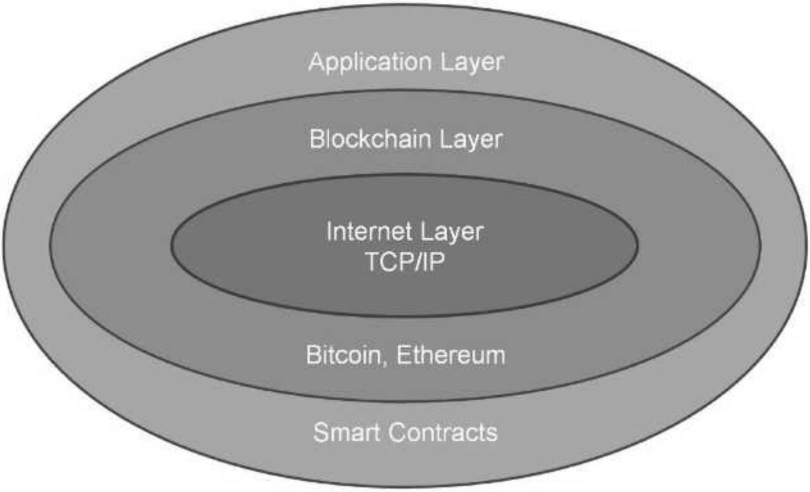


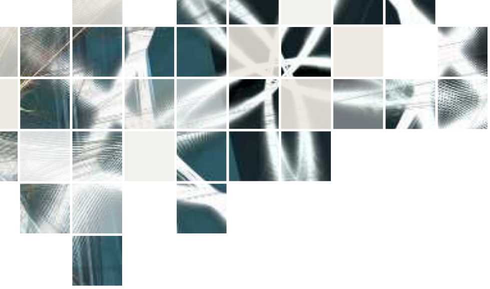
Figure 2. The three basic levels in the network structure

2.2. The Blockchain

Blocks are data structures generated by network nodes. A block is a record with new transactions, which once completed is added to the chain, thus creating the blockchain. Each block is composed of a set of elements, defined in each particular blockchain implementation, which thus has its own characteristics. It consists of control headers and an information field, in which transactions, applications, data, etc. are stored.

The header includes fields with information regarding the block itself and the chain, such as the following:

- A sequence number or block size
- The version of the protocol used to create the block
- The *Hash* of the header of the previous block
- The *Merkle Root*, the root of a *hash* tree obtained from the *hash* of all previous blocks



Blockchain and Distributed Ledger Technologies (DLTs) are one of the most disruptive digital technologies for the Humankind. This is the case in the financial field, since DLTs embody the technological engine of a cryptocurrency of notorious success, Bitcoin. Blockchain, however, is much more than Fintech, its possible uses being manifold already today.

This is the case with private blockchains (owner-controlled), no matter how modest their technological and legal interest may be. And with public blockchains as well (such as Bitcoin or Ethereum), whose revolutionary technology generates equally revolutionary consequences on the legal sphere, which in fact explain the very birth of this book, where public blockchains take a central place.

«Blockchain runs over the Internet», and in fact, it works like the other protocols built on the «application» layer of the Internet, for example the World Wide Web (WWW). When invented in 1989, also the WWW was only «one more protocol», which joined the pre-existing email, among others. By 1995, the WWW had revolutionized the Internet and was largely responsible for its massive social emergence. Nothing should prevent Blockchain, also «just another protocol», from generating similar results.

This is what we believe, the authors of this work, which tries to condense the key technological aspects of Blockchain, together with the main challenges and contents of its legal regulation, while at the same time, in a very synthetic way, provide answers to the many doubts that this promising technology has raised in the legal and regulatory field.

ISBN: 978-84-9020-984-4

9 788490 209844

3652K28961

Wolters Kluwer