INVESTIGA R&D&I 2018/2019

SPECIFIC WORK GUIDE ON "BLOCKCHAIN TECHNOLOGY"

Text byFrancisco Javier Cárceles Moreno

October 2018

Introduction

As it so happens, since information technology has appeared in human beings' lives, **breakthroughs** are continually being made. One of the latest ones has been the creation and implementation of **blockchain**.

Fruit of an initiative by programmers who in the '90s define a solution for the completion of**electronic payments**, blockchain emerges, which would serve back then and nowadays, to**create electronic currencies** or cryptocurrenciesand for**other functions** which use this technology.

Blockchain is a breakthrough recognized worldwide as the**fifth evolution of computing**.

What is blockchain? And what technology does it use?

Blockchain is a technology which is based on three pillars.

- A data structure organized in units called**blocks**.
- Encryption of the**links**in the chain so that it cannot be deciphered or changed.
- A network of**nodes**whichhandle the management, creation and validation of the data structure.

These three pillars are supported by**computer programs**which, in each of them, cover all the required functionalities.

What is each of the blockchain parts for?

- **Block**: is the component which saves the**data associated with a cryptocurrency transaction**, relative to a **smart contract** or**another type of data** which can be saved in electronic format.

  Each of the blocks**contains information from the previous block,**so this information is also part of the block. This peculiarityenables that the contents of a block cannot be changed without altering the entire chain.

  The data stored in each block can be of a diverse nature. In the environment of virtual currencies or cryptocurrencies, it serves to indicate who is the**holder** of one of them, in Ethereum environments it serves so that the parties that want to**sign agreements**through**smart contracts**. Any data that is registered in the block can be consulted by the users, thanks to**asymmetric cryptography**.

- **Chain** or link: is a**hash** or coding generated by cryptography which**unites two blocks**and which is created from the data that is contained in the previous block. In this way the code is unique and constitutes a **digital fingerprint**of this data, blocking it in**time**and in the**position** in the block.

  Each hash is created from initial information which will be the**content of the previous block** except for the first one in the chain, which is created without that characteristic. These hashes are created by**cryptographic programs**which use up a lot of operation time since they need to carry out**many mathematical operations**. The idea then is for the nodes to help to create those hashes and obtain a reward, in the way of coins generally, so that they keep helping their generation.

Such is the power and time used in generating hashes by the nodes that in order to be able to know the initial information of thehash, a single computer would be making calculations for years and would not manage to achieve it.

The**modification**of any of the**blocks**which make up the chain would reveal that the information**is not correct**so the nodes which support the modified chain must be rejected.

- **Network of nodes**: is made up of the computer network which contains a**copy of the blockchain**and**generatesdigital forms**, **approves transactions**and**registers**them in the chain.

  The network consisting of the nodes or equipment which work for the chain is based on **P2P (Peer to Peer) technology**, which is a network where there are no servers and all the computers work as equals.

  This network enables the nodes to create the blocks and validate them,**collaborating**with one another and**exchanging** the necessary information. The process by which the blocks are validated is called**POW (Proof-Of-Work)**and is based on the validation of the blockby the nodes which are working in the P2P network.

But then, can anyone write in the chain and read from it?

The blockchain is a data structure which**is not centralized**and its support is therefore based on a**community of users**who have it shared in their computers. Some of these users help to create the blocks and save them once the community validates them. Therefore, if the blockchain isn't private, it does not belong to anyone although it depends on many people to help in its maintenance and creation.

The people who have **client software**will be able to view the data in the chain if they have the right permits to do so. They will also be able to use it, carrying out the **transactions** or **operations** allowed by said software through the chain's programs.

How many types of blockchain are known?

There are several types of blockchainsin connection with their access:

1. **Public**ones which are shared on the Internet and which are usually produced by free shared software. An example could be the one which manages**bitcoins** or**Ethereum**.
2. **Protected**ones which are accessible through a credential and the use made of it will depend on the level of access obtained. One example of them is**Ripple**.
3. **Private** ones which are usually very small and operate within a consortium or entity.

There are also chains which are built for specific types of purposes such as:

1. **Cryptocurrencies:**most blockchains are used to produce and manage virtual currencies like Bitcoin, Litecoin, Dash, etc.
2. **Smart Contracts:** their purpose is for the agreements made and registered by two or more parties to be executed. Smart contracts are programs which**evaluate the fulfillment of the agreement**and carry out the scheduled operations which were agreed upon by the parties. One operation could be to deposit bitcoins in an electronic wallet.
3. **Other functions:**as we have seen, the blockchain acts as an operations register book. These registers which are validated by the communityserve for a great many specific operations as could be: notary registries, intellectual property registries, traceability of products, automation of processes, etc.

Concepts and matters of debate.

After seeing the characteristics of blockchain at a functional level, I propose that, in order to be able to advance in the research, the following concepts should be studied and the following questions should be answered:

Concepts:

1. Cryptography, Fingerprint, Hash,Timestamp.
2. Consensus algorithms and proof-of-work.
3. Cryptocurrencies.
4. Blockchain mining.
5. Smart contracts.
6. Distributed applications.

Questions:

1. How does the Bitcoin blockchain work?
2. How does the Ethereum blockchain work?
3. How does the Ripple blockchain work?
4. If the blockchain is a distributed and reconciled database, what would be the sectorsin which its use would be an added value?
5. Is blockchain a trustworthy intermediary? Why?
6. The sum of the power of the computers making up the nodes in the network is very high.Do you think it is an inconvenience for implementing blockchain? And if it is, what would be the projects where said power wouldn't be an inconvenience?
7. In short, what could be the future uses for this technology?

Sources of information

- Blockchain For Dummies®, Published by: John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774
- The Science of the Blockchain Roger Wattenhofer, Inverted Forest Publishing
- "Blockchain Revolution" Tapscott, Don. "Penguin Random House LLC 375 Hudson Street, New York, New York 10014"
- https://learn.unimooc.com/student/courses/course?course=bitcoin;utm_source=desktop&utm_medium=txt
- https://es.wikipedia.org/wiki/Ethereum
- https://es.wikipedia.org/wiki/Cadena_de_bloques
- https://ripple.com/