CURSO DE CIÊNCIA DA COMPUTAÇÃO – TCC	
( ) PRÉ-PROJETO ( ) PROJETO	ANO/SEMESTRE:

PROTOCOLO PARA CORREIO ELETRÔNICO BASEADO EM BLOCKCHAIN

Ruan Schuartz Russi

Mauro Marcelo Mattos

1 INTRODUÇÃO

A popularidade do protocolo Simple Mail Transfer Protocol (SMTP) é inegável. Estima-se que, a cada minuto, 188 milhões de novos e-mails são enviados (PEZZOTTI, 2019). No ano de 2019, o número global de usuários de correio eletrônico totalizava 3,9 bilhões de usuários, sendo que o número deve crescer para 4,3 bilhões até 2023, número esse equiparado a metade da população mundial (NITRONEWS, 2020). Toda essa popularidade é atribuída a diversos fatores, sendo um deles a sua idade. O e-mail é considerado o serviço online mais antigo do mundo, tendo a primeira mensagem da história sido enviada no ano de 1971 (OLIVEIRA, 2020).

Apesar de ser uma tecnologia difundida e robusta, a idade da solução acaba trazendo para a mesma alguns pontos negativos. Na época em que os serviços de correio eletrônico foram desenhados, a internet como se apresenta hoje não existia e as redes de computadores existentes eram restritas a ambientes acadêmicos, não sendo liberado acesso para a população (TRAININI, et al, 2005). Neste ambiente controlado, a preocupação com a segurança da informação era mínima e dispositivos de segurança geralmente não eram implementados. O cenário mudou com o advento da criação e popularização da internet. A rede se tornou um lugar hostil e perigoso, sendo utilizada por usuários mal-intencionados para a realização de práticas ilícitas. Por não ter sido criado com este ambiente hostil em mente, os serviços de correio eletrônico possuem uma diversidade de vulnerabilidades passíveis de serem exploradas como envio de spam, propagação de vírus, vazamento de mensagens e falsificação de identidade (TRAININI et al, 2005).

Uma característica importante dos servidores de e-mail é que eles formam uma rede descentralizada não existindo assim uma entidade com poder absoluto sobre as outras. Apesar disso, a implementação, devido a época em que foi feita, não aproveita características importantes de redes descentralizadas modernas. A Blockchain por exemplo, tecnologia criada para dar vida ao Bitcoin, permite ter um histórico imutável de tudo que foi feito. A implementação do Bitcoin consegue garantir que um determinado usuário realizou uma transação financeira para outro de forma imutável. Já com o SMTP, é impossível determinar de modo fidedigno que um usuário enviou uma mensagem para outro. Além disso, atualmente é comum a utilização de serviços de e-mail de terceiros. Em 2016, o serviço de correio eletrônico da Google, o Gmail, chegou a marca de 1 bilhão de usuário ativos mensalmente (ESTADÃO, 2016). Essa dependência com entidades terceiras acaba exigindo que os usuários tenham plena confiança nas mesmas pois nada impede que as mesmas modifiquem, excluam ou vazem mensagem privadas. Elas podem chegar até ao ponto de mandarem mensagens se passando pelo usuário.

Comentado [FAP1]: elas

Para resolver os problemas acima citados, o ideal seria a implementação de um protocolo totalmente novo que já nasça sem a presença destas falhas. O problema é que devido a já relatada alta utilização dos serviços de e-mail, uma mudança abrupta de tecnologia se torna inviável pois envolve uma mudança significativa na rotina de milhões de usuários. Diante deste cenário, o presente trabalho propõe o desenvolvimento e a implementação de um protocolo baseado em Blockchain que consiga enviar e receber mensagens de correio eletrônico de modo descentralizado e seguro e que seja compatível com o protocolo SMTP permitindo assim uma migração gradual de tecnologia.

1.1 OBJETIVOS

O objetivo deste trabalho é disponibilizar um protocolo de envio e recebimento de e-mails baseado em Blockchain e que seja compatível com o protocolo SMTP.

Os objetivos específicos são:

a) Especificar um modelo de envio e recebimento de mensagens baseado no conceito de blockchain;
b) Desenvolver um protótipo de cliente para demonstrar a funcionalidade do protocolo;
c) Criar um conjunto de casos de testes para validar o protocolo desenvolvido.

2 TRABALHOS CORRELATOS

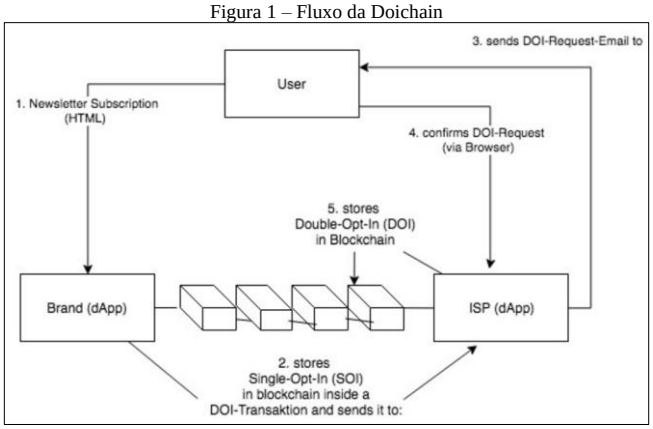
Nesta seção são apresentados trabalhos que apresentam semelhança com os principais objetivos do trabalho proposto. O primeiro é a implementação de uma Blockchain capaz de armazenar e validar inscrições de usuários em newsletters (KRAUSE, 2018). O segundo é o estudo e implementação de um protocolo p2p para a troca segura de mensagens (WARREN, 2012). Por fim, na seção 2.3 será apresentada uma dissertação de mestrado que busca fazer a ligação entre envio de e-mails e transações de criptomoeda (GROTTENTHALER;2017).

2.1 CONTROLE DE INSCRIÇÃO PARA RECEBIMENTE DE E-MAIL PROMOCIONAL

O trabalho desenvolvido por Krause (2018) consiste em um sistema baseado em Blockchain que é capaz de provar que um determinado usuário se inscreveu em uma campanha de mail marketing. A motivação para o trabalho é resolver alguns casos comuns de spam e possibilitar a adesão de empresas de mail marketing a leis de proteção de dados. Para tal, o autor propôs uma Blockchain que armazena as inscrições dos usuários e pode ser consultada pelo dono da campanha de marketing antes de o mesmo enviar algum e-mail para o usuário. Para se comunicar com a Blockchain, o autor desenvolveu um aplicativo chamado dApp que serve unicamente para realizar esta comunicação. Tanto o dono da campanha de marketing quanto o dono do servidor de e-mail que o usuário está utilizando precisam configurar uma instância local do dApp.

O fluxo da plataforma proposta por Krause (2018) pode ser conferido na Figura 1. Primeiramente, o usuário (User) se inscreve em alguma campanha de e-mail. Um método comum de inscrição é a submissão do e-mail em um formulário presente em algum site. A empresa responsável pela campanha (Brand), ao receber a inscrição envia para a Blockchain uma transação ainda não confirmada. O servidor de e-mail do usuário (Internet Service Provider - ISP), ao receber a transação não confirmada, envia ao usuário (User) um e-mail pedindo que o mesmo confirme a inscrição. Caso a inscrição seja confirmada, a transação é confirmada na Blockchain. Sendo assim, sempre que for enviar algum e-mail, o dono da campanha pode checar se o usuário realmente se inscreveu para aquela campanha.

Figura 1 – Fluxo da Doichain



Fonte: Krause (2018).

O trabalho de Krause (2018) consegue de fato ser uma solução para o problema que ele se propõe a resolver, porém, implantar tal solução em um cenário produtivo acaba exigindo bastante esforço. Por mais que a migração seja transparente para o usuário, a solução exige que pelo menos os servidores de e-mail mais populares do mercado se adequem a plataforma para que a mesma tenha algum efeito. Além disso, os donos das campanhas precisariam também configurar do seu lado o dApp para passar a validar as inscrições dos usuários. O grande ponto é, mesmo exigindo tamanho esforço, a plataforma se limita a resolver um cenário muito específico deixando ainda uma série de problemas sem solução.

2.2 PROTOCOLO P2P SEGURO PARA TROCA DE MENSAGENS

O protocolo desenvolvido por Warren (2012) visa resolver os problemas atuais que o protocolo SMTP apresenta como segurança das mensagens e envio de spam. A ideia é baseada no funcionamento do Bitcoin e trás alguns conceitos da arquitetura da criptomoeda para o mundo do correio eletrônico. Um desses conceitos, é um sistema de Proof of Work para envio de mensagens. Sempre que um determinado usuário decidir enviar uma mensagem, ele precisa realizar algum processamento computacional que é configurado para durar em média quatro minutos. Desse modo, um usuário ao tentar fazer envio de spam estaria limitado a enviar apenas uma mensagem a cada quatro minutos. Outro ponto inspirado no Bitcoin é o endereçamento baseado em chaves públicas. No

Comentado [FAP2]: traz

protocolo proposto, não existe o conceito de domínio de e-mail. O endereço utilizado para identificar um usuário é um hash gerado a partir das suas chaves. É impossível que qualquer um que não seja o remente ou o destinatário da mensagem identifique os endereços envolvidos nela.

O fluxo da proposta de Warren (2012) se inicia com um usuário querendo enviar uma mensagem para algum outro usuário da rede. O remetente precisa, antes de tudo, da chave pública do destinatário. Em posse da chave pública, ele faz a criptografia da mensagem e envia para a rede. Todos os nós conectados na rede recebem a mensagem, porém, o único que consegue ler é o detentor da chave privada correspondente a chave pública utilizada na criptografia. Ao receber a mensagem, o destinatário precisa enviar uma confirmação de recebimento. Caso o remetente não receba a confirmação em até dois dias ele faz a retransmissão após mais dois dias. O processo de retransmissão será feito até que o destinatário confirme o recebimento.

Pelo fato de a solução de Warren (2012) se propor a ser uma rede descentralizada, todos os nós da rede armazenam todas as mensagens, porém, para evitar a necessidade de uma alta capacidade de armazenamento, cada nó está configurado para apagar as mensagens não referentes a ele a cada dois dias. Mesmo assim é possível que a capacidade de armazenamento para guardar todas as mensagens dos últimos dois dias seja muito grande. Devido a isso, o autor implementou uma lógica que, após um determinado limite de armazenamento ser atingido, os nós começam a se agrupar em clusters dividindo o armazenamento entre si.

A solução de Warren (2012) também apresenta uma proposta para campanhas de marketing. Primeiramente, o dono da campanha precisa publicar uma chave que consiga descriptografar as mensagens enviadas por ele. Os usuários que quiserem receber as mensagens precisam pegar a chave e configurar o seu nó para aceitar mensagens para ela. Deste modo, sempre que um nó receber uma mensagem, ele vai tentar primeiramente abrir ela com a chave privada do usuário e, não tendo sucesso, vai tentar com todas as chaves presentes na lista de inscrições do nó.

O trabalho de Warren (2012) consegue resolver a grande maioria dos problemas atuais envolvendo correio eletrônico. Ele é fácil de usar e configurar e já possuí criptografia por padrão eliminando a necessidade de tecnologias como PGP/GPG que tendem a ser menos seguras devido a necessidade de compartilhamento da chave, e também serem de difícil utilização, principalmente por usuários não técnicos. Apesar dos seus vários pontos positivos, a solução tem o grande problema de não ser compatível com o SMTP. Desse modo, seria necessária uma mudança abrupta de tecnologia, o que acaba se tornando inviável devido a grande utilização dos serviços de e-mail. Além disso, por mais que o fato de ser impossível identificar as partes relacionadas em uma mensagem seja bom em casos que a privacidade seja necessária, isso acaba dificultando a adoção da tecnologia em diversos cenários como por exemplo no meio corporativo.

2.3 LIGAÇÃO DE E-MAILS COM TRANSAÇÕES DE CRIPTOMOEDAS

O trabalho desenvolvido por Grottenthaler (2017) busca resolver alguns problemas encontrados na implementação de correio eletrônico criando um relacionamento de cada e-mail enviado com uma transação de criptomoeda. As transações são salvas e validadas por uma Blockchain. O estudo realizado foca na solução de dois problemas: envio de spam e confirmação do recebimento de mensagens.

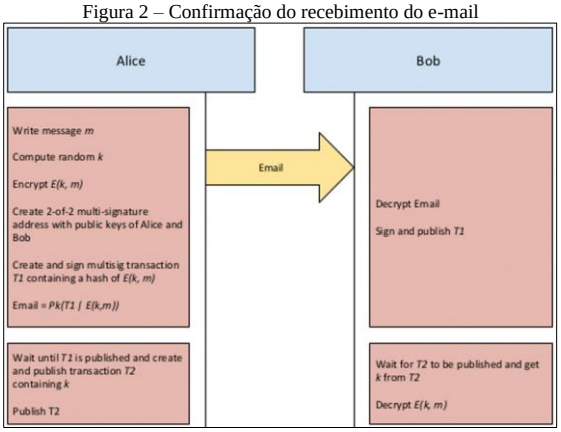
O fluxo da plataforma proposta por Grottenthaler (2017) inicia com um usuário querendo enviar um e-mail para outro usuário. O remetente, para realizar o envio do e-mail, precisa adicionar dois cabeçalhos na requisição: Mailcoin-Txid e Mailcoin-Header. O Mailcoin-Txid é o id da transação que será salva na Blockchain e serve para o destinatário identificar a transação e validar se a mesma é autêntica. O Mailcoin-Header contém informações referentes ao envio, sendo elas a versão do sistema, a data atual, o e-mail do destinatário e um valor gerado de modo aleatório que serve unicamente para evitar conflitos no momento em que um hash precisar ser gerado utilizando tais dados. Após a geração dos valores, o remetente cria uma nova transação na Blockchain contendo como id o Mailcoin-Txid e como valor um hash gerado a partir do Mailcoin-Header e então faz o envio do e-mail. O destinatário, ao receber o e-mail, recupera o Mailcoin-Txid do cabeçalho e busca pela transação na Blockchain. Se ele confirmar que a transação existe, ele recupera o valor do hash armazenado na transação, gera o hash utilizando o valor que vier no cabeçalho Mailcoin-Header e então compara os valores. Se forem iguais, a mensagem é autêntica.

Para o tratamento dos casos de spam, a solução criada por Grottenthaler (2017) exige que qualquer envio de e-mail exija algum custo financeiro para o remetente. Esse custo é descontado das criptomoedas que o usuário possui na Blockchain. O valor cobrado é muito baixo, porém, levando isso para um cenário de milhares de envios como acontece nos casos de spam, o valor final ficaria muito alto e dificultaria a prática de tal atividade. Um problema aparente é que qualquer pessoa teria custo para enviar e-mails, mesmo que ela não esteja enviando spam. Para resolver este problema a plataforma encoraja que, no momento em que um usuário receber um e-mail que o

mesmo identifique como autêntico, o valor do envio seja devolvido em outra transação para o remetente, assim eliminando o custo. Mesmo que um usuário desonesto não devolva o valor, o custo para envio de um e-mail acaba sendo pequeno, porém, ao não receber o valor de volta, o remetente pode decidir não enviar mais mensagens para aquele usuário, desencorajando assim tal prática.

A arquitetura do fluxo desenvolvido para identificar se um usuário de fato recebeu um e-mail é apresentada na Figura 2. Grottenthaler (2017) propôs um sistema baseado em dupla assinatura, onde, para um usuário conseguir ler um e-mail, ele obrigatoriamente precisa notificar o remetente que recebeu a mensagem. Por exemplo, a usuária Alice, ao enviar um e-mail para o usuário Bob, criptografa a mensagem com uma chave aleatória `k` e cria uma transação no qual assina com a sua chave privada. No momento que Bob recebe a transação, ele identifica que é uma transação de dupla assinatura e que então, para ler o conteúdo do e-mail, o mesmo precisa da chave `k`. Sendo assim, ele assina a transação recebida e a envia para a Blockchain. Quando Alice recebe a confirmação de que a transação foi assinada, a mesma cria uma nova transação contendo a chave `k`. Bob então com o valor da chave `k` consegue acessar o conteúdo do e-mail. Com tal sistema é possível identificar se o usuário recebeu o e-mail pois basta verificar se ele realizou o processo de assinatura da transação.

Figura 2 – Confirmação do recebimento do e-mail



Fonte: Grottenthaler (2017).

O trabalho de Grottenthaler (2017) consegue criar uma extensão para o protocolo STMP trazendo para o mesmo várias vantagens oriundas da utilização de Blockchain, porém, por se tratar de uma extensão, a base de tudo ainda continua sendo o SMTP. Desse modo, a solução não consegue resolver problemas que são inerentes do protocolo como, por exemplo, a garantia de imutabilidade das mensagens e a garantia que um determinado usuário enviou de fato uma mensagem com um determinado conteúdo.

3 PROPOSTA DO PROTOCOLO

Nesta seção serão apresentadas as justificativas para o desenvolvimento do estudo proposto, bem como um quadro comparativo com os trabalhos correlatos, os requisitos funcionais e não funcionais e a metodologia utilizada no desenvolvimento da solução.

3.1 JUSTIFICATIVA

No ano de 2019, o número global de usuários de correio eletrônico totalizava 3,9 bilhões de usuários, sendo que o número deve crescer para 4,3 bilhões até 2023 (NITRONEWS, 2020). Devido a essa grande massa de usuários, os servidores de e-mail passaram a ser um alvo muito atraente para criminosos. Eles buscam explorar as mais diversas vulnerabilidades encontradas em servidores de e-mail como propagação de vírus, vazamento de mensagens e falsificação de identidade (TRAININI et al, 2005). Além disso, existe uma tendência mundial para a concentração de usuários em servidores SMTP de terceiros como Gmail e Outlook. Isso acaba exigindo que os usuários confiem suas informações pessoais e mensagens a empresas privadas que podem realizar qualquer tipo de processo sobre elas, como modificar, excluir, ler e até mesmo falsificar as mensagens. Diante desse cenário, é

natural que existam trabalhos que tentam resolver tais problemas. O Quadro 1 faz uma análise das características dos trabalhos correlatos encontrados.

Quadro 1 – Comparativo entre os trabalhos correlatos

Características	Doichain	MailCoin	Bitmessage
Compatível com SMTP	Sim	Sim	Não
Sistema de Proof of Work	Não	Sim	Sim
Controle de inscrição em newsletter	Sim	Não	Não
Mensagens imutáveis	Não	Não	Sim
Assinatura de mensagens	Não	Sim	Sim
Controle para spam	Não	Sim	Sim
Identificação dos usuários	Sim	Sim	Não

Fonte: elaborado pelo autor.

Conforme análise do Quadro 1, é possível identificar que os trabalhos buscam resolver diferentes problemas. O Doichain, por estar unicamente centrado no processo de identificar se um usuário se inscreveu em um newsletter, acaba não abordando nenhum outro cenário. O MailCoin consegue abordar um universo maior de possibilidades, porém ele acaba deixando de fora um ponto importante que é a garantia de imutabilidade e histórico das mensagens. Isso acontece pois o mesmo mantém como base o protocolo SMTP. Já o Bitmessage, por se tratar de um protocolo novo consegue ter solução para a grande maioria dos problemas citados, porém, ele tem o grande ponto fraco de exigir uma completa mudança de tecnologia o que dificulta a migração para o protocolo. Além disso, o Bitmessage não permite que um terceiro usuário identifique os usuários envolvidos em uma mensagem. Isso se torna um impeditivo em ambientes corporativos.

Comentado [FAP3]: ele

Neste contexto, o presente trabalho se torna relevante na medida em que pretende utilizar uma tecnologia mais atualizada na perspectiva de superar problemas clássicos do protocolo SMTP. Pretende-se que ele não seja visto como base e sim um protocolo totalmente novo que já nasça sem a presença dos problemas acima citados. Além disso, ele se propõe a criar uma solução que seja compatível com o SMTP, tornando assim possível uma migração gradual de tecnologia e não exigindo uma mudança abrupta para os usuários.

3.2 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO

Os requisitos funcionais são:

a) permitir enviar um e-mail de um servidor que esteja utilizando o novo protocolo para um servidor SMTP que não esteja utilizando o novo protocolo;
b) permitir enviar um e-mail de um servidor SMTP para um servidor que esteja utilizando o novo protocolo;
c) permitir o envio de mensagens entre dois nós da rede utilizando o novo protocolo;
d) permitir identificação dos usuários através de um endereço;
e) permitir padrões diferentes de endereços para identificação de domínios pertencentes a organizações;
f) disponibilizar uma API que se comunique com a Blockchain;

Comentado [FAP4]: Para que?

Os requisitos não funcionais são:

a) implementar os nós da rede utilizando a linguagem Golang;
b) utilizar a arquitetura REST para a API para comunicação com a Blockchain;
c) receber mensagens na porta 8334;

Comentado [FAP5]: Por qual razão esta porta?

d) receber mensagens SMTP na porta 587;
e) armazenar as mensagens em uma Blockchain compartilhada entre todos os nós da rede;
f) obrigar a realização de um processo de Proof of Work para envio de mensagens;
g) assinar as mensagens com chave pública e garantir que só o usuário com a chave privada correspondente consiga visualizar o conteúdo da mesma;

Comentado [FAP6]: Assinaturas de mensagens de e-mail são padronizadas pelo S/MIME. Não falasses nada de assinatura até aqui, não faz parte dos teus objetivos, assinatura não é parte do SMTP, portanto não considero relevante para teu trabalho: tira isso!

3.3 METODOLOGIA

O trabalho será desenvolvido observando as seguintes etapas:

a) levantamento bibliográfico: realizar levantamento bibliográfico com relação a implementação de soluções utilizando Blockchain. Pesquisar também a bibliografia referente a implementação de servidores SMTP.

b) elicitação de requisitos: nesta etapa será feito o refinamento dos requisitos tomando como base a pesquisa realizada.

c) especificação da arquitetura da Blockchain: nesta etapa será definido como a Blockchain deverá funcionar. Será especificada a estrutura de armazenamento, assinaturas e envio dos e-mails.

d) desenvolvimento da Blockchain: será realizada a implementação da Blockchain utilizando a linguagem Golang. Será desenvolvida com base na arquitetura especificada no passo c.

e) desenvolvimento da API: nesta etapa será desenvolvida a API responsável por fazer a interface com a Blockchain.

f) desenvolvimento do servidor SMTP: implementar a compatibilidade dos nós com o protocolo SMTP.

g) testes: realizar o teste da rede, fazendo o envio entre nós dentro da rede, enviando de um servidor SMTP fora da rede para um servidor SMTP dentro da rede e realizar o teste contrário, enviando um e-mail de um nó dentro da rede para um servidor SMTP fora da rede.

As etapas serão realizadas nos períodos relacionados no Quadro 2.

Quadro 2 - Cronograma

	2021									
	fev.		mar.		abr.		mai.		jun.	
etapas / quinzenas	1	2	1	2	1	2	1	2	1	2
levantamento bibliográfico										
Elicitação de requisitos										
Especificação da arquitetura da Blockchain										
Desenvolvimento da Blockchain										
Desenvolvimento da API										
Desenvolvimento do servidor SMTP										
Testes										

Fonte: elaborado pelo autor.

4 REVISÃO BIBLIOGRÁFICA

Será inicialmente feito um estudo acerca das vulnerabilidades dos sistemas de correio eletrônico. A ideia é ter uma visão ampla dos problemas que devem ser resolvidos pela solução. O ponto de partida será a análise do trabalho de Trainini (2005), onde é possível ter uma visão geral das vulnerabilidades. Após isso, será feito o estudo sobre o trabalho de Ferraz (2015) para identificar como tais vulnerabilidades são exploradas.

Após o levantamento de vulnerabilidades, será feito o estudo referente a arquitetura e implementação da Blockchain. A obra base para o estudo é o trabalho de Nakamoto (2008), onde é descrita a arquitetura da primeira Blockchain implementada. Será revisada também a obra de Buterin (2013), que contém um estudo referente a uma plataforma descentralizada para criação de aplicações tendo como base a Blockchain.

Finalmente, será realizado o estudo referente a implementação do modo de compatibilidade com o protocolo SMTP. Para tal, será utilizado primeiramente a RFC 5321 (2008) para implementação das funcionalidades do servidor. Serão também utilizados os documentos da RFC 3501 (2003) e da RFC 1939 (1996) para implementação do acesso ao servidor para leitura dos e-mails.

REFERÊNCIAS

BUTERIN, Vitalik. **A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM**. [2013]. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 02 out. 2020.

Comentado [FAP7]: Sugiro não tratar disso neste trabalho

ESTADÃO. **Gmail supera 1 bilhão de usuários ativos no mundo**. [S.l.], [2016]. Disponível em: https://link.estadao.com.br/noticias/cultura-digital,gmail-supera-1-bilhao-de-usuarios-ativos-no-mundo,10000028528. Acesso em: 01 out. 2020.

FERRAZ, João Henrique et al. **Análise e Teste de Vulnerabilidade do Protocolo SMTP (Correio Eletrônico)**. São Paulo: Faculdade de Tecnologia de Bauru. 2015. Disponível em: http://www.fatecbauru.edu.br/ojs/index.php/CET/article/download/196/165. Acesso em: 30 set. 2020.

GROTTENTHALER, Martin. **MailCoin — Blockchain Technology for Emails**. 2017. Tese de mestrado - University of Applied Sciences Upper Austria, Hagenberg.

KRAUSE, Nico. **Doichain: The Atomic "Double-Opt-In" and email spam protection system on the blockchain**. [2018]. Disponível em: https://raw.githubusercontent.com/Doichain/dapp/master/doc/Doichain-WhitePaper.pdf. Acesso em: 01 out. 2020.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. [2008]. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 02 out. 2020.

NITRONEWS. **10 estatísticas de email marketing que você precisa conhecer**. [S.l.], [2020]. Disponível em: https://www.nitronews.com.br/blog/10-estatisticas-de-email-marketing-que-voce-precisa-conhecer/. Acesso em: 30 set. 2020.

OLIVEIRA, Bruno Ribeiro de. **Conheça a história do e-mail e como evoluiu até hoje**. [2020]. Disponível em: https://www.linknacional.com.br/blog/historia-do-email/. Acesso em: 30 set. 2020.

PEZZOTTI, Renato. **Com 3,9 bilhões de usuários no mundo, o que acontece na web em um minuto?**. São Paulo, [2019]. Disponível em: https://economia.uol.com.br/noticias/redacao/2019/04/01/com-39-bilhoes-de-usuarios-no-mundo-o-que-acontece-na-web-em-um-minuto.htm. Acesso em: 30 set. 2020.

RFC 5321. **Simple Mail Transfer Protocol**, [2008]. Disponível em: https://tools.ietf.org/html/rfc5321. Acesso em: 02 out. 2020.

RFC 3501**. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1**, [2003]. Disponível em: https://tools.ietf.org/html/rfc3501. Acesso em: 02 out. 2020.

RFC 1939. **Post Office Protocol - Version 3**, [1996]. Disponível em: https://tools.ietf.org/html/rfc1939. Acesso em: 02 out. 2020.

TRAININI, Paulo Ricardo Silveira et al. **Análise das Vulnerabilidades do Sistema de Correio Eletrônico**. Porto Alegre: Instituto de Informática, Universidade Federal do Rio Grande do Sul. 2005. Disponível em: https://www.researchgate.net/profile/Alexandre_Carissimi/publication/237499799_Analise_das_Vulnerabilidades_do_Sistema_de_Correio_Eletronico/links/564cd5cb08aeafc2aaaf8985/Analise-das-Vulnerabilidades-do-Sistema-de-Correio-Eletronico.pdf. Acesso em: 30 set. 2020.

WARREN, Jonathan. **Bitmessage: APeer-to-Peer Message Authentication and Delivery System**. [2012]. Disponível em: https://bitmessage.org/bitmessage.pdf. Acesso em: 01 out. 2020.

ASSINATURAS

(Atenção: todas as folhas devem estar rubricadas)

Assinatura do(a) Aluno(a): _____

Assinatura do(a) Orientador(a): _____

Assinatura do(a) Coorientador(a) (se houver): _____

Observações do orientador em relação a itens não atendidos do pré-projeto (se houver):

FORMULÁRIO DE AVALIAÇÃO – PROFESSOR AVALIADOR

Acadêmico(a):Ruan Schuartz Russi _____

Avaliador(a): Francisco Adell Péricas_____

	ASPECTOS AVALIADOS[1]	atende	atende parcialmente	não atende
ASPECTOS TÉCNICOS	1. INTRODUÇÃO O tema de pesquisa está devidamente contextualizado/delimitado?	X		
	O problema está claramente formulado?	X		
	1. OBJETIVOS O objetivo principal está claramente definido e é passível de ser alcançado?	X		
	Os objetivos específicos são coerentes com o objetivo principal?	X		
	2. TRABALHOS CORRELATOS São apresentados trabalhos correlatos, bem como descritas as principais funcionalidades e os pontos fortes e fracos?	X		
	3. JUSTIFICATIVA Foi apresentado e discutido um quadro relacionando os trabalhos correlatos e suas principais funcionalidades com a proposta apresentada?	X		
	São apresentados argumentos científicos, técnicos ou metodológicos que justificam a proposta?	X		
	São apresentadas as contribuições teóricas, práticas ou sociais que justificam a proposta?	X		
	4. REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO Os requisitos funcionais e não funcionais foram claramente descritos?		X	
	5. METODOLOGIA Foram relacionadas todas as etapas necessárias para o desenvolvimento do TCC?	X		
	Os métodos, recursos e o cronograma estão devidamente apresentados e são compatíveis com a metodologia proposta?	X		
	6. REVISÃO BIBLIOGRÁFICA (atenção para a diferença de conteúdo entre projeto e pré-projeto) Os assuntos apresentados são suficientes e têm relação com o tema do TCC?	X		
	As referências contemplam adequadamente os assuntos abordados (são indicadas obras atualizadas e as mais importantes da área)?	X		
ASPECTOS METODOLÓGICOS	7. LINGUAGEM USADA (redação) O texto completo é coerente e redigido corretamente em língua portuguesa, usando linguagem formal/científica?	X		
	A exposição do assunto é ordenada (as ideias estão bem encadeadas e a linguagem utilizada é clara)?	X		

PARECER – PROFESSOR AVALIADOR:
(PREENCHER APENAS NO PROJETO)

O projeto de TCC ser deverá ser revisado, isto é, necessita de complementação, se:

- qualquer um dos itens tiver resposta NÃO ATENDE;
- pelo menos **5 (cinco)** tiverem resposta ATENDE PARCIALMENTE.

PARECER: (X) APROVADO ( ) REPROVADO

Assinatura: Francisco Adell Péricas_____ Data: 18/10/2020 _____

[1] Quando o avaliador marcar algum item como atende parcialmente ou não atende, deve obrigatoriamente indicar os motivos no texto, para que o aluno saiba o porquê da avaliação.

CURSO DE CIÊNCIA DA COMPUTAÇÃO – TCC	
(x) PRÉ-PROJETO ( ) PROJETO	ANO/SEMESTRE:

PROTOCOLO PARA CORREIO ELETRÔNICO BASEADO EM BLOCKCHAIN

Ruan Schuartz Russi

Mauro Marcelo Mattos

1 INTRODUÇÃO

A popularidade do protocolo Simple Mail Transfer Protocol (SMTP) é inegável. Estima-se que, a cada minuto, 188 milhões de novos e-mails são enviados (PEZZOTTI, 2019). No ano de 2019, o número global de usuários de correio eletrônico totalizava 3,9 bilhões de usuários, sendo que o número deve crescer para 4,3 bilhões até 2023, número esse equiparado a metade da população mundial (NITRONEWS, 2020). Toda essa popularidade é atribuída a diversos fatores, sendo um deles a sua idade. O e-mail é considerado o serviço online mais antigo do mundo, tendo a primeira mensagem da história sido enviada no ano de 1971 (OLIVEIRA, 2020).

Apesar de ser uma tecnologia difundida e robusta, a idade da solução acaba trazendo para a mesma alguns pontos negativos. Na época em que os serviços de correio eletrônico foram desenhados, a internet como se apresenta hoje não existia e as redes de computadores existentes eram restritas a ambientes acadêmicos, não sendo liberado acesso para a população (TRAININI, et al, 2005). Neste ambiente controlado, a preocupação com a segurança da informação era mínima e dispositivos de segurança geralmente não eram implementados. O cenário mudou com o advento da criação e a popularização da internet. A rede se tornou um lugar hostil e perigoso, sendo utilizada por usuários mal-intencionados para a realização de práticas ilícitas. Por não ter sido criado com este ambiente hostil em mente, os serviços de correio eletrônico possuem uma diversidade de vulnerabilidades passíveis de serem exploradas como envio de spam, propagação de vírus, vazamento de mensagens e falsificação de identidade (TRAININI et al, 2005).

Uma característica importante dos servidores de e-mail é que eles formam uma rede descentralizada não existindo assim uma entidade com poder absoluto sobre as outras. Apesar disso, a implementação, devido a época em que foi feita, não aproveita características importantes de redes descentralizadas modernas. A Blockchain por exemplo, tecnologia criada para dar vida ao Bitcoin, permite ter um histórico imutável de tudo que foi feito. A implementação do Bitcoin consegue garantir que um determinado usuário realizou uma transação financeira para outro de forma imutável. Já com o SMTP, é impossível determinar de modo fidedigno que um usuário enviou uma mensagem para outro. Além disso, atualmente é comum a utilização de serviços de e-mail de terceiros. Em 2016, o serviço de correio eletrônico da Google, o Gmail, chegou a marca de ~~1~~ um bilhão de usuários ativos mensalmente (ESTADÃO, 2016). Essa dependência com entidades terceiras acaba exigindo que os usuários tenham plena confiança nas mesmas pois nada impede que as mesmas modifiquem, excluam ou vazem mensagem privadas. Elas podem chegar até ao ponto de mandarem mensagens se passando pelo usuário.

Para resolver os problemas acima citados, o ideal seria a implementação de um protocolo totalmente novo que já nasça sem a presença destas falhas. O problema é que, devido a ~~já relatada~~ alta utilização dos serviços de e-mail, uma mudança abrupta de tecnologia se torna inviável, pois envolve uma mudança significativa na rotina de milhões de usuários. Diante deste cenário, o presente trabalho propõe o desenvolvimento ~~e a implementação~~ de um protocolo baseado em Blockchain que consiga enviar e receber mensagens de correio eletrônico de modo descentralizado e seguro, ~~e que seja~~ compatível com o protocolo SMTP permitindo assim uma migração gradual de tecnologia.

1.1 OBJETIVOS

O objetivo deste trabalho é disponibilizar um protocolo de envio e recebimento de e-mails baseado em Blockchain e que seja compatível com o protocolo SMTP.

Os objetivos específicos são:

a) Especificar um modelo de envio e recebimento de mensagens baseado no conceito de blockchain;
b) Desenvolver um protótipo de cliente para demonstrar a funcionalidade do protocolo;
c) Criar um conjunto de casos de testes para validar o protocolo desenvolvido.

2 TRABALHOS CORRELATOS

Nesta seção são apresentados trabalhos que apresentam semelhança com os principais objetivos do trabalho proposto. O primeiro trabalho apresenta é a implementação de uma Blockchain capaz de armazenar e validar inscrições de usuários em *newsletters* (KRAUSE, 2018). O segundo é o estudo e implementação de um protocolo p2p para a troca segura de mensagens (WARREN, 2012). Por fim, na seção 2.3 será apresentada o

Comentado [AS1]: De quem?

Comentado [AS2]: O que significa?

Comentado [AS3]: Rever.

Comentado [AS4]: Use linguagem formal

Comentado [AS5]: Quem?

Comentado [AS6]: - Não está no estilo.
- Enumeração inicia com letra minúscula.

Formatado: Fonte: Itálico

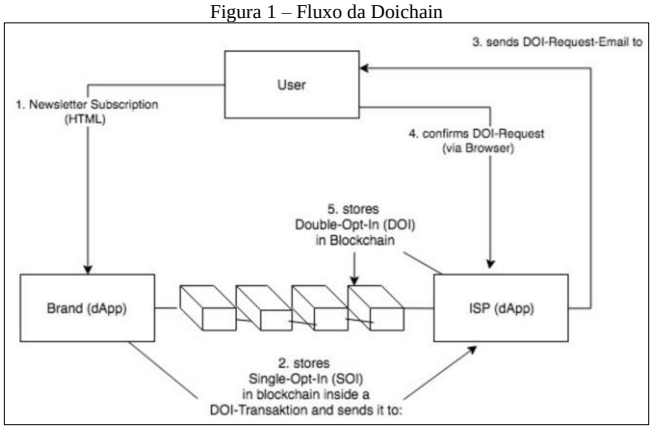
trabalho de AUTOR(ANO) ~~uma dissertação de mestrado~~ que busca fazer a ligação entre envio de e-mails e transações de criptomoeda ~~(GROTTENTHALER;2017)~~.

2.1 CONTROLE DE INSCRIÇÃO PARA RECEBIMENTE DE E-MAIL PROMOCIONAL

O trabalho desenvolvido por Krause (2018) consiste em um sistema baseado em Blockchain que é capaz de provar que um determinado usuário se inscreveu em uma campanha de mail marketing. A motivação para o trabalho é resolver alguns casos comuns de spam e possibilitar a adesão de empresas de mail marketing a leis de proteção de dados. Para tal, o autor propôs uma Blockchain que armazena as inscrições dos usuários e pode ser consultada pelo dono da campanha de marketing antes de ~~o mesmo~~ enviar algum e-mail para o usuário. Para se comunicar com a Blockchain, o autor desenvolveu um aplicativo chamado dApp que serve unicamente para realizar esta comunicação. Tanto o dono da campanha de marketing quanto o dono do servidor de e-mail que o usuário está utilizando precisam configurar uma instância local do dApp.

O fluxo da plataforma proposta por Krause (2018) pode ser conferido na Figura 1. Primeiramente, o usuário (User) se inscreve em alguma campanha de e-mail. Um método comum de inscrição é a submissão do e-mail em um formulário presente em algum site. A empresa responsável pela campanha (Brand), ao receber a inscrição envia para a Blockchain uma transação ainda não confirmada. O servidor de e-mail do usuário (Internet Service Provider - ISP), ao receber a transação não confirmada, envia ao usuário (User) um e-mail pedindo que a ~~o mesmo~~ confirmação~~e~~ da inscrição. Caso a inscrição seja confirmada, a transação é confirmada na Blockchain. Sendo assim, sempre que for enviar algum e-mail, o dono da campanha pode checar se o usuário realmente se inscreveu para aquela campanha.

Figura 1 – Fluxo da Doichain



Fonte: Krause (2018).

O trabalho de Krause (2018) consegue de fato ser uma solução para o problema que ele se propõe a resolver, porém, implantar tal solução em um cenário produtivo acaba exigindo bastante esforço. Por mais que a migração seja transparente para o usuário, a solução exige que pelo menos os servidores de e-mail mais populares do mercado se adequem a plataforma para que ~~a mesma~~ tenha algum efeito. Além disso, os donos das campanhas precisariam também configurar do seu lado o dApp para passar a validar as inscrições dos usuários. O grande ponto é, mesmo exigindo tamanho esforço, a plataforma se limita a resolver um cenário muito específico deixando ainda uma série de problemas sem solução.

2.2 PROTOCOLO P2P SEGURO PARA TROCA DE MENSAGENS

O protocolo desenvolvido por Warren (2012) visa resolver os problemas atuais que o protocolo SMTP apresenta como segurança das mensagens e envio de spam. A ideia é baseada no funcionamento do Bitcoin e ~~trás~~traz alguns conceitos da arquitetura da criptomoeda para o mundo do correio eletrônico. Um desses conceitos, é um sistema de *Proof of Work* para envio de mensagens. Sempre que um determinado usuário decidir enviar uma

Comentado [AS7]: Relacionadas?

Comentado [AS8]: Coloque o recurso de referência cruzada para a figura. Faça isso em todo o texto.

Comentado [AS9]: Redundante. Rever.

Comentado [AS10]: confuso

Formatado: Fonte: Itálico

mensagem, ele precisa realizar algum processamento computacional que é configurado para durar em média quatro minutos. Desse modo, um usuário ao tentar fazer envio de spam estaria limitado a enviar apenas uma mensagem a cada quatro minutos. Outro ponto inspirado no Bitcoin é o endereçamento baseado em chaves públicas. No protocolo proposto, não existe o conceito de domínio de e-mail. O endereço utilizado para identificar um usuário é um *hash* gerado a partir das suas chaves. É impossível que qualquer um que não seja o remente ou o destinatário da mensagem identifique os endereços envolvidos nela.

O fluxo da proposta de Warren (2012) se inicia com um usuário querendo enviar uma mensagem para algum outro usuário da rede. O remetente precisa, antes de tudo, da chave pública do destinatário. Em posse da chave pública, ele faz a criptografia da mensagem e envia para a rede. Todos os nós conectados na rede recebem a mensagem, porém, o único que consegue ler é o detentor da chave privada correspondente a chave pública utilizada na criptografia. Ao receber a mensagem, o destinatário precisa enviar uma confirmação de recebimento. Caso o remetente não receba a confirmação em até dois dias ele faz a retransmissão após mais dois dias. O processo de retransmissão será feito até que o destinatário confirme o recebimento.

Pelo fato de a solução de Warren (2012) se propor a ser uma rede descentralizada, todos os nós da rede armazenam todas as mensagens, porém, para evitar a necessidade de uma alta capacidade de armazenamento, cada nó está configurado para apagar as mensagens não referentes a ele a cada dois dias. Mesmo assim é possível que a capacidade de armazenamento para guardar todas as mensagens dos últimos dois dias seja muito grande. Devido a isso, o autor implementou uma lógica que, após um determinado limite de armazenamento ser atingido, os nós começam a se agrupar em clusters dividindo o armazenamento entre si.

A solução de Warren (2012) também apresenta uma proposta para campanhas de marketing. Primeiramente, o dono da campanha precisa publicar uma chave que consiga descriptografar as mensagens enviadas por ele. Os usuários que quiserem receber as mensagens precisam pegar a chave e configurar o seu nó para aceitar mensagens para ela. Deste modo, sempre que um nó receber uma mensagem, ele vai tentar primeiramente abrir ela com a chave privada do usuário e, não tendo sucesso, vai tentar com todas as chaves presentes na lista de inscrições do nó.

O trabalho de Warren (2012) consegue resolver a grande maioria dos problemas atuais envolvendo correio eletrônico. Ele é fácil de usar e configurar e já possuí criptografia por padrão eliminando a necessidade de tecnologias como PGP/GPG que tendem a ser menos seguras devido a necessidade de compartilhamento da chave, e também serem de difícil utilização, principalmente por usuários não técnicos. Apesar dos seus vários pontos positivos, a solução tem o grande problema de não ser compatível com o SMTP. Desse modo, seria necessária uma mudança abrupta de tecnologia, o que acaba se tornando inviável devido a grande utilização dos serviços de e-mail. Além disso, por mais que o fato de ser impossível identificar as partes relacionadas em uma mensagem seja bom em casos que a privacidade seja necessária, isso acaba dificultando a adoção da tecnologia em diversos cenários como por exemplo no meio corporativo.

2.3 LIGAÇÃO DE E-MAILS COM TRANSAÇÕES DE CRIPTOMOEDAS

O trabalho desenvolvido por Grottenthaler (2017) busca resolver alguns problemas encontrados na implementação de correio eletrônico criando um relacionamento de cada e-mail enviado com uma transação de criptomoeda. As transações são salvas e validadas por uma Blockchain. O estudo realizado foca na solução de dois problemas: envio de spam e confirmação do recebimento de mensagens.

O fluxo da plataforma proposta por Grottenthaler (2017) inicia com um usuário querendo enviar um e-mail para outro usuário. O remetente, para realizar o envio do e-mail, precisa adicionar dois cabeçalhos na requisição: Mailcoin-Txid e Mailcoin-Header. O Mailcoin-Txid é o id da transação que será salva na Blockchain e serve para o destinatário identificar a transação e validar se ~~a mesma~~ é autêntica. O Mailcoin-Header contém informações referentes ao envio, sendo elas a versão do sistema, a data atual, o e-mail do destinatário e um valor gerado de modo aleatório que serve unicamente para evitar conflitos ~~no momento em que~~quando um hash precisar ser gerado utilizando tais dados. Após a geração dos valores, o remetente cria uma ~~nova~~ transação na Blockchain contendo como id o Mailcoin-Txid e como valor um hash gerado a partir do Mailcoin-Header e então faz o envio do e-mail. O destinatário, ao receber o e-mail, recupera o Mailcoin-Txid do cabeçalho e busca pela transação na Blockchain. Se ele confirmar que a transação existe, ele recupera o valor do hash armazenado na transação, gera o hash utilizando o valor que vier no cabeçalho Mailcoin-Header e então compara os valores. Se forem iguais, a mensagem é autêntica.

Para o tratamento dos casos de spam, a solução criada por Grottenthaler (2017) exige que qualquer envio de e-mail exija algum custo financeiro para o remetente. Esse custo é descontado das criptomoedas que o usuário possui na Blockchain. O valor cobrado é muito baixo, porém, levando isso para um cenário de milhares de envios

Comentado [AS11]: explique o que é.

Formatado: Fonte: Itálico

Comentado [AS12]: confuso

Comentado [AS13]: Frase longa. Rever.

Comentado [AS14]: Quem?
- Frase longa. Rever.

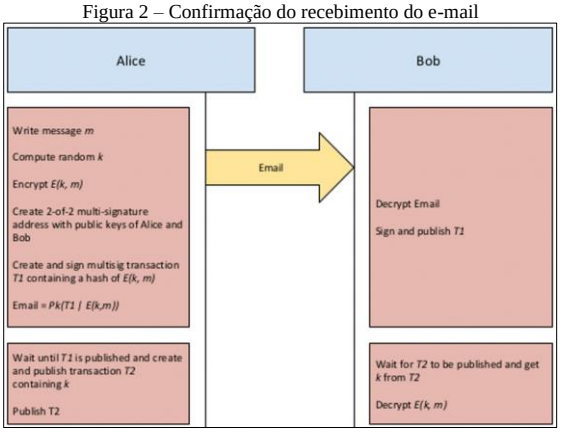
Comentado [AS15]: Frase confusa e longa. Rever.

como acontece nos casos de spam, o valor final ficaria muito alto e dificultaria a prática de tal atividade. Um problema aparente é que qualquer pessoa teria custo para enviar e-mails, mesmo que ela não esteja enviando spam. Para resolver este problema a plataforma encoraja que, no momento em que um usuário receber um e-mail que o mesmo identifique como autêntico, o valor do envio seja devolvido em outra transação para o remetente, assim eliminando o custo. Mesmo que um usuário desonesto não devolva o valor, o custo para envio de um e-mail acaba sendo pequeno, porém, ao não receber o valor de volta, o remetente pode decidir não enviar mais mensagens para aquele usuário, desencorajando assim tal prática.

Comentado [AS16]: Rever frase.

A arquitetura do fluxo desenvolvido para identificar se um usuário de fato recebeu um e-mail é apresentada na Figura 2. Grottenthaler (2017) propôs um sistema baseado em dupla assinatura, ~~onde~~na qual, para um usuário conseguir ler um e-mail, ele obrigatoriamente precisa notificar o remetente que recebeu a mensagem. Por exemplo, a usuária Alice~~,~~ ao enviar um e-mail para o usuário Bob, criptografa a mensagem com uma chave aleatória `k` e cria uma transação no qual assina com a sua chave privada. No momento que Bob recebe a transação, ele identifica que é uma transação de dupla assinatura e que então, para ler o conteúdo do e-mail~~, o mesmo~~ precisa da chave `k`. Sendo assim, ele assina a transação recebida e a envia para a Blockchain. Quando Alice recebe a confirmação de que a transação foi assinada, ~~a mesma~~ela cria uma nova transação contendo a chave `k`. Bob então com o valor da chave `k` consegue acessar o conteúdo do e-mail. Com tal sistema é possível identificar se o usuário recebeu o e-mail pois basta verificar se ele realizou o processo de assinatura da transação.

Figura 2 – Confirmação do recebimento do e-mail



Fonte: Grottenthaler (2017).

O trabalho de Grottenthaler (2017) consegue criar uma extensão para o protocolo STMP trazendo para ~~o mesmo~~ várias vantagens oriundas da utilização de Blockchain, porém, por se tratar de uma extensão, a base de tudo ainda continua sendo o SMTP. Desse modo, a solução não consegue resolver problemas que são inerentes do protocolo como, por exemplo, a garantia de imutabilidade das mensagens e a garantia que um determinado usuário enviou de fato uma mensagem com um determinado conteúdo.

3 PROPOSTA DO PROTOCOLO

Nesta seção serão apresentadas as justificativas para o desenvolvimento do estudo proposto, bem como um quadro comparativo com os trabalhos correlatos, os requisitos funcionais e não funcionais e a metodologia utilizada no desenvolvimento da solução.

3.1 JUSTIFICATIVA

No ano de 2019, o número global de usuários de correio eletrônico totalizava 3,9 bilhões de usuários, sendo que o número deve crescer para 4,3 bilhões até 2023 (NITRONEWS, 2020). Devido a essa grande massa de usuários, os servidores de e-mail passaram a ser um alvo muito atraente para criminosos. Eles buscam explorar as mais diversas vulnerabilidades encontradas em servidores de e-mail como propagação de vírus, vazamento de mensagens e falsificação de identidade (TRAININI et al, 2005). Além disso, existe uma tendência mundial para a concentração de usuários em servidores SMTP de terceiros como Gmail e Outlook. Isso acaba exigindo que os

Comentado [AS17]: Informação repetida da introdução

Comentado [AS18]: et al. (em itálico e com “.”). Rever todos no texto.

usuários confiem suas informações pessoais e mensagens a empresas privadas que podem realizar qualquer tipo de processo sobre elas, como modificar, excluir, ler e até mesmo falsificar as mensagens. Diante desse cenário, é natural que existam trabalhos que tentam resolver tais problemas. O Quadro 1 faz uma análise das características dos trabalhos correlatos encontrados.

Comentado [AS19]: Use linguagem formal

Comentado [AS20]: Coloque o recurso de referência cruzada para quadro/tabela. Faça isso em todo o texto.

Quadro 1 – Comparativo entre os trabalhos correlatos

Características	Doichain	MailCoin	Bitmessage
Compatível com SMTP	Sim	Sim	Não
Sistema de Proof of Work	Não	Sim	Sim
Controle de inscrição em newsletter	Sim	Não	Não
Mensagens imutáveis	Não	Não	Sim
Assinatura de mensagens	Não	Sim	Sim
Controle para spam	Não	Sim	Sim
Identificação dos usuários	Sim	Sim	Não

Fonte: elaborado pelo autor.

Conforme análise do Quadro 1, é possível identificar que os trabalhos buscam resolver diferentes problemas. O Doichain, por estar unicamente centrado no processo de identificar se um usuário se inscreveu em um newsletter, acaba não abordando nenhum outro cenário. O MailCoin consegue abordar um universo maior de possibilidades, porém ~~ele~~ acaba deixando de fora um ponto importante que é a garantia de imutabilidade e histórico das mensagens. Isso acontece pois ~~o mesmo~~ mantém como base o protocolo SMTP. Já o Bitmessage, por se tratar de um protocolo novo consegue ter solução para a grande maioria dos problemas citados, porém, ele tem o grande ponto fraco de exigir uma completa mudança de tecnologia, o que dificulta a migração para o protocolo. Além disso, o Bitmessage não permite que um terceiro usuário identifique os usuários envolvidos em uma mensagem. Isso se torna um impeditivo em ambientes corporativos.

Comentado [AS21]: Evite usar superlativos.

Neste contexto, o presente trabalho se torna relevante na medida em que pretende utilizar uma tecnologia mais atualizada na perspectiva de superar problemas clássicos do protocolo SMTP. Pretende-se que ele não seja visto como base e sim um protocolo totalmente novo que já nasça sem a presença dos problemas acima citados. Além disso, ele se propõe a criar uma solução que seja compatível com o SMTP, tornando assim possível uma migração gradual de tecnologia e não exigindo uma mudança abrupta para os usuários.

Comentado [AS22]: Qual a contribuição teóricas, práticas ou sociais que justificam a proposta.

Comentado [AS23]: Use linguagem formal

3.2 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO

Os requisitos funcionais são:

a) permitir enviar um e-mail de um servidor que esteja utilizando o novo protocolo para um servidor SMTP que não esteja utilizando o novo protocolo;
b) permitir enviar um e-mail de um servidor SMTP para um servidor que esteja utilizando o novo protocolo;
c) permitir o envio de mensagens entre dois nós da rede utilizando o novo protocolo;
d) permitir identificação dos usuários através de um endereço;
e) permitir padrões diferentes de endereços para identificação de domínios pertencentes a organizações;
f) disponibilizar uma API que se comunique com a Blockchain~~.~~;

Os requisitos não funcionais são:

a) implementar os nós da rede utilizando a linguagem Golang;
b) utilizar a arquitetura REST para a API para comunicação com a Blockchain;
c) receber mensagens na porta 8334;
d) receber mensagens SMTP na porta 587;
e) armazenar as mensagens em uma Blockchain compartilhada entre todos os nós da rede;
f) obrigar a realização de um processo de Proof of Work para envio de mensagens;

g) assinar as mensagens com chave pública e garantir que só o usuário com a chave privada correspondente consiga visualizar o conteúdo ~~da mesma~~correspondente.~~;~~

3.3 METODOLOGIA

O trabalho será desenvolvido observando as seguintes etapas:

a) levantamento bibliográfico: realizar levantamento bibliográfico com relação a implementação de soluções utilizando Blockchain. Pesquisar também a bibliografia referente a implementação de servidores SMTP~~;~~

b) elicitação de requisitos: nesta etapa será feito o refinamento dos requisitos tomando como base a pesquisa realizada~~;~~

c) especificação da arquitetura da Blockchain: nesta etapa será definido como a Blockchain deverá funcionar. Será especificada a estrutura de armazenamento, assinaturas e envio dos e-mails~~;~~

d) desenvolvimento da Blockchain: será realizada a implementação da Blockchain utilizando a linguagem Golang. Será desenvolvida com base na arquitetura especificada no passo c~~;~~

e) desenvolvimento da API: nesta etapa será desenvolvida a API responsável por fazer a interface com a Blockchain~~;~~

f) desenvolvimento do servidor SMTP: implementar a compatibilidade dos nós com o protocolo SMTP~~;~~

g) testes: realizar o teste da rede, fazendo o envio entre nós dentro da rede, enviando de um servidor SMTP fora da rede para um servidor SMTP dentro da rede e realizar o teste contrário, enviando um e-mail de um nó dentro da rede para um servidor SMTP fora da rede.

Comentado [AS24]: Confuso. Rever.

As etapas serão realizadas nos períodos relacionados no Quadro 2.

Quadro 2 - Cronograma

	2021									
	fev.		mar.		abr.		mai.		jun.	
etapas / quinzenas	1	2	1	2	1	2	1	2	1	2
levantamento bibliográfico										
Elicitação de requisitos										
Especificação da arquitetura da Blockchain										
Desenvolvimento da Blockchain										
Desenvolvimento da API										
Desenvolvimento do servidor SMTP										
Testes										

Fonte: elaborado pelo autor.

Comentado [AS25]: Início na segunda quinzena de fevereiro.

4 REVISÃO BIBLIOGRÁFICA

Será inicialmente feito um estudo acerca das vulnerabilidades dos sistemas de correio eletrônico. A ideia é ter uma visão ampla dos problemas que devem ser resolvidos pela solução. O ponto de partida será a análise do trabalho de Trainini (2005), onde é possível ter uma visão geral das vulnerabilidades. Após isso, será feito o estudo sobre o trabalho de Ferraz (2015) para identificar como tais vulnerabilidades são exploradas.

Comentado [AS26]: Falta uma introdução da seção.

Comentado [AS27]: Escreva em linguagem formal

Após o levantamento de vulnerabilidades, será feito o estudo referente a arquitetura e implementação da Blockchain. A obra base para o estudo é o trabalho de Nakamoto (2008), onde é descrita a arquitetura da primeira Blockchain implementada. Será revisada também a obra de Buterin (2013), que contém um estudo referente a uma plataforma descentralizada para criação de aplicações tendo como base a Blockchain.

Finalmente, será realizado o estudo referente a implementação do modo de compatibilidade com o protocolo SMTP. Para tal, será utilizado primeiramente a RFC 5321 (2008) para implementação das funcionalidades do servidor. Serão também utilizados os documentos da RFC 3501 (2003) e da RFC 1939 (1996) para implementação do acesso ao servidor para leitura dos e-mails.

REFERÊNCIAS

BUTERIN, Vitalik. **A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM**. [2013]. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 02 out. 2020.

ESTADÃO. **Gmail supera 1 bilhão de usuários ativos no mundo**. [S.l.], [2016]. Disponível em: https://link.estadao.com.br/noticias/cultura-digital,gmail-supera-1-bilhao-de-usuarios-ativos-no-mundo,10000028528. Acesso em: 01 out. 2020.

FERRAZ, João Henrique et al. **Análise e Teste de Vulnerabilidade do Protocolo SMTP (Correio Eletrônico)**. São Paulo: Faculdade de Tecnologia de Bauru. 2015. Disponível em: http://www.fatecbauru.edu.br/ojs/index.php/CET/article/download/196/165. Acesso em: 30 set. 2020.

GROTTENTHALER, Martin. **MailCoin — Blockchain Technology for Emails**. 2017. Tese de mestrado - University of Applied Sciences Upper Austria, Hagenberg.

KRAUSE, Nico. **Doichain: The Atomic "Double-Opt-In" and email spam protection system on the blockchain**. [2018]. Disponível em: https://raw.githubusercontent.com/Doichain/dapp/master/doc/Doichain-WhitePaper.pdf. Acesso em: 01 out. 2020.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. [2008]. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 02 out. 2020.

NITRONEWS. **10 estatísticas de email marketing que você precisa conhecer**. [S.l.], [2020]. Disponível em: https://www.nitronews.com.br/blog/10-estatisticas-de-email-marketing-que-voce-precisa-conhecer/. Acesso em: 30 set. 2020.

OLIVEIRA, Bruno Ribeiro de. **Conheça a história do e-mail e como evoluiu até hoje**. [2020]. Disponível em: https://www.linknacional.com.br/blog/historia-do-email/. Acesso em: 30 set. 2020.

PEZZOTTI, Renato. **Com 3,9 bilhões de usuários no mundo, o que acontece na web em um minuto?**. São Paulo, [2019]. Disponível em: https://economia.uol.com.br/noticias/redacao/2019/04/01/com-39-bilhoes-de-usuarios-no-mundo-o-que-acontece-na-web-em-um-minuto.htm. Acesso em: 30 set. 2020.

RFC 5321. **Simple Mail Transfer Protocol**, [2008]. Disponível em: https://tools.ietf.org/html/rfc5321. Acesso em: 02 out. 2020.

RFC 3501**. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1**, [2003]. Disponível em: https://tools.ietf.org/html/rfc3501. Acesso em: 02 out. 2020.

RFC 1939. **Post Office Protocol - Version 3**, [1996]. Disponível em: https://tools.ietf.org/html/rfc1939. Acesso em: 02 out. 2020.

TRAININI, Paulo Ricardo Silveira et al. **Análise das Vulnerabilidades do Sistema de Correio Eletrônico**. Porto Alegre: Instituto de Informática, Universidade Federal do Rio Grande do Sul. 2005. Disponível em: https://www.researchgate.net/profile/Alexandre_Carissimi/publication/237499799_Analise_das_Vulnerabilidades_do_Sistema_de_Correio_Eletronico/links/564cd5cb08aeafc2aaaf8985/Analise-das-Vulnerabilidades-do-Sistema-de-Correio-Eletronico.pdf. Acesso em: 30 set. 2020.

WARREN, Jonathan. **Bitmessage: APeer-to-Peer Message Authentication and Delivery System**. [2012]. Disponível em: https://bitmessage.org/bitmessage.pdf. Acesso em: 01 out. 2020.

ASSINATURAS

(Atenção: todas as folhas devem estar rubricadas)

Assinatura do(a) Aluno(a): _____

Assinatura do(a) Orientador(a): _____

Assinatura do(a) Coorientador(a) (se houver): _____

Observações do orientador em relação a itens não atendidos do pré-projeto (se houver):

FORMULÁRIO DE AVALIAÇÃO – PROFESSOR TCC I

Acadêmico(a): Ruan Schuartz Russi

Avaliador(a): Andreza Sartori

	ASPECTOS AVALIADOS[1]	atende	atende parcialmente	não atende
ASPECTOS TÉCNICOS	1. INTRODUÇÃO O tema de pesquisa está devidamente contextualizado/delimitado?	x		
	O problema está claramente formulado?	x		
	2. OBJETIVOS O objetivo principal está claramente definido e é passível de ser alcançado?	x		
	Os objetivos específicos são coerentes com o objetivo principal?	x		
	3. JUSTIFICATIVA São apresentados argumentos científicos, técnicos ou metodológicos que justificam a proposta?	x		
	São apresentadas as contribuições teóricas, práticas ou sociais que justificam a proposta?		x	
	4. METODOLOGIA Foram relacionadas todas as etapas necessárias para o desenvolvimento do TCC?	x		
	Os métodos, recursos e o cronograma estão devidamente apresentados?		x	
	5. REVISÃO BIBLIOGRÁFICA (atenção para a diferença de conteúdo entre projeto e pré-projeto) Os assuntos apresentados são suficientes e têm relação com o tema do TCC?		x	
ASPECTOS METODOLÓGICOS	6. LINGUAGEM USADA (redação) O texto completo é coerente e redigido corretamente em língua portuguesa, usando linguagem formal/científica?			x
	A exposição do assunto é ordenada (as ideias estão bem encadeadas e a linguagem utilizada é clara)?			x
	7. ORGANIZAÇÃO E APRESENTAÇÃO GRÁFICA DO TEXTO A organização e apresentação dos capítulos, seções, subseções e parágrafos estão de acordo com o modelo estabelecido?			
	8. ILUSTRAÇÕES (figuras, quadros, tabelas) As ilustrações são legíveis e obedecem às normas da ABNT?		x	
	9. REFERÊNCIAS E CITAÇÕES As referências obedecem às normas da ABNT?	x		
	As citações obedecem às normas da ABNT?	x		
	Todos os documentos citados foram referenciados e vice-versa, isto é, as citações e referências são consistentes?	x		

PARECER – PROFESSOR DE TCC I OU COORDENADOR DE TCC
(PREENCHER APENAS NO PROJETO):

O projeto de TCC será reprovado se:
- qualquer um dos itens tiver resposta NÃO ATENDE;
- pelo menos **4 (quatro)** itens dos **ASPECTOS TÉCNICOS** tiverem resposta ATENDE PARCIALMENTE; ou
- pelo menos **4 (quatro)** itens dos **ASPECTOS METODOLÓGICOS** tiverem resposta ATENDE PARCIALMENTE.

PARECER: ( ) APROVADO ( ) REPROVADO

Assinatura: Andreza Sartori_____ Data: 20/10/2020 _____

[1] Quando o avaliador marcar algum item como atende parcialmente ou não atende, deve obrigatoriamente indicar os motivos no texto, para que o aluno saiba o porquê da avaliação.