Future Generation Computer Systems 88 (2018) 173–190

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

On blockchain and its integration with IoT. Challenges and opportunities

Ana Reyna *, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz

Department of Languages and Computer Science, University of Málaga, Boulevar Louis Pasteur 35, 29071 Málaga, Spain

HIGHLIGHTS

- Challenges to address the integration of the IoT with blockchain.
- Analysis of blockchain potential benefits for the IoT.
- Blockchain IoT applications and platforms for the development of IoT solutions.
- Possible topologies to that integration.
- Evaluation of blockchain nodes in IoT devices.

ARTICLE INFO

Article history:
Received 21 December 2017
Received in revised form 3 April 2018
Accepted 21 May 2018
Available online 24 May 2018

Keywords:
Internet of Things
Blockchain
Smart contract
Trust

ABSTRACT

In the Internet of Things (IoT) vision, conventional devices become smart and autonomous. This vision is turning into a reality thanks to advances in technology, but there are still challenges to address, particularly in the security domain e.g., data reliability. Taking into account the predicted evolution of the IoT in the coming years, it is necessary to provide confidence in this huge incoming information source. Blockchain has emerged as a key technology that will transform the way in which we share information. Building trust in distributed environments without the need for authorities is a technological advance that has the potential to change many industries, the IoT among them. Disruptive technologies such as big data and cloud computing have been leveraged by IoT to overcome its limitations since its conception, and we think blockchain will be one of the next ones. This paper focuses on this relationship, investigates challenges in blockchain IoT applications, and surveys the most relevant work in order to analyze how blockchain could potentially improve the IoT.

1. Introduction

The rapid evolution in miniaturization, electronics and wireless communication technologies have contributed to unprecedented advances in our society. This has resulted in an increase in the number of suitable electronic devices for many areas, a reduction in their production costs and a paradigm shift from the real world into the digital world. Therefore, the way in which we interact with each other and with the environment has changed, using current technology to gain a better understanding of the world. The Internet of Things (IoT) has emerged as a set of technologies from Wireless Sensors Networks (WSN) to Radio Frequency Identification (RFID), that provide the capabilities to sense, actuate with and communicate over the Internet [1]. Nowadays, an IoT device can be an electronic device from a wearable to a hardware development platform and the range of applications where it can be used encompass many areas of the society. The IoT plays a central role in turning current cities into smart cities, electrical grids into smart grids and houses into smart homes, and this is only the beginning. According to various research reports, the number of connected devices is predicted to reach anywhere from 20 to 50 billion by 2020 [2] mainly due to the vast number of devices that the IoT can place on the scene.

The IoT visualizes a totally connected world, where things are able to communicate measured data and interact with each other. This makes possible a digital representation of the real world, through which many smart applications in a variety of industries can be developed. These include: Smart homes, Weareables, Smart cities, Healthcare, Automotive, Environment, Smart water, Smart grid, etc. IoT solutions are being deployed in many areas, optimizing production and digitizing industries. IoT applications have very specific characteristics, they generate large volumes of data and require connectivity and power for long periods. This, together

* Corresponding author.
E-mail addresses: reyna@lcc.uma.es (A. Reyna), cmf@lcc.uma.es (C. Martín), hfc@lcc.uma.es (J. Chen), esc@lcc.uma.es (E. Soler), mdr@lcc.uma.es (M. Díaz).

https://doi.org/10.1016/j.future.2018.05.046

with the limitations in memory, computer capacity, networks and limited power supply pose a high number of challenges.

The huge expansion of the IoT has to be supported by standard mechanisms and protocols in order to reduce the existing heterogeneity in the field. This heterogeneity leads to vertical silos and reduces the adoption of the IoT. However, aside from the heterogeneity and integration challenges present in the IoT, the trustworthiness of its data is also an important issue to bear in mind. Nowadays, we trust in the information of financial entities and the government among others, but can we be sure that the information provided by them and by other external entities, such as IoT companies, has not been tampered/altered/falsified in any way? This is a difficult question to answer in centralized architectures. Untrusted entities can alter information according to their own interests, so the information they provide might not be completely reliable. This brings about the need to verify that the information has never been modified.

One way to provide trustworthiness in IoT data is through a distributed service trusted by all its participants that guarantees that the data remains immutable. If all participants have the data and they have the means to verify that the data have not been tampered with since the first definition, trustworthiness can be achieved. Moreover, having a system that guarantees data reliability would allow governments to share and securely transfer information with citizens.

In many areas where an exhaustive traceability of assets during their life cycle is required by regulations, data immutability becomes a key challenge. Concretely, European Union (EU) regulations require food producers to trace and identify all raw materials used in the elaboration of their food products in addition to the final destination of each of them. For example, in the case of a large food company with thousands of manufacturing suppliers and millions of clients, the information needs to be digitized and its processing automated to comply with regulation. One example of strong regulation in terms of traceability is the pork supply, regulated in many countries. In this scenario, in addition to tracing the raw material used in pig feed and treatments and the final destination of the pork, the transportation of the animals between factories must also be registered by law. These scenarios involve many participants, some of them still relying on non-automated information handling methods. In the case of food contamination, which has been an important issue for the world population's health throughout history, information that is lost or difficult to find implies delays in the location of the problem's focus. This can also result in the public's mistrust of the contaminated products and a large decrease in their demand. According to the World Health Organization (WHO), it is estimated that every year around 600 million people in the world suffer illness from eating contaminated food, of which 420,000 die from the same cause [3]. So, missing or inaccessible information can affect food security and customer health. In these kinds of scenarios the IoT has the potential to transform and revolutionize the industry and society, digitizing the knowledge so that it can be queried and controlled in real time. This technology can be used to improve current processes in many areas such as cities, industry, health and transportation.

Although the IoT can facilitate the digitization of the information itself, the reliability of such information is still a key challenge. In this sense, a new technology that was born as the first decentralized cryptocurrency has the potential to offer a solution to the data reliability problem: Bitcoin, which has revolutionized the mechanisms in money transfers. The Bitcoin cryptocurrency, and many of its upcoming variants, can be globally transferred without financial entities and foreign exchanges, with a digital and nontransferable wallet. Bitcoin is supported by a protocol that details the infrastructure responsible for ensuring that the information remains immutable over time. This protocol is known as the blockchain. It has been applied to many other areas, and the information immutability is guaranteed in applications that go beyond the cryptocurrencies. Blockchain has revolutionized trustworthiness of information as well. For instance, this technology has been used in voting systems by government entities, renting and data storage among others [4].

In this paper the current challenges of IoT and blockchain and the potential advantages of their combined use will be analyzed.

Disruptive applications in this area will be highlighted in addition to a review of the available blockchain platforms to address these challenges.

The main contributions of the paper are:

1. Survey on blockchain technology, analyzing its unique features and open challenges.
2. Identification and analysis of the different ways of integrating IoT and blockchain.
3. Study of challenges, potential benefits and open issues of the integration of blockchain and IoT.
4. Study of existing blockchain–IoT platforms and applications.
5. Evaluation and comparison of the performance of different blockchains in an IoT device.

The rest of the paper is organized as follows. Section 2 introduces the blockchain technology and analyzes its main challenges. In Section 3 IoT and blockchain integration is addressed, analyzing the challenges that this integration involves. A state of the art in blockchain platforms for IoT and IoT–blockchain applications is presented in Section 4. Lastly, our conclusions and future work are presented in Section 5.

2. Blockchain

The problem of trust in information systems is extremely complex when no verification nor audit mechanisms are provided, especially when they have to deal with sensitive information, such as economic transactions with virtual currencies. In this context, Satoshi Nakamoto, in 2008 [5] presented two radical concepts that have had a great repercussion. The first of these is Bitcoin, a virtual cryptocurrency that maintains its value without support from any centralized authority or financial entity. Rather, the coin is held collectively and securely by a decentralized P2P network of actors that make up an auditable and verifiable network. The second of the concepts, whose popularity has gone even further than the cryptocurrency itself, is blockchain.

Blockchain is the mechanism that allows transactions to be verified by a group of unreliable actors. It provides a distributed, immutable, transparent, secure and auditable ledger. The blockchain can be consulted openly and fully, allowing access to all transactions that have occurred since the first transaction of the system, and can be verified and collated by any entity at any time. The blockchain protocol structures information in a chain of blocks, where each block stores a set of Bitcoin transactions performed at a given time. Blocks are linked together by a reference to the previous block, forming a chain.

To support and operate with the blockchain, network peers have to provide, the following functionality: routing, storage, wallet services and mining [6]. According to the functions they provide, different types of nodes can be part of the network. Table 1 summarizes the most common node types in the Bitcoin network.

The routing function is necessary to participate in the P2P network, this includes transaction and block propagation. The storage function is responsible for keeping a copy of the chain in the node (the entire chain for full nodes, and only a part of it for light nodes). Wallet services provide security keys that allow users to order transactions, i.e., to operate with their Bitcoins. Finally the mining function is responsible for creating new blocks by solving the proof