Lucas Fausto Medeiros

Matrícula: 211080055

Avaliação II de Metodologia Científica - Blockchain: uma solução para a garantia de copyright no cenário acadêmico.

Campina Grande, 2021

Lucas Fausto Medeiros

Avaliação de Metodologia Científica

Avaliação da disciplina de Metodologia científica apresentado como requisito parcial para obtenção de nota da primeira unidade

Professor:

Dr. Nivaldo Geroncio da Silva Filho

Campina Grande, 2020

Sumário

1.0 - Blockchain: uma solução para a garantia de copyright.

1.1 – Introdução e Motivação

Estamos seguros na internet? Essa pergunta pode soar bastante retorica, visto que a cada dia noticias e mais noticias surgem de ataques de hackers a sistemas públicos e privados mundo a fora. Essas notícias nos fazem questionar se realmente há segurança em nossos dados que estão presentes e armazenados na internet, o que garante que os dados que cedemos as grandes lojas de *e-comerce* digital como, cartão de credito, CPF, identidade e outros, não caiam nas mãos erradas? O que parece é que essa real garantia, isto é, a garantia de que 100% dos nossos dados estão seguros não e devidamente apresentada e garantida.

Neste sentido, não só dados pessoais podem ser alvos de negligencia ou de vazamento e roubo, enquanto mais o mundo e a tecnologia avançam, mais coisas passam a utilizar a internet para a comunicação e funcionamento, é notório que o armazenamento na *nuvem* fica mais perto de nos e dos nossos dispositivos, ou seja, a cada dia ficamos mais distante de nossos dados de forma física, o que pode sim diminuir a chance de perdemos estes dados, mas ficamos mais vulneráveis a ataques e vazamentos do mesmo, em outras palavras, é uma faca de dois gumes, a chances de nos perdemos os arquivos se o tivemos em forma física, e de termos o mesmo vazado se o tivemos em forma digital. Entretanto, esse problema infere também no cenário corporativo ou de maiores indivíduos conectados à rede em questão como é o caso de centros acadêmicos.

No cenário acadêmico a preocupação com a segurança dos dados do centro é ainda mais importante, pois, a garantia que o acervo acadêmico tenha a plena funcionalidade, autoria e segurança é o que faz o centro ou o campus capaz de se mostras produtivo. Um centro acadêmico onde a segurança de dados não possui garantia se mostra um centro inviável para o trabalho e defesa de artigos e pesquisas cientificas, a inviabilidade está diretamente ligada ao quesito de estrutura de segurança para os acadêmicos., e é nesse quesito que o sistema computacional de dados de blockchain demonstra sua serventia principal, pois, o mesmo é capaz de garantir, ainda que 99% dos dados esteja seguro a invasões e plágios de forma digital.

1.2 – Fundamentação teórica

1.2.1 – O blockchain

O blockchain é uma resolução apresentada por o/os então desconhecido/os Satoshi Nakamoto como uma solução para transações financeiras que ainda se baseavam em instituições para intermediar os registros, que são de confianças porem ainda se sujeita a fraudes.

Blockchain nada mais é que uma rede computadores que fazem este serviço de intermediar as transações, cada computador que se interliga nessa rede é chamado de nó ou node, esses nós são responsáveis por registrar todas as transações feitas, conferir os cálculos sem a necessidade de um intermediador. Entretanto, essa de cadeia de computadores que basicamente faz a checagem de valores que cada nó da, ou seja, o comportamento de cada nó é gravado na cadeia, na rede em que se liga, no próprio blockchain, ou seja, cada alteração, transação ou registro feito é gravada e registrada em cada um dos nós da rede, então, quando se faz determinada transação, cada nó faz a checagem dentro da rede.

Os nós fazem cálculos necessários para saber se as transações são validas e checam se determinado produto da transação não foi ou está sendo usado ao mesmo tempo, impedido fraudes. Para alterar qualquer registro, é necessário que ele se altere em mais da metade dos nós que esse registro nele exista, ou seja, para fazer essa alteração, é necessário possuir um poder computacional absurdo.

Entretanto, o blockchain nos dá a alternativa de deixarmos arquivos públicos e ao mesmo tempo deixarmos seguros, pois, para que determinado arquivo ou registro seja alterado de sua forma original, deve haver um consenso computacional gigantesco, é uma forma de segurança de dados que dificilmente será quebrado, é uma forma de garantir que dados acadêmicos continuem com sua integridade autoral, uma forma de garantir o Copyright © e mesmo assim deixar o arquivo público.

Ademais, as soluções em blockchain também exclui a necessidade de grandes estruturas e equipamentos para o armazenamento seguro de arquivos, sejam digitais ou de papel, ou seja, quaisquer documentos podem ser autenticados, digitalizados, registrados e em segurança utilizando o blockchain.

1.2.2 – Lei do Copyright

Direitos autorais são aqueles que pertencem ao criador de uma obra intelectual, ou seja, que tenha a imaterialidade como principal característica. Produções artísticas, culturais e científicas são exemplos de obras intelectuais protegidas por esses direitos. A forma mais tradicional na expressão dos direitos autorais em todo o mundo é o copyright, que faz referência a “todos os direitos reservados”. Isso significa que o autor se reserva todos os direitos garantidos pela legislação de seu país, impedindo que a redistribuição, utilização e modificação do trabalho original sejam realizados sem o seu consentimento. A ideia sobre os direitos do autor a respeito de sua criação tem sustento no artigo 5º da Constituição Federal. Em sua essência, defende como justa e necessária a proteção ao autor que dedicou àquela obra o seu talento, tempo, conhecimento e dinheiro.

1.2.2.1 – Como funciona a Lei do Copyright - Lei nº 9.610 (Lei dos Direitos Autorais – LDA)

Em território nacional, a Lei nº 9.610 (Lei dos Direitos Autorais – LDA), em vigor desde 1998, garante a conservação dos direitos autorais. Sua principal premissa é que qualquer reprodução, distribuição e alteração de uma obra intelectual devem ser aprovadas pelo autor com antecedência, pois, conforme explica o documento, autor é a pessoa física criadora de obra literária, artística ou científica.

O autor detém os direitos morais e patrimoniais a respeito de sua criação, independentemente de registrar sua obra junto a um órgão público competente. A lei ainda designa quais produções estão sujeitas aos direitos autorais, quais não estão e em que situações as obras podem ser usadas sem violar esses direitos.

1.3 – Objetivo especifico I: A falha na Segurança dos dados.

Segurança de dados é um quesito bastante importante nos dias atuais, cedemos dados o tempo todo no meio virtual, o que mais se questiona é onde esses dados estão armazenando estes dados e se eles estão devidamente seguros. Para obtermos essa resposta, é importante primeiro sabermos quais estruturas são utilizadas pelas grandes corporações para o armazenamento das devidas informações.

Os data centers são grandes instalações na qual empresas como o Google, Microsoft, IBM, Amazon utilizam para armazenar os dados de seus usuários, o que constitui essas datas centers é basicamente grandes servidores com capacidade de armazenar zetabytes de dados nestas instalações. No entanto, mesmo sendo fortemente vigiados, esse

sistema de data center pode ser invadido de uma forma um tanto quanto fácil, um único acesso a qualquer porta física destes servidores, fará com que o invasor tenha o total acesso ao data center por inteiro, ou seja, o que realmente garante a segurança dos dados não é um meio virtual, mas sim a presença de uma segurança externa não necessariamente formado por um meio “logico”, mas uma gama de segurança que não faz parte do sistema de armazenamento dos dados.

Neste sentido, se mostra visível, ainda que muito difícil, que nossos dados que “pertencem” as grandes corporações digitais podem ser alvejadas, vazadas e divulgadas no meio digital a qualquer momento, basta uma única falha no sistema de segurança. Estes sistemas de armazenamento em servidores, unidade física única de armazenamento, é utilizado em diversas outras corporações, como exemplo as universidades, escolas e faculdade.

Entretanto, se até mesmo, como já foi visto, grandes datas centers podem ser vulneráveis, consideremos os sistemas de armazenamento de uma universidade, um servidor que é, ainda que não expostamente, mas que, de fácil acesso a qualquer um, o comprometimento dos dados é facilmente fácil para um invasor fazer o que bem tiver disposto, além também de problemas físicos, como falha do equipamento em si, o que se mostra outra grande vulnerabilidade no acesso a esses dados.

1.3.1 - Princípios Fundamentais de Segurança

Segurança e privacidade são princípios basilares de qualquer sistema de informação. Nos referimos a segurança como a combinação de Integridade, Disponibilidade e Confidencialidade. Normalmente é possível obter segurança usando uma combinação de autenticação, autorização e identificação. Esses conceitos são definidos a seguir:

- Integridade: Certeza que uma informação não foi alterada, exceto por quem tem o direito de realizar estas alterações. A integridade dos dados é a garantia de que os dados não foram manipulados, estão corretos. No contexto da Blockchain é a garantia de que os dados que constam nas transações não podem ser modificados intencionalmente ou por eventos fortuitos, como surtos de energia ou erros na propagação dos dados. Mecanismos criptográficos de verificação de integridade são comumente utilizados para sua confirmação.
- Disponibilidade: Garante que os usuários de um determinado sistema conseguirão utilizá-lo sempre que for necessário. Em outras palavras, os serviços estará sempre

ativo quando solicitado por um usuário legítimo. Isso requer que tanto a infraestrutura de comunicação quanto as bases de dados possam ser utilizadas. A Blockchain alcança estes objetivos ao permitir que os usuários estabeleçam conexão com vários usuários e ao manter os blocos de maneira descentralizada com várias cópias dos blocos na rede.

- Confidencialidade: É a garantia de que a informação não será obtida por pessoas não autorizadas. Isto é, apenas aqueles com os direitos e privilégios necessários serão capazes de acessar a informação, esteja ela armazenada, em processamento ou em trânsito. Na rede Bitcoin, para garantir este princípio são utilizados mecanismos de pseudo anonimização do usuário, como uso dos endereços Bitcoin. Os endereços Bitcoin são resumos criptográficos das chaves públicas.
- Autenticação, Autorização e Auditoria: Busca verificar a identidade de quem realiza uma determinada função em um sistema, verificar que direitos esse usuário possui e armazenar informações de uso desse usuário. A estrutura da Blockchain é totalmente desenvolvida para garantir estas três funções, pois somente os usuários que possuem as chaves privadas podem realizar transações, e todas as transações são públicas e auditáveis.
- Não Repúdio: Garantia que a pessoa não negue ter feito uma determinada ação em um sistema. O não repúdio fornece provas de que um usuário realizou uma determinada ação, como transferir dinheiro, autorizar uma compra, ou enviar uma mensagem. Como todas as transações são assinadas, um usuário não pode negar que a realizou.

A privacidade pode ser definida como o direito que um indivíduo tem em compartilhar suas informações. Os usuários do Bitcoin usam um pseudônimo (endereço) para realizar suas transações. Normalmente cada usuário possui centenas de endereços. Uma transação pode ser vista como uma cadeia de assinaturas que comprovam a posse e a transferência de valores, de maneira aditável. Assim uma das preocupações é que essas transações possam revelar informações do usuário que vão além de simplesmente uma identificação, como hábitos de compra e locais frequentados do usuário.

O conceito de privacidade em Blockchain consiste em manter o anonimato e a desvinculação de transações. O anonimato de transações exige que não seja possível vincular uma transação particular a um usuário, para isto, o usuário utiliza um endereço diferente a cada nova transação. A desvinculação das transações exige que duas transações do mesmo indivíduo não possa ser vinculadas como tal.

1.3.2 – Quais os principais mecanismos e ferramentas de segurança de dados atualmente?

Basicamente, as empresas realizam dois tipos de controles em relação aos seus dados e informações: os controles físicos e os controles lógicos. Os controles físicos são aqueles que abrangem barreiras que limitem o contato ou o acesso direto à informação e à infraestrutura criada e mantida para garantir a existência dos dados.

Por exemplo: portas, paredes, trancas, sistemas de senhas, biometria, vigias, blindagem e outros mecanismos para proteger a entrada de pessoas não autorizadas em áreas como a central de dados. Já o controle lógico envolve aquelas barreiras que impedem ou limitam o acesso aos dados que estão em ambiente eletrônico ou virtual.

Alguns exemplos de ferramentas usadas atualmente são:

1) criptografia: mecanismos de segurança que usam esquemas matemáticos e algoritmos para codificar os dados em textos inelegíveis, os quais só podem ser decodificados por pessoas que detém a chave de acesso;

2) assinatura digital: conjunto de dados criptografados que garantem a integridade de um documento, mas não a confidencialidade;

3) honeypot: software usado para detectar ou impedir ações de crackers, spammers e outros agentes externos não autorizados;

4) controles diversos de acesso: palavras-chaves, biometria, cartões inteligentes, firewall etc. são mecanismos dessa categoria.

1.4 – Objetivo especifico II: Blockchain e a segurança dos dados

Para exemplificar a forma como o blockchain garante a segurança, pode-se utilizar três termos para exemplificar:

- Descentralização: O sistema blockchain, por se tratar de uma rede de computadores e não de um servidor principal, dificulta ainda mais que dado “arquivo” seja localizado, o que leva a entender que não possui uma massa de dados em uma única maquina,
- Rastreamento: Como na descentralização, o rastreamento fica bastante complexo para um nó (um computador) que não está inserido diretamente na rede.

- Criptografia de ponta: Para isso, o blockchain codifica a informação ou a transação utilizando duas chaves, dois códigos ou duas senhas. A primeira senha ou chave é pública, ela é responsável por seu endereço, carteira ou login. A segunda chave é uma senha, uma chave privada, que é necessária para realizar qualquer transação. Neste sentido, a junção destas duas chaves é transformada em um bloco de texto chamado hash, que é compartilhado com cada um dos nós da rede e, acrescentado ao banco de dados que cada nó possui.

Para um sistema de banco de dados centralizado que é atualmente o mais utilizado para armazenar uma grande massa de arquivos, basta apenas uma “brecha” em uma das portas do servidos para o invasor tenha acesso a grade da maioria dos arquivos e dos dados sem maiores problemas.

No blockchain isso é bem mais complexo, por utilizar um sistema de criptografia e segurança baseada em duas chaves, para o invasor ter algum controle do sistema (da rede no caso do blockchain) é necessário que o mesmo assuma o controle de pelo menos 51% das maquinas que estão conectadas a rede, além de toda movimentação ser rastreável.

Isso quer dizer que, mesmo o invasor conseguindo alterar o arquivo em apenas uma máquina ou em menos de 51% dos computadores, os outros que possuem o arquivo ou o dado original não validariam tal alteração, pois o bloco, a rede, fica em constante verificação de seus registros.

1.5 – Metodologia: A incrementação do blockchain no ambiente acadêmico:

A maior funcionalidade do sistema incrementado diretamente no ambiente acadêmico é a capacidade de gerar com certas clarezas, um sistema de reputação, um mecanismo eficiente baseado na tecnologia do blockchain, um mecanismo que permite o individuo nele inserido consiga o maior controle sobre seus dados, desde quem visualizou, utilizou, gravou, modificou ou danificou. Então, fica bastante visível que a garantia dos direitos de determinado artigo ou pesquisa seja garantida.

O sistema ainda pode ajudar o campo acadêmico a realizar autenticações e validações dos conteúdos na web inseridos com a utilização de um sistema de plugins instalados

nos computadores de quem utiliza ou necessita utilizar o sistema acadêmico, seja para lançar ou receber informação, então, deste modo o plugin gera um relatório do acesso de dado dispositivo e, armazena na *hash* no qual o arquivo que foi utilizado está gravado.

Ademais, outra grande vantagem que a rede blockchain dá a um ambiente como os acadêmicos é a grande possibilidade de assinar contratos e arquivos, pois, quando um documento é **certificado em blockchain,** como já foi visto, fica quase que impossível a alteração de tal registro ou certificado.

No mais, a rede de blockchain iria garantir que os sistemas de registros de artigos e pesquisas dos campus acadêmicos tivesse uma funcionalidade mais limpa, otimizada e segura para a grade de dados científicos, uma garantia única para os ambientes, um sistema livre de falhas, livre de quedas e livre de invasões, seria uma garantia de que todos nossos recursos científicos ficassem descentralizados e criptografados e ainda assim seguros contra quaisquer dano, é a garantia de nosso trabalho seguro.

1.6 – Resultados:

Com a incrementação do sistema nos ambientes acadêmicos, quedas de sistemas como o CNPq – que teve o sistema fora do ar no dia 26/07/2021 por motivos de falhas no sistema – não seriam frequentes e nem prováveis, pois, com a gama de rede instalado na grade do sistema do blockchain, o serviço estaria de certa forma garantido a todos sem quaisquer formas de interrupção, e uma malha e um avanço a ser percorrido na tecnologia da informação e na garantia de dados.

Ademais, a utilização do sistema eliminaria a necessidade de equipamentos físicos nas universidades, ou seja, a unidades de armazenamento, os servidores, teriam um fim, eliminando gastos em manutenção e operações destes sistemas, pois, a descentralizações dos arquivos fariam com que a gama de arquivos não estivessem fixos em um único ponto, eliminando riscos, aos arquivos e até o local no qual o servidor fica armazenado, é uma forma de avançar *"ecologicamente"* e inteligente para inovações que são de fáceis acessos e de fáceis utilização.

Referências Bibliográficas:

Criptomoedas, blockchain e Altcoins | Nerdologia Tech

https://www.youtube.com/watch?v=PQQ0NpwgMIg&list=TLPQMzAwNzIwMjFTZlhIGl1w-A&index=3

Bitcoin e Blockchain EXPLICADOS!

https://www.youtube.com/watch?v=QrVMjwF4VKs&list=TLPQMzAwNzIwMjFTZlhIGl1w-A&index=2

Blockchain e segurança de dados: como aplicar na sua empresa

https://www.eveo.com.br/blog/blockchain-e-seguranca-de-dados/

Uso de Blockchain para Privacidade e Segurança em Internet das Coisas

https://www.researchgate.net/profile/Vanessa-Rocha-Leandro-Chicarino/publication/321966650_Uso_de_Blockchain_para_Privacidade_e_Seguranca_em_Internet_das_Coisas/links/5a3b92aaaca272774f9baf5a/Uso-de-Blockchain-para-Privacidade-e-Seguranca-em-Internet-das-Coisas.pdf

LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998.

http://www.planalto.gov.br/ccivil_03/leis/l9610.htm

COMO O BLOCKCHAIN PODE AJUDAR A SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS?

https://blogbrasil.comstor.com/como-o-blockchain-pode-ajudar-a-seguranca-da-informacao-nas-empresas

Segurança de dados e Blockchain: entenda as relações

https://blog.bitcointrade.com.br/seguranca-de-dados/