USING BLOCKCHAIN TECHNOLOGY FOR IMPLEMENTATION OF AN ANDROID GRAPHICS SIMULATION APPLICATION

Paulo Oliveira Siqueira Júnior
Student, Universidade Paulista UNIP
Computer Science Course Manaus-AM, Brazil.
juninhooliveira22@hotmail.com

Ítalo Rodrigo Soares Silva
Student, Universidade Paulista UNIP
Computer Science Course Manaus-AM, Brazil.
italo.computation@gmail.com

Ricardo Silva Parente
Student, Universidade Paulista UNIP
Computer Science Course Manaus-AM, Brazil.
ricardosilvaparente@gmail.com

Jorge de Almeida Brito Júnior
Research department, Galileo Institute of Technology and Education of the Amazon – ITEGAM
Manaus-AM, Brazil.
jorge.brito@itegam.org.br

Alyson de Jesus dos Santos
Research department, Galileo Institute of Technology and Education of the Amazon – ITEGAM
Manaus-AM, Brazil.
alysson.santos@itegam.org.br

Manoel Henrique Reis Nascimento
Research department, Galileo Institute of Technology and Education of the Amazon – ITEGAM
Manaus-AM, Brazil.
hreys@iegam.org.br

Abstract

The Blockchain technology can be used for many purposes on the web, the main one being the financial branch, having in mind the present article clearly presents the technology concepts behind Bitcoin called Blockchain and is shown throughout the work to implementation of a mobile application developed in the Android platform, where it makes use of blockchain to simulate the operation of its own, being a practical

guide to blockchain, can be used to teach technology to lay visually, the tool uses principles such as hash function, chain of blocks, consensus algorithm among others that are linked to the technology of crypto coins.

Keywords: *Blockchain; Consensus Algorithm; Bitcoin.*

1. Introduction

In a computerized world, one always thinks of using the best technologies to facilitate and assist in the daily routines of each user, a routine commonly used is the conferring and feeding of bank or digital accounts, in this small universe can occur many occurrences such as transactions , deposits, transfers among many others, but in the midst of these operations there are always malicious people called cyber criminals who manipulate and distort the reality of a digital world through techniques or malicious algorithms aimed at achieving a goal, In order to avoid such events, the central idea of the present research focuses on a technology widely used in the digital world of Bitcoin. This method consists of distributing and mining digital coins as a decentralized financial bank independence the big corporations or governments to move money being considered the first currency crypto in the world.

To understand how Bitcoin works it is necessary to know the concepts of all the logical development and structure of operation that takes place behind this service that is called Blockchain, therefore through this technology the digital currency exists and operates safely through analyzed algorithms and tested for this type of situation, so the present research will address concepts, examples and demonstrate their use through an android application that simulates the use of Blockchain and how a distributed database becomes important for data mining and assuring the reliability of each block in the security context.

Implement an android application using blockchain to demonstrate the usefulness of the technology and that it is possible to use it in various branches of activity, from financial to certifications, even in mobile software to simulate the technology itself in a visual way, thus it is possible to learn the technology of didactic form, starting from basic objectives like: To approach basic concepts for the understanding of Blockchain, to demonstrate and to approach algorithms related to the technology, to implement a mobile application to simulate the own technology Blockchain making use of the same one.

2 . Theoretical Foundation - Basic Concepts

2.1 Cryptography

According to Pires, public key cryptography, also known as asymmetric encryption, is the cryptographic technique that makes use of two distinct keys, a public key to encrypt the message and a private key to decrypt the message. This technique is in opposition to the private key model, which is called by several symmetric key authors, where the characterization of this key is due to the same key being used to encrypt and decrypt the message [1]. "With the advent of electronic communication, many essential activities depend on secrecy in the exchange of messages, especially those involving financial transactions and the secure use of the Internet" [2].

2.2 Hash Function

For Hosner hashes is "a one-way math function, which creates a cryptographic summary of a message. You feed a text into a hash function, and it returns a block of fixed-length ciphertext that can not be reverted to the original message "[3].

For Oliveira, the digital signature that is obtained through the use of public key cryptography, also known as asymmetric cryptography, unfortunately can not be used solitarily in practice, if it is necessary to use a certain mechanism that is essential for the adequate use of digital signature and strengthening of the encryption used. The fundamental mechanism is the hash function [4].

2.3 Hash Function

According to Nakamoto, Bitcoin is an electronic crypto-currency that has by definition a chain of digital signatures, where the transfer of values occurs by sending the digitally signed code to the next node and is added to the end of the coin, where it is digitally signed is used, the Bitcoin network maintains a block containing all transactions made from all public addresses in the system. It is this list of public addresses of transactions that gives transparency to all operations, since all nodes serve as witnesses to the transaction, since anonymity and privacy are guaranteed uniformly, since it is not possible to know who owns each address public, because what is recorded on the block are not the names of the people but their digital signatures [5].

According to Mougayar:

"In the first four years after Satoshi launched Bitcoin in January 2009, there was a lot of attention focused on the currency, including its pay aspects and its functioning as an alternative way of stocking value. In 2013, attention has begun to turn to blockchain 2.0 applications: the use of the same technology that relies on security and bitcoin decentralization in other applications, ranging from domain name registration, financial contracts, collaborative finance and even to games "[6].

2.4 Blockchain

According to Diniz, the blockchain proposes a new paradigm of reliability in the web, being an inexpensive and secure way of validating and storing records of data in the network. And because a lot of our social and commercial affinities are linked to certificate registrations, the blockchain would be the big fuse of a new technological revolution, reaching a wide area of applications, this revolution being the main one since the web spread 20 years ago [7].

Silva mentions that bank computing systems can prevent many problems that are not ended in their rules, but there are also disadvantages in this centralized model, promoting errors in credit auditing or in another area in this branch, which is why there is room for the use of new technologies such as blockchain [8].

According to Niforos, the technology behind bitcoin is called blockchain and can be defined as being a distributed database system that serves as a record that allows the transfer of information without the existence of a third party mediating validation between parties. Validation rather than being done by a third party is done by all peers, shared and distributed throughout the network [9].

For Roman:

"A blockchain is a technology based on the decentralization of information control. When control can be based on the power of a single individual, the integrity of an information system is directly dependent on it, whereas, in a decentralized system, the integrity of the information depends on the members of the ecosystem. Thus, to change a record, not only the unilateral will of a participant is sufficient "[10].

According to Kypriotaki, Zamani and Giaglis, the blockchain is a database distributed on the network, which is publicly located on the web and can be upgraded by any device on the network to which the database belongs, is based on the consensus among the nodes and ensures the validation through an algorithm called Proof-of-Work, which has as its main goal to provide data integrity and to hinder cyber attacks [11].

According to Ferreira, Pinto and Dos Santos, one of the great advantages of blockchain technology in relation to technologies that use centralized solutions for data protection and authenticity is that it is not enough to only change the information in a network peer, since all nodes are interconnected and all have the same information, to circumvent the integrity of the information is necessary to change the information in 51% of all nodes of the network, and this is impractical because the network grow very fast, making it almost impossible to circumvent the system using blockchain, the data preservation increases even more when the network has many nodes, the larger the number of peers, the more impractical the practice of changing information in the network [12].

Seguindo o que escreveu Šurda, a tecnologia da Bitcoin como já citada anteriormente é chamada de blockchain, na qual funciona como um livro que possui um registro e que só pode ser escrito uma vez, ao qual está interligado ao registro antecedente e posterior, como uma corrente é ligada pelos elos, daí o nome blockchain [13].

Segundo Pires, o blockchain não trabalha essencialmente com pessoas, e sim com hashes de endereços que são totalmente públicos. É muito comum pessoas dizerem que “Alice” transferiu uma certa quantia n para “Bob” utilizando alguma moeda digital criptografada, como é o caso do bitcoin, essa afirmação é errônea, o que acontece na verdade é que a chave privada de “Alice” assinou um registro de transferência de valor para a chave pública de “Bob”. Porém, os nomes das pessoas em si nunca foram memorizados no blockchain, apenas suas assinaturas e chaves públicas são gravadas. Portanto desta forma, é correto dizer que o blockchain não exige identificação para seu uso, mas não está correto dizer que ele prover confidencialidade, já que as chaves e assinaturas são totalmente públicas [1].

De acordo com Diniz, “em pouco tempo o blockchain entrou na agenda como alternativa para diversas atividades comerciais e sociais, e não apenas para as criptomoedas”. Assim o mercado para essa tecnologia é bastante grande [7].

3. Development

3.1 Application

For this research, an application was proposed that demonstrated the use of Blockchain concepts as well as a graphical demonstration using the android platform, to allow the reader a brief knowledge about how a cryptomedical transaction can be performed in a network environment through intelligent algorithms which allow the creation of blocks and determine the integrity of the data.

The application will demonstrate a basic and explanatory tutorial as the user's navigation and usability guide, a Local Blockchain simulator, and a Blockchain Distributed simulator that exemplifies its use on three random, non-virtualized computers.

Figure 1 - SBlock app home screen

Source: Authors (2019).

The guide focuses on addressing the general concept of blockchain algorithms and technology as shown in figure 2.

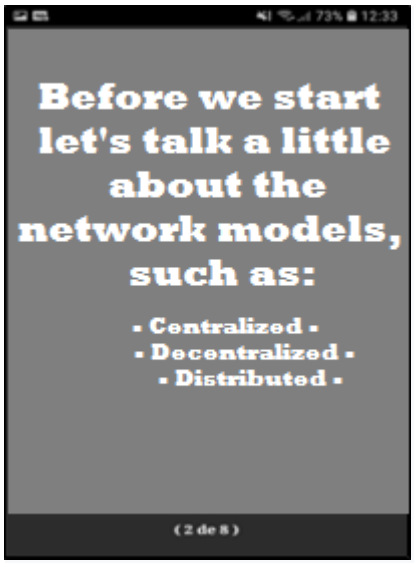

Figure 2 - Explanatory screen of the network models

Source: Authors (2019).

As you navigate through the guide the user will understand each model presented.

Figura 1 - Modelos de rede

Fonte: Autores (2019).

The next figure conceptualizes the application context that is Blockchain.

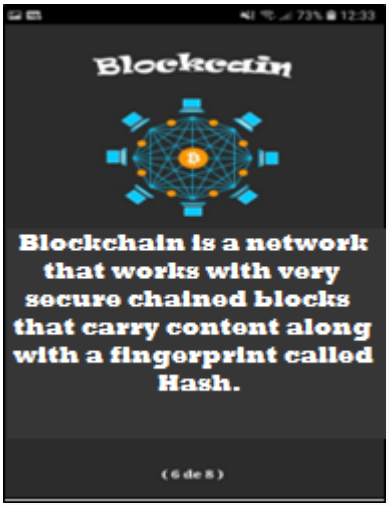

Figure 4 - Blockchain Concept

Source: Authors (2019).

3.2 How Blockchain Works

Blockchain is nothing more than an open and distributed database, composed of Blocks and all of them are linked together in a sequence. In computing jargon consists of techniques that allow to distribute a certain service in a secure way as in the case of Bitcoin, equivalent to existing electronic or digital banks, it is possible to monetize in different financial accounts immutable.

The model proposed by the application uses the Proof of Work consensus algorithm, which in particular allows to understand how the mass growth of this technology in a network occurs and the computational investment demanded.

3.3 Proof of Work

This algorithm aims to prove the work that is persisted through the generation of hashs and the mining of the blocks. One of its characteristics is that transactions are verified by network participants and can not be circumvented, this method is also used to prevent spam and DDOS attacks.

Defining the concept of Proof-of-Work (PoW), is the mathematical process to be performed by the miner and is related to the cryptographic hash algorithm SHA-256 [5].

In the projected application the algorithm has the purpose of defining and generating hashs as unique identifiers that validate the integrity of the compound data in each generated block Da Silva Rodrigues, Silva and Codesso commented that "The authenticity of each transaction is protected by digital signatures, associated with the addresses bitcoin of those who performed them "[14]. When the payer of a transaction in bitcoins sends a certain amount to another user of the system it is as if that payer were signing a public document that attests the transfer of ownership of that amount to that other user. The signature of this transaction is performed by the concept of asymmetric key pair [15].

The model predicts bottlenecks in this way the mines will solve each one to later generate new blocks that will confirm future transactions, so it is impossible to say how complex a bottleneck can become, because it is justified by the maximum number of users, current minimum power and load the network.

3.4 Digital Signature

The new blocks come with the Hash function that will come to have the join of the same hash of the previous block. In this way, the network adds an extra layer of protection and avoids any kind of violation and when a miner resolves a chord, a new block is created and the transaction is confirmed.

Figure 5 exemplifies a hash model in which the overall difficulty of the system is 1, this hash becomes invalid because it does not begin with a zero.

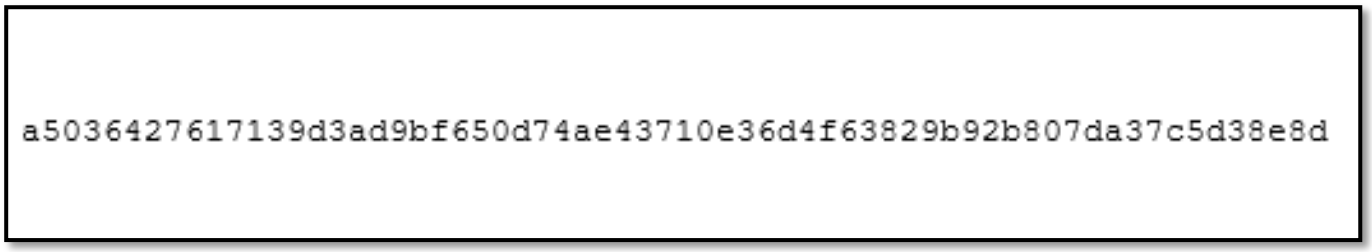

Figure 5 - Invalid Hash Model

Source: Authors (2019).

On the other hand, figure 6 shows another hash example where its value is valid since it starts with 0.

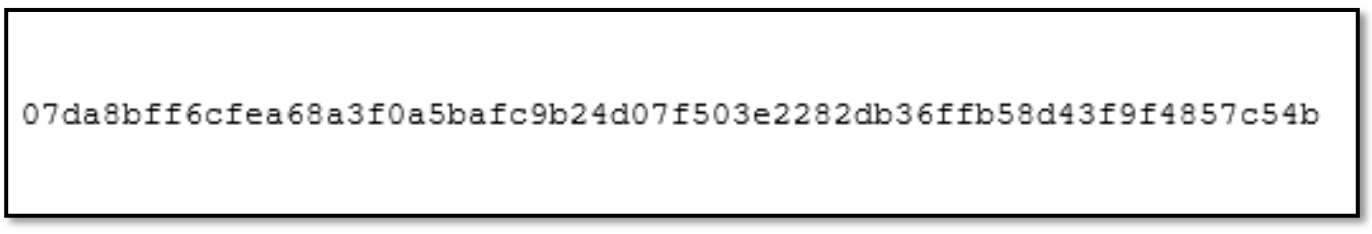

Figure 6 - Valid Hash Model

Source: Authors (2019).

Figure 7 illustrates the function used to generate the hash in the android application, the idea is based on when a user creates a new block, he will need to create several hashes until one has the number of zeros in the beginning, causing the system rule is met and thereby ensure a unique identifier that specifies its content in that block.

```
public String str() {
    return (""+index+ nonce + previousHash + dados);
}

public String calcularHash() {
    MessageDigest digest;
    try {
        digest = MessageDigest.getInstance("SHA-256");
    } catch (NoSuchAlgorithmException e) {
        return null;
    }
    byte bytes[] = digest.digest(str().getBytes());
    StringBuilder builder = new StringBuilder();
    for (byte b : bytes) {
        String hex = Integer.toHexString(0xff & b);
        if (hex.length() == 1) {
            builder.append('0');
        }
        builder.append(hex);
    }
    return builder.toString();
}
```

Figure 7 - Function responsible for generating the hash

Source: Authors (2019).

Another way to generate hashes is demonstrated in the next figure using the Node Js language where it is possible to identify the use of encryption using the sha256 method.

```
const sha256 = require('crypto-js/sha256')

class Block {
    constructor(index = 0, previousHash = null, data = 'Genesis block') {
        this.index = index
        this.previousHash = previousHash
        this.data = data
        this.timestamp = new Date()
        this.hash = this.generateHash()
    }

    generateHash() {
        return sha256(this.index + this.previousHash + JSON.stringify(this.data) + this.timestamp).
    }
}

module.exports = Block
```

Figure 8 - Use of the sha256 function in Node JS

Source: Authors (2019).

3.5 Block Structure

Each block will consist of the identifier, value Nonce, Previous Hash and Hash as shown in the figure below.

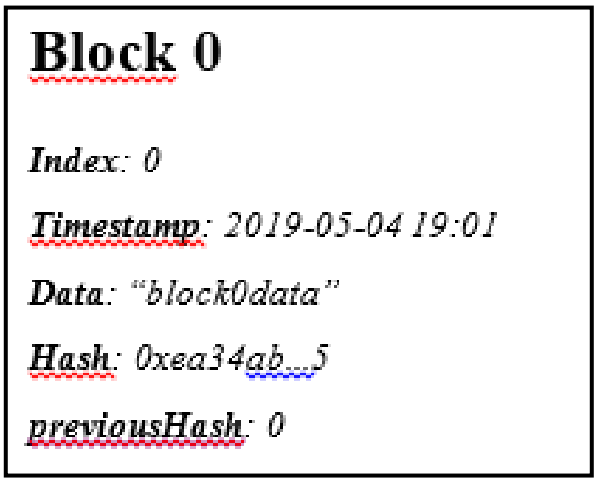

Figure 9 - Block model

Source: Authors (2019).

In the application the item that works with local Blockchain has a screen with a field where you can determine the value Nonce and another field where the personal data will be placed, the figure below shows the model of this screen.

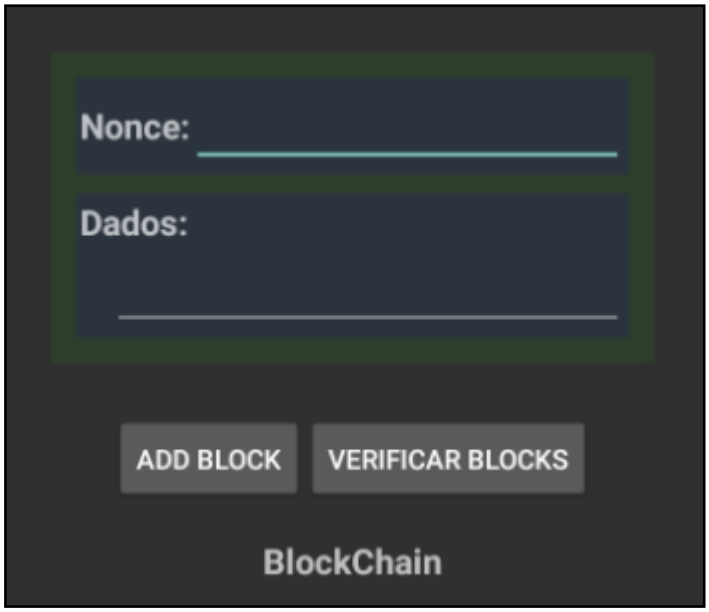

Figure 10 - Screen for adding new block

Source: Authors (2019).

To exemplify the operation in practice a list of Block objects is created at runtime to store each block generated by the user in order to obtain a block chain that is also graphically demonstrated by the application.

```
public void addBlock(String non, String data) {
    Block block = new Block(Index(blocks), nonce(non), previousHash(blocks), data);
    blocks.add(block);
}
```

Figure 11 - Method for storing blocks

Source: Authors (2019).

For the item to generate distributed blocks three lists of objects of type Block are used, in it it is possible to identify how they are generated in different machines and the responsibility that is assigned to the hash in ensuring only the identification of the data of each block. The following model demonstrates how a set of blocks is mentalized by the application so that each hash stores the contents of the previous block, so any change implies a cascade action which requires a great computational power since the creation will be networked by countless users.

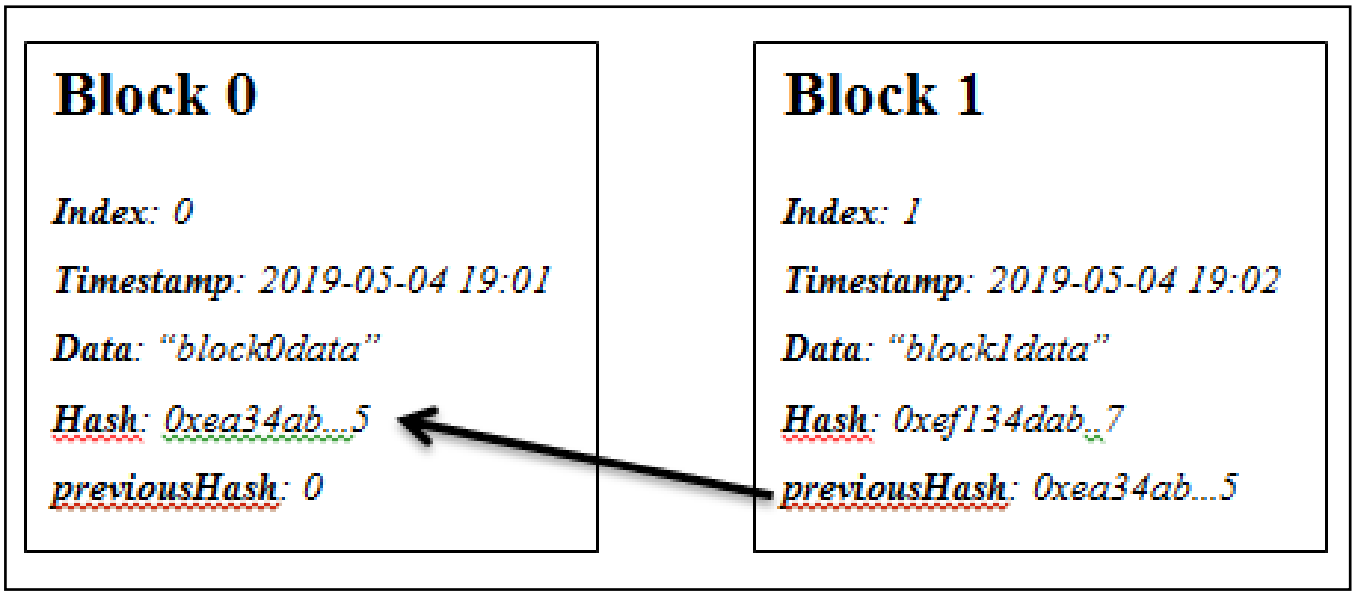

Figure 12 - Block set model

Source: Authors (2019).

3.6 Mining

The mining consists of preventing the creation of new blocks in a random way without consistency in the identifier of each block giving holes to attacks DOS or spam, so the concept of proof of work is used, which will do the job of leaving the most complex identifier as shown in Figure 6, one way to do this is to iterate a hash such that the number of leading zeros is satisfactory by the amount of variables involved as shown in the figure below.

```
1  mine() {
2      this.hash = this.generateHash()
3
4      while (!(/^0*$/.test(this.hash.substring(0, this.difficulty)))) {
5          this.nonce++
6          this.hash = this.generateHash()
7      }
8  }
```

Figure 13 - Hash mining example

Source: Authors (2019).

In the application the method consists of the same way, the difference is that the concept of proof of work will be used where we have the approach of the level of difficulty when 1 is invalid, when 0 is valid, this model implies in the difficulty imposed in the hash, generate a new block the concept is checked as the figure below.

```
for (byte b : bytes) {
    String hex = Integer.toHexString(0xff & b);
    if (hex.length() == 1) {
        builder.append('0');
    }
    builder.append(hex);
}
return builder.toString();
```

Figure 14 - Checking the difficulty level for the hash

Source: Authors (2019).

With this it is possible to obtain safe and valid blocks through the general difficulty of the system and thus to construct the set of blocks and as a result is demonstrated in the figure below where it defines the real idea of the application in the present article.

Figure 15 - Generation of blocks by the app

Source: Authors (2019).

4. Final Considerations

The program developed using Blockchain met the expectations of the authors, showing in a useful way the concepts and algorithms used by the technology, being successful in the application and demonstration of

the digital tool as a resource and service in a network visually displaying the whole process that characterizes the technology involved in bitcoin.

The tool uncovers graphically and creatively how the process of creating data mining in a network that gives rise to bitcoin, through techniques and algorithms like Proof of Work and encryption, it is possible to protect and encapsulate confidential data that will be processed in the network and to demonstrate the range of possibilities that can be achieved by using this type of methodology in the context of distributed systems, given the failures that may occur or even security techniques in the prevention of DDoS or spam attacks, it is a fact that the type of procedure it is done by means of a lot of effort knowing that the quantity of blocks that can be generated occurs exponentially and therefore it is necessary a great computational power to arrive at the required data and thus to be able to manifest a malicious act.

It is a fact that the presented technology has a great disadvantage that makes put in check its popularization among the big companies, that is the database replicated to all the peers of the network as commented in the course of the development, causing that over time the amount of data stored on each peer's disk is large, reaching a very large amount of GigaByte (GB) space where not all nodes in the network can store this data. Even with this great problem, the technology is innovative and has great potential as regards the reliability of the data on the internet and allows a new model and concept of monetization when related to bitcoin, clearly it is possible to understand that its use can be applied in several areas and therefore the study of the same is feasible.

5. Acknowledgement

The Paulista University - UNIP and the Galileo Institute of Technology and Education of the Amazon - ITEGAM for technical and scientific support and collaboration.

6. References

[1] PIRES, Timoteo. Pimenta. Tecnologia blockchain e suas aplicações para provimento de transparência em transações eletrônicas. Universidade de Brasília. Departamento de Engenharia Elétrica. TCC em Engenharia de redes de comunicação. 2016.

[2] MALAGUTTI, Pedro. Atividades de Contagem a partir da Criptografia. Rio de Janeiro, IMPA, 2015.

[3] HOSNER, Charlie, “Security Elite hash outEncryption Alternatives”, 2005.

[4] OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. Segurança Digital [Revista online], v. 31, p. 11-15, 2012.

[5] NAKAMOTO, Satoshi et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[6] MOUGAYAR, William. Blockchain para negócios: promessa, prática e aplicação da nova tecnologia

da internet. Alta Books Editora, 2018.

[7] DINIZ, Eduardo. O blockchain veio para ficar. GV-executivo, v. 17, n. 3, p. 51, 2018.

[8] SILVA, Jd. Gestão e análise de risco de crédito. São Paulo : Atlas, 2008., 2008. ISBN: 9788522450428.

[9] NIFOROS, Marina. Internactional Finance Corporation. World bank Groupe, Blockchain in development – Part I: a new mechanism of 'trust'? 2017.

[10] ROMAN, Denys. Como as blockchains podem ser utilizadas para gerar maior confiança na asseguração de dados ambientais, sociais e de governança corporativa. 2018. Tese de Doutorado.

[11] KYPRIOTAKI, K. N.; ZAMANI, E. D.; GIAGLIS, G. M. From bitcoin to decentralized autonomous corporations: Extending the application scope of decentralized peer-to-peer networks and blockchains. ICEIS 2015 - 17th International Conference on Enterprise Information Systems, 2015. 284-290.

[12] FERREIRA, J. E.; PINTO, F. G. C.; DOS SANTOS, S. C. Estudo De Mapeamento Sistemático Sobre As Tendências E Desafios Do Blockchain. UFPE. Revista Gestão.Org, v. 15, Edição Especial, 2017. p. 108-117.

[13] ŠURDA. Peter. Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?. Diploma Thesis, Wirtschaftsuniversität Wien, 2012.

[14] DA SILVA RODRIGUES, Carlo Kleber; SILVA, Paulo Caetano da; CODESSO, Maurício. UMA PROPOSTA PARA AUTOMATIZAR A GESTÃO PÚBLICA ORÇAMENTÁRIA E FINANCEIRA DO BRASIL USANDO O SISTEMA BLOCKCHAIN/BITCOIN. Revista de Sistemas e Computação-RSC, v. 8, n. 2, 2019.

[15] KUROSE, J. F.; ROSS, K. W. Computer networking: A top-down approach featuring the Internet. 6th ed. New York: Pearson Education, 2013.