Abstract

A disruptive technology often used in finance, Internet of Things, healthcare, and more, blockchain can reach consensus within a decentralized network - potentially composed of large amounts of unreliable nodes - and to permanently and irreversibly store data in a tamper-proof manner. This technology can lead to many research opportunities and business innovations. Taking these aspects into consideration, in this thesis, we propose a guide for the implementation of software applications based on blockchain technology. We also present a series of innovative implementations applied in Intelligent Transportation Systems (ITS) and healthcare, alternative solutions to the current centralized systems.

Considering that blockchain is increasingly used in a variety of fields, we propose a series of recommendations that must be taken into consideration in order to design software solutions using blockchain technology. The key points presented are the basis of an analysis of the research carried out so far, while a classification on architecture layers is also proposed. The guide is presented systematically so that developers can figure out if blockchain is the best solution and, if so, how to model all the necessary components, such as actors, data, interactions, functionalities, performance, efficiency, security, and audibility, considering the legislative framework.

Regarding smart city, car navigation systems is one of the main research directions that aims to streamline traffic and calculate travel routes. Existing applications such as Google Traffic or Waze are often used, but for users worried about their personal data, these systems are something of a black box. Using blockchain technology, we propose the architecture of a car navigation system in which personal data protection is a major concern. The model was presented during "IEEE International Conference on Computational Science and Engineering" and was published in the article "Blockchain privacy-preservation in Intelligent Transportation Systems". [1]

The second model applied in ITS implements a blockchain-based reputation system. It considers the users interested in traffic information as the main actors of the architecture. They securely share their data which are collectively validated by other users. Users can choose to employ either such crowd-sourced validated data or data generated by the system to travel between two locations. The data saved is reliable, based on the providers' reputation and cannot be modified. We present results with a simulation for three cities: San Francisco, Rome and Beijing. We have demonstrated the impact of malicious attacks as the average speed decreased if erroneous information was stored in the blockchain as an implemented routing algorithm guides the honest cars on other free routes, and thus crowds other intersections. The solution is presented in the article "Blockchain-based Reputation for Intelligent Transportation Systems". [2]

In the medical field, data sharing, privacy, and interoperability must be major concerns. Currently, no computer system encompasses all these aspects. Using blockchain technology, we describe the architecture of a healthcare system where we consider all the aspects mentioned. Our proposal includes all the actors involved, ensuring the security of the information saved. This concept was presented at the conference BDA 2018 "34th Conference on Data Management - Principles, Technologies and Applications" and published in "Proceedings of the BDA 2018 Conference" under the name "Blockchain privacy-preserving in healthcare". [3]

Moving forward in the thesis, we present a system design where blockchain technology is proposed to be used in the healthcare system, where the vital information regarding the medical analysis are shared between hospitals, medical clinics and research institutes based on access policies defined by the patients. In order to protect confidential data, our solution involves the

use of two types of chains: a private one, the sidechain, which keeps information about real ID of the patients, and a public one, the mainchain, which stores information about patients' health data marked with a temporary ID. To test it, we developed the design using Hyperledger Fabric framework. Presented experimental results show good performance of the system in relation to the following metrics: 1) time required for acceptance a new transaction, 2) the mainchain propagation time of all the blocks within the peer to peer network, and 3) the time needed to identify the medical data for a particular patient. The solution was presented at the conference "IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)" and described in the article "Blockchain-based approach for e-health data access management with privacy protection". [4]