https://dx.doi.org/10.22161/ijaers.6736 ISSN: 2349-6495(P) | 2456-1908(O)

Blockchain Technology applied to Education

David Nadler Prata[1], Humberto Xavier de Araújo[2], Cleórbete Santos[3]

[1,3]Department of Computer Science, Federal University of Tocantins, Palmas-TO, Brazil
[2]Department of Electrical Engineering, Federal University of Tocantins, Palmas-TO, Brazil

***Abstract*— *The purpose of the present work is offer an implementation of a private blockchain infrastructure for data storage, specifically the certificates of completion or participation issued by the Federal University of Tocantins, Campus Palmas-TO, Brazil, aiming to avoid their falsification by means of validation using hashing. Some institutions, such as the Massachusetts Institute of Technology and Holberton School in San Francisco, use Bitcoin's public blockchain to maintain and validate their certificates, but paying fees for each operation. The blockchain implementation adopted for this project is Multichain, a solution that, because it is open source, reduces deployment costs, facilitates its installation and maintenance of its infrastructure, and doesn't request the payment of any fees for information storage. Because of its security features and transparency in data storage, Blockchain has been used in a number of technologies, such as the Bitcoin cryptocurrency, smart contracts, shared economy, corporate governance, intellectual property protection, Internet of Things (IoT), management of identity, among others, and also in education, focus of this work.*

***Keywords*— education, technology, blockchain, cryptography.**

I. INTRODUCTION

Blockchain is a distributed database technology that allows maintain a growing list of records, called blocks. Each block contains a creation date and time information and a link that points to a previous block. A blockchain is typically managed by a peer-to-peer network that uses a specific protocol to validate new blocks collectively (ANTONOPOULOS, 2010). By design definitions, blockchains are inherently resistant to unauthorized modification of their data. Once recorded, the data in any block can not be changed retroactively without changing all subsequent blocks and validating the entire interconnected block network.

Functionally, a blockchain can serve as an open and distributed ledger that can record transactions between two parties efficiently and verifiably. The ledger can also be programmed to trigger transactions automatically (WATTENHOFFER, 2016). The first blockchain was conceptualized by Satoshi Nakamoto in 2008 and implemented in the following years as the main component of the Bitcoin, where it serves as a public ledger for all transactions related to this cryptocurrency (NAKAMOTO, 2008).

Blockchain solutions applied to education are present in institutions such as the Massachusetts Institute of Technology and the Holberton School in San Francisco, where the storage and delivery of certificates issued are made using the public blockchain of Bitcoin, by means of payment of a small amount to each certificate generated, as a measure to avoid forgery of these documents. In this work, a private blockchain (Multichain) is used as a repository of the certificates issued by the Federal University of Tocantins (Brazil). Multichain is an open source version of blockchain, becoming a more economical alternative for the institutions that adopt it, generating reliability, security and transparency in the storage of its digital assets.

II. MULTICHAIN BLOCKCHAIN AS A SAFE REPOSITORY FOR CERTIFICATES

Private blockchains are inherently faster than public ones, since in private versions real decentralization is not required and its participants do not need to mine blocks of data, but instead only validate transactions (GUEGAN, 2017). In any case, it should be noted that private blockchains have their applicability restricted to certain situations, and, in the same way, the public ones (GARZIK, 2015).

Holberton School in San Francisco, a software development school that offers project-based education as an alternative to college courses, has used Blockchain to store and deliver its issued certificates. This strategy is seen as a measure to prevent the use of counterfeit certificates. Encryption and two-factor authentication are used to create, sign, and add certificates to the blockchain database. The school still gives paper copies of its certificates to its students, but a Decentralized Clearing Number (DCN) for certificates is generated by the system and allows authentication by employers (HOLBERTON SCHOOL, 2015).

The Massachusetts Institute of Technology (MIT) has also adopted Blockchain to issue its certificates through a project called *Blockchain certificates* (MIT MEDIA LAB, 2016). The project consists of a set of tools that allow storaging and management of digital credentials. An open source initiative developed by the same institute is available for use by any interested party, including for commercial purposes, at http://www.blockcerts.org. The Blockcerts community provides open-sourcing, ready-made software libraries, tools and applications that enable the implementation of decentralized, standardized and secure computing ecosystems through Blockchain and related technologies. Some examples of institutions using certificates created and maintained with tools from the Blockcerts community are: MIT itself (certifying its students), the Learning Machine company (which generates certificates for its employees), and the Mexico City Laboratory, which certifies participants in their workshops (BLOCKCERTS, 2016).

Another educational institution that adopted certificates stored and managed in blockchains was the University of Nicosia, which reports that no other technology, other than Blockchain, was used for the project, so that any individual can authenticate certificates issued by the university without contact with the institution, and the records, because they are distributed, will remain available even if the institution website is out or the university no longer exist (UNIVERSITY OF NICOSIA, 2016).

Blockchain technology is a kind of distributed database designed to process and store transactions. And while most of today's blockchain implementations are used in financial operations (TOKENMARKET, 2018), such infrastructures serve to store various digital assets, such as timestamps of documents and files.

In terms of access privileges, blockchains can be classified in public and private. A public blockchain is one in which there are no restrictions on reading data from blockchain or even for inclusion of transactions in your infrastructure. One of the most famous examples of public implementation of blockchain is the Bitcoin cryptocurrency. In contrast, private blockchains require, through access control, certain privileges for specific users, both to read the data in the blockchain and to include new data, ie transactions (GARZIK, 2015).

Another classification applicable to blockchains is the permission to validate blocks that will be inserted in the network. When the blockchain is configured so that only certain users have block validation privileges, this blockchain is called permissioned, that is, it has permission rules. On the other hand, when block validation can be done by any user of the network, there is a permissionless blockchain, that is a network where anyone interested can join and mine data. Again Bitcoin figures as a notorious example of permissionless blockchain (GARZIK, 2015).

A performance difference between permissionless and permissioned blockchains is that the first ones use algorithm-based mining, such as Proof of Work (PoW), which requires miners computational power and slows it down than permissioned blockchains. Private blockchains do not need mining based on computational power to reach the consensus of the transactions generated by their users, since they are all previously registered in the system and for this reason, known and with guaranteed mining powers (ANTONOPOULOS, 2016). Some consensus algorithms commonly used in permissioned blockchains are RAFT, Paxos and PBFT.

Other relevant issues to consider when choosing which type of blockchain to use are data privacy, the entity responsible for the network, scalability and access control. In public blockchains data are accessible by any interested party, and if this is not desired the ideal is the adoption of a private blockchain. However, when choosing it, there must necessarily be a centralizing entity, which will maintain the network and take the decentralized operation, characteristic typically belonging to public blockchains. As far as scalability is concerned, permissioned blockchains are better scalable in relation to permissionless because they do not need incrementally computational power to process their transactions. Finally, if the goal is refined access control, again the best choice would be for private and permissioned blockchains, which assign user-level privileges to read and write data, and at the level of miners, for validation of blocks (ANNAMALAI, 2016). For the project of this work the choice for blockchain private and permissioned is the open source solution Multichain (www.multichain.com).

Multichain is an open source platform for creating private blockchains. The user is allowed to define parameters of the blockchain to be created, and the technology, in turn, allows the storage of several types of digital contents, called assets. The platform is available for download and installation on Windows and Linux machines, and its source code can be accessed at Github, specifically at https://github.com/MultiChain/multichain. Multichain extends Bitcoin's Application Programming Interfaces (APIs) and has a similar protocol and transaction format. A Multichain client node can act as a node for the Bitcoin and Bitcoin test networks.

For blocks created using Multichain, the protocol allows creators to determine which permissions a new entrant will have without needing to receive them directly from one of the network administrators. When blockchain is started, its creators determine the powers of the administrators, as well as whether any interested party can connect, without restriction, to the network. Administrators can also dynamically control permissions for specific users of the blockchain while it is running. These permissions include sending, receiving, and creating actions (assets), as well as creating blocks. Subsequent decisions to change permissions are made by consensus among administrators. The proportion of administrators who must accept user privilege modification is set before the blockchain goes live.

Because of its private blockchain behavior, Multichain solves data mining and privacy issues through integrated access control to the solution itself. The solution is: a) ensure that any activity in the blockchain is visible only to authorized participants, b) permit privileges and definitions of which transactions are allowed on the network, and c) allow mining to occur without Proof of Work (PoW) and therefore, computational and energy resources do not need to be allocated. In addition, Multichain allows multiple blockchains to be deployed on the same server and multiple servers work together to maintain the network.

Another aspect taken into consideration for the choice of Multichain as a solution to be adopted for this project is that it derives (via fork) from the Bitcoin blockchain official code, and therefore its maintenance and updating are practically transparent to the community of developers, resulting in better scalability and greater compatibility with existing standards and infrastructures.

The first step in using Multichain is to install it on any available server computer, from the Internet address https://www.multichain.com/download-install/, respecting the requirements below:

- Linux: 64-bit; Compatible distributions: Ubuntu 12.04+, CentOS 6.2+, Debian 7+, Fedora 15+, RHEL 6.2+.
- Windows: 64-bit; Supported versions: 7, 8, 10, Server 2008 and later.
- Mac: 64-bit; Compatible Version: OS X 10.12.
- 512 MB of RAM or higher.
- 1 GIGA of disk space or higher.

For this work, it is assumed that the server computer to be used for installation and configuration of Multichain technology it is a Linux Mint 64 bit, version 18.3 codenamed "Sylvia", with 16 GIGA of RAM and 1 TERA of space in disk. In Figure 11 there is the sequence of steps to be performed for installation and use of Multichain.

The installation of Multichain is done in a traditional way for Linux environments. First it is necessary to download the desired package, extract it and copy the binaries from Multichain to the /usr/local/bin directory. After installation is necessary create one or more blockchains by running the utility "multichain-util" (followed by its parameters). When this command is executed, the message "Blockchain parameter set was successfully generated. It possible edit it in <path>/.multchain/chain1/params.dat before running multichaind for the first time", signaling that the new blockchain was created successfully and indicating the path to your configuration file (params.dat) which can be modified with the use of a traditional text editor such as Vim. Params.dat is a properties file that has several keys followed by their values.

Once the blockchains have been created, they can be started with the *multichaind* utility (followed by their parameters). If high network availability is a goal, other servers may be added to the blockchain. This procedure is done by generating a wallet number (which will identify the new server in the network), with the authorization of the new wallet of the blockchain main server, and finally with the connection of the new server to the network.

Multichain technology allows user commands to be sent at their own prompt through an interactive mode, available through the *multichain-cli* utility. The following listing demonstrates some executable commands of Multichain, also, in interactive mode, that aim to facilitate its use:

- getblockchainparams: Displays a list of blockchain parameters (from the params.dat file).
- getpeerinfo: Displays a list of clients connected to the blockchain.
- grant: Gives permissions to node addresses.
- revoke: Revokes permissions from node addresses.
- listpermissions: Displays a list of permissions that have been explicitly granted to node addresses.
- liststreams: Displays a list containing all the streams in the blockchain.
- listblocks: Displays a list of the blocks in the blockchain.
- getnetworkinfo: Displays a list containing network information, such as the port to which the node is connected, as well as its IP address.

- getinfo: Displays general information about the node where the command was executed and about the running blockchain.
- help: Displays a list of commands available to the user.

Streams in Multichain allow the blockchain to be used as a repository of files, providing timestamping, notarization, and immutability. A Multichain blockchain can contain numerous streams, where the data stored in them will be stored, therefore, on all the nodes that hold the network. Each stream in Multichain is an ordered list of items, where each item has the following characteristics:

- One or more publishers who have signed the item.
- A key with a size between 0 and 256 bytes.
- Information about item and block transactions.

The creation of streams respects the access control built into Multichain. It is possible, for example, create streams that only accept information sent by users with write privileges. It is frightened that stream names are case-sensitive and can not be repeated in the same blockchain. In Multichain, uploading files to a stream is called *publishing* (items), and *subscribe* is the operation that results in access to the stream and, consequently, to your items.

In the case of the certificates issued by the Federal University of Tocantins (Brazil), the hash of the certificates will be recorded in streams of the same chain, using the algorithm SHA256. Subsequently, if any interested party wishes to confer the authenticity of the certificates, it may do so through the following operations: generate a hash of the certificate to be validated and compare the hash generated with the hash in the blockchain.

III. CONCLUSION

Blockchain is one of the most advanced technologies of the present time, mainly known for being a digital mesh behind the famous Bitcoin cryptocurrency. Blockchain works as a safe database of records, shared by users and devices from all over the globe, connected together in a large distributed network.

In this work was explained the creation of a private blockchain for use at the Federal University of Tocantins (Brazil) with the primary objective of storing the certificates issued by this institution, as well as their hashes, so that any public can validate both in order to avoid the possibility of forgery.

In United States, MIT - Massachusetts Institute of Technology and Holberton School in San Francisco have similar projects and pay fees to store their records in the public Bitcoin Blockchain. This project offers a solution based on private and permissioned blockchain using an open source solution, ensuring the scalability, compatibility and low cost implementation for the Federal University of Tocantins (Brazil).

Public blockchain implementations generally are decentralized, while the private versions have an owner deciding which users and devices are allowed to join the network under predefined access privileges. Furthermore, the solution explained in this paper doesn’t use Proof of Work (PoW), what means that isn’t necessary allocation of computational assets and high spending of electrical energy for the mining process, resulting in efficiency in the use of resources.

REFERENCES

[1] Antonopoulos, Andreas M (2010). Mastering Bitcoin. O'Reilly.

[2] Wattenhoffer, Roger (2016). The Science of the Blockchain. CreateSpace Independent Publishing Platform.

[3] Nakamoto, Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.

[4] Guegan, Dominique (2017). Public Blockchain versus Private blockhain. Sorbonne.

[5] Garzik, Jeff (2015). Public versus Private Blockchains. Bitfury.

[6] Holberton School to Authenticate Its Academic Certificates With the Bitcoin Blockchain (2015). Retrieved from http://www.marketwired.com/press-release/holberton-school-authenticate-its-academic-certificates-with-bitcoin-blockchain-2065768.htm.

[7] What we learned from designing an academic certificates system on the blockchain (2016). Medium. Retrieved from https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196.

[8] Blockchain Certificates (2017). Blockcerts. Retrieved from http://www.blockcerts.org/guide/.

[9] Blockchain certificates (2016). UNIC. Retrieved from https://www.unic.ac.cy/iff/blockchain-certificates/.

[10] Blockchains (2018). Tokenmarket. Retrieved from https://tokenmarket.net/blockchain/.

[11] Annamalai, Deva (2017). Blockchain – What Is Permissioned Vs. Permissionless. Linkedin. Retrieved from https://www.linkedin.com/pulse/blockchain-what-permissioned-vs-permissionless-deva-annamalai/.