

**CENTRO UNIVERSITÁRIO DE CIÊNCIAS E TECNOLOGIA DO MARANHÃO -
UNIFACEMA
CURSO DE ANÁLISE E DESENVOLVIMENTO DE SISTEMAS – ADS**

SÁVIO PALÁCIO FONTES

BLOCKNOTARY: desenvolvimento de Blockchain para serviços de cartório.

CAXIAS-MA

2019

SÁVIO PALÁCIO FONTES

BLOCKNOTARY: desenvolvimento de Blockchain para serviços de cartório.

Trabalho monográfico apresentado à Coordenação do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Centro Universitário de Ciências e Tecnologia do Maranhão - UNIFACEMA, para a obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: Esp. Natássia Rafaelle Medeiros Siqueira.

CAXIAS-MA

2019

SÁVIO PALÁCIO FONTES

BLOCKNOTARY: desenvolvimento de Blockchain para serviços de cartório

Trabalho monográfico apresentado à
Coordenação do Curso de Tecnologia em
Análise e Desenvolvimento de Sistemas do
Centro Universitário de Ciências e
Tecnologia do Maranhão - UNIFACEMA,
para a obtenção do grau de Tecnólogo em
Análise e Desenvolvimento de Sistemas.

DATA DE APROVAÇÃO: ____ de ____ de ____

BANCA EXAMINADORA

Esp. Natássia Rafaelle Medeiros Siqueira - UNIFACEMA
Orientador

- UNIFACEMA
Membro

- UNIFACEMA
Membro

AGRADECIMENTOS

Em memória do meu avô, José Maria Fontes. Agradeço tudo em primeiro lugar a ele, que tanto me ajudou na minha caminhada até aqui, quando estava ao meu lado deu todo o suporte ao seu alcance.

A meus pais e minha vó, que estão sempre ao meu lado me dando suporte emocional e financeiro nessa longa jornada árdua. Sem eles não teria condições de chegar onde estou hoje. Muito obrigado por tudo.

A minha namorada, Thamara. Que me deu carinho, boa conversa, sempre ajudando a superar a tristeza e cansaço do dia a dia.

A minha professora e orientadora Natassia, que esteve nesse período guardando um pouco do seu tempo corrido em finais de semana e até mesmo em madrugadas, me cobrando, lendo e tendo paciência para dar dicas e corrigir meus erros.

Agradeço também ao professor Thiago que foi orientador no começo desse projeto, ajudou na escolha do tema e a estruturar quase todo o trabalho. Sem esquecer das pessoas que se transformaram em amigos e colegas na turma, que ajudaram a adquirir experiência e conhecimento de mundo.

E enfim, agradeço a todos que suportaram esses dias finais deste trabalho tão difíceis ao meu lado, meu mau humor das várias noites sem dormir e estresse. Muito obrigado a todos.

RESUMO

A Blockchain pode ser definida como uma base de dados, que armazena informações em blocos de forma imutável com o uso de *HASHs*, criptografia assimétrica e rede P2P. Essa tecnologia pode ser usada para diversas finalidades, como: moeda virtual, segurança da informação, rastreio de materiais, registro de informação e tantas outras. Cartórios sofrem com o acúmulo de informações físicas, fazendo com que o serviço fique lento ou a perda de dados. Com todas essas possibilidades de serviços que a *Blockchain* pode ser utilizada, foi escolhido para esta monografia o desenvolvimento de uma *Blockchain* para dar maior autenticidade às informações salvas em Cartório, especificando atividades de venda de veículos por pessoas físicas, podendo ser utilizado em navegadores.

Palavra-Chave: *Blockchain*, cartório, P2P, *HASH*, autenticação, PoW, *JavaScript*, criptografia.

ABSTRACT

Blockchain can be defined as look like a database, which stores information in blocks immutably using HASHs, asymmetric encryption, and P2P networking. This technology can be used for various purposes such as virtual currency, information security, material tracking, information logging and many others. Notaries suffer from the accumulation of physical information, causing service to slow down or data loss. With all these possibilities of services that Blockchain can be used, it was chosen for this monograph the development of a Blockchain to give greater authenticity to the information saved in the Registry, specifying activities of sale of vehicles by individuals, and can be used in browsers.

Keywords: *Blockchain*, notary's office, P2P, *HASH*, authentication, PoW, *JavaScript*, cryptography.

LISTA DE SIGLAS

P2P	<i>Peer-to-Peer</i>
PoW	<i>Proof-of-Work</i>

LISTA DE FIGURAS

Figura 1: Exemplo do funcionamento básico da criptografia assimétrica.....	12
Figura 2: Serviços ofertados pela OriginalMy.....	16
Figura 3: Conquistas da OriginalMy.....	17
Figura 4: Blocos interligados em uma Blockchain.....	17
Figura 5: Demonstração do processo de mineração e recompensa.....	19
Figura 6: Representação das várias correntes que formam a Blockchain.....	21
Figura 7: Diagrama de Caso de Uso Geral.....	30
Figura 8: Diagrama de Sequência Geral.....	31
Figura 9: Tela inicial do sistema.....	32
Figura 10: Representação das informações nos blocos da corrente.....	33

LISTA DE TABELAS

Tabela 1: Requisitos funcionais (RF).....	28
Tabela 2: Requisitos não funcionais (RNF).....	29

SUMÁRIO

1. INTRODUÇÃO.....	11
2. REFERENCIAL TEÓRICO.....	15
2.1. Cartório.....	15
2.2. Blockchain.....	17
2.2.1. Segurança.....	19
2.2.2. Consenso.....	20
2.2.3. Prova-de-Trabalho.....	22
2.2.4. Ponta-a-Ponta.....	22
3. MÉTODOS E FERRAMENTAS.....	22
3.1. Modelo de Pesquisa.....	23
3.1.1. Aplicada.....	23
3.1.2. Exploratória.....	23
3.1.3. Qualitativa.....	24
3.2. Levantamento Bibliográfico.....	24
3.3. Ferramentas.....	24
3.3.1. Javascript.....	24
3.3.1.2. NodeJS.....	24
3.3.2. Editor de Texto.....	25
3.3.3 Linux.....	25
3.3.4 Git e Github.....	25
4. DESENVOLVIMENTO DO SISTEMA.....	26
4.1. Requisitos e Implementação.....	26
4.2. UML.....	28
4.2.1. Diagrama de Caso de Uso.....	28
4.2.2. Sequência.....	29
4.3. Telas e Operações do Sistema.....	30
5. CONCLUSÃO.....	32
5.1. Trabalhos Futuros.....	32

REFERÊNCIAS BIBLIOGRÁFICAS

1. INTRODUÇÃO

Todas as atividades humanas podem gerar muitos dados que são impressos em papel, sendo o mesmo amplamente utilizado para manter e legitimar informações, no intuito de assegurar o direito sobre a propriedade de bens de um indivíduo ou instituição jurídica. Por isso, a informação é gravada em papéis que são reconhecidos como fonte fidedigna de informação nos cartórios públicos.

Existem casos comprovados de corrupção e fraudes na validação dos registros físicos de propriedade de pessoas físicas ou jurídicas (DONDOSSOLA, et al., 2019). Mesmo assim, a sociedade ainda prefere trabalhar de uma forma que sejam necessárias entidades reguladoras centralizadas gerenciando operações como autenticação de informação.

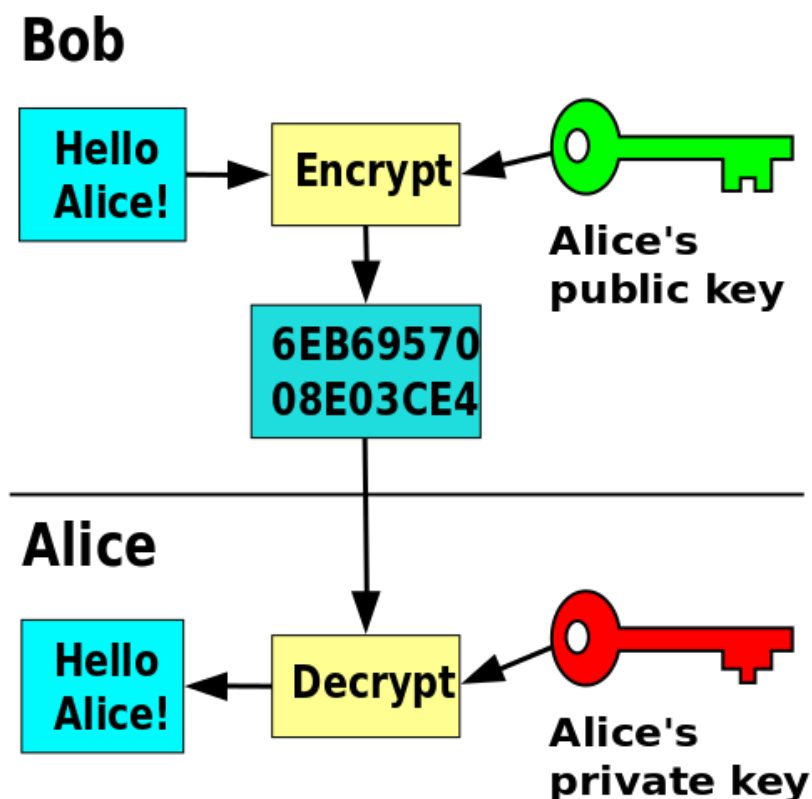
No entanto, está emergindo um novo sistema virtual que não exige um intermediador para validar informações ou negociações. O nome dessa tecnologia chama-se *Blockchain* consistindo em uma rede de computadores *peer-to-peer* que armazenam informações criptografadas sobre diversos recursos (propriedades, bens móveis e imóveis e outros), fornecendo serviço sobre a verificação da validade e a autenticidade de documentos, bem como garantindo que estes documentos assinados digitalmente não vão ser acessados indevidamente.

A *Blockchain* implementou os conceitos de Segurança da Informação cumprindo os das seguintes formas: disponibilidade, a informação deve estar sempre disponível para ser acessada por indivíduos ou entidades que tenham a permissão de acesso; integridade, os dados não podem ser modificados para manter a originalidade da informação; auditabilidade, é possível saber quem gerou ou alterou alguma informação digital.

Uma boa forma de garantir a autenticidade da informação é com a criptografia assimétrica. A criptografia consiste em embaralhar os dados de um documento digital utilizando chaves de acesso. Assim, uma mensagem só é legível e entendível por quem detém as chaves. No modelo assimétrico existem duas chaves, uma pública que serve para encriptar os dados e uma privada para descriptografar a

informação cifrada, chave essa que é somente de conhecimento de uma única pessoa. Esses passos são exemplificados na Figura 1 (Göthberg, 2006).

Figura 1: Exemplo do funcionamento básico da criptografia assimétrica



Fonte: Göthberg (2006)

Na blockchain os dados são gravados em uma espécie de livro razão digital, os dados textuais podem guardar informações bem variadas como uma letra de música, poema, moeda ou documento, e são gravados dentro de um bloco, sendo uma das principais: duas *hash*, em que a primeira identifica bloco atual, e a outra representa o bloco anterior para criar a ligação entre esses blocos. A junção desses blocos forma uma corrente interligada que é espalhada entre as milhares de máquinas na rede distribuída.

Para validar as informações em um blockchain utiliza-se um algoritmo de consenso, existem diversos algoritmos de consenso, o mais famoso é a Prova de Trabalho que consiste em resolver um problema matemático que demanda do

hardware um grande esforço para encontrar a resposta, em que vence a disputa quem possuir o maior poder computacional de processamento. Todos os blocos são calculados e autenticados por esses métodos para que sejam a prova de ataques.

Sistemas como uma Blockchain potencializam operações de autenticar documentos por motivo de sua transparência e segurança. Como documentos que comprovam propriedades que necessitam ser da fé pública de acordo com o Art. 3 da Lei nº 8.935 de 18 de Novembro de 1994 (Brasil, 1994), por ser de interesse do proprietário e da comunidade em geral. Documentos como esses devem ser livres de quaisquer dúvidas relacionadas a validade falsa, para que possam ser aceitos por pessoas jurídicas e físicas.

Dessa forma, desenvolver uma Blockchain para operacionalizar o funcionamento de um cartório de registro de vendas de propriedades, especificamente em processos de registros para certidões de propriedades pode tornar mais confiável a autenticidade dos dados de um cartório.

Nesse contexto, este trabalho possui como objetivo geral desenvolver um sistema de blockchain para armazenar registros associado a transferência de posse sobre veículos, podendo dar uma prova de autenticidade a mais. Para alcançar esse objetivos torna-se necessário realizar os seguintes objetivos específicos:

- 1) Desenvolver uma rede *peer-to-peer* em javascript para dar suporte ao funcionamento da Blockchain;
- 2) Identificar e aplicar os algoritmos de criptografia necessário para o funcionamento do sistema;
- 3) Determinar os campos de dados associados a registros de automóveis que serão salvos em blocos na Blockchain;
- 4) Desenvolver uma interface web que possibilite aos usuários acessar os serviços disponibilizados.

Por fim, o restante do trabalho está organizado da seguinte forma: o Capítulo 2 apresenta o referencial teórico contextualizando todos os tópicos importantes para o embasamento científico da pesquisa; o Capítulo 3 apresenta formalmente o modelo de pesquisa aplicado, às fases do trabalho, bem como a metodologia de desenvolvimento e as ferramentas utilizadas para construir a Blockchain; o Capítulo

4 apresenta os requisitos, a modelagem e o desenvolvimento da Blockchain; e o Capítulo 5 apresenta as conclusões e as possíveis continuações da pesquisa.

Este projeto demonstrará um sistema digital capaz de resolver problemas do mundo real, comprovando que em um futuro próximo as Blockchains poderão resolver conflitos de informação duplicada e falsas, empregando algoritmos de criptografia e descentralização da rede.

2. REFERENCIAL TEÓRICO

Neste capítulo será apresentado um resumo dos conceitos sobre cartórios e a descrição de abstrações e conceitos da tecnologia Blockchain com o estudo de caso do Bitcoin.

2.1. Cartório

A história dos cartórios brasileiros se inicia no período colonial, motivados pelo controle das capitanias hereditárias pela Coroa portuguesa, o império português dividiu o território brasileiro e nomeou pessoas de confiança para administrar as terras, desde então há órgão responsáveis por autenticar informações de terceiros e que abrangem várias áreas que requerem de processos e documentos autênticos. Um cartório é encarregado de gravar e guardar arquivos transações materiais entre indivíduos, dando autenticidade as informações contidas nos documentos, e várias outras funções como registrar distribuição, protesto, pessoas jurídicas. (PINTO, 2014)

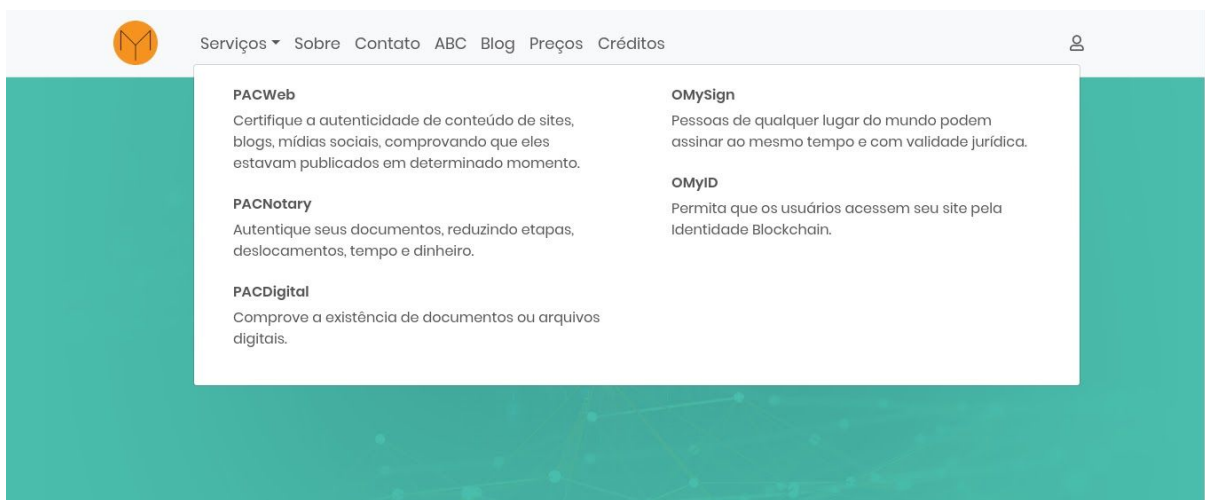
Para registrar propriedades ou oficializar casamentos de acordo com o Código Civil (Lei n. 10.406, de 10 de Janeiro de 2002) sintetiza com o artigo 125 “Art. 215. A escritura pública, lavrada em notas de tabelião, é documento dotado de fé pública, fazendo prova plena” (BRASIL, 2002), o que exemplifica o modelo seguido pelas sociedades em geral.

Notícias como a recente confirmação da primeira criança registrada com uma Blockchain no Brasil são promissoras, sem necessitar de se locomover até um cartório ou de documentos físicos. A empresa por trás desse feito se chama Growth Tech com seu serviço Notary Ledgers, que utiliza a plataforma de Blockchain da IBM. (ORTEGA, 2019)

O caso da empresa OriginalMy, que se transferiu para a Estônia pela facilidade de empreendimento e grande mercado de autenticação com Blockchain,

reforça o crescimento dessa tecnologia em conjunto com serviços cartoriais. A seguir nas imagens 2 e 3 é possível constatar a grande gama de serviços e possibilidades desse mercado inovador ofertado pela OriginalMy. (ANDRION, 2019)

Figura 2: Serviços ofertados pela OriginalMy



Fonte: OriginalMy (2019)

Figura 3: Conquistas da OriginalMy

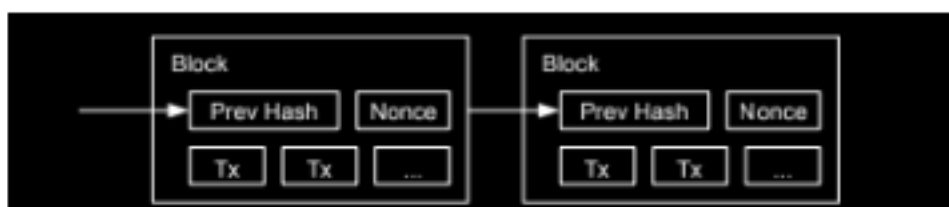


Fonte: OriginalMy (2019)

2.2. Blockchain

Como já foi abordado anteriormente, Blockchain é uma tecnologia que guarda informações em células, ou blocos como é geralmente denominado. Esta informação pode ser desde um simples texto ou algum valor econômico como no caso de uma criptomoeda, e cada bloco está ligado a outro bloco formando uma corrente imutável, esta ligação é simplificada com a seguinte imagem (NAKAMOTO, 2008).

Figura 4: blocos interligados em uma Blockchain



Fonte: Nakamoto (2008)

A *Blockchain* resolveu o problema da necessidade de delegar a confiabilidade em grandes organizações e entidades com poder centralizado para realizar simples transações ou autenticação de propriedades, a forma de pensar da *Blockchain* original é fazer uma grande base de dados global e a confiança seja gerada por não permitir a alteração da informação anterior e verificação provada por cada usuário na rede (RODRIGUES, 2017).

Esta é uma tecnologia criada para dar suporte a lógica do Bitcoin, que teve seu artigo publicado em 2008 com o pseudônimo Satoshi Nakamoto, por meio desta publicação a *Blockchain* foi exposta ao mundo para ser aplicada para soluções financeiras como em criptomoedas, como outras diversas como cartórios, prontuários médicos, rastreamento de alimentos e tantas outros problemas atuais.

A *Blockchain* sendo utilizada para fins monetários armazena cada transação em blocos, que são ligados de forma que o atual é conectado ao anterior depois de ter sido validado por uma prova de trabalho PoW. (RODRIGUES, 2017)

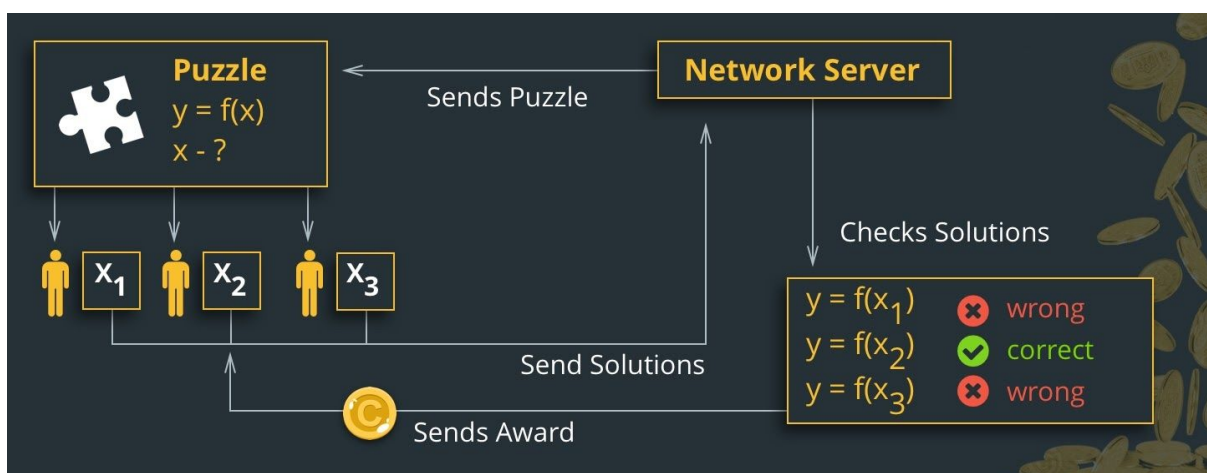
O primeiro bloco é conhecido como gênese, geralmente guarda valor 0 ou as primeiras moedas mineradas como no caso do *Bitcoin* (*Genesis of Bitcoin*) em cada um desses blocos na *Blockchain* original contém informações como: número de transação, é a contagem da quantidade de transações realizadas; transação, valor da transação armazenada no bloco ou qualquer outro tipo de informação; e o cabeçalho que contém metadados sobre o bloco.

Os dados armazenados no cabeçalho dos blocos são muito importantes, com o objetivo de apontar um bloco a outro com a hash e guardar dados como: versão do protocolo; uma síntese das transações das informações das transações do bloco atual; *timestamp*, momento da criação do bloco; dificuldade, nível de dificuldade de mineração pelas pontas; nonce, número ou letra buscado pelo problema matemático da mineração e raiz da árvore de Merkle, que é explicado por Agner, (2018, pag. 75) “são estruturas de dados utilizadas para criar um resumo de dados com integridade criptograficamente verificável de forma eficiente”.

Os blocos são gerados a partir da mineração dos dados, que visa explorar e analisar uma grande quantidade de dados disponibilizados pelos usuários da rede. Para que seja realizada essa mineração de dados, os mineradores como são

definidos, precisam de máquinas super potentes para extrair e evidenciar filtros, visando encontrar padrões que são obtidos através da simplificação de dados, sobre qualquer tipo de informação que esteja alocada na rede. Todo esse processo é realizado sem necessitar de uma autoridade centralizada, assim fazendo com que a rede continue se expandindo. (NAKAMOTO, 2008)

Figura 5: demonstração do processo de mineração e recompensa do Bitcoin.



Fonte: Tar, 2018

2.2.1. Segurança

A Segurança da Informação possui cinco principais elementos, são eles: Privacidade, Integridade, Disponibilidade, Autenticidade e Não Repúdio (CABRAL; FERREIRA; SONNENSTRAHL, 2013). Todos esses tópicos serão abordados e demonstrando na implementação feita na Blockchain do Bitcoin.

Enquanto a Blockchain pode ser equiparada a um livro aberto de contas, isso pode passar a impressão de que não existe privacidade nas transações entre os nós, mas em teoria a identidade de cada usuário não é revelada a não ser sua chave anônima pública, esta chave é o identificador de cada ponta nas transações. Caso uma chave pública seja ligada a uma identidade real, toda a privacidade de outros

nós que teriam feito transações com o mesmo poderia ser quebrada. (NAKAMOTO, 2008)

A autenticidade da informação na Blockchain se dá por meio de *HASHs*, em que uma frase é criptografada irreversivelmente (SERAFIM, 2012), mais especificamente o *SHA-256* no caso do Bitcoin, com valor único e sempre mesmo tamanho, criadas a partir do resumo de várias informações do bloco e com a necessidade de gastar esforço computacional, gravando o momento exato que foi criado. (NAKAMOTO, 2008)

Em uma Blockchain toda informação criada é guardada para sempre, não possibilitando a edição de dados posteriormente gravados. Esse mecanismo dá confiança de que os dados são íntegros e auditabilidade pública, evitando que um nó desmintas uma transação ou informação. (CASTRO; DENNY; PAULO, 2017)

A Blockchain suporta uma quantidade exorbitante de usuários, pelo fato de ser acessada em uma rede *P2P*, não necessitando de um servidor ou vários servidores centrais espalhados estrategicamente pelo mundo. Por suportar muitos usuários e ter sido pensada com uma lógica que com o acréscimo de nós dá maior segurança a rede, dá um grande suporte de acesso em escala global. (JÚNIOR; REIS, 2018)

Diante do exposto tem-se que a blockchain trabalha com nós que são definidos como os usuários inseridos na rede, que compartilham informações definido como o tráfego de dados e os protocolos de segurança garantem a confiabilidade desse processo, fazendo com que a blockchain seja considerada uma das tecnologias inovadoras, utilizando criptografia, autenticidade, confiabilidade em todo seu processo, gerando informações totalmente rastreáveis e confiáveis.

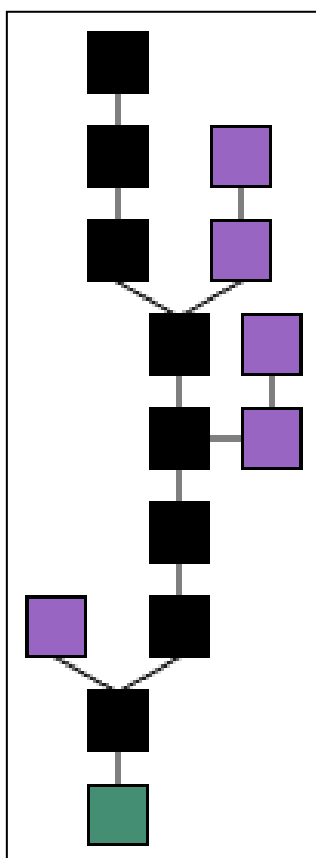
2.2.2. Consenso

Uma Blockchain necessita de vários mecanismos para gerar confiança no público. Para uma moeda ser confiável ela deve ser única, não podendo ter o identificador duplicado, o Bitcoin utiliza um servidor que grava a marca temporal, mais conhecido como *timestamp*; guarda o momento que o bloco foi criado, gerando

uma hash para cada um deles e formando uma lista encadeada em que um bloco é ligado ao anterior. (NAKAMOTO, 2008)

Após o nó ter realizado o dificultoso cálculo da *hash* com o *PoW* ele é compartilhado por toda a rede, todos os blocos testam esta nova transação e se é validada cria-se um novo bloco, o próximo bloco que for criado será ligado a hash este bloco que agora será o anterior. Toda a rede utiliza a maior corrente e seguirá acrescentando blocos a mesma, caso outra ponta consiga ser mais rápida e forme outra corrente maior e ela será a atual corrente de toda a rede, demonstrada na figura três a seguir. (NAKAMOTO, 2008)

Figura 6: representação das várias correntes que formam a Blockchain



Fonte: Nakamoto, 2008

2.2.3. Prova-de-Trabalho

Cada bloco nesse servidor de *timestamp* é autenticado pela rede caso possua uma hash que foi calculada com vários parâmetros até chegar em um valor único. A prova de Trabalho ou *Proof-of-Work/PoW* tem a tarefa de realizar esse cálculo da hash, utilizando o padrão *SHA-256*, e por obrigação cada hash deve começar com um determinado número de zeros na frente do código. A quantidade de zeros define a dificuldade do cálculo para chegar até o resultado da hash. (NAKAMOTO, 2008)

O artigo de Nakamoto cita o Hashcash, um algoritmo criado por Adam Back que inicialmente foi desenvolvido para impedir o spam de emails com a Prova-de-Trabalho, gerando um *token* ao custo de um processamento computacional por meio de um desafio requerido pelo servidor. O *PoW* do Hashcash é semelhante ao do Bitcoin, diferenciando que a mineração do Bitcoin demanda maior poder computacional e utilizar uma criptografia de hash mais atual. (BACK, 2002)

2.2.4. Ponta-a-Ponta

Uma rede *P2P* pode ser resumidamente definida como uma conexão direta entre duas ou mais máquinas, em que não necessita de um servidor centralizado para administrar as demais máquinas dando os mesmos direitos e obrigações para usuário nessa rede. (CALLADO *et al.*, 2004)

Atualmente a arquitetura predominante de conexão é o cliente-servidor, mas o início da história da Internet com a ARPANET que se iniciou em 1969 era bem diferente. As máquinas que estavam nessa rede se comunicavam livremente, executando funções de cliente e servidor compartilhando informações por igual, como em uma rede *P2P* deve ser. Com a popularização da internet e chegada de grandes corporações a rede fez com que esse modelo mais direto tenha sido quase que esquecido. (CALLADO *et al.*, 2004)

Essa arquitetura de rede está voltando a ser popularizada nos dias atuais graças a projetos *open source* e descentralizadas como o Bitcoin, que motivou a criação de diversas novas criptomoedas e outras utilizações para a Blockchain.

3. MÉTODOS E FERRAMENTAS

Neste capítulo será abordado os processos que foram seguidos na pesquisa e desenvolvimento da aplicação e esta monografia, explanando a pesquisa bibliográfica até a programação do sistema e suas as ferramentas envolvidas.

3.1. Modelo de Pesquisa

Este trabalho consiste em um pesquisa aplicada, exploratório e de caráter qualitativo. O processo de desenvolvimento é apoiado na metodologia espiral, na qual o desenvolvimento do sistema passa por vários ciclos bem definidos adicionando adicionando funcionalidades a cada etapa, e ao fim da fase de desenvolvimento espera-se obter um de blockchain funcional.

Na pesquisa foi utilizado o levantamento bibliográfico para adquirir conhecimento teórico, utilizando a abordagem qualitativa observando fatores como melhoria nas qualidades do serviço e segurança de cartórios, e a pesquisa é de caráter prático por ter a finalidade de ser aplicado a um sistema que pode ser usado no mercado real.

3.1.1. Aplicada

A pesquisa aplicada foi selecionada por dar a possibilidade de o pesquisador pôr em prática os conhecimentos adquiridos ao decorrer do curso e pesquisa no trabalho, em conjunto com a prática em projetos diversos no desenvolvimento de softwares para chegar no produto que é o objetivo deste trabalho. (METODOLOGIA..., 2018)

3.1.2. Exploratória

O pesquisador coloca em prática a pesquisa exploratória com o propósito de se aprofundar mais no tema, saindo do conhecimento raso que possuía e adquirindo mais conteúdo para poder reproduzi-lo em trabalhos e projetos. (RIBEIRO, 2017)

3.1.3. Qualitativa

Pensando no objetivo do sistema que é solucionar problemas de pessoas que necessitam de serviços de cartório, o método qualitativo foi escolhido por dar a possibilidade de valorar melhor a eficiência do sistema proposto em relação a satisfação dos usuários comparado com o funcionamento atual dos cartórios por eles. (LÜDORF, 2017)

3.2. Levantamento Bibliográfico

Para a construção do referencial teórico, utilizou-se pesquisa bibliográfica desenvolvida por meio eletrônico como fonte de obtenção de dados para o trabalho. A pesquisa bibliográfica, ou de fontes secundárias, abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico etc. até meios de comunicação orais: rádio, gravações eletrônicas, audiovisuais, filmes e programas de televisão. Sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto, inclusive conferências seguidas de debates que tenham sido transcritos por alguma forma, quer publicadas quer gravadas (MARCONI; LAKATOS, 2017)

Este trabalho utilizou somente fontes eletrônicas e em grande parte na linguagem inglesa, por meio das seguintes bases de dados: Google Books, Google Scholar. Pesquisando com as palavras chaves: Blockchain, Cartório, P2P, Bitcoin, PoW, NodeJs, JavaScript, criptografia assimétrica, Hash.

Para a criação da aplicação, as etapas serão: definir os requisitos funcionais e não funcionais. Elaboração de diagramas para demonstração da interação do sistema, construção da rede p2p e desenvolvimento da *Blockchain*. Em seguida, será feita a parte de modelagem, juntamente com a escolha do melhor editor de texto para o desenvolvimento com JavaScript.

3.3. Ferramentas

Será apresentado neste capítulo as principais ferramentas utilizadas no desenvolvimento do sistema, com suas devidas empregabilidades no projeto.

3.3.1. Javascript

O *Javascript* é uma das linguagens mais utilizadas no mundo. Ela foi criada em 1995 e atualmente está em primeiro lugar na quantidade de projetos compartilhados no *Github*, geralmente utilizado no *Frontend* ele também pode ser utilizado no *Backend*. Possui uma sintaxe semelhante a do *Java* e *C* mas dando liberdade ao desenvolvedor de utilizar ou não ponto e vírgula e o paradigma que deseja. Por esses motivos o *Javascript* foi escolhido para este Projeto. (GRONER, 2017)

3.3.1.1. NodeJS

A partir de 2009, o uso do *Javascript* no *Backend* foi possível com o *NodeJs*. Rodando com o mesmo motor do *Google Chrome* chamado de V8 desenvolvido com C++, possibilitando servidores robustos e escaláveis em conjunto com uma vasta quantidade de bibliotecas gerenciadas pelo *NPM*. (MORAES, 2018)

3.3.2. Editor de Texto

Todo o código foi desenvolvido com o editor *Visual Studio Code*. Este editor *Open Source* foi desenvolvido pela *Microsoft*, lançado em 2015 e programado em *Javascript*, *Typescript* e *CSS*, é disponível utilizá-lo nas plataformas: *Windows*, *Linux* e *MacOS*. Tem uma boa quantidade de *plugins* que aumentam a produtividade no desenvolvimento para várias linguagens diferentes.

3.3.3. Linux

O Linux é o Sistema Operacional *Open Source* mais utilizado no mercado. Utiliza a licença GNU e existem inúmeras distros Linux disponíveis de graça para serem baixadas. Nesse projeto foi utilizado o *Xubuntu*, por ser da família *Debian* dá bastante confiança ao sistema em relação a segurança e garantia de um longo período de atualizações, o conjunto de aplicações para desenvolvimento de softwares nesse sistema é amplo e não deixa a desejar em relação a outros sistemas.

3.3.4. Git e Github

O *Git* é um sistema de versionamento para código criado por Linus Torvalds. Pensado para resolver problemas de organizar diferentes versões de um sistema escritos por grupos ou programadores individuais, recomendado mundialmente para gerenciamento de versão de scripts e também registro de histórico de diversos tipos de arquivos.

Para completar essas funcionalidades do *Git* e o mundo open source foi criada a plataforma *Github*. Podendo armazenar projetos públicos ou privados versionados pelo *Git*, muito utilizado por programadores para compartilhar sistemas

e ideias entre a comunidade. Neste projeto foi utilizado o *Git* para versionamento, e *Github* para hospedar e compartilhar o trabalho em: github.com/savio777/tcc.

4. DESENVOLVIMENTO DO SISTEMA

Neste capítulo será mostrado o escopo com os requisitos do funcionamento do sistema, detalhes do desenvolvimento deste sistema que foi nomeado de *BlockNotary* e a modelagem com seus diagramas.

4.1. Requisitos e Implementação

De acordo com as pesquisas citadas anteriormente, uma *Blockchain* tem valor pragmático para diversas aplicações no mundo real como: auditorias, criptomoedas, rastreamento de materiais e autenticação de informação. Sendo assim possível um cartório funcionar com uma base de dados autenticada e salva com uma *Blockchain*.

Por esses motivos a criação do sistema deste trabalho foi pensado. Salvar dados do valor e CRV do veículo com a assinatura digital (Chave pública), que estará ligada aos documentos pessoais do criador e participante de transações em um banco de dados como a ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).

Com a verificação feita pela chave pública e privada, o criador do bloco pode utilizar essa informação como segunda fonte de comprovação, por ter sido somente escrito somente pelo dono da chave pública, e a informação autenticada por não poder ser modificado posteriormente.

A implementação da *Blockchain* foi possível pelas bibliotecas do *NodeJs*, sendo elas: *crypto-js* para geração de *HASH* com padrão 256 e *elliptic* para criação de chaves públicas e privadas. A parte de conexão ponta a ponta foi utilizada a biblioteca *signalhub* que possibilitou a comunicação de usuários na rede e *budo* para carregar script *CSS* e *JavaScript* em tempo real. O *Frontend* é estilizado com uma

biblioteca chamada *Materialize*. O sistema foi testado em ambiente *localhost* em navegadores diferentes e as bibliotecas podem ser baixadas pelo *NPM*.

De acordo com Oliveira (2019, p. 32), “os requisitos funcionais são aqueles que descrevem o comportamento do software e o que o software deve realizar”, além de claro poder definir o que não deve ser realizado pelo sistema. Para Machado (2018), os requisitos não funcionais tem a função de descrever o comportamento e a qualidade do sistema na execução de suas tarefas. Nas tabelas 1 e 2, serão listados os requisitos funcionais e não funcionais.

Tabela 1: Requisitos funcionais (RF)

Requisito(s)	Título	Descrição
RF001	Salvar dados na Blockchain	O sistema deve salvar de forma permanente e imutável as informações enquanto o sistema estiver rodando em alguma ponta
RF002	Validar corrente	O sistema deve testar se a corrente é válida
RF003	Validar usuário	O sistema deve testar a chave pública e privada do usuário para confirmar validar a informação gravada

Fonte: Autor (2019)

Tabela 2: Requisitos não funcionais (RNF)

Requisito(s)	Título	Descrição
RNF001	Navegador <i>Desktop</i> ou <i>Mobile</i>	O sistema deve ser utilizado em navegadores <i>desktop</i> ou <i>mobile</i> com acesso ao domínio
RNF002	Autenticar a chave pública	Os dados só serão salvos caso o usuário envie a sua chave pública e privada corretamente
RNF003	Mensagem de erro	Caso algum campo esteja em branco ou as chaves não sejam correspondentes será mostrado uma mensagem de erro
RNF004	Disponibilidade	O sistema deve estar disponível para vários usuários simultaneamente online na

		rede, podendo adicionar novos blocos e visualizar a informação
RNF005	Transparência	O usuário deve ser informado na tela que a corrente é válida e sua chave pública e privada estão corretas

Fonte: Autor (2019)

4.2. UML

De acordo com Carvalho *et. al* (2019, pag. 3), “A UML estabelece um padrão de modelagem de projetos de sistemas, incluindo seus aspectos conceituais”. Essa linguagem de alto nível foi usada para produzir diagramas com a finalidade de explicitar funcionalidades do sistema.

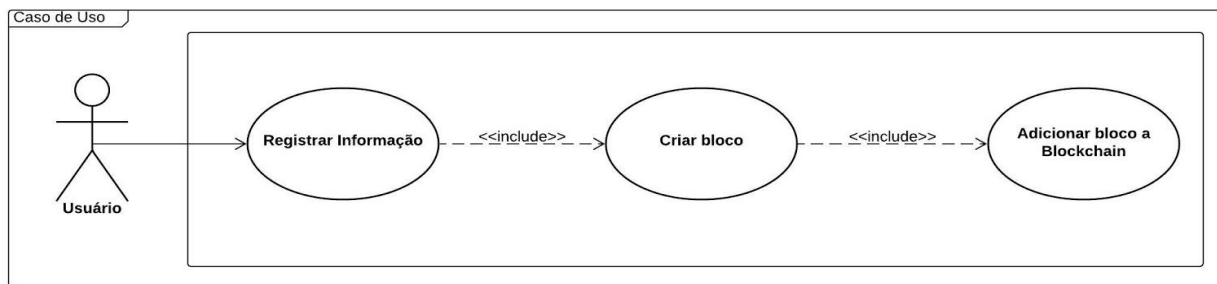
4.2.1. Caso de Uso

De acordo com Guedes (2018),

Os casos de uso são utilizados para capturar os requisitos funcionais do sistema, ou seja, referem-se a serviços, tarefas ou funcionalidades identificados como necessários ao software e que podem ser utilizados de alguma maneira pelos atores.

A seguir na figura 7 é possível acompanhar as funcionalidades do sistema de forma resumida.

Figura 7: Diagrama de Caso de Uso Geral

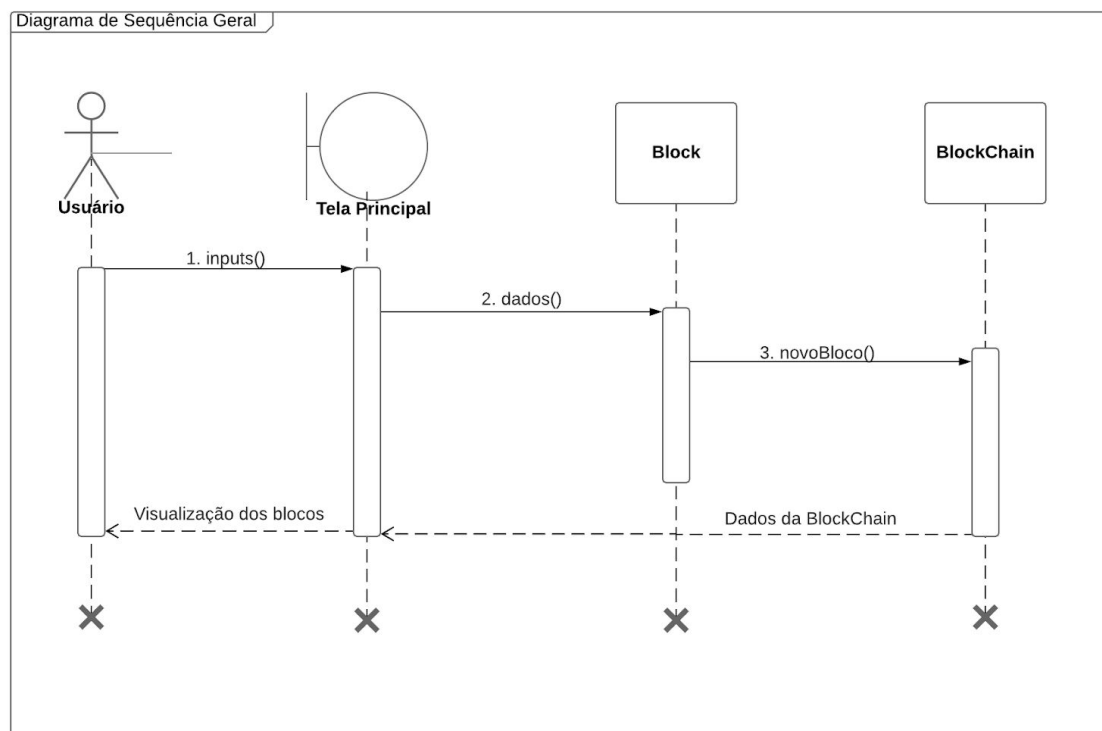


Fonte: Autor (2019)

4.2.2. Diagrama de Sequência

De acordo com Guedes (2018, pag. 6), “O diagrama de sequência é um diagrama comportamental que se preocupa com a ordem temporal em que as mensagens são trocadas entre objetos envolvidos em um determinado processo”. Na figura 8 é possível entender a execução do sistema de acordo com a ação do usuário, e na sequência o passo a passo da execução de tarefas até retornar resultados ao usuário.

Figura 8: Diagrama de Sequência Geral

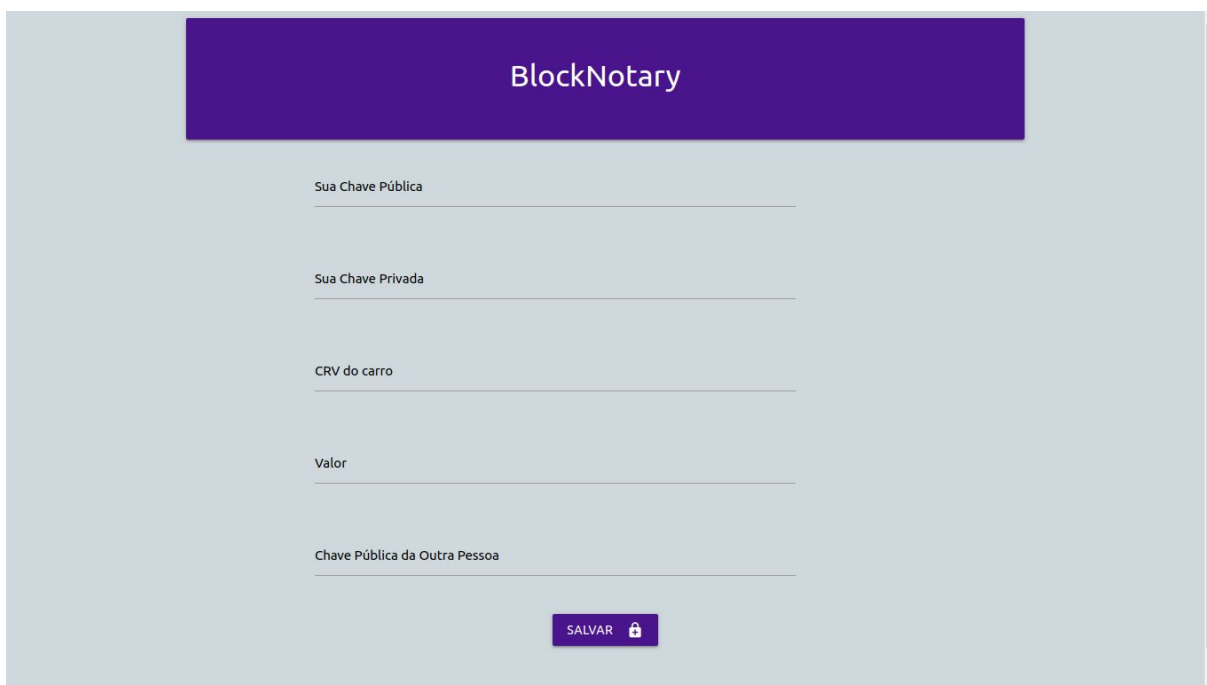


Fonte: Autor (2019)

4.3. Telas e Operações do Sistema

Após o usuário acessar o sistema ele verá a tela inicial mostrado na figura 9 e 10, verá um formulário com *inputs* que o usuário deve preencher, primeiramente ele deve inserir a sua chave pública e a seguir sua chave privada correspondente, após isso o usuário fornecerá a chave pública da outra parte que participará da transação e por último ele irá adicionar a descrição da operação.

Figura 9: Tela inicial do sistema



The screenshot displays the BlockNotary web application interface. At the top, there is a dark purple header with the text "BlockNotary" in white. Below the header, the form consists of five input fields, each with a label and a horizontal line for text entry. The labels are: "Sua Chave Pública", "Sua Chave Privada", "CRV do carro", "Valor", and "Chave Pública da Outra Pessoa". At the bottom of the form, there is a purple button with the text "SALVAR" and a small lock icon to its right.

Fonte: Autor (2019)

Após enviarem as informações para a *Blockchain* clicando no botão salvar, o usuário verá *cards* com as informações do bloco que acabou de ser criado anteriormente apontando para os próximos. Essa visualização é mostrado na figura 10.

Figura 10: Representação das informações nos blocos da corrente

Corrente é válida: true

Chave é válida: true

#1: 00be7a40da78fcff0087b2064f80b775bda2f42304e9d7d920c9b65bfff10faf5

Chave anterior 381180aa18f9adce8cac37ed3cb5fc44999e9f1307c9463f0fcc58e8919cdbe0

Chave Primária: 046cdcdac03e408a4b26a57add18bd5d7dac8964e9739fd4b32ef9d4153326a6f05ca69ed1c8e2f2db465b3afc0ba244fdd579d56b3f0dcac794c571e1525c991f

Timestamp: Tue Nov 19 2019 05:34:16 GMT-0300 (Brasília Standard Time)

Valor: 3242342.34

CRV do veículo: 234242342

Chave do comprador: 046220567d354204bb88b1f28f8175177afb29b24853f5cbcd890646111dad485d864e39fdbfa5ed7944e704e93b8e3fa230706712f03aac80272e7ffee9057a64



#2: 00a3938bd1fa33668fa842c1287fd3509e0482f581f82fb47d03917488fa6da1

Chave anterior 00be7a40da78fcff0087b2064f80b775bda2f42304e9d7d920c9b65bfff10faf5

Chave Primária: 046220567d354204bb88b1f28f8175177afb29b24853f5cbcd890646111dad485d864e39fdbfa5ed7944e704e93b8e3fa230706712f03aac80272e7ffee9057a64

Timestamp: Tue Nov 19 2019 05:34:43 GMT-0300 (Brasília Standard Time)

Valor: 45345345.45

CRV do veículo: 232777788

Chave do comprador: 046cdcdac03e408a4b26a57add18bd5d7dac8964e9739fd4b32ef9d4153326a6f05ca69ed1c8e2f2db465b3afc0ba244fdd579d56b3f0dcac794c571e1525c991f



Fonte: Autor (2019)

5. CONCLUSÃO

Este trabalho concentra-se na implementação de um modelo de sistema baseado em Blockchain para fornecer serviços de cartório focados em autenticação de documentos enfatizando os processos de transferência de veículos entre pessoas físicas de acordo com regras do Detran, e o sistema podendo ser acessado abertamente por qualquer navegador em celular ou desktop.

Com o intuito de simular uma rede *Blockchain* baseada em um cartório público, salvar dados de forma imutável e verificar sua autenticidade, as chaves pública e privada são testadas para confirmar identidade do usuário.

As pesquisas demonstram o sucesso de empresas privadas no mercado de autenticação de informação. De tamanhos variados de empresas como por exemplo a gigante IBM que oferece vários serviços em Blockchain ou a *startup* brasileira OriginalMy que atende atualmente o mercado estoniano.

Conclui-se que, os objetivos almejados foram alcançados, os testes se mostraram satisfatórios na conexão com vários navegadores e na validação de dados. Para uma quantidade de usuários controlada no qual o sistema foi testado se apresentou eficiente, podendo ser continuado para suportar mais serviços e mais usuários.

5.1. Trabalhos Futuros

Como trabalhos futuros, são sugeridos os seguintes tópicos, almejando a construção de uma blockchain mais poderosa e eficiente, podendo a mesma ser aplicada em diversos setores.

- Automatizar funções e dar mais segurança com contratos inteligentes;
- Mais testes com maior quantidades de usuários acessando o sistema ao mesmo tempo, para confirmar se a linguagem Javascript e bibliotecas usadas suportariam uma Blockchain funcional;
- Permanência das informações salvas em arquivos Json para recuperação de dados caso o sistema caia em todas as pontas;
- Aperfeiçoamento do visual;

- Mais informações documentais a serem guardados na Blockchain;
- Testes em plataforma mobile com React-native;
- Correção de pequenos bugs;

REFERÊNCIAS BIBLIOGRÁFICAS

AGNER, Marco. **Bitcoin para Programadores**. [S.N.], 2018. Disponível em: <<https://btcparaprogramadores.marcoagner.org/>>. Acesso em: 10 de outubro de 2019.

ANDRION, Roseli. **Startup brasileira de blockchain faz sucesso na Estônia**. Disponível em: <<https://olhardigital.com.br/video/startup-brasileira-de-blockchain-faz-sucesso-na-estonia/91933>>. Acesso em: 30 de outubro de 2019.

ARAÚJO, H.; SILVA, Rebecca. **A tecnologia digital Blockchain: análise evolutiva e pragmática**. 2017. [S.I.].

BACK, Adam. **Hashcash: A Denial of Service Counter-Measure**. [S.I.]. 2002.

Blockchain e a Integridade de Dados na Validação de Sistemas Computadorizados | Boas Práticas. 2018. Disponível em: <<http://boaspraticasnet.com.br/blockchain-e-a-integridade-de-dados-na-validacao-de-sistemas-computadorizados/>>. Acesso em: 23 de setembro de 2019.

BRASIL. Lei n. 8.935, de 18 de nov. de 1994. **Dos Serviços Notariais e de Registros**. O Presidente da República. Brasil. p. 1. Constituição Federal, dispondo sobre serviços notariais e de registro. (Lei dos cartórios).

CABRAL, Heleno; FERREIRA, Andrew; SONNENSTRAHL, Thiago. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**. 2013. Santa Maria, RS.

CARDOSO, A.; COSTA, E.; SILVEIRA, F. **CRIPTOMOEDAS E BLOCKCHAIN NO PROCESSOS DE INOVAÇÃO SOCIAL**. 2018. [S.I.].

CENEVIVA, Walter. **LEI DOS NOTÁRIOS E DOS REGISTRADORES COMENTADA**. [S.I.]: Editora Saraiva, 2017.

CHRISTIDIS, K.; DEVETSIKIOTIS, M.. **Blockchains and Smart Contracts for the Internet of Things**. 2016. [S.I.].

Comunicação de venda. Disponível em: <<https://www.detran.sp.gov.br/wps/wcm/connect/portaldetran/detran/sa-veiculos/sa-s>>

ervicosonline/sa-comunicacaoavenda/sa-fichaservicosolicitacaocomunicacaoavenda/96830253-ea0a-45a6-b184-d0480535db78>. Acesso em: 14 de novembro de 2019.

COSTA, Daniel. **A Blockchain vai acabar com os cartórios?**. 2018. Disponível em: <<http://blog.mercatorio.com.br/2018/07/26/a-blockchain-vai-acabar-com-os-cartorios>>. Acesso em: 29 de agosto de 2019.

COSTA, Rostand. et al. **Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos. Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain_SBRC)**, [S.I.]. 2018.

CROSBY. M. et al. **BlockChain Technology: Beyond Bitcoin**. [S.I.]. 2016.

DENNY, D.; PAULO, R.; CASTRO, D.. **Blockchain and Agenda 2030**. 2017. [S.I.].

DONDOSSOLA, E. et al. **Força-tarefa prende 15 em operação contra fraudes em cartórios do RJ**. 2019. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/02/28/forca-tarefa-faz-operacao-p-ara-prender-quadrilha-suspeita-de-praticar-fraudes-em-cartorios-da-baixada-fluminense.ghtml>>. Acesso em: 09 de agosto de 2019.

FERDINAND, L.; NICOLAU, M. **As Redes de Compartilhamento P2P e as Novas Formas de Interação e Relacionamento na Internet**. 2014. [S.I.].

Fernando, ULRICH. **Defendendo o Bitcoin em Mordor**. 2017. Disponível em: <<https://www.mises.org.br/Article.aspx?id=2722>>. Acesso em: 21 de outubro de 2019.

FERREIRA, J.; PINTO, F.; SANTOS, S.. **Estudo De Mapeamento Sistemático Sobre As Tendências E Desafios Do Blockchain**. 2017. Recife, PE.

FLEURY, M.; WERLANG, S.. **Pesquisa aplicada: conceitos e abordagens**. 2016. [S.I.].

FONTES, Edison. **SEGURANÇA DA INFORMAÇÃO**. [S.I.]: Editora Saraiva, 2017.

Genesis Block Bitcoin. Disponível em:

<<https://www.blockchain.com/pt/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>>. Acesso em: 08 de novembro de 2019.

GREVE, F. et al. **Blockchain e a Revolução do Consenso sob Demanda.** 2018. [S.I.].

GRONER, Loiane. **Estruturas de dados e algoritmos em JavaScript:** Aperfeiçoe suas habilidades conhecendo estruturas de dados e algoritmos clássicos em JavaScript. [S.I.]: Novatec Editora, 2017.

GUEDES, Gilleanes. **UML 2: Uma Abordagem Prática.** 3. ed. [S.I.]: Novatec Editora, 2018.

HOGEMANN, Edna. **O futuro do Direito e do ensino jurídico diante das novas tecnologias.** 2018. Valença, RJ.

Incêndio queima milhares de documentos em cartório no Centro de Indaial.

2018. Disponível em:

<<https://www.nsctotal.com.br/noticias/incendio-queima-milhares-de-documentos-em-cartorio-no-centro-de-indaial>>. Acesso em: 23 de outubro de 2019.

LAKATOS, E.; MARCONI, M. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas, 2003.

LORETO, S.; ROMANO, S. **Real-Time Communication with WebRTC:**

Peer-to-Peer in the Browser. [S.I.]: O'Reilly Media, 2014.

LÜDORF, Sílvia. **Metodologia da Pesquisa:** Do Projeto ao Trabalho de Conclusão de Curso. [S.I.]: Appris Editora e Livraria Eireli - ME, 2017.

LUPS, Yuri. **Qual a história da origem do cartório?** 2018. Disponível em:

<<https://cartorionobrasil.com.br/servicos-de-cartorio/qual-a-historia-da-origem-do-cartorio/>>. Acesso em: 07 de agosto de 2019.

MACHADO, Felipe. **Análise e Gestão de Requisitos de Software:** Onde nascem os sistemas. [S.I.]: Editora Saraiva, 2018.

MIRANDA, Ana. **Cartórios**: onde a tradição tem registro público. 2000. Niterói, RJ.

MORAES, William. **Construindo aplicações com NodeJS**. 2. ed. [S.I.]: Novatec Editora, 2018.

MOREIRA, Márcio. **ECDSA (Elliptic Curve Digital Signature Algorithm)**. 2006. Uberlândia, MG.

MOUGAYAR, William. **Blockchain para negócios**: Promessa, prática e aplicação da nova tecnologia da internet. [S.I.]: Alta Books Editora, 2018.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-to-Peer Electronic Cash System. 2008. [S.I.].

OLIVEIRA, Henrique. **Análise de sistemas**. [S.I.]: Editora Senac São Paulo, 2019.

ORCUTT, Mike. **Why Nasdaq Is Betting On Bitcoin's Blockchain**. 2015.

Disponível em:

<<https://www.technologyreview.com/s/539171/why-nasdaq-is-betting-on-bitcoins-blockchain/>>. Acesso em: 5 de agosto de 2019.

ORTEGA, João. **Brasil tem primeira certidão de nascimento digital registrada em blockchain**. Disponível em:

<<https://www.startse.com/noticia/nova-economia/70387/brasil-tem-primeira-certidao-de-nascimento-digital-registrada-em-blockchain>>. Acesso em: 10 de novembro de 2019.

PACDigital: Blockchain garantindo uma Prova Legal de Autenticidade, Assinatura Digital, Certificação Digital e Registro de Autenticidade | OriginalMy.com. Disponível em: <<https://originalmy.com/>>. Acesso em: 20 de outubro de 2019.

PINTO, Danilo. **UM ANTROPÓLOGO NO CARTÓRIO: O CIRCUITO DOS DOCUMENTOS**. 2014. [S.I.].

PIRES, Timoteo. **TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS**. 2016. Brasília, DF.

REIS, D.; JÚNIOR, W, . **USO DO PROTOCOLO BLOCKCHAIN PARA REGISTRO DE AUTENTICIDADE DE CONTRATOS RÁPIDOS**. 2018. [S.I.].

RIBEIRO, Janete. **Pesquisa de marketing**. [S.I.]: Senac, 2017.

ROCHA, J. et al. **Peer-to-Peer**: Computação Colaborativa na Internet. 2004. [S.I.].

ROCHA. Roberto. **WebRTC - Evolução na Web**. 2014. [S.I.].

RODRIGUES , Carlo. **UMA ANÁLISE SIMPLES DE EFICIÊNCIA E SEGURANÇA DA TECNOLOGIA BLOCKCHAIN**. 2017. Brasília, Brasil.

SENAI-SP. **Metodologia da pesquisa aplicada à tecnologia**. [S.I.]: SESI SENAI Editora, 2018.

TAR, Andrew. **Prova de trabalho (PoW), Explicado**. 2018. Disponível em: <<https://br.cointelegraph.com/explained/proof-of-work-explained>>. Acesso em: 17 de setembro de 2019.

Tire suas dúvidas no Cartório 24 Horas. Disponível em: <<https://www.cartorio24horas.com.br/duvidas>>. Acesso em: 15 de outubro de 2019.