

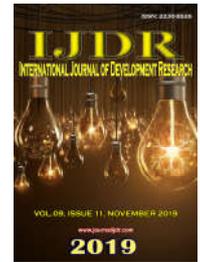


ISSN: 2230-9926

Available online at <http://www.journalijdr.com>

IJDR

International Journal of Development Research
Vol. 09, Issue, 11, pp. 31860-31867, November, 2019



RESEARCH ARTICLE

OPEN ACCESS

ESTUDO COMPARATIVO DOS ALGORITMOS DE TRANSAÇÕES UTILIZADAS PELAS CRIPTOMOEDAS BITCOIN E LITECOIN

*¹Adriana Maria Miguel Peixe, ²Jorge Balsan and ³Jose Simão de Paula Pinto

¹Doutoranda em Gestão da Informação - UFPR

²Mestre em Gestão da Informação - UFPR

³Dr. Em Medicina, Com foco em Informática Aplicada ao Ensino e Pesquisa em Cirurgia

ARTICLE INFO

Article History:

Received 17th August, 2019

Received in revised form

21st September, 2019

Accepted 06th October, 2019

Published online 30th November, 2019

Key Words:

Cryptography; Criptomoeadas;
Virtual currency; Bitcoin; Litecoin.

*Corresponding author: Kamila Cruz Alves

ABSTRACT

With the globalization and democratization of virtual networks, there has been the advancement of commercial means, citing e-commerce as an example. With all this movement and advances came a new currency, which meets the needs of today's world. The study aimed to disclose the difference in algorithms between the two main virtual currencies today: Bitcoin and Litecoin. To reach the results of this research, we used the exploratory methodology, with research in books relevant to the subject, forums and academic journals, as well as other articles related to the subject and materials available in education portals, such as Google Scholar and Scielo, based on Yin's methodology (2001, 2010, 2016). The two cryptocurrencies explained in the study have many peculiarities and differences, operating in different ways and having pros and cons that make them unique in fulfilling certain purposes. It is inferred that the main difference of this new type of currency is that it does not have a centralized power to mediate financial operations, and may bring harm to irregular or criminal operations, given the anonymity and non-identification of operators that act directly with this coin.

Copyright © 2019, Adriana Maria Miguel Peixe et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Citation: Adriana Maria Miguel Peixe, Jorge Balsan and Jose Simão de Paula Pinto. 2019. "Estudo comparativo dos algoritmos de transações utilizadas pelas criptomoeadas bitcoin e litecoin", *International Journal of Development Research*, 09, (11), 31860-31867.

INTRODUCTION

Desde os primórdios há como reflexo de um processo civilizatório o comércio de forma variada e desde sempre houve a necessidade de negociações, promovendo o bem-estar de todos. Durante esse período, na economia primitiva por falta de moedas, as transações eram realizadas por meio do escambo, que passou a ser regulamentado quando o Estado assume e a partir disso, começa a gerir essas comercializações. Atualmente com a inserção da tecnologia em nosso meio de forma crescente e inovadora, surgem com elas as mudanças na economia mundial e na forma de fazer negócios, o que tem culminado em criações de novas moedas e estas de forma digital. Conforme corrobora o historiador Rainer Souza (2018) em um estudo referente a história da moeda publicado no portal *Google Scholar*, ao longo dos anos, a moeda passou por diversas transformações, tal que, a cada nova atualização, agregava-se mais valor e importância entre a população e a economia mundial, além de que, existe mais segurança e proteção pela forma que a moeda passou a funcionar, sendo

administrada e intermediada por um órgão centralizado (RAINER SOUZA, 2018). Desde a década passada, os avanços tecnológicos permitiram que as tecnologias virtuais e as complexas linguagens de programação comesçassem a conquistar cada vez mais seu espaço em meio a uma sociedade que precisa de novas soluções para as intervenções por parte do governo e de instituições particulares que objetivavam o lucro em cima desses movimentos. Um dos grandes impactos atuais está na substituição do trabalho humano por inteligência artificial, causando mudanças nas profissões e impulsionando o surgimento de algumas adaptações a outras. É política do governo e da sociedade em geral, estabelecer estruturas e atividades que facilitam o acesso ao novo conceito (BRISTOT *et al.*, 2018). De acordo com Bastos (2015), às organizações virtuais descrevem um modelo organizacional baseado na Tecnologia da Informação (TI), normalmente essas organizações não possuem espaço nem recursos fisicamente alocados. Com esse surgimento, e seu acelerado desenvolvimento tecnológico, ocorreram mudanças de grande impacto no cenário corporativo, e consequentemente para a sociedade num todo. Para Bastos (2015):

As organizações virtuais caracterizam-se por não possuir fronteiras rígidas como as organizações tradicionais e na sua maioria caracterizam-se por um caráter transitório. São concebidas para que a sua existência perdure quando o objetivo que as originou não esteja alcançado, (BASTOS, 2015). Percebe-se que o supracitado autorevidencia que tal qual seja o intuito, assim as organizações virtuais trabalharão a fim de suprir a necessidade que se alça. Diante desse contexto surge o problema de estudo: quais as técnicas e tipos de algoritmos que são utilizados entre as criptomoedas (moedas virtuais) *Bitcoin (BTC)* e *Litecoin (LTC)* ao realizar transações criptografadas?

E evidenciado como conceito de Algoritmo de forma simplificada que é o mesmo é uma "receita" para executarmos uma tarefa ou resolver algum problema. E como toda receita, a mesma deve ser finita. Nesse sentido o estudo teve por objetivo comparar as técnicas e tipos de algoritmos utilizados entre as criptomoedas *Bitcoin (BTC)* e *Litecoin (LTC)* ao realizar transações criptografadas. A criptografia serve essencialmente para a moeda digital manter-se segura. O sistema utilizado para que exista esta segurança é semelhante aos números de série ou listas encontradas em cédulas impressas para impedir que sejam falsificadas. No caso das criptomoedas, são códigos muito complicados de serem quebrados. Justifica-se o estudo pois as moedas criptografadas, cujos principais intuídos é facilitar, ampliar e melhorar as trocas financeiras, flexibilizando ou substituindo o uso de moeda papel, cartões, permitindo que ao utilizar uma moeda digital, como *bitcoins*, não se precisa usar reais, dólares ou euros. As moedas virtuais entram em um contexto globalizado, sem um controle governamental específico, ou seja, não existe uma autoridade central que controle a rede *bitcoin*. Isso significa que a moeda não pode ser cercada por um governo ou por um banco central (ADVFN, 2019). A tecnologia aplicada por trás das moedas criptografadas se faz útil aos anseios da sociedade com a devida informação para a comunidade, além de mostrar que todos podem ter acesso aos benefícios das Criptomoedas. Este estudo está estruturado em quatro seções: a primeira retrata o quadro teórico para fundamentar o artigo. A seguir, tem-se a metodologia proposta para acessar os dados e analisá-los. A terceira seção analisa e discute o estudo de caso e por fim, têm-se as considerações finais e recomendações para pesquisas futuras.

RETRATO DO QUADRO TEÓRICO

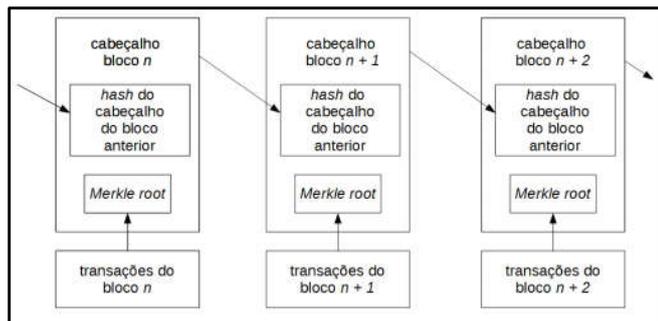
Nesta abordagem do retrato do quadro teórico apresenta-se: Sistemas Distribuídos; Componentes de Entrada; Componentes de Processamento; componentes de saída; Componentes de Realimentação; Tipos de Sistemas de Informação nas Organizações; O Advento da *Internet* e a Criação das Criptomoedas; Criptografias e as Moedas Virtuais; História das Moedas Digitais: Conhecendo o *Bitcoin* e o *Litecoin* (Ouro e Prata); As Diferença e Peculiaridades entre *Bitcoin* e *Litecoin*; A Diferença de Algoritmos entre *Bitcoin* e *Litecoin*.

Sistemas Distribuídos: Quando tem-se sistemas computadorizados independentes, interligados, trocando mensagens e coordenação entre si por meio de uma rede, com objetivo único e definido temos um sistema distribuído. A distância entre os computadores (nós) pode ser tão pequena quanto equipamentos em um rack ou tão grande quanto de um continente a outro. Tais sistemas são altamente dependentes de

redes de computadores, sendo que a internet é o maior exemplo de sistema distribuído que temos (COULOURIS; DOLLIMORE; KINDBERG; 2007; TANENBAUM; STEEN, 2007). O termo aplica-se igualmente à computação em nuvem e à computação móvel, outros exemplos atuais de sistemas distribuídos, são tipicamente escaláveis, ou seja, podem crescer rápida e confiavelmente. Dentre suas características, temos: questões inerentes à segurança (de rede e dos sistemas em si); a citada escalabilidade; questões de desempenho (da rede, dos sistemas, das transações); a necessidade intrínseca de segurança quanto a falhas e a necessidade de comunicação confiável entre seus diversos componentes. Problemas comuns a estes sistemas relacionam-se principalmente em situações de concorrência e na inexistência de um sincronismo (relógio) global. Outros desafios passam pela questão da heterogeneidade de hardwares, softwares e sistemas de telecom envolvidos na interligação dos equipamentos, que devem ser vistos como únicos porém como aplicação comum, de forma a serem um sistema distribuído; da necessidade de utilização de padrões abertos, de tal forma a possibilitar a comunicação entre as partes, já que um sistema 'proprietário' obriga todos os participantes a seguirem suas regras; e da qualidade do serviço como um todo, que deve ser conferida ao usuário ou aplicação final, passando por todos os pontos de falha possíveis (número este que aumenta consideravelmente com o aumento de componentes) (COULOURIS; DOLLIMORE; KINDBERG; 2007; TANENBAUM; STEEN, 2007). Quanto à questão da distribuição, pode-se distribuir em essência memória, processamento ou armazenamento, ou uma combinação destes. Para fins deste artigo, esta breve explanação dos sistemas distribuídos vai ao encontro das necessidades de processamento descentralizado das operações relativas às moedas digitais: as mesmas possuem processamento tipicamente distribuído, fazem uso de criptografia para garantir a segurança das transações distribuídas, devem ser escaláveis e confiáveis, oferecem desempenho compatível às operações que suportam e baseiam a qualidade de serviço na existência de uma escriturablockchain.

As informações na *blockchain* são armazenadas em blocos. Cada bloco contém uma *hash*, que contém todo o histórico de transações até o bloco atual, sendo de valor de identificação único, diferenciando-se de outros blocos. Quando um novo bloco é criado, sua *hash* é calculada e a cada nova mudança no bloco sua *hash* é recalculada, permitindo facilmente a detecção de mudanças. O último elemento de um bloco é a *hash* do bloco anterior. Assim, com este "empilhamento" de blocos, um vinculado ao anterior, é formado a *blockchain* (LEE et al. 2016). A principal característica que o distingue é que uma vez que uma informação é registrada ela nunca será apagada ou modificada. O "passado" de um *blockchain* é imutável, apenas o "presente" continua sendo registrado e, a qualquer momento, é possível rever toda a "história" desse banco de dados, o que não apenas resulta em uma grande confiabilidade, mas torna trivial qualquer eventual auditoria (LUCENA; HENRIQUES, 2016). Para Lucena e Henriques (2016), o valor *hash* obtido ao final de todo processo é denominado *Merkle root*. Desta forma, é praticamente inviável alterar qualquer transação sem que se quebre toda esta cadeia, pois seus elementos estão fortemente ligados por meio de seus valores hash. Por fim, é calculado o valor hash do resultado final da operação entre as transações, *Merkle root*, com o valor *hash* do cabeçalho do bloco anterior do *blockchain*. Desta forma, qualquer alteração em uma transação ou em um bloco anterior é facilmente

detectada por qualquer peer da rede *blockchain*. Conforme mencionado na Figura 1, (LUCENA; HENRIQUES, 2016).



Fonte: Lucena; Henriques, (2016).

Figura 1. Modelo simplificado do blockchain do Bitcoin

Por fim, um *blockchain* necessita do processo de geração de novos blocos. Quando o *blockchain* está atrelado a uma criptomoeda, este processo pode estar ligado à criação de novas moedas, o que é denominado mineração.

Tipos de Sistemas de Informação nas Organizações: Os sistemas de informação dentro de uma organização podem ser classificados em três diferentes níveis, são eles: operacional, estratégico e tático (FLORENZANO, 2014). Para compreender um Sistema de Informação é necessário entender suas dimensões mais amplas, ou seja, a organização, as pessoas envolvidas no ambiente organizacional e as tecnologias a serem utilizadas; bem como seu poder de fornecer soluções para os desafios e problemas no ambiente organizacional (LAUDON; LAUDON, 2013). Falkenberg et al (1998), corrobora que os Sistemas de Informação nas organizações é um campo de estudo que se preocupa com alguns componentes básicos da Tecnologia da Informação (TI), a saber: tecnologia, desenvolvimento, uso e gerenciamento, razão pela qual existem problemas em defini-lo exatamente.

Destaca ainda o autor Falkenberg et al (1998) que para o nível operacional, temos os Sistemas de Processamento de Transações (SPT), que consiste em monitorar, coletar, armazenar e processar os dados que são gerados em todas as transações da empresa, esses dados posteriormente, alimentam o banco de dados da organização. Os sistemas de processamento de transações têm como características: os dados são coletados, por pessoas ou sensores, e são adicionados por meio de um componente de entrada em algum computador, para que posteriormente, o sistema possa processar os dados de acordo com suas necessidades. Quando você, por exemplo, paga por algum produto em uma determinada loja, o sistema irá registrar a venda, reduzir o produto do estoque, aumenta o valor do caixa e aumenta a quantidade de vendas. Esse tipo de sistema pode ser utilizado em várias aplicações, como por exemplo: processamento de pedidos, fatura, controle de estoque, contas a pagar, contas a receber, compras, recebimento, expedição, folha de pagamento, contabilidade geral. Se tratando do nível tático podemos classificar em Sistemas de Informação Gerenciais, e em Sistema de Apoio à Decisão (SAD). Podemos dizer que os Sistemas de Informação Gerenciais oferecem informações em relatórios para o nível gerencial das organizações, apoiando o planejamento e o controle de operações. Um SIG pode oferecer cinco tipos de relatórios conforme :O'BRIEN, (1999).

(1) Relatórios de Rotina: são aqueles produzidos em intervalos programados. Podendo variar desde relatórios

de controle de qualidade por hora, até relatórios mensais de taxas de absenteísmo. (2) Relatórios Detalhados: são aqueles que mostram um nível de informações com maiores detalhes. (3) Relatórios Indicadores Principais: resumem o desempenho de atividades críticas. (4) Relatórios Comparativos: comparam o desempenho de diferentes unidades de negócios ou período de tempo. (5) Relatórios de Exceção: excluem apenas informações que estão fora de padrões de limites (O'BRIEN, 1999).

Os sistemas são configurados para monitorar o desempenho, comparar o desempenho real com os padrões e identificar exceções predefinidas. Quando tratamos do Sistema de Apoio à Decisão, podemos dizer que é um sistema computadorizado que realiza uma série de combinações entre modelos e dados, buscando resolver problemas semiestruturados e não-estruturados, essa atividade necessita de forte interação do usuário.

Algumas de suas principais características são: possibilidade de examinar várias alternativas em um curto espaço de tempo com muito mais eficiência e velocidade, realizar a análise de um risco sistemático, a possibilidade da integração entre os sistemas de comunicação e bancos de dados, e são utilizados para incentivar o trabalho em grupo.

A estrutura dos SAD's pode ser classificada em: subsistemas de gerenciamento de dados, subsistemas de gerenciamento de modelos, interface com o usuário, usuário, subsistemas baseados em conhecimento. Por fim, no topo da estrutura, podemos encontrar o nível estratégico, que é amparado pelos Sistemas de Informação Executiva (SIE), que além de ser uma tecnologia computadorizada projetada em resposta às necessidades específicas dos altos executivos, os SIE ainda fornecem rápido acesso as atuais informações.

Em atenção ao gráfico abaixo, é possível identificar os níveis de sistema de informação. Conforme se mostra:



Fonte: Elaborada pelos autores, (2019).

Figura 2. Níveis dos Sistemas de Informação

Os SIE são baseados em gráficos, por este motivo, se tornam de fácil uso, podendo ainda ser conectados aos serviços on-line e de e-mails. Podem se incluir aos SIE o apoio à análise, comunicações, automação de escritórios e apoio à inteligência.

O Advento da Internet e a Criação das Criptomoedas: Com o advento e a democratização da internet houve novas vertentes de negócios e modelos de mercado. Ao passo que o *e-commerce* cresceu e se desenvolveu, outras instituições de

caráter financeiro também se desenvolveram. A criação das criptomoedas é prova de que os modelos comerciais estão cada vez mudando e se tornando promissores, a moeda digital surge para revitalizar, em plena ressaca da pior crise financeira dos Estados Unidos, em 2008 o mercado financeiro, trazendo um novo modelo de funcionamento de negócio, (MINSK, 1986; KAMINSKY, 2003; SILBER, 2010; CHAINE, 2013; FREGUETE; NOSSA; FUNCHAL, 2015).

Rogojanu e Badea (2014), por exemplo, estudaram as vantagens e as desvantagens relativas das bitcoins face a outras moedas. Katsiampa (2017) reconhece que o aparecimento das criptomoedas coloca desafios aos governos, reguladores, consumidores, economistas e empreendedores. Cabe salientar que atualmente o mercado das criptomoedas se mostra em crescente movimento, tendo inúmeros tipos de criptomoedas com seus diferentes funcionamentos. Além disso, os códigos e algoritmos são tão complexos e diferentes, que cada moeda virtual passa a ter suas peculiaridades, facilitando ou não as transações financeiras e algumas se destacam conforme a necessidade de quem as usa. De forma simples, sistemas criptográficos permitem que um emissor 'E' proteja a mensagem a ser transmitida de tal sorte que um desconhecido 'D' não consiga decifrar a mensagem 'M', caso ela venha a ser interceptada durante o processo de transmissão. Teoricamente, apenas o receptor 'R' é capaz de decifrar a mensagem 'M' enviada. A proteção mencionada consiste em aplicar um algoritmo de criptografia que codifica a mensagem 'M' de texto em claro em um texto cifrado antes de transmitir, (RODRIGUES, 2017). Os algoritmos de criptografia dos sistemas mais modernos são de domínio público.

Criptografias e as Moedas Virtuais

Estudos destacam que a moeda virtual *bitcoin* foi a primeira criptomoeda criada com sucesso e é também a criptomoeda à qual são efetuados mais estudos acadêmicos (Gandal et al., 2018). Algumas exceções são o trabalho de Ciaian et al., (2018), que estudou o preço de 17 criptomoedas, as *bitcoins* e outras 16 *altcoins*, e o estudo de Corbet et al. (2017), que analisa os preços da *bitcoin* da *ethereum*. Li e Wang (2017) estudaram empiricamente o valor da *bitcoin* e Bolt e van Oordt (2016) desenvolveram um modelo teórico para a determinação da cotação das criptomoedas. Hayes (2017) desenvolveu um modelo para a determinação do valor das bitcoins com base nos custos de produção. Ciaian et al. (2016) inferiram que a atratividade de uma criptomoeda para o investidor exerce um papel importante no seu preço. Katsiampa (2017) estudou a volatilidade das criptomoedas e concluiu que as *bitcoins* têm sido utilizadas mais como um ativo do que como uma moeda, atendendo à sua natureza especulativa e à sua volatilidade.

As moedas virtuais, conhecidas como criptomoedas empregam a criptografia como sua base de funcionamento, impedindo assim a sua falsificação, bem como, mantém a identidade de seus usuários anônimos, estes fregueses são vistos apenas como algarismos criptografados, i.e., por meio de suas firmas digitais, com fins específicos de ratificação de autoria, propriedade e/ou concordância, sem a identificação nominal. Isso preserva a inteira privacidade dos clientes. As moedas virtuais não são emitidas por uma instituição financeira ou quer seja uma autoridade central, como um banco oficial do governo de um país. Por esta razão, a se faz imune, em teoria, a influências por membro do governo, impedindo-o de gerar custos ou diminuir os. Torna-se perceptível que estar livre da interferência do governo e ter garantido o anonimato nas

transações executadas têm o seu lado negativo também. Essa circunstância faz a criptomoeda favorável para o seu uso em transações de caráter duvidoso, por exemplo, lavagem de dinheiro, evasão fiscal e financiamento de ações terroristas.

Também, há que se considerar no que concerne a implementação tecnológica do sistema de criptomoedas em si, é o caso de que, como se tratava de um preceito virtual e sem um repositório de dados logicamente centralizado, o saldo dos usuários do sistema pode ser simplesmente apagado em virtude de uma pane computacional generalizada, caso não exista um robusto e consistente back-up de todos os dados do sistema, (RODRIGUES, 2017). Conforme Rodrigues, (2017), no que diz respeito a indecifrábilidade da mensagem 'M' é o conceito do emprego de chaves utilizado pelo algoritmo de criptografia, conforme explicado a seguir. Na transmissão, a entrada do algoritmo de criptografia é a mensagem 'M', em texto claro, e a chave 'KE' do emissor. Essa chave consiste em uma cadeia de caracteres alfanuméricos. A saída do algoritmo de criptografia é o texto cifrado 'KE' (m), que é transmitido por meio da rede. Nesse caso, o algoritmo de criptografia é dito algoritmo de encriptação. Na recepção, quando a mensagem em texto cifrado chegar ao destino, um processo inverso é realizado, pois o receptor utiliza a sua chave 'KR' e o texto cifrado 'KE' (m) como entrada do algoritmo de criptografia, o qual fornece, como saída, a mensagem de texto em claro novamente: 'KR' (KE (m)) = m. Nesse caso, o algoritmo de criptografia é dito algoritmo de decifração (ou descifração), (RODRIGUES, 2017).

Sintetizando de uma forma geral, a ação de um algoritmo de criptografia, considerando o processo de encriptação, consiste em substituir uma cadeia de caracteres do texto em claro por outra cadeia diferente de caracteres, resultante de uma operação matemática e correspondendo ao texto cifrado. Já a ação referente ao processo de decifração consiste em realizar exatamente o oposto: identificar a cadeia de caracteres original que corresponde a cadeia que é recebida. Em sistemas criptográficos de chaves simétricas, o Emissor 'E' e o Receptor 'R' têm chaves idênticas, ou seja, KE = KR. Dois conhecidos padrões para sistemas desse tipo são o Data Encryption Standard (DES) e o Advanced Encryption Standard (AES), (TANENBAUM; WETHERALL 2010; KUROSE; ROSS 2013). No caso dos sistemas criptográficos para Rodrigues, (2017) um par de chaves diferentes é utilizado: uma chave privada e uma chave pública. A chave privada é de conhecimento exclusivo do Emissor 'E' ou do Receptor 'R', mas nunca de ambos. Já a chave pública é de conhecimento tanto do Emissor 'E' quanto do receptor 'R', além de todos que estão na rede. A operação desse tipo de sistema é relativamente simples, conforme RODRIGUES, (2017), resumida a seguir.

Cumprido dizer que a chave privada e a chave pública do Receptor 'R' são KP e KB, respectivamente. Para transmitir uma mensagem para o Receptor 'R', o Emissor 'E' então utiliza a chave pública KB para cifrar a mensagem 'M', obtendo, na saída do algoritmo, o texto cifrado KB(m). No destino, o Receptor 'R' precisa apenas utilizar sua chave privada KP para decifrar a mensagem KP (m) então recebida do Emissor 'E'. Em notação simbólica, o processo no Receptor 'R' seria então: KP(KB(m)) = m. Lembremos que a chave pública KB do Receptor 'R' é conhecida por todos que estão na rede. Por definição, é importante dizer que esse sistema goza

dapropriedade: $KB(KP(m)) = KP(KB(m)) = m$,
(RODRIGUES, 2017).

Conforme se observa no supra paragrafo, é notória a preocupação explanada a seguir. Uma vez que a chave pública KBdo Receptor 'R'tem visibilidade ao alcance de todos que estão na rede, qualquer usuário desconhecido pode transmitir uma mensagem criptografada KB(m) sem a necessidade de se identificar. Ou seja, não é possível saber com certeza quem transmitiu a mensagem 'M'para o Receptor 'R'.Dentre os padrões utilizados na implementação de sistemas criptográficos de chave pública, aquele denominado de RSA(Rivest, Shamir e Adleman) merece destaque por sua eficiência e ampla aceitação. A seleção da chave pública e da chave privada considera um processo matemático intrincado baseado em dois números primos. Por fim, o algoritmo de criptografia utilizado (criptação e decifração) é baseado em operações matemáticas complexas envolvendo exponenciação módulo, (TANENBAUM; WETHERALL, 2010; KUROSE; ROSS 2013; RODRIGUES, 2017; ISMIBEYLI; GUNBATALIEV, 2019).

História das Moedas Digitais: Conhecendo o Bitcoin e o Litecoin (Ouro e Prata)

Seguindo a linha de sistema de informações, chegando a era tecnológica e o advento da *internet* como meio de socialização e globalização, eis que surge um novo modelo de moedas: as criptomonedas ou moedas digitais, como são conhecidas popularmente. Tais moedas surgem como instituto de desenvolvimento financeiro, objetivando quebrar barreiras físicas da era comerciária no que se refere as operações financeiras. Dentre as moedas que se destacam entre as centenas criadas até hoje, duas delas ganham notoriedade por serem ao mesmo tempo tão iguais, mas com suas peculiaridades que se adequam a necessidade da globalização para este tipo de meio mercantil, são elas: Bitcoin e Litecoin.

Para Ulrich (2014, p 17):

[...] “Bitcoin é uma Moeda Digital peer-to-peer (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central. Entre muitas outras coisas, o que faz o Bitcoin ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. Ainda que à primeira vista possa parecer complicado, os conceitos fundamentais não são difíceis de compreender”.

O *bitcoin* foi criado em 31 de Outubro de 2008, quando em um sala virtual sobre criptografia, um programador desconhecido, publicou que havia criado um sistema financeiro de dinheiro eletrônico *P2P*. Na mesma sala virtual, publicou um artigo mostrando suas características e peculiaridades, muito se desacreditou do *bitcoin*. Mas nesse caso, o *bitcoin* é anos de pesquisa, mesmo que antes, por não haver um banco central controlador, não ter prosperado. Não é controlado por ninguém individualmente. Segundo Mafrá (2018, p 6):

[...] “*Litecoin* é uma criptomoneda (moeda virtual) descentralizada. Uma forma alternativa de pagamento que não é controlada por uma entidade ou governo. A *Litecoin* símbolo (LTC) é uma moeda virtual ou digital e não possui a característica física como o dinheiro” (MAFRÁ, 2018, p 6).

O *Litecoin* é um *hard fork* do *Bitcoin* original, diferenciando-se do mesmo por ter um tempo reduzido de geração de blocos, uma maior quantidade de moedas a serem emitidas, e utiliza um algoritmo de criptografia diferente do *Bitcoin* (*Scrypt* ao invés do *SHA-256*). A moeda como conhecemos hoje não é tão antiga como se pensa, no que tange a esse tema, a moeda papel está intimamente ligada ao surgimento e desenvolvimento do capitalismo, a partir do final do século XVIII, e à sofisticação dos instrumentos de troca que se originaram a partir daí. Apesar da informação a respeito da criação da moeda, outros meios de moeda existiam primordialmente, como trocas de coisas e conveniências. No entanto, a segurança desejada e sua aceitação plena foram adquiridas nos últimos duzentos anos. Essa aparente dicotomia entre conveniência, de um lado, e segurança e aceitação plena, de outro, resolvia-se, nos quatro mil anos iniciais de história da moeda, mediante acordos tácitos de equivalência da moeda a três metais preciosos, basicamente: prata, ouro e cobre. Portanto, a associação entre moeda e metal precioso sempre foi muito estreita, na forma de moeda mercadoria. Do ponto de vista econômico, os metais preciosos preenchiam a condição de conveniência, pois homogêneos e passíveis de serem pesados e com grande valor de escambo, eram a principal moeda. Para Ulrich (2014), as moedas digitais podem ser classificadas como simplesmente um dinheiro eletrônico, assim como dólar e real, para realizar transações comuns. Mas, pelo fato de ser uma moeda digital, tem algumas diferenças. A maior diferença do *Bitcoin*, é o modo de funcionamento, pois não é regulamentada, não há um poder centralizador e não depende de um intermediário, além disso, os *bitcoins* não inflacionam.

A segurança da realização de uma transação no sistema *Bitcoin* não se respalda exclusivamente na robustez do algoritmo criptográfico utilizado, ou seja, na impossibilidade da quebra de uma chave criptográfica. A segurança desse sistema considera ainda o tempo de registro da transação então realizada. Nesse sentido, quanto mais antigo é o registro da transação no sistema, maior é a segurança e, conseqüentemente, menos provável a sua violabilidade. A operação do sistema *Bitcoin* é essencialmente baseada na gerência eficiente de um *ledger* público (livro-razão) denominado de *blockchain*. Esse *ledger* contém todas as transações realizadas desde a criação do sistema, permitindo a todos os participantes verificar o histórico de cada transação, tendo sua autenticidade de cada transação protegida por assinaturas digitais, associadas aos endereços *bitcoin* de quem as realizou. Qualquer participante do sistema pode realizar a validação de transações e ganhar uma recompensa por esse serviço. Essa tarefa é chamada de mineração, e aquele que a realiza é chamado de mineiros (ou minerador). Toda vez que uma transação é realizada e verificada, o *ledger* público é atualizado em todos os nós do sistema, (RODRIGUES, 2017). Devido ao algoritmo utilizado para a prova-de-trabalho do processamento de transações, as máquinas que são utilizadas atualmente para mineração de *Bitcoins* (ASICs) não são muito eficientes para a mineração do *Litecoin*.

As Diferenças e Peculiaridades entre Bitcoin e Litecoin: *Litecoin* e *Bitcoin*, as duas moedas virtuais do momento possuem várias diferenças entre si, incluindo no que diz respeito a forma de mineração, de transação, diferentes algoritmos e capitalização de mercado. Atualmente a *Bitcoin* detém maior capitalização de mercado seguido de perto pelo XRP. Outras criptomonedas com altas capitalizações de

mercado incluem *Litecoin*, *Ripple* e *Ethereum*. A primeira e uma das principais diferenças entre *Litecoin* e *Bitcoin* é a o limite de moedas, ou seja, o valor total da moeda que cada moeda virtual pode produzir. Enquanto o *Bitcoin* não pode produzir mais do que 21 milhões de moedas, o limite de moedas do *Litecoin* é de 84 milhões de moedas. No entanto, as duas moedas virtuais suportam subdivisão em quantidades muito pequenas. A natureza do *Bitcoin* permite que os usuários completem suas transações em frações, enquanto o *Litecoin* suporta transações unitárias inteiras, (RODRIGUES, 2017).

Secundariamente, no que diz respeito a velocidade das transações o *Litecoin* vem superando, *Litecoin* e *Bitcoin* têm diferentes redes de operação, portanto diferem nas velocidades operacionais. Entre os dois *cryptos*, o *Litecoin* tem a maior velocidade de transação. A criptografia é capaz de confirmar transações mais rapidamente graças à sua rede única. Embora as transações nas redes *Litecoin* e *Bitcoin* ocorram quase instantaneamente, as transações exigem um certo tempo para serem concluídas. Este é basicamente o tempo gasto por outros membros da rede para confirmar transações. *Litecoin* é projetado para processar várias transações de uma só vez. Ele possui uma geração de bloco exclusiva que lida perfeitamente com altos volumes de transações rapidamente. No entanto, este não é o caso do *Bitcoin*. A geração de blocos do *Bitcoin* só pode confirmar algumas transações de uma só vez. A geração de blocos do *crypto* é muito lenta e deve ser atualizada para coincidir com a do *Litecoin*, (RODRIGUES, 2017). O tempo de bloqueio rápido do *Litecoin* minimiza significativamente a possibilidade de gastos duplicados. Isso é útil quando as redes envolvidas estão experimentando um poder de *hashings* similar. Embora a geração de blocos do *Litecoin* permita que a moeda virtual processe várias transações de uma só vez, há um problema. A capacidade do *Litecoin* de lidar com altos volumes de transações se traduz em um grande *blockchain*, e isso abre espaço para blocos órfãos. A informação acima significa que; com o *Bitcoin*, você terá que esperar mais tempo para uma confirmação do que você faria com o *Litecoin*. O *Bitcoin* leva até 10 minutos para confirmar uma única transação enquanto as transações são confirmadas em cerca de 2.5 minutos no *Litecoin*.

A diferença de algoritmos entre *bitcoin* e *litecoin*: A diferença técnica mais significativa entre as duas criptomoedas deve ser seus algoritmos criptográficos. O *Litecoin* e o *Bitcoin* utilizam algoritmos únicos que podem ser usados para separá-los. Quando se trata de *Litecoin*, a moeda digital emprega um novo algoritmo criptográfico chamado *Script*. Por outro lado, o *Bitcoin* emprega um algoritmo tradicional conhecido como *SHA-256*. A principal diferença entre o algoritmo *Script* e o algoritmo *SHA-256* é como eles afetam no processo de mineração. Cabe lembrar que muito poder computacional é necessário para confirmar transações tanto no *Litecoin* quanto no *Bitcoin*. No entanto, um grupo de indivíduos em uma rede criptografada, popularmente chamada de mineiros, usa uma quantidade substancial de seu poder computacional para confirmar as transações de outros membros. Como recompensa, os mineiros recebem uma quantidade específica da criptografia que extraíram. Embora o algoritmo *SHA-256* seja um pouco complicado que o *Script*, ele suporta melhor o processamento paralelo. Isso permite que os mineradores de *Bitcoin* façam uso de métodos de mineração melhores e mais avançados.

Um método de mineração de *Bitcoin* que vale a pena mencionar é o método de circuitos integrados de aplicação específica comumente conhecido como ASICs. Neste método, os sistemas de *hardware* modernos são personalizados para mineração de *Bitcoin*. A única desvantagem com este método é que tornou a mineração de *Bitcoin* quase impossível para o usuário médio. Observe que o *Script* não suporta mineração de moedas usando sistemas de *hardware*, como os ASICs. Em vez disso, o algoritmo suporta apenas métodos simples de mineração de moedas usando GPUs e CPUs conforme estudos efetuados por autores como Tacconie Tsunoda, (2019). Devido a esse simples fato, o *Litecoin* e outras moedas virtuais que empregam o algoritmo *Script* se tornaram cada vez mais disponíveis para o usuário comum. Eles são fáceis e mais baratos de minerar, tornando-os mais fáceis de acessar do que as moedas digitais baseadas em *SHA-256*, como o *Bitcoin*. Apesar alguns jogadores introduziram sistemas de *hardware* modernos, como os ASICs, para minerar moedas virtuais baseadas no *Script*, usuários comuns ainda podem extrair o *Litecoin* usando GPUs e CPUs simples.

METODOLOGIA

O estudo em questão possui natureza descritiva e exploratório quanto aos procedimentos, caracteriza-se como uma pesquisa documental, bibliográfica e estudo de caso. E quanto ao problema de pesquisa qualitativa. De acordo com Yin o estudo de caso é: “um dos empreendimentos mais desafiadores na pesquisa” (YIN, 2010, p. 23). Este método teve sua origem no campo da Medicina, e constitui hoje uma das principais modalidades de pesquisa qualitativa no campo das ciências humanas e sociais e teve seus procedimentos convencionados de forma adequada a partir da obra de Robert Yin nos anos de 1990 no século XX. O método de investigação utilizado é o indutivo, pois parte de uma premissa particular, dados e fatos constatados para uma premissa geral de conclusão. Salienta, ainda, Gil (2017) que, no raciocínio indutivo, não se deve buscar a generalização a priori, mas constatá-la e a partir da observação de casos concretos confirmados da realidade percebida. Sendo considerado como estudioso de estudo de caso Robert Yin (2001, 2010, 2016), uma das definições deste especialista é que o estudo de caso é uma análise que investiga um fenômeno contemporâneo dentro de um contexto da vida real. Yin (2016) enfatiza em seus estudos, que estudar o caso é a maneira mais adequada a ser utilizada quando é preciso responder a questões do tipo “como” e “por que”. Nesse contexto indo de encontro ao questionamento neste estudo comparativo dos algoritmos de transações utilizadas pelas criptomoedas *bitcoin* e *litecoin*; “quais as técnicas e tipos de algoritmos são utilizados entre as criptomoedas *Bitcoin* (*BTC*) e *Litecoin* (*LTC*) ao realizar transações criptografadas”. Acrescenta-se que, existem pelo menos cinco situações em que o estudo de caso se aplica para: (1) explicar vínculos causais em intervenções na vida real que são muito complexas para estratégias experimentais; (2) quando é preciso descrever intervenções no contexto em que ocorrem; (3) ilustrar determinados tópicos em uma investigação; (4) explorar uma situação complexa de resultados, e (5) como uma forma de meta-avaliação de determinados processos (YIN, 2010). Os autores Costa et al., (2013) inferem que o Estudo de Caso se aplicado corretamente pode contribuir como método e ajudar a ampliar as pesquisas em Ciência da Informação no Brasil e que na área das Ciências Sociais Aplicadas, o estudo de caso tem conquistado um espaço relevante nas pesquisas desenvolvidas.

Uma das principais características do estudo de caso é sua especificidade. Um caso pode ser modelar ou pode estar enquadrado como um tipo “patológico”, no sentido durkheimiano, onde sua novidade e suas particularidades vão ajudar a compreender “(...) uma das pontas do processo de transformação social que é o da realidade concreta” (ROESE, 1999. p. 192). No primeiro momento, serão apresentadas de forma geral as Criptomoedas *Bitcoin* e *Litecoin*, e a forma como elas conquistaram seu espaço na economia tanto real como virtual na sociedade atual, e como a capacidade de expansão que essa tecnologia vem ganhando no meio alternativo de pagamentos de bens e na aquisição de recursos. Além disso, serão apresentadas uma abordagem geral desse tipo de tecnologia, os tipos de algoritmos que são utilizados para realizar as transações criptografadas, as vantagens e desvantagens dessas moedas.

Analisar E Discute O Estudo De Caso: As moedas aqui estudadas dentre as moedas que se destacam na atualidade ganham notoriedade por serem ao mesmo tempo tão iguais, mas com suas peculiaridades que se adequam a necessidade da globalização para este tipo de meio mercantil, são elas denominadas de *Bitcoin* e *Litecoin*. A primeira aqui mencionada é uma Moeda Digital *peer-to-peer* (par a par ou, simplesmente, de ponto a ponto), de código aberto, que não depende de uma autoridade central. Entre muitas outras coisas, o que faz o *Bitcoin* ser único é o fato de ele ser o primeiro sistema de pagamentos global totalmente descentralizado. Ainda que à primeira vista possa parecer complicado, os conceitos fundamentais não são difíceis de compreender”. Já a segunda denominada nesse contexto de “*Litecoin*” é uma criptomoeda (moeda virtual) descentralizada como a *Bitcoin*. Uma forma alternativa de pagamento que não é controlada por uma entidade ou governo não possuindo a característica física como o dinheiro”, conforme estudos de Mafra, (2018). O segundo aqui mencionado diferencia-se então por ter um tempo reduzido de geração de blocos, uma maior quantidade de moedas a serem emitidas, e utiliza um algoritmo de criptografia diferente do *Bitcoin*. As máquinas que são utilizadas atualmente para mineração de *Bitcoins* (ASICs) não são muito eficientes para a mineração do *Litecoin*, isso é ocasionado devido ao algoritmo utilizado para a prova-de-trabalho do processamento de transações. As duas moedas virtuais possuem diferentes forma de mineração, de transação, diferentes algoritmos e capitalização de mercado (TACCONI; TSUNODA, 2019). Devido a esse simples fato, o *Litecoin* e outras moedas virtuais que empregam o algoritmo *Scrypt* se tornaram cada vez mais disponíveis para o usuário comum.

Considerações finais e recomendações para pesquisas futuras: O homem médio está cada vez mais antenado e disposto a incrementar as novas tecnologias as operações financeiras corriqueiramente; com o advento das moedas criptografadas, houve a necessidade de entender as diferentes vertentes de moedas virtuais, bem como, seu funcionamento e a segurança por trás delas. *Litecoin* e *Bitcoin* atualmente dominam o mundo da criptografia. Os dois têm altos limites de mercado, tornando-os as criptomoedas mais procuradas. Embora os dois compartilhem várias semelhanças, eles também diferem de várias maneiras, como explanado no decorrer da pesquisa, por exemplo, enquanto toda a rede *Bitcoin* está limitada a cerca de 21 milhões de moedas, a rede *Litecoin* pode suportar mais de 84 milhões de moedas, tempo de processamento de operações e criptografia das transações.

Além disso, essas moedas virtuais diferem na velocidade da transação. A rede *Litecoin* confirma transações muito mais rápidas que a rede *Bitcoin*. Os dois criptos também empregam diferentes algoritmos criptográficos. Os algoritmos *SHA-256* e *Scrypt* são utilizados por *Bitcoin* e *Litecoin*, respectivamente. Pode-se dizer com clareza que para operações corriqueiras, de caráter rápido, o *Litecoin* apresenta um algoritmo melhor para realizar tais operações. Cabe lembrar, muito embora não seja o foco central da presente pesquisa, que nenhuma das duas moedas apresentam total segurança, haja vista ambas as moedas possuírem riscos reais, não devendo subestimar a funcionalidade das moedas virtuais.

REFERÊNCIAS

- Advfn Brasil: 2019. Portal de investimentos em ações da bolsa de valores do Brasil, com cotações da Bovespa e BM&F. Por que usar Bitcoin? Disponível em: <<https://br.advfn.com/investimentos/criptomoedas/por-que-usar-bitcoin>> Acesso em: 17 out. 2019.
- Becker, H. S. 1999. Métodos de pesquisa em ciências sociais. 4. ed. São Paulo: Hucitec.
- BOLT, W., VAN OORDT, M. R. On the value of virtual currencies. <http://www.bankofcanada.ca/wp-content/uploads/2016/08/swp2016-42.pdf>.
- Bristol, V. M.; Guimarães Filho, P. L.; Gonçalves Junior, A. C., Felisberto, R. S.; Demo, P. A. de S. 2018. Industry 4.0 In Brazil. International Journal of Development Research Vol. 08, Issue, 12, pp.24803-24805, December.
- Chaine, M. 2013. Contágio como mecanismo de transmissão da crise financeira de 2008. Dissertação submetida ao programa de Pós-Graduação em Economia da Faculdade de Ciências Econômicas da UFRGS. Disponível em: <<https://coinrevolution.com/pt/qual-%C3%A9-a-diferen%C3%A7a-entre-o-litecoin-e-o-bitcoin%3F/>> Acesso em: 03 out. 2019.
- Ciaian, P., Rajcaniova, M., E Kancs, D. 2016. The economics of Bitcoin price formation. *Applied Economics*, 48 (19), pp.1799-1815.
- Coinrevolution. 2018. Qual é a diferença entre Litecoin e Bitcoin. São Paulo.
- Corbet, S., Lucey, B., Yarovya, L. 2017. Datestamping the Bitcoin and Ethereum bubbles. *Finance Research Letters*, doi:10.1016/j.frl.2017.12.006.
- Costa, A. de S.; Nascimento, A. V. do; Cruz, E. B.; Terra, L. L.; Ramalho; Silva, M. 2013. The use of case study method in Information Science in Brazil. InCID: R. Ci. Inf. e Doc., Ribeirão Preto, v. 4, n. 1, p. 49-69, jan./jun.
- Coulouris, G.; Dollimore, J.; Kindberg, T. 2007. Sistemas distribuídos. Conceitos e projeto. 5 Ed. Porto Alegre :Bookman.
- Exame. 2013. Legitimação de Bitcoin dispara seu valor e provoca dúvidas. São Paulo. Disponível em: <<http://exame.abril.com.br/tecnologia/noticias/legitimacao-de-bitcoin-dispara-seu-valor-e-provoca-duvidas>> Acesso em: 03 out. 2019.
- Falkenberg, et al. 1998. A framework of information systems concepts (The FRISCO-Report). IFIP, Department of Computer Science, University of Leiden, The Netherlands.
- Fobe, Nicole Julie. 2016. O bitcoin como uma moeda paralela-uma visão econômica e a multiplicidade de desdobramentos jurídicos. XX f.122 Monografia de Direito –Escola de Direito da Fundação Getúlio Vargas, São Paulo.

- Freguete, L. M.; Nossa, V., Funchal, B. 2015. Responsabilidade Social Corporativa e Desempenho Financeiro das Empresas Brasileiras na Crise de 2008. RAC, Rio de Janeiro, v.19, n.2, pp.232-248.
- Gandal, N., Hamrick, J.T., Moore, T., e Oberman, T. 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, v.95, pp. 86-96.
- Gil, Antônio Carlos. 2012. Como elaborar projetos de pesquisa. São Paulo: Atlas.
- Hayek, F. A. 1990. Denationalisation of Money. 3ª. ed. São Paulo: The Institute of Economic Affairs. História da Moeda. Rainer Sousa, equipe Brasil Escola. Disponível em: <<https://brasilecola.uol.com.br/historia/historia-da-moeda.htm>>. Acessado em 03 out. 2019.
- Hayes, A. S. 2017. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, v.34 (7), pp.1308-1321.
- Ismibeyli, R.E.; Gunbataliev, E. Z. 2019. Computer Analysis of Magnetic Devices of Information Control Systems Automatics. *International Journal of Development Research* v. 09, Issue, 07, pp. 28866-28874, July.
- Kaminsky, G. L.; Reinhart, C. M.; Vegh, C. A. 2003. The Unholy Trinity OF Financial Contagion. *Journal of Economic Perspectives*, v.17, n.4, pp.21-74.
- Katsiampa, P. 2017. Volatility estimation for bitcoin: A comparison of GARCH models. *Economic Letters*, v.158, pp.3-6.
- Keynes, John Maynard. 2002. As Consequências Econômicas da Paz. Brasília: UnB.
- Kurose, J. F.; Ross, K. W. 2013. Computer networking: A top-down approach featuring the Internet. Pearson Education, 6th ed., New York.
- Laudon, K. C. S.; Laudon, J. P. 1996. Management of information systems: a contemporary perspective. [S.l.]: MacMillan.
- Laundon, K. C.; Laundon, J. P. 2013. Sistemas de Informação Gerenciais. 9.ed.- São Paulo: Pearson Praticce House.
- Lee, K. e James, J. I. e Ejeta, T. G e Kim, H. J. Electronic Voting Service Using Block-Chain. *Journal of Digital Forensics, Security and Law*. Artigo 8, 2016.
- Li, X., Wang, C. A. 2017. The technology and economic determinants of cryptocurrency exchange rates: The case of bitcoin. *Decision Support Systems*, v.95, pp.49-60.
- Lucena, A. U.; Henriques, M. A. A. Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum. Universidade Estadual de Campinas, 2016.
- Menezes, A. J., Van Oorschot P. C. and Vanstone S.A. 1996. Handbook of Applied Cryptography. Waterloo: CRC Press.
- Minsky, H. P. 1986. Stabilizing an unstable economy. N. YORK: McGraw Hill Professional. Retrieved from <http://digamo.free.fr/minsky86.pdf>.
- Moia, G.H.V; Henquires, M.A.A. Avaliação da segurança de protocolos criptográficos usados em moedas virtuais
- Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Eletronic Cash System. Disponível em: <http://bitcoin.org/bitcoin.pdf>
- O que são organizações virtuais? 2015. Portal Gestão, Portugal, 30 mar. Disponível em: <<https://www.portal-gestao.com/artigos/organizações-virtuais.html>>. Acesso em: 03 out. 2019.
- O'Brien, J. A. 1999. Sistemas de Informação e as Decisões Gerenciais na era da Internet. Ed. Saraiva. The McGraw-Hill Companies, Inc.
- Oliveira, D. de P. R. de. 2011. Sistema de informações Gerenciais: Estratégias, Táticas e Operacionais. 14 ed. São Paulo. Atlas.
- Pires, H. F. 2017. Bitcoin: a moeda do ciberespaço. Geousp – Espaço e Tempo (Online), v. 21, n. 2, p. 407-424, agosto. ISSN 2179-0892. Disponível em: <<http://www.revistas.usp.br/geousp/article/view/134538>>. Acesso em: 30.set. 2019.
- Pressman, R. S. 1995. Engenharia de software. São Paulo: Makron Books.
- Rodrigues, C. K. S. 2017. Sistema Bitcoin: uma análise da segurança das transações iSys | Revista Brasileira de Sistemas de Informação, Rio de Janeiro, v. 10, No. 3, pp. 5-23.
- Roese, M. 1999. A metodologia do estudo de caso. *Cadernos de sociologia*, Porto Alegre, PPGS/UFRGS, v. 9, pp. 189-200.
- Rogojanu, A.; Badea, L. 2014. The issue of competing currencies. Case study-bitcoin, *Theoretical Applications Economics*, v. 21(1), pp.103-114.
- Santos, C. D.; Valentim, M. L. P. 2014. As Interconexões Entre a Gestão da Informação e a Gestão do Conhecimento para o Gerenciamento dos Fluxos Informacionais. *Perspectivas em Gestão e Conhecimento, João Pessoa*, v. 4, n. 2, pp. 19-33. jul./dez.
- Schneier B. 1996. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2 ed. Wiley.
- Senna, J. J. 2010. Política Monetária: ideias, experiências e evolução. 1ª. ed. Rio de Janeiro: Editora FGV.
- Silber, S. D. 2010. A economia mundial após a crise financeira de 2007 e 2008. *Revista USP*. São Paulo, v. 85, pp. 82-93.
- Singer, T. 2012. Tudo conectado: conceitos e representações da internet das coisas. Simpósio em Tecnologias Digitais e Sociabilidade – Práticas Interacionais em Rede.
- Stair, R. M. 2008. Princípios de sistemas de informação: uma abordagem gerencial. São Paulo: Cengage Learning.
- Stair, Ralph M. 2011. Princípios de sistemas de informação / alph M. Stair, George W. Reynolds; (tradução HarueAvitscher ; revisão técnica Flávio Soares Corrêa da Silva). -- 9. ed -- São Paulo. Disponível em: <<https://www.cbsi.net.br/2015/04/tipos-de-sistemas-de-informacao-nas-organizacaoes.html>>. Acesso em: 02 mai. 2019.
- Stallings W. 2008. Criptografia e Segurança de redes. 4 ed. São Paulo: Pearson Prentice Hall.
- Tacconi, L. H.; Tsunoda, D. F. 2019. Prazo Médio de Processos no Segundo Grau de Jurisdição: Um Estudo Baseado em Mineração de Dados em uma Organização Jurídica. *International Journal of Development Research* Vol. 09, Issue, 10, pp. 30274-30279, October.
- Tanenbaum, A. S.; Steen, M. Van. 2007. Sistemas distribuídos. Princípios e paradigmas 2.Ed. São Paulo: Pearson.
- Tanenbaum, A. S.; Wetherall, D. J. 2010. Computer networks. Pearson Education, 5th ed., New York. Tipos de Sistemas de Informação nas organizações, Comunidade Brasileira de Sistemas de Informação (CBSI), escrito por Claudio Florenzano, equipe CBSI.
- Urlich, Fernando. 2014. Bitcoin: a moeda na era digital: Instituto Ludwig von Mises Brasil. São Paulo.
- Yin, R.K. 2016. Pesquisa qualitativa do começo ao fim. 2ª Nova Iorque: The Guilford Press. ISBN: v.978-1-4625-1797-8. 386.
- Yin, Robert. 2001. Estudo de caso: planejamento e métodos. Editora ArtMeo. Porto Alegre.