UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
UNIDADE ACADÊMICA DE GARANHUNS

ADEMÁRIO JOSÉ DA SILVA

QRQUEIJO: SISTEMA PARA VALIDAÇÃO E EMISSÃO DE IDENTIFICADORES DE QUEIJOS UTILIZANDO BLOCKCHAIN

Garanhuns
2019

ADEMÁRIO JOSÉ DA SILVA

QRQUEIJO: SISTEMA PARA VALIDAÇÃO E EMISSÃO DE IDENTIFICADORES DE QUEIJOS UTILIZANDO BLOCKCHAIN

Trabalho de Conclusão de Curso submetido à Universidade Federal Rural de Pernambuco - Unidade Acadêmica de Garanhuns, como requisito necessário para obtenção do grau de Bacharel em Ciência de Computação, sob a orientação do Prof. Sérgio Francisco Tavares de Oliveira Mendonça.

Garanhuns
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Ariano Suassuna, Garanhuns-PE, Brasil

S586q Silva, Ademário José da
QRQueijo: sistema para validação e emissão de identificadores de queijos utilizando Blockchain / Ademário José da Silva. – 2019.
58 f. : il.

Orientador: Sérgio Francisco Tavares de Oliveira Mendonça
TCC (Ciência da Computação) – Universidade Federal Rural de Pernambuco, Unidade Acadêmica de Garanhuns, Garanhuns, BR-PE, 2019.
Inclui referências

1. QRQueijo 2. Blockchain 3. Segurança da informação 4. Rastreabilidade I. Mendonça, Sérgio Francisco Tavares de Oliveira, orient. II. Título

CDD 004

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

ADEMÁRIO JOSÉ DA SILVA

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciência da Computação, sendo aprovado em sua forma final pela banca examinadora:

Orientador: Prof. Ms. Sérgio Francisco Tavares de Oliveira Mendonça
Universidade Federal Rural de Pernambuco - UFRPE

Prof. Diogo de Lima Lages
Universidade Federal Rural de Pernambuco - UFRPE

Prof. Igor Medeiros Vanderlei
Universidade Federal Rural de Pernambuco - UFRPE

Garanhuns, 12 de julho de 2019

Este trabalho é dedicado aos meus pais,
Maria de Fátima e Mário Antônio que com muito carinho e apoio,
não mediram esforços para realização do sonho de seu amado filho.

Agradecimentos

Dedico este trabalho primeiramente a Deus, por abençoar minha vida e me dar forças para sempre continuar.

A minha mãe Maria de Fátima da Silva, que mesmo a distância, não deixou de me apoiar com seus conselhos e carinho.

Ao meu pai Mário Antônio da Silva, que sempre me entendeu e nunca disse um não para os meus sonhos, que me ensinou o valor e a dignidade do trabalho.

A minha querida irmã Jéssica Karolainy, por sua amizade e carinho de irmã, que foi essencial para manter a minha autoestima e me mostrar os valores da amizade.

A minha companheira Marcela Larissa, que me acompanhou desde o princípio, em cada desafio e nos bons e maus momentos.

Agradeço também ao meu colega Anderson Melo, que sempre esteve disposto a me ajudar durante todo o trabalho, contribuindo com seus conhecimentos e experiência.

Ao prof. Ms. Sérgio Mendonça, que esteve disposto a trabalhar comigo, me dando conselhos e conhecimentos no decorrer deste trabalho, que levarei para sempre comigo tudo que aprendi.

E por último, aos meus amigos que moraram comigo, Moisés Carlos, Francisco Ramiro e Ihago Santos e a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

Resumo

A cadeia produtiva no ramo alimentício tem gerado cada vez mais informações sobre os seus processos. Garantir a integridade e segurança dessas informações tem sido um desafio. O trabalho atual tem com objetivo entender e avaliar quais tipos de informações são geradas nesses processos, assim como a partir dos resultados obtidos, implementar uma solução que possa gerar identificadores para queijos e por meio de uma rede Blockchain local validar essas informações, bem como a partir de uma aplicação móvel ser possível visualizar esses dados. Para isso foi necessário entender sobre a estrutura da Blockchain e suas características em relação a segurança da informação por meio de uma pesquisa bibliográfica. Foi identificado pontos importantes da rastreabilidade para os processos produtivos de alimentos. Com os resultados foi possível modelar e implementar um sistema *web* capaz de registrar dados sobre um queijo e seu fabricante em uma rede Blockchain local, validar as informações fornecidas e disponibilizar para os seus consumidores por meio da aplicação QRQuejio (*Android*), além de identificar as localidades em que o queijo foi transportado. E, utilizando-se de um sistema de consulta em múltiplos níveis, averiguar a autenticidade dos registros por meio de uma leitura na base de dados do sistema e na Blockchain local, para a confirmação da autenticidade do registro.

Palavras-chave: Blockchain. Segurança da informação. Rastreabilidade.

Abstract

The food chain in the food industry has generated more and more information about its processes. Ensuring the integrity and security of this information has been a challenge. The current work aims to understand and evaluate what kind of information is generated in these processes, as well as from the results obtained, implement a solution that can generate identifiers for cheeses and through a local Blockchain network validate this information, as well as from a mobile application it is possible to view this data. For this, it was necessary to understand the structure of Blockchain and its characteristics in relation to information security through a bibliographic search. Important points of traceability have been identified for food production processes. With the results it was possible to model and implement a web system capable of recording data about a cheese and its manufacturer in a local Blockchain network, validating the information provided and made available to its consumers through the QRQuejio (Android) application, in which the cheese was transported. And, using a multi-level query system, check the authenticity of the records by reading the system database and the local Blockchain to confirm the authenticity of the record.

Keywords: Blockchain. Information security. Traceability.

Lista de ilustrações

Lista de tabelas

Lista de códigos

Lista de abreviaturas e siglas

IoT	Internet of things
TI	Tecnologia da Informação
QR	Quick Response
GPS	Global Positioning System
SGBDs	Sistemas Gerenciadores de Banco de Dados

Sumário

1 Introdução

A presença da tecnologia na vida das pessoas é atualmente vista pela sociedade como algo comum, estando inserida em ambientes domésticos, sociais, acadêmicos, profissionais e também industriais. Se bem utilizados, os recursos tecnológicos contribuem para melhores resultados nas diversas áreas do cotidiano. Segundo o Gartner (2019), os setores de Tecnologia da Informação (TI), por se tratarem de serviços e produtos gastos mundialmente, devem atingir US$ 3,76 trilhões em 2019, com um aumento esperado de 3,2% em relação a 2018.

A rápida evolução tecnológica implica em um aumento da disponibilidade e alcance das informações, consequencia do grande consumo desses recursos pela população. A informação, segundo Moresi (2000), tem um grande valor para tomadas de decisões e agrega valores para as necessidades, interesses e para o conhecimento. A preocupação com a segurança e a integridade dessas informações são fatores primordiais para todos que às mantém.

Sistemas distribuídos são exemplos dessas tecnologias, utilizados para atender as necessidades dos usuários e/ou fornecedores, buscando atingir os melhores resultados dentro do que se espera. Segundo Tanenbaum (2007), esses sistemas são definidos como sendo "uma coleção de computadores independentes entre si, que se apresenta ao usuário como um sistema único e coerente". Sendo assim, pode-se afirmar que os sistemas distribuídos estão em todos os lugares, ou melhor, acessíveis a partir de qualquer lugar, permitindo aos usuários a possibilidade de compartilhamento de informações, transações financeiras, redes sociais e outros.

Garantir a segurança em qualquer sistema é um fator importante no desenvolvimento de um projeto. Para o alcance dos objetivos e adequado funcionamento de um projeto, há uma necessidade de proteção das informações sejam garantidas. Em sistemas distribuídos, muitos dados que trafegam pela rede são sensíveis, logo, a segurança é primordial. Portanto, três fatos são considerados essenciais para a seguridade das informações: a confiabilidade, disponibilidade e integridade (SCARFONE; JANSEN; TRACY, 2008).

Segundo Nakamoto (2008), a rede Blockchain garante os fatores de segurança da informação, pois, visa a descentralização como aspecto para tal função. A base de dados dessa tecnologia é distribuída, onde a geração de novos registros são chamados de blocos e são listados de forma encadeada. Cada novo bloco possui suas informações criptografadas e mantém a identificação para o bloco anterior. Dessa forma, o conteúdo de um bloco se alterado, mudaria o estado de seu identificador

e com isso os decorrentes precisariam ser gerados novamente. Sendo assim, para uma rede com grandes quantidades de registros, seria impossível computacionalmente realizar a geração de todos os blocos posteriores, tornando assim a Blockchain uma rede imutável.

Este trabalho propôs o estudo do tema, estimulado a partir de uma experiência como consumidor de queijos regionais, onde os mesmos não possuíam informações sobre suas características e localidade. O interesse de pesquisa sobre a temática parte também do evidente comprometimento das informações desses queijos e da falta de garantia para os consumidores. Fato este comprovado por notícias como “a destruição de 13 mil queijos de leite cru da Serra da Canastra por terem sidos mantidos em estoque e comercializados sem registro em órgão fiscalizador e sem identificação de origem (MOL, 2015)”, levantando discussões como a rastreabilidade do queijo, desde a origem da matéria-prima, até o produto final.

O projeto objetivou a implementação de um sistema que utiliza a rede Blockchain, um conjunto de regras que permitem os usuários a possibilidade de adquirir queijos sem ter que se preocupar com as informações atribuídas nas embalagens, pois o Blockchain possui as características necessárias para a segurança das informações da aplicação (NAKAMOTO, 2008), diminuindo assim os riscos de fraudes por meio dos fornecedores e fabricantes. Além disso, buscou desenvolver um aplicativo Android para os consumidores, com o propósito de disponibilizar as informações sobre o queijo na “palma da mão”, permitindo saber aspectos como: validade, data de fabricação, nome e endereço do fabricante, bem como o percurso do queijo até a mesa do consumidor.

1.1 Objetivos

O objetivo principal deste trabalho é o desenvolvimento de um sistema computacional utilizando a rede Blockchain, capaz de garantir aos consumidores de queijos a integridade e autenticidade das informações geradas, desde a fabricação até a mesa do consumidor. E, através de uma aplicação baseada no sistema operacional Android, ser capaz de visualizar essas informações.

1.1.1 Objetivos Específicos

- Investigar casos de riscos e casos reincidentes sobre queijos no Brasil para identificar falhas de segurança;
- Identificar os princípios para a criação de uma estrutura Blockchain e suas características;
- Analisar o uso de um banco de dados e uma Blockchain;

- Definir os requisitos e desenvolver uma aplicação capaz de validar e gerar identificadores utilizando os princípios de segurança da Blockchain para garantir a autenticidade e integridade das informações dos queijos;

- Construir uma aplicação *Android* para a visualização dos resultados com segurança utilizando as propriedades da rede Blockchain.

1.2 Metodologia

Esta pesquisa utilizou como metodologia a classificação de Prodanov e Freitas (2013). Desta maneira, este trabalho caracteriza-se como uma pesquisa aplicada, que tem como objetivo *"gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Envolve verdades e interesses locais"*.

O método científico para realização deste trabalho é definido como hipotético-dedutivo, classificado a partir de um problema, formulando as hipóteses com base nas dificuldades que constituem o problema e, com essas hipóteses, entende-se as consequências que serão testadas ou falseadas, ou seja, refutadas.

Para uma melhor clareza sobre o problema e consequentemente formular as hipóteses sobre o mesmo, os objetivos de estudos deste trabalho foram classificados como exploratórios. Sendo assim, a abordagem foi definida como qualitativa.

O mecanismo técnico utilizado foi a pesquisa bibliográfica, que permitiu identificar informações em conteúdos já publicados e em materiais online, para análise posterior desses resultados.

A composição deste trabalho foi dada da seguinte forma: 1) Definição do tema de estudo; 2) Definição dos objetivos; 3) Revisão bibliográfica sobre a segurança da informação e seus princípios, os conceitos que regem a estrutura da Blockchain e suas aplicabilidades atualmente e, sobre a definição da rastreabilidade de produtos alimentícios para a integridade das suas informações; 4) Estruturação da modelagem de uma aplicação, a partir dos resultados da revisão, que consistiu na geração de um identificador confiável que pode garantir a integridade das informações geradas para um determinado queijo; 5) Implementação do sistema desenvolvido, com análise da sua confiabilidade.

1.3 Estrutura do Trabalho

O capítulo 2 se inicia com a fundamentação teórica para a compreensão do tema em estudo, apresentando a rede Blockchain e suas características. Além disso é ilustrado dados sobre a segurança da informação, seus princípios, autenticidade e

rastreabilidade. No capítulo 3, é apresentado de forma detalhada a implementação da aplicação desenvolvida. Por fim, o capítulo 4 é composto pelos os resultados obtidos no decorrer do trabalho, bem como as conclusões e trabalhos futuros.

2 Fundamentação Teórica

Este capítulo apresenta uma breve descrição dos tópicos importantes para fornecer um melhor entendimento e contribuição para o trabalho em questão.

2.1 Blockchain

Em uma transação financeira tradicional, como a transferência de dinheiro, é exigido uma instituição financeira intermediária confiável, como por exemplo, os bancos, para que seja assegurado que ocorra de forma esperada. Sistemas assim são considerados centralizados, com cobrança de taxas e o aplicação de um tempo de espera na transação.

A ideia do Blockchain, surgiu em 2008 por meio de um whitepaper (artigo) chamado "Bitcoin: A Peer-to-Peer Electronic Cash System", mais conhecido atualmente pela criptomoeda Bitcoin, com autoria de uma pessoa ou grupo, cujo codinome é Satoshi Nakamoto (NAKAMOTO, 2008). O termo criptomoeda foi descrito pela primeira vez em 1998, por Dai, em seu trabalho sobre o "Dinheiro B", que é um sistema eletrônico e anônimo de pagamentos (DAI, 1998).

Nakamoto (2008) descreveu em seu artigo sobre uma moeda digital, o Bitcoin, a primeira moeda digital a permitir transações financeiras sem intermediários, portanto descentralizada. A possibilidade de transações sem um intermediário é feita por meio de um banco de dados distribuído, na qual são gravadas e verificadas por todos os usuários (nodos) da rede, definida por Nakamoto como Blockchain. Este recurso torna desnecessário o controle de uma entidade administradora, impossibilitando a manipulação nos valores e emissões das moedas.

A ideia da criação da criptomoeda Bitcoin e da rede Blockchain, trouxe de volta a confiança aos investidores, que vivenciavam uma grave crise financeira na época, que teve seu início com a chamada “bolha imobiliária” (BRESSER-PEREIRA, 2009), ocasionando várias consequências para o mundo financeiro, sendo uma delas a desconfiança dos investidores.

Segundo Christidis e Devetsikiotis (2016), Blockchain é uma estrutura de dados distribuída, que é replicada e compartilhada entre os membros de uma rede. Esta estruturação permite que cada um dos nodos da rede (os chamados mineiros) avaliem as transações, validando e adicionando informações no banco de dados distribuído, chamado livro-razão.

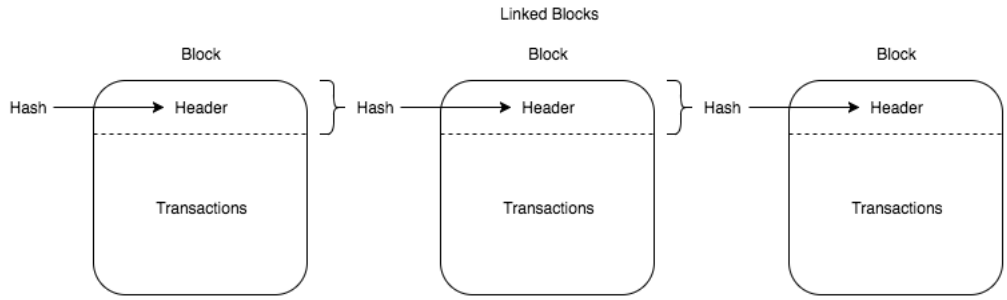
2.1.1 Transações

Na rede Blockchain as transações possuem endereços de entrada e saída. O endereço de entrada possuí os valores onde serão retirados, já o de saída informa quem receberá esses valores. Essa é a definição mais simples que se tem em uma transação no Blockchain. Em outras palavras, este recurso funciona como um "livro razão", armazenando todas as transações realizadas na rede. Cada bloco (nó) possui uma "digital", chamada de hash, que deverá conter o número do bloco atual e o número do próximo, formando uma “cadeia de blocos” (Blockchain).

Para escrever no livro razão, cada nova transação deverá ser validada para garantir a integridade da rede. Está forma de validação é conhecida como mineração, realizada por todos os blocos da cadeia através de uma prova de trabalho (PoW, na sigla em inglês) ou de uma Prova-de-Posse (PoS, na sigla em inglês), que se utilizam do poder de processamento e, consequentemente, gera um grande gasto de energia para solucionar cálculos matemáticos (CHICARINO et al., 2017).

Encontrar o hash válido permitirá que a nova transação seja inserida no Blockchain e quem o encontra recebe uma recompensa. Ao localizar o determinado hash, todos os nós deverão atualizar com a nova transação, buscando garantir a integridade da rede, assegurando que nenhum bloco possa ser inserido ou modificado na cadeia, sem que seja verificado pelos outros nós da rede (NAKAMOTO, 2008). A figura 1, apresentada abaixo, demonstra uma estrutura das transações na rede Blockchain.

Figura 1 – Estrutura de transações da rede Blockchain



Fonte: Liu (2019).

A primeira transação da cadeia gera o bloco gênesis, o bloco é um caso especial, pois ele não possuí um bloco anterior e, para a Bitcoin e quase todos os seus derivados, produz um subsídio não-sustentável. Ele é codificado no *software* para agir no estado inicial do sistema, podendo conter informações sobre as regras ou instruções que os demais blocos deverão obedecer. Na criptomoeda Bitcoin, o (s) utilizador (s) do

codinome Satoshi Nakamoto, lançou o bloco gênesis no dia 3 de janeiro de 2009, tendo como recompensa as primeiras 50 bitcoins.

2.1.2 Estrutura de um Bloco

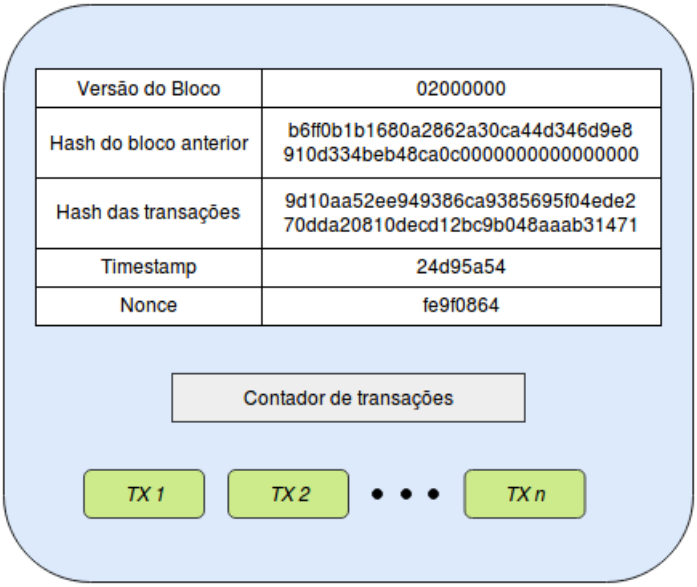
Segundo Zheng et al. (2016), um bloco possui em sua estrutura o cabeçalho e o corpo. O corpo representa os dados das transações que são armazenados no bloco. Enquanto o cabeçalho inclui em sua estrutura: a versão do bloco que possui o conjunto de regras para a validação do próximo bloco; a hash do bloco anterior; a hash de todas as transações; o *timestamp*, que leva em consideração um ponto específico na linha do tempo; e o nonce, um número que só pode ser utilizado apenas uma vez. Ferreira et al. (2017), além de destacar esses atributos, acrescenta como características a dificuldade e a altura de um bloco, como é mostrado na Figura 2.

- **Transações:** como já mencionado anteriormente, uma transação possui um endereço de entrada e saída. No Bitcoin, por exemplo, uma transferência de um valor tem uma conta associada que será a entrada da transação. Por outro lado, existe uma conta de saída, que no processo é informado o endereço de quem irá receber o valor da transferência. Para cada transação, cria-se um bloco na rede Blockchain que precisará ser validado, para que seja inserido no "livro razão"dos demais blocos da rede. Para que a transação seja incluída na rede, todo novo bloco precisa ser minerado, para garantir a integridade dos dados.
- **Hash do bloco anterior:** no cabeçalho dos blocos, está presente uma hash que aponta para o bloco anterior da cadeia. Essa hash de 256 bits, identifica a hash do bloco anterior, como também é inserido no cabeçalho do próximo bloco. Formando assim uma corrente, que tem no seu inicio o bloco gênesis.
- **Nonce:** segundo Zheng et al. (2016), o nonce é um campo em um bloco que possui um tamanho de 4 *bytes*, que em geral começa com 0 e vai aumentando para cada cálculo de hash. É utilizado como prova-de-trabalho na mineração, pois, caso o encontre, as regras estabelecidas na rede consideram-se cumpridas.
- **Dificuldade:** segundo Ferreira et al. (2017), a dificuldade é uma colisão parcial de hash. O processo de mineração de um bloco tem como objetivo encontrar a hash que satisfaça as condições da colisão espacial. Em vista disso, a alteração de qualquer informação dos dados de um bloco, acarretará na mudança de seu hash, sendo assim, a utilização do nonce é necessária, pois, se houver qualquer mudança o hash também será alterado, impondo assim uma dificuldade. Para o minerador poder encontrar a hash necessária e validar o bloco na cadeia, o minerador precisará de poder computacional para a realização dos cálculos de prova de trabalho e consequentemente precisará consumir energia.

- **Versão do bloco:** na estrutura do bloco de uma cadeia, o seu principal identificador é a hash do cabeçalho, ou seja, a versão do bloco, obtido ao realizar uma operação de resumo criptográfico no próprio cabeçalho. Além disso, é inserido no bloco posterior, interligando os blocos da rede.
- **Altura do bloco:** a inserção dos blocos na cadeia, é feita de forma linear em ordem cronológica. Os novos blocos recebem números de ordem e a altura é determinada pela diferença entre o bloco gênesis e o primeiro bloco. A altura nem sempre é usada para identificar um bloco.
- **Timestamp:** na geração de cada bloco, é armazenado o timestamp, que representa o tempo atual do bloco gerado e os segundos decorridos desde o dia 01 de janeiro de 1970.

  Abaixo, na figura 2, é representado a estrutura de um bloco com mais detalhes.

Figura 2 – Estruturas de um bloco do Blockchain



Fonte: próprio autor

A representação do bloco na figura 2, demonstra como é a sua estrutura em uma rede Blockchain. Na parte superior está localizado o cabeçalho do bloco. O cabeçalho contém as informações da versão do bloco, hash do bloco anterior para a identificação da sequência da cadeia, assim como o hash das transações, o timestamp que faz o registro do momento da geração do bloco e o nonce que realiza a validação do bloco na cadeia. Na parte inferior está representado as transações que são inseridas nos blocos, sendo que cada bloco realiza as inserções das transações até que se atinja o limite.

2.1.3 Aplicabilidade do Blockchain

Por possuir características primordiais para pagamentos eletrônicos, a tecnologia Blockchain é de aplicabilidade bem mais integral (HUCKLE et al., 2016). A seguir, será apresentado algumas de suas aplicabilidades.

2.1.3.1 Internet das Coisas

A existência da Internet das Coisas (IoT, sigla em inglês para *Internet of Things*), é atualmente uma das mais promissoras tecnologias de informação e comunicação (TIC). Segundo Atzori, Iera e Morabito (2010), a IoT é proposta para integrar as coisas (também chamadas de objetos inteligentes) na Internet e fornece aos usuários vários serviços, como: automotivas para energia, assistência médica, casas inteligentes, dentre outros recursos.

A previsão de crescimento dessa tecnologia para 2020, é de mais de 25 bilhões de dispositivos conectados à internet, de acordo com oGartner (2015). São tantas conexões que possibilitarão que os dados usados sejam analisados e gerenciados e, a partir disso, permitirá que as tomadas de decisões sejam feitas de forma autônoma.

A IoT abrange o processamento de dados e a comunicação entre dispositivos de plataformas, com capacidades diferentes, de forma autonômica e sem intervenção humana. Nas últimas décadas esse termo despontou como uma evolução da internet e um novo paradigma tecnológico, social, cultural e digital.

A internet das coisas é considerada uma extensão da internet atual (SANTOS et al., 2016), visto que proporciona aos objetos do dia-a-dia (eletrodomésticos, meios de transporte e até acessórios, como óculos e relógios) a capacidade computacional e de comunicação ao se conectarem a Internet. A conexão com a rede mundial de computadores viabilizará o controle remoto dos objetos e permitirá que os próprios objetos sejam acessados como provedores de serviços, tornando-os inteligentes ou smart objects. Os objetos inteligentes possuem capacidade de comunicação e processamento aliados a sensores.

Dentre as principais características associadas a Iot, destacam-se:

- autenticação segura;
- transmissão segura de dados;
- segurança dos dados utilizados pelos dispositivos de IoT;
- acesso seguro aos dados por pessoas autorizadas;
- protocolos de autenticação;

2.1.3.2 *Smart Contracts*

A introdução de programas de computadores executáveis na rede blockchain, que possibilitam a execução de métodos por meio de condições lógicas de negócios, complicadas e programáveis, é conhecida como *Smart Contracts* (Wang et al., 2019). Para que um contrato seja considerado inteligente, o envolvimento de duas ou mais partes deve existir. Entretanto, para a firmação do contrato não deve existir o envolvimento direto das partes, assim como a linguagem escrita nos contratos não se remetem a linguagem jurídica, como um contrato comum, mas declara as obrigações, os benefícios e as penalidades das partes envolvidas (CHRISTIDIS; DEVETSIKIOTIS, 2016). Todo o contrato é realizado por meio de condições pré-definidas que são executadas em computadores a partir dos resultados obtidos.

Segundo Szabo (1997), que na década de 90 formalizou a ideia de *Smart Contracts*, definiu o termo como sendo “um protocolo de transação informatizado que executa os termos de um contrato". Para além disso, o autor listou seus objetivos gerais, afirmando sobre os requisitos necessários para satisfação de condições contratuais do *Smart Contracts*, sendo elas:

- condições de pagamento;
- ônus;
- confidencialidade;
- cumprimento;

e para os objetivos econômicos relacionados a reduções:

- perdas por fraude;
- arbitragens;
- custos de execução;
- e outros custos de transação;

O Blockchain possui propriedades que podem garantir a segurança destes contratos, tendo o potencial de permitir que todo o processo seja automatizado de forma virtual. Porém, também existe a possibilidade de contratos serem mistos, com uma complementação feito a papel. Segundo Luu et al. (2016), a segurança é garantida pois a execução do código é totalmente descentralizada e distribuída pela rede, como também não é possível alterar os resultados, uma das características da Blockchain.

2.2 Segurança da Informação

É notório o crescente e constante aumento no consumo abundante de informações através dos dispositivos tecnológicos hoje em dia, em qualquer lugar do mundo. Garantir a segurança desses dados é um grande desafio atual. Para Junior (2018), a seguridade dessas informações são mais valorizadas quando há ocorrências de ataques cibernéticos, por exemplo. Para assegurar essas informações, foi necessário a criação de normas que as preservassem, citando a norma ABNT NBR ISO/IEC 27002:2013, que afirma que "segurança da informação é a proteção de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT, 2013).

Para McGee (1994), pode-se entender informação como sendo um conjunto de dados armazenados e que organizados possuem um significado, portanto um valor. Enquanto Sêmola (2003) afirma que as informações representam a inteligência e um ativo intangível, que possui um valor que proporciona vantagens competitivas às organizações.

2.2.1 Princípios de segurança

A segurança da informação atua em três princípios básicos que sempre devem ser respeitados ou a segurança correrá riscos. Estes princípios segundo, Campos (2007), são:

- **Confidencialidade:** garantir o acesso às informações somente por indivíduos autorizados, mantendo-as em sigilo;
- **Integridade:** impossibilitar a modificação de informações indevidamente;
- **Disponibilidade** disponibilizar as informações sempre que consultadas, mas somente para pessoas autorizadas a obterem tais informações.

2.2.2 Uso de Blockchain para atender aos princípios de segurança

Greve et al. (2018), apresenta em seu trabalho o uso da Blockchain para atender aos princípios de segurança, como na identificação dos usuários, que ocorre tradicionalmente na análise de documentos físicos, emitidos habitualmente pelos governos. Para a segurança dos usuários, na rede Blockchain os mesmos possuem uma chave criptografada do seu endereço na rede, que garantem o seu anonimato, proporcionando assim o princípio da confidencialidade, onde somente os usuários que estão devidamente registrados possuem acesso as informações.

A Blockchain também pode garantir o princípio da integridade. Pois, para cada nova transação inserida na rede, jamais poderá ser alterada futuramente, porque mesmo que ocorra falhas na base de dados, as informações permanecem inalteradas por permitir a replicação dos seus dados em distribuições pela rede.

Também em decorrência de seus dados estarem distribuídos em base de dados por toda a extensão da rede, a Blockchain assegura o princípio da disponibilidade, permitindo que seus dados sejam mantidos sempre a disposição, quando consultados por usuários autorizados, mesmo na ocasião de falhas na rede.

2.3 Assinatura Digital

SegundoGandini, Salomão e Jacob (2001), um documento digital é definido como:

> Aquele que nos representa um fato, mas para termos acesso a ele é necessária a intervenção de um programa de computador. Assim, podem ser conceituados como aqueles que se encontram arquivados em formato digital, não podendo ser percebido pelo homem sem o auxílio de um computador. É ele uma sequencia de bits, que, traduzida, nos representará um fato.

Atualmente a criação de documentos e contratos digitais estão presentes em muitos lugares e permeiam desde a criação de contas em redes sociais, até a compra de um simples insumo alimentício. Esse novo modelo de documentação tem como principal vantagem, seu rápido compartilhamento de informações Gandini, Salomão e Jacob (2001).

Alguns desses documentos necessitam de uma assinatura e a forma tradicional em alguns casos não pode utilizada. Para isso foi desenvolvida a assinatura digital, que proporciona integridade e autenticidade aos documentos assinados (KAZIENKO et al., 2003).

Os documentos eletrônicos, mesmo com suas formas de seguranças, ainda possuem falhas, permitindo esses possam ser alterados ou falsificados. As assinaturas digitais tem como função selar o conteúdo do documento, garantindo assim sua integridade ou, se caso alterado, possibilita a identificação da fraude, bem como garante a autenticidade e a tempestividade (KAZIENKO et al., 2003). A ideia de assinar digitalmente pode ser estendida para outras formas de autenticidade e garantias de segurança, como mostra a próxima seção.

2.3.1 Registro de autenticidade com Blockchain

Mesmo com a existência de mecanismos para assegurar a integridade das informações e evitar alterações em documentos digitais, ainda é possível ultrapassar essas barreiras impostas pela computação. Uma das soluções atuais para esse problema é a utilização da Blockchain, que possui características essenciais para garantir a segurança. Muito utilizado atualmente por empresas e cartórios para a autenticidade dos seus documentos.

A Blockchain permite que diversos tipos de documentos digitais sejam registrados através de um carimbo de tempo, oferecido por uma rede Blockchain pública em suas validações, que comprova a existência de qualquer tipo de documento. A empresa Originalmy se destaca, pois, foi a primeira empresa brasileira a fazer uso da Blockchain. Criada em 2015, utilizava a rede inicialmente para efetuar provas de autenticidade para documentos digitais (ORIGINALMY, 2017).

O trabalho realizado por Morais (2019), teve como objetivo a avaliação da viabilidade do uso de Blockchain para garantir segurança na emissão de diplomas digitais por Instituições de Ensino Superior. Seus resultados demonstram a possibilidade de geração de diplomas digitais validados pela Blockchain, garantindo assim a integridade das informações geradas, assim como a sua autenticidade. Este processo é validado por meio de um sistema de consulta em múltiplos níves da base local, verificando se o mesmo também é existente na rede, antes de confirmar a autenticidade.

A implementação da Blockchain é uma ótima solução para quem busca garantir a autenticidade das informações em seus documentos digitais, por possuir princípios de segurança que permitem isso, desde a descentralização das informações, à disponibilidade dessas informações somente a usuários autorizados.

2.4 Banco de dados

Segundo Elmasri et al. (2005), um banco de dados é uma coleção de dados relacionados, que podem ser gravados e que possuem um significado implícito. O autor ainda afirma que a definição de banco de dados, mencionada anteriormente, é muito genérica e descreve as seguintes propriedades implícitas:

- Um banco de dados representa alguns aspectos do mundo real, sendo chamado, às vezes, de minimundo ou de Universo de Discurso (UoD). As mudanças no minimundo são refletidas em um banco de dados;
- Banco de dados é uma coleção lógica e coerente de dados com algum significado inerente. Uma organização de dados ao acaso (randômica) não pode ser

corretamente interpretada como um banco de dados;

- Banco de dados é projetado, construído e povoado por dados, atendendo a uma proposta específica. Possui um grupo de usuários definido e algumas aplicações preconcebidas, de acordo com o interesse desse grupo de usuários.

Para Silberschatz et al. (1997), um banco de dados *"é uma coleção de dados inter-relacionados, representando informações sobre um domínio específico"*, ou seja, agrupando informações que se relacionam e procedem de um mesmo assunto, pode-se afirmar que se tem um banco de dados. Alguns exemplos de banco de dados podem ser citados para situações comuns, como: uma lista de produtos de um supermercado; registro de arquivos; e até mesmo o controle financeiro de uma empresa. As informações registradas no banco de dados podem ser colocadas a disposição dos usuários caso haja uma consulta, uma inserção ou uma atualização dos dados (KUHNEN, 2016).

O banco de dados ainda permite que os dados sejam gerenciados, para facilitar a criação e manutenção dos mesmos. A partir disso, surgiu os Sistemas Gerenciadores de Bancos de Dados (SGBDs). Para Silberschatz et al. (1997), *"o principal objetivo de um SGDB é proporcionar um ambiente tanto conveniente quanto eficiente para a recuperação e armazenamento das informações do banco de dados"*. Outra definição para o SGBD é um sistema que possui funcionalidades básicas, como operações para inserção, atualização, exclusão e consulta de dados de um determinado sistema (ELMASRI, 2008). Outras funcionalidades mais avançadas são atribuídas a esse recurso, como:

- Controle de redundância;
- Restrição de acesso não autorizado;
- Garantia de armazenamento persistente para objetos programas;
- Garantia de armazenamento de estruturas para o processamento eficiente de consultas;
- Garantia de backup e restauração;
- Fornecimento de múltiplas interfaces para os usuários;
- Forçar as restrições de integridade;
- Permitir interferências e ações usando regras.

2.4.1 Blockchain vs Banco de dados

A Blockchain segundo Nakamoto (2008), é uma estrutura de dados distribuída, permitindo que suas transações sejam registradas como um "livro razão". Para cada nova transação pelos seus usuários (nós), é gerado um novo bloco. Antes de registrar as informações da transação, cada usuário calcula e atualiza as novas entradas do banco de dados (BAUERLE, 2018). Portanto, os nós trabalham juntos, validando e verificando cada nova inserção antes de registrar na rede, garantindo assim segurança.

Em comparação com um banco de dados qualquer, a Blockchain possui propriedades que se diferenciam, atendendo aos princípios de segurança (GREVE et al., 2018). A integridade também é uma das características sobressalentes na Blockchain, sendo impossível alterar um dado já registrado, pois seria exigido muito poder computacional para recalcular todos os nós posteriores. Sendo assim, um banco de dados permite que ocorra alterações em seus dados por meio de seu gerenciamento, entretanto a imutabilidade é presente na Blockchain.

Outro ponto que se destaca, é que a Blockchain possui sua base de dados descentralizada, permitindo que partes diferentes, que não se conheçam e nem se confiam, compartilhem informações sem ter a necessidade de um administrador central. Cada nó avalia as transações, validando e adicionando no banco de dados distribuído, havendo a necessidade de um mecanismo de consenso que permita o compartilhamento dos registros simultaneamente. Em um banco de dados centralizado, há a necessidade de um administrador central e, caso ocorra a perda dos dados por invasão, falhas ou desastres naturais, esta será permanente. Diferentemente da Blockchain que possui seus dados replicados e sempre disponíveis (CHRISTIDIS; DEVETSIKIOTIS, 2016). A tabela 1, apresenta a comparação entre banco de dados e Blockchain para o melhor entendimento.

Tabela 1 – Comparação entre Banco de dados e Blockchain

Características	Banco de dados	Blockchain
Tipo de acesso	Com permissão	Sem permissão
Controle	Centralizado	Descentralizado
Tipos de dados	Não persistentes	Imutável
Sensível a falhas	Sim	Não
Administrador	Sim	Não
Desempenho	Extremamente Rápido	Médio Lento

Fonte: Schlapkohl (2019).

2.5 Rastreabilidade

Nos últimos anos a população vem crescendo de forma exponencial e, em decorrência deste fato, a busca por alimentos tem demandado um aumento da performance dos produtores e novos métodos de produção começam a surgir, muitas vezes irregulares ou indesejáveis. Consequentemente, desperta uma maior preocupação dos consumidores, que exigem cada vez mais informações sobre os impactos econômicos, ambientais e sociais da produção desses alimentos (LIRANI, 2005).

A rastreabilidade por meio de seus registros, consegue identificar a diferenciação que possa haver em seus ingredientes ou que tenha acontecido em diferentes processos de sua produção (BRASIL, 2012). Existe ainda a capacidade de recuperação do histórico, da aplicação ou da localização de uma entidade (ou item) por meio de identificações registradas (MACHADO, 2005). Segundo padrões internacionais, o Regulamento no178/2002, da comunidade Europeia, define a rastreabilidade como:

> A capacidade de detectar a origem e de seguir o rasto de um gênero alimentício, de um alimento para animais, de um animal produtor de gêneros alimentícios ou de uma substância, destinados a ser incorporados em gêneros alimentícios ou em alimentos para animais, ou com probabilidades de o ser, ao longo de todas as fases da produção, transformação e distribuição"(EUROPEU, 2002)."

As consequências da falta da rastreabilidade são noticiadas pelas mídias, citando como exemplo o casos de apreensão de 14 toneladas de queijo coalho durante uma operação na cidade do Recife, em Pernambuco, onde investigadores apontaram que rótulos eram falsificados e validades adulteradas (G1, 2018). Bem como, o caso associado a marca *“Serra da Canastra”*, onde 14 quilos de queijo foram apreendidos por possuir selo e rótulo falsificados na cidade de Rio Claro (BAUER, 2017). Casos assim são recorrentes todos os anos no Brasil e tais dados mostram que a falta da rastreabilidade acaba trazendo fragilidade na segurança das informações.

Para Resende e Lopes (2004), a rastreabilidade possui fatores positivos para o gerenciamento, controle de riscos e garantia de qualidade de um produto. No que tange aos riscos, a rastreabilidade permite uma melhor tomada de decisão com ações corretivas ou preventivas durante o processo. Além disso, são ressaltados outros benefícios atrelados a cadeia produtiva (BRASIL, 2012):

- diagnóstico de problemas na produção e na imputação de responsabilidade;
- cumprimento da legislação, quando existente;
- agilidade e eficácia nos procedimentos de *recall*, protegendo a reputação da marca;

- minimização dos custos associados a uma retirada de produto do mercado;
- possibilidade de identificação de produtos diferenciados ou que possuam atributos não facilmente perceptíveis ou, ainda, de difícil mensuração;
- valorização dos atributos de processo diferenciados, como a produção agroecológica, criação ao ar livre, criações que respeitem o bem-estar animal e também produções ambientalmente e/ou socialmente corretas;
- possibilita a identificação da origem de problemas relacionados com a presença de resíduos e/ou contaminantes nos produtos;

Entretanto, a criação de um sistema de rastreabilidade, não garante por si só a segurança e qualidade do alimento, salienta Marins e Miranda (2006). Portanto, para assegurar os objetivos desejados com a rastreabilidade, o sistema implantado dependerá principalmente da escolha da complexidade e da profundidade que o sistema adotará. Durante a cadeia produtiva, a quantidade de dados registrados e uma melhor comunicação junto a transmissão dos dados, permitirão com que os processos gerados possuam melhores informações, vantagens e privilégios para quem implantar a rastreabilidade.

3 Implementação do Sistema

Neste capítulo será apresentado o desenvolvimento de uma aplicação que irá realizar a geração de identificadores digitais para queijos e como será possível manter a integridade, inserindo-o em uma rede Blockchain local. A seção 3.1 especificará os requisitos funcionais e não funcionais que serão necessários para o funcionamento e qualidade do sistema. Na seção 3.2, será apresentada a prototipação do sistema, onde será exibido as principais telas da aplicação e as funcionalidades de cada uma delas. Por último, a seção 3.3, será constituída das informações sobre o funcionamento da rede Blockchain local, utilizada neste projeto.

3.1 Definição dos requisitos

O sucesso de um projeto de *software*, parte a princípio da necessidade da engenharia de requisitos como um importante mecanismo da aplicação. Segundo Pressman (2006), a engenharia de requisitos ajuda os *engenheiros de softwares* a compreender melhor os desafios que eles precisarão solucionar no desenvolvimento. Como também, contribui para um melhor entendimento dos impactos do produto sobre o negócio e, dos interesses do cliente quanto aos usuários finais que irão interagir com o software. Dentre os citados requisitos existem: os Requisitos Funcionais (RF) e os Requisitos Não-Funcionais (RNF), ambos apresentados na próxima subseção.

3.1.1 Requisitos funcionais

Os Requisitos Funcionais (RF) definem recursos específicos do sistema, assim como as funções de um sistema e seus componentes, podendo ser cálculos, comportamentos, manipulação de dados, dentre outras (SOMMERVILLE, 2007). A Tabela 2 apresenta os RF que retratam as principais funcionalidades que a aplicação deverá apresentar.

Tabela 2 – Requisitos Funcionais

ID	Nome	Prioridade
RF 01	Registro de um produto	Essencial
RF 02	Geração de identificador	Essencial
RF 03	Registro do identificador na Blockchain	Essencial
RF 04	Registro do identificador na base de dados	Essencial
RF 05	Validação dos identificadores	Essencial
RF 06	Disponibilização dos registros	Essencial

Na tabela acima pode-se observar os requisitos funcionais fundamentais da aplicação. Tais funcionalidades, como o cadastro e registro de um produto na base de dados, é realizado através de informações fornecidas sobre a localização do fabricante e o produto, para que seja feita a geração do identificador, onde o mesmo é registrado na Blockchain local como na base de dados para potenciais consultas. Além da validação do identificador gerado de um documento emitido, será verificado o novo hash calculado, se o mesmo se encontra inserido na Blockchain na base de dados local da aplicação, para a confirmação. E, por último, a disponibilização dos registros para verificação dos dados de cada produto cadastrado no sistema.

Ainda sobre a tabela 2, é exibido na coluna “ID” a lista dos RF de forma sequencial, enquanto que na coluna “Prioridade”, temos o grau de prioridade que a aplicação deverá ter para cada funcionalidade, aplicando a definição de “Essencial” para todos os RF, pois são funcionalidades principais para a aplicação.

3.1.2 Requisitos Não-Funcionais

E também existe os Requisitos Não-Funcionais (RNF) definido por Davis (1993), como *“os atributos globais requeridos pelo sistema, incluindo portabilidade, confiabilidade, eficiência, testabilidade, compreensibilidade e modificabilidade”*. A Tabela 3, apresenta os requisitos não funcionais desta aplicação.

Tabela 3 – Requisitos Não-Funcionais

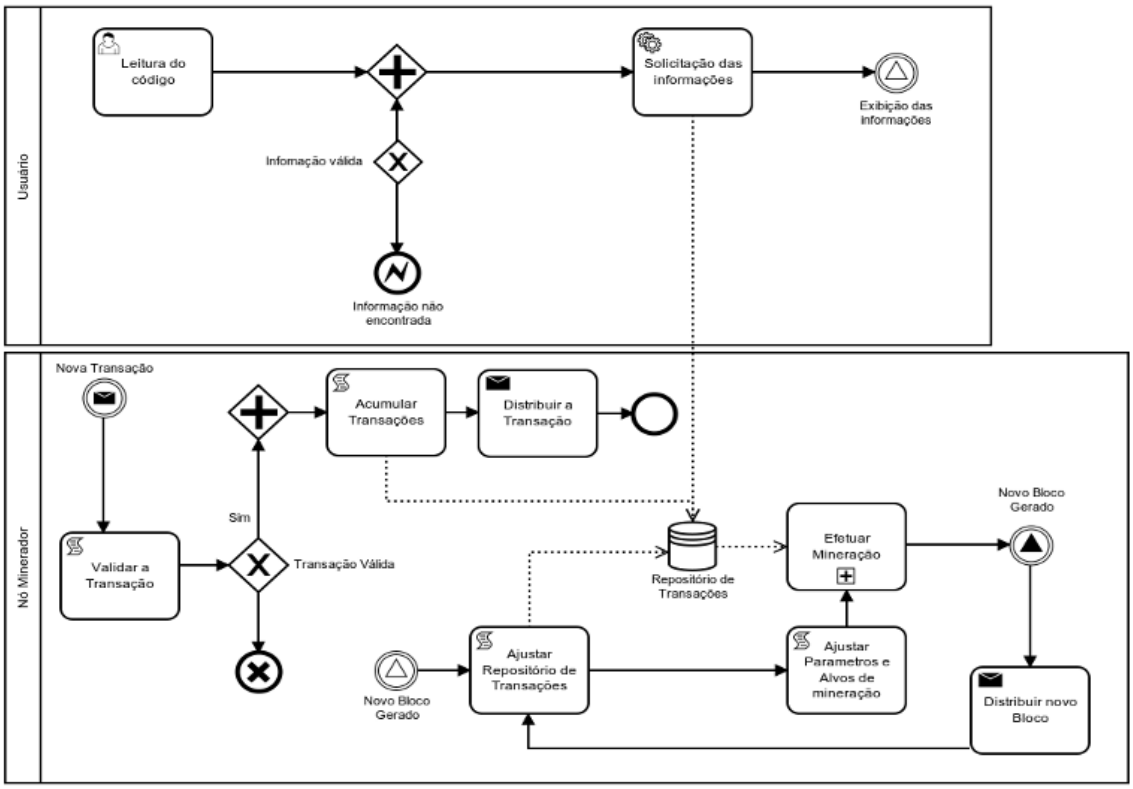
ID	Nome	Prioridade
RNF 01	Segurança dos dados	Essencial
RNF 02	Design responsivo	Desejável
RNF 03	Escalabilidade da aplicação	Essencial
RNF 04	Divisão arquitetural em camadas	Essencial
RNF 05	Facilidade de aprendizagem e recordação	Desejável

Os RNF apresentados na tabela, mostram que nem todos são de nível de prioridade “Essencial”. Entretanto, observa-se que a segurança de dados apresenta uma prioridade “Essencial” para a aplicação. Para que usuários, mesmo não autorizados, possam acessar informações da base de dados sem que haja comprometimento com da segurança. A escalabilidade permitirá que a aplicação cresça e atenda a determinadas requisições rapidamente, como também facilita a sua manutenção com o aumento da coesão e redução do acoplamento. As prioridades consideradas desejáveis, apresentam também sua importância para aplicação, mas não comprometem o funcionamento do sistema. Tais prioridades colaboram para a uma boa experiênia do usuário, como também mantém uma usabilidade agradável, a partir de ícones ou designer responsivo.

3.2 Diagrama de atividades

Para um melhor entendimento das funcionalidades, foi construído um diagrama de atividades. Rumbaugh, Booch e Jacobson (1998) afirmam que diagramas são utilizados pela indústria para representar a interação dentro das funcionalidades de forma simples e clara, logo, a busca e a avaliação da usabilidade se torna imprescindível através dos mesmos. A Figura 3, apresenta o diagrama de atividades da aplicação QRqueijo.

Figura 3 – Diagrama de atividades



Fonte: próprio autor

No diagrama, o usuário representa o consumidor de queijos no mundo real. O consumidor deverá possuir um dispositivo móvel para realizar a leitura do código, que se encontrará na embalagem do queijo. A partir disso, o código que foi lido é verificado pela aplicação na base de dados e na rede Blockchain local. Ao validar e identificar as informações, essa é exibida para o consumidor que fez a leitura, caso contrário, informa que não há registro na base de dados. A representação da Blockchain, é identificado no diagrama como sendo o "Nó minerador", que apresenta uma nova transação na rede, como também é exibido a validação e a geração de um novo bloco. A cada nova transação, será inserida as informações necessárias para o registro de um queijo, estas serão validadas de acordo com as regras programadas. Ao serem validadas, serão inseridas na rede para a geração de um novo bloco, que seguirá os passos necessários

para a validação do mesmo. Inicialmente será ajustado de acordo com o repositório de transações, que deverão receber os dados necessários para o registro. Em seguida são ajustado os parâmetros que serão alvos para a mineração, onde permitirá que um identificador seja gerado para o queijo. Por fim, após o minerador validar o novo bloco gerado e encontrando o seu *hash_id*, é então distribuído pela rede, informando que existe um novo bloco gerado.

3.3 Prototipação

Nesta seção, é descrito quais ferramentas foram utilizadas para o desenvolvimento da aplicação. Após a definição dos requisitos nas seções anteriores, foram implementadas as funcionalidades citadas. A seguir veremos a descrição das ferramentas e através de imagens, exibiremos os resultados obtidos.

3.3.1 Ferramentas utilizadas

Para a implementação da aplicação, as seguintes ferramentas foram utilizadas no desenvolvimento:

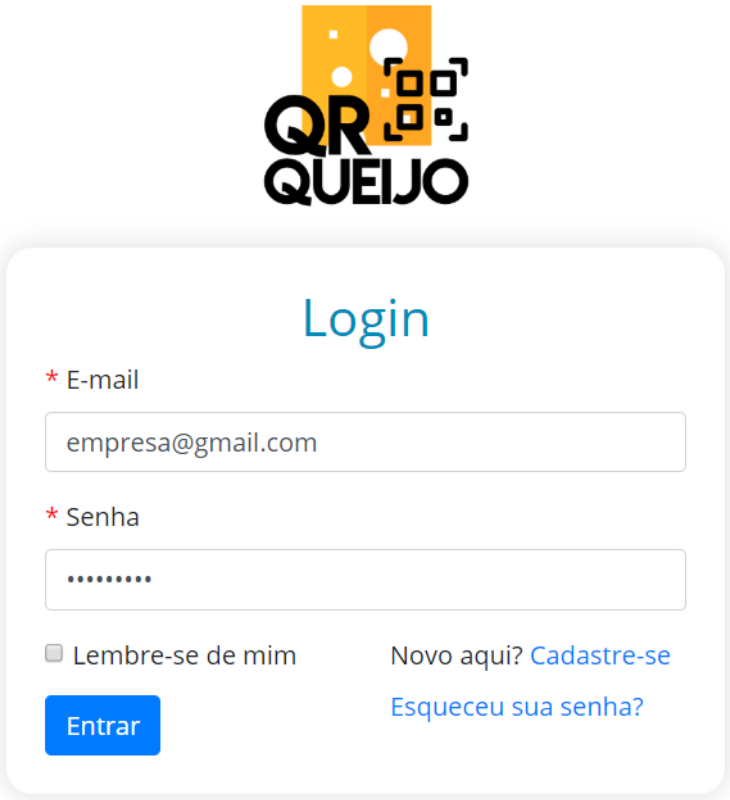
- **Ruby on Rails:** por promover velocidade, facilidade de desenvolvimento e uma boa escalabilidade, a ferramenta Ruby on Rails, versão 5.2.3, foi escolhida para o desenvolvimento da aplicação;
- **HTML5/CSS3:** utilizada visando a usabilidade do sistema, com intuito de facilitar e melhorar a experiência de uso do usuário;
- **MySQL:** a escolha da base dados, se deu por sua popularidade e facilidade no seu uso para aplicações, com sua versão 8.0.13;
- **Docker:** com sua versão 18.09.2, foi escolhida por permitir a criação de ambientes virtuais que podem instanciar serviços de forma eficiente, simulando até o comportamento de sistemas operacionais inteiros. E, para a rede Blockchain local, essa ferramenta permitirá a criação de nós para a simulação da rede;
- **GIT:** utilizada para o controle de versões da aplicação, buscando manter alocado o nosso código, criando assim um repositório remoto na plataforma GitHub, versão utilizada foi a 1.9.4;
- **Visual Studio Code:** para a edição dos textos, sua versão 1.36.1 pode suportar uma grande quantidade de linguagens de programação e ser multiplataforma, além de exibir os arquivos da aplicação de forma simples;

- **Android Studio:** para o desenvolvimento da aplicação Android utilizada pelos os usuários, por permitir desenvolver aplicações nativas do sistema. Sua versão utilizada foi a 3.4.1.

3.3.2 Detalhes da aplicação

A Figura 4 apresenta a interface de autenticação do usuário na aplicação. Como observado, o acesso a aplicação necessita que o usuário possua um e-mail para login e senha. Como segurança no momento do login, validações são realizadas por meio de um mecanismo de autenticação disponibilizado pelo Ruby on Rails, chamado *Warden*. Caso o usuário tente fazer qualquer autenticação que não esteja de acordo com as regras da aplicação, como: campos em branco, e-mail e senha inválidos ou também se o usuário não possuir cadastro na aplicação, é exibida uma informação ao usuário caso haja algum erro. Para aqueles que não possuem cadastros, é possível ser realizado através do redirecionamento para a tela de cadastro e, os usuários autenticados, são redirecionados para a tela principal da aplicação.

Figura 4 – Imagem da tela de login da aplicação



Fonte: próprio autor

Um trecho do código da autenticação do usuário na aplicação, é apresentado no Código 3.1. Na linha 3, pode ser observado a chamada do *Warden* para a validação

do usuário que deseja logar no sistema.

Código 3.1 – Código de autenticação da tela de login

```
# POST /resource/sign_in
def create
    self.resource = warden.authenticate!(auth_options)
    set_flash_message!(:notice, :signed_in)
    sign_in(resource_name, resource)
    yield resource if block_given?
    respond_with resource, location: after_sign_in_path_for(
       resource)
end
```

O usuário ao realizar a validação com sucesso, é redirecionado para a página principal da aplicação. A Figura 5 apresenta a interface principal, onde é possível observar que o mesmo tem a disposição as principais funcionalidades, como: visualizar a sua rede Blockchain; cadastrar um novo queijo; detalhar algum queijo já validado na rede; ou sair da aplicação.

Figura 5 – Imagem da tela inicial da aplicação

Fonte: próprio autor

A aplicação foi desenvolvida visando desde o princípio um ambiente real, portanto, o cadastro de novos queijos pode ser feito através de um botão na parte superior da interface, intitulado "Novo Queijo". A tela de cadastro é apresentada na Figura 6, onde é possível informar os dados sobre o queijo específico (como fabricação, validade, tipo, empresa e endereço). Ao clicar em salvar, é gerado o bloco no sistema

contendo as informações de transação e em seguida validado na rede Blockchain, sendo redirecionado para a tela de principal após a validação.

Figura 6 – Tela de cadastro de novo queijo

Fonte: próprio autor

A seguir é mostrado no Código 3.2, como é realizado o cadastro de um novo queijo na aplicação. A princípio é recebido por parâmetros as informações necessárias para o cadastro, em seguida é instanciado um modelo chamado *"Transaction"*, para que sejam inseridas as informações. Após o preenchimento do modelo, é chamado o método *save* que se localiza na linha 20. O mesmo verifica se o modelo é um novo registro para o banco de dados, caso contrário, o registro existente será atualizado.

Código 3.2 – Código de cadastro de um novo queijo

```
1  def self.generate(block, transactions)
2      transactions.each do |transaction|
3        block_transaction = Transaction.new
4        block_transaction.block_id = block.id
5        block_transaction.pais = "Brasil"
6        block_transaction.uf = transaction[:uf]
7        block_transaction.cidade = transaction[:cidade]
8        block_transaction.bairro = transaction[:bairro]
9        block_transaction.rua = transaction[:rua]
10       block_transaction.numero = transaction[:numero]
11       block_transaction.cep = transaction[:cep]
12       block_transaction.endereco = transaction[:endereco]
13       block_transaction.fabricacao = transaction[:fabricacao]
14       block_transaction.validade = transaction[:validade]
15       block_transaction.tipo = transaction[:tipo]
16       block_transaction.empresa = transaction[:empresa]
```

```
17        block_transaction.data = I18n.l Date.today
18        block_transaction.horario = I18n.l Time.now, :format =>
              :horario
19
20        block_transaction.save
21      end
22  end
```

Retornando a tela principal na Figura 5, podemos observar nos queijos já cadastra- dos que a tela possui um botão chamado "Detalhar". Ao clicar no referido botão, é exibido as informações que foram cadastradas, o bloco gerado pela validação e também a imagem do QRcode, que contém como informação o "hash_id"do bloco gerado. A Figura 7, apresenta o queijo que foi cadastrado e gerado na aplicação, como também o QRcode.

Figura 7 – Tela de detalhe de um queijo registrado

Fonte: próprio autor

O Código 3.3 apresenta como a geração do bloco é realizada. A princípio duas informações são passadas por parâmetros para o método, o bloco que foi criado e o usuário que está logado no sistema. Com a informação do usuário, podemos então localizar a transação que foi cadastrada como é mostrado na linha 2. Destaca-se a linha 8, que faz a mineração do bloco através da prova de trabalho até que seja encontrado uma "hash_id"válida e seja inserida na rede Blockchain local da aplicação.

Código 3.3 – Código da geração de um novo bloco

```
1  def self.validation_block(block, current_user)
2      transactions = Transaction.where("block_id = ?", block.id
           )
```

```
3     transactions_count = transactions.count
4     last_block = Blockchain.where("user_id = ?", current_user
         .id).last
5     blockchain = Blockchain.new
6     blockchain.previous_hash = last_block.nil? ? '0' :
         last_block.hash_id
7     # prova de trabalho
8     proof_of_work = blockchain.compute_proof_of_work(block,
         transactions, transactions_count, blockchain)
9
10    #Se validado, insira na rede blockchain
11    if proof_of_work[0]
12        blockchain.nonce = proof_of_work[1]
13        blockchain.hash_id = proof_of_work[2]
14        new_block_in_blockchain = Blockchain.
             set_block_in_blockchain(block, transactions,
                      transactions_count, blockchain,
             current_user)
15        return new_block_in_blockchain
16    else
17        return new_block_in_blockchain
18    end
19  end
```

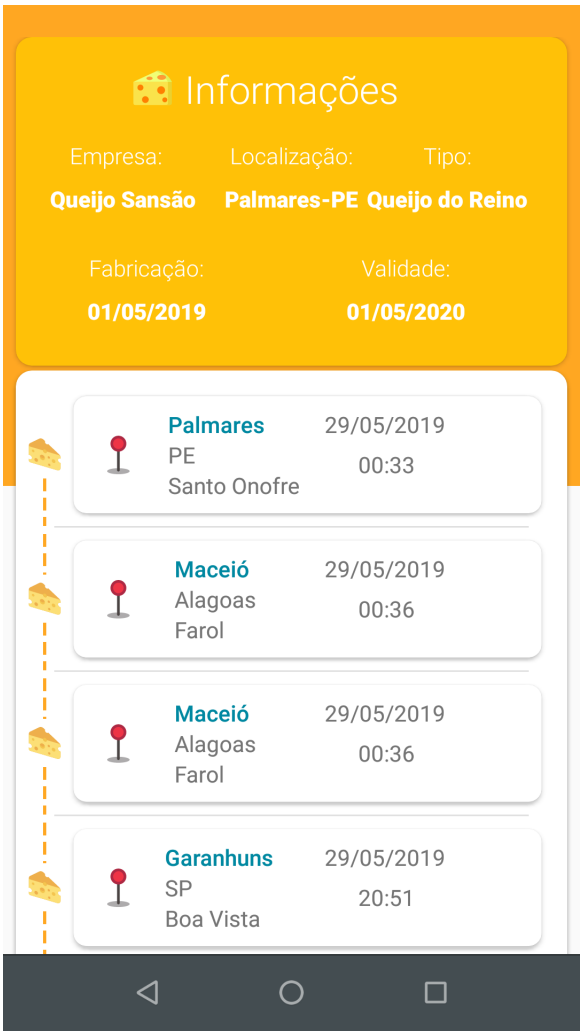
3.3.3 Aplicativo para leitura de dados

Para os vendedores, seus clientes, através do aplicativo QRQueijo, poderão se beneficiar a partir do escaneamento do código QR (do inglês *Quick Response*), mais conhecido como *QR code*, que é um código de barras bidimensional. O que permite que um queijo registrado com informações seja identificado. Para que isso seja possível, o queijo deverá conter o seu identificador (*QRcode*) impresso na embalagem do produto. A Figura 8 apresenta a tela principal do aplicativo QRQueijo.

Figura 8 – Aplicativo QRQueijo - Tela principal

Fonte: próprio autor

Figura 9 – Tela de informações sobre um queijo cadastrado



Fonte: próprio autor

O aplicativo além de realizar a leitura dos dados do queijo, também realizará a atualização da localização do queijo registrado. Para cada nova leitura de um *QRcode*, um novo bloco será gerado contendo as mesmas informações do queijo e a sua nova localização, que é obtida por meio da permissão do usuário, para a utilização da localização, conhecido como GPS (em inglês *Global Positioning System*) do dispositivo móvel que possui o aplicativo QRQueijo instalado.

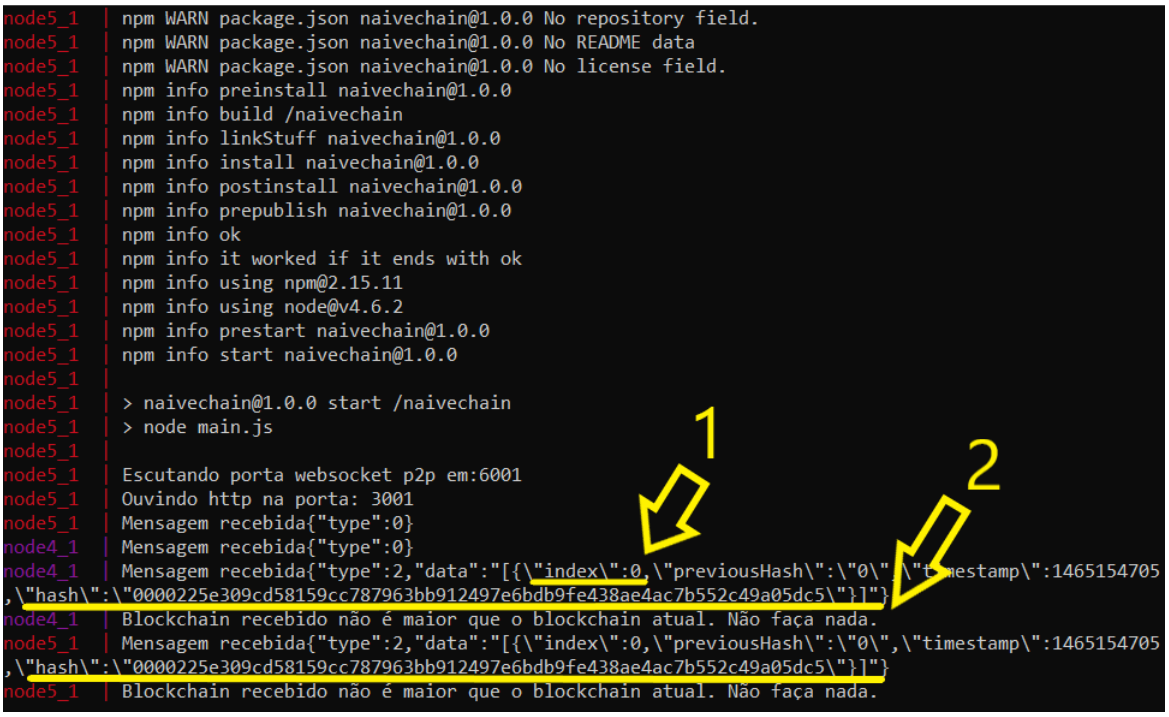
3.4 Rede Blockchain local

Como simulação de uma rede Blockchain distribuída, foi realizada a implementação de uma rede local, com o intuito de ser didática. Utilizamos como base para a implementação, a aplicação desenvolvida por Hartikka (2017), que em 200 linhas de códigos implementou uma rede Blockchain simples, utilizando Node.js. A aplicação foi

portanto integrada ao nosso sistema, com algumas alterações necessárias para que melhor se adequasse.

Com isso, a simulação de uma rede distribuída local foi possível, gerando a princípio a criação de cinco nós e o bloco gênesis, fazendo o uso do Docker. Cada nó verifica o tamanho da rede, sempre atualizando a sua rede para o nó que possuir o maior tamanho, e ao validar um novo bloco, os outros nós verificam se esse bloco é realmente válido e se pode ser inserido na rede. Observando a Figura 10, é possível visualizar o momento em que os nós 4 e 5 recebem a mensagem contendo o bloco gênesis. Na seta indicada com o número 1, pode ser visualizado o index zero, identificando o bloco gênesis. Já na seta 2, temos o hash identificador do bloco.

Figura 10 – Os nós do blockchain contendo inicialmente apenas o bloco gênesis



Fonte: próprio autor

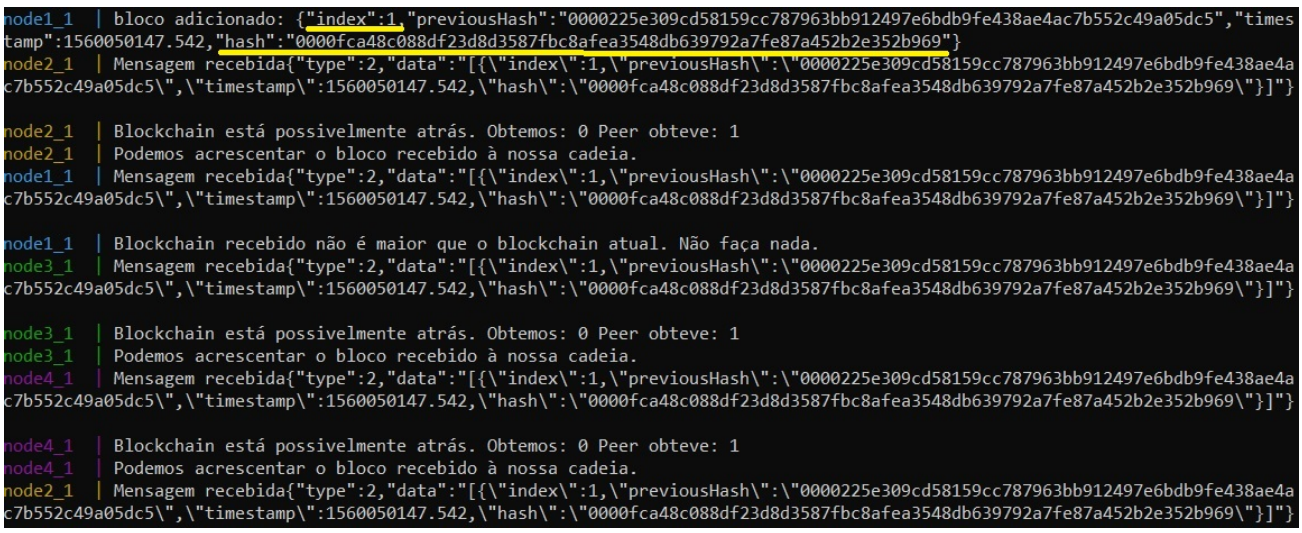
Para a visualização completa da rede blockchain, um usuário com permissões de administrador foi criado para que fosse permitido visualizar a rede. A Figura 11 apresenta a tela principal do administrador, com todos os blocos da rede. Para visualizar os detalhes de um bloco, o administrador poderá clicar no botão “detalhar” da linha específica de um bloco na tabela.

Figura 11 – Tela principal do administrador

Fonte: próprio autor

Ao cadastrar novos queijos, a aplicação irá validar automaticamente e registrar na base de dados local, caso a validação for um sucesso. Com isso, ao simularmos a rede local distribuída, fizemos uma comunicação via *http* com o primeiro nó da distribuição, enviando o *hash_id* no corpo da requisição. Os outros nós realizam as validações necessárias para garantir a integridade da rede. A Figura 12, mostra a validação do novo bloco que é adicionado a rede.

Figura 12 – Inserção de um novo bloco na rede



Fonte: próprio autor

A partir do exposto, é possível afirmar que a aplicação desenvolvida possui grande potencial de benefício a população e ao próprio fornecedor, fornecendo informações seguras e atualizadas sobre os queijos adquiridos.

4 Considerações Finais

O presente capítulo apresenta as considerações finais a respeito deste trabalho. A sessão 4.1, expõe sobre os resultados que foram obtidos e suas contribuições para a sociedade. Na sessão 4.2 apresenta os possíveis trabalhos futuros.

4.1 Conclusões

O objetivo principal deste trabalho foi desenvolver uma solução que garantisse a integridade e autenticidade das informações geradas por um fabricante de queijos e permitir a disponibilidade dessas informações de forma segura para os consumidores. Para que fosse possível chegar aos resultados apresentados, uma revisão bibliográfica foi realizada para entender as temáticas que seriam devidamente abordados. A princípio, foi possível investigar casos reincidentes sobre fraudes e desinformações de queijos no Brasil, que mostraram falhas de segurança das informações como: identificadores de queijos e suas embalagens que são facilmente violadas e falsificadas; validades adulteradas; e também a falta de uma registro em um órgão fiscalizador.

Além disso, identificou-se os princípios para a criação de uma estrutura Blockchain, bem como a estrutura de um bloco e seu funcionamento, que foram definidas pelo seu criador Nakamoto (2008). A revisão sobre a Blockchain, foi determinante para o desenvolvimento do sistema e apontou características importantes de segurança da informação, bem como a garantia da integridade das informações, sendo impossível alterar as informações já registradas na rede. Além de disponibilizar as informações sempre que consultadas, como também garantir a confidencialidade ao permitir somente o acesso autorizado, mantendo sempre o sigilo dos indivíduos.

A possibilidade de utilização de somente o banco de dados para as transações dos dados da aplicação, foi refutada após uma análise sobre o uso do mesmo e da Blockchain. A Blockchain, segundo Greve et al. (2018), possui propriedades que garantem a segurança de seus dados, pois contém uma estrutura descentralizada e imutável. Embora bancos de dados possuam segurança, ainda é suscetível a falhas por possuir a centralização de seus dados, além de permitir que seus dados sejam alterados por gerenciadores e permitir existência de controladores que permanecem com uma autoridade central. Diferente da Blockchain, onde cada nó valida e verifica em cada nova transação para garantir a segurança e igualdade em todas as distribuições.

Para que os consumidores de queijo recebessem informações relevantes, foi necessário entender sobre a necessidade da rastreabilidade para a sociedade, onde

a mesma acaba impactando na economia, no ambiente e também na produção dos alimentos. Como citado por Machado (2005), a localização de uma entidade (ou item) por meio de identificações registradas, é uma forma de se utilizar a rastreabilidade de alimentos. Portanto, para a aplicação *Android* QRQueijo, permitiu-se que a localização de um queijo fosse registrada na rede Blockchain por meio do *GPS*, garantindo assim que o queijo que sai de seu fabricante é o mesmo queijo que o consumidor adquire.

Além disso, foram definidos os requisitos funcionais e não-funcionais da aplicação, para o sucesso do QRQueijo. Para tal, foi modelado uma aplicação *web* com as melhores ferramentas de desenvolvimento e as mais atuais, permitindo com que a aplicação fosse capaz de registrar um determinado fabricante de queijo e registrar seus produtos em uma rede Blockchain local, fornecendo informações importantes para a geração de um identificador único de cada queijo. A identificação por meio do QRcode, permite que esse queijo possua uma assinatura digital, que tem como função selar o conteúdo, garantindo assim sua integridade ou, se caso seja alterado, segundo (KAZIENKO et al., 2003).

A aplicação além de fazer o registro, realiza verificação de autenticidade e disponibiliza essas informações aos consumidores. Portanto, o QRQueijo é capaz de garantir aos consumidores a integridade e autenticidade das informações geradas pelos fabricantes de queijos, desde a produção, até a mesa dos seus clientes.

4.2 Trabalhos futuros

Como trabalhos futuros, destaca-se possíveis direções, como por exemplo:

- **Melhoramento na rastreabilidade:** para possibilitar que os consumidores tenham mais transparência em relação a cadeia produtiva, como também ajudar aos fabricantes a garantir mais segurança e qualidade aos seus produtos, permitindo uma visão mais clara sobre os processos. Para isso, seria necessário a realização de um estudo que abordasse a importância da rastreabilidade para os produtores e consumidores de queijos junto a TI.
- **Continuação da implementação da aplicação Android:** com o objetivo de melhorar a segurança dos dados disponibilizados, possibilitando a realização de testes para assegurar a disponibilidade, integridade e a estrutura em relação a ataques. Para a localização via GPS, é proposto uma melhor precisão, como também outras formas de leitura dos dados para o QRcode.
- **Implementação de uma rede Blockchain pública:** com a finalidade de garantir mais uma camada de segurança ao sistema de registros e geração de identificadores.

Referências

ABNT. *Associação Brasileira de Normas Técnicas*. 2013. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 09.06.2019. Citado na página 33.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Comput. Netw.*, Elsevier North-Holland, Inc., New York, NY, USA, v. 54, n. 15, p. 2787–2805, out. 2010. ISSN 1389-1286. Disponível em: <http://dx.doi.org/10.1016/j.comnet.2010.05.010>. Citado na página 31.

BAUER, L. *RC: Vigilância Sanitária apreende queijos com selo e rótulo falsificados*. 2017. Disponível em: <https://www.jornalcidade.net/vigilancia-sanitaria-de-rio-claro-apreende-queijos-com-selo-e-rotulo-falsificados/41912/>. Acesso em: 22.06.2019. Citado na página 38.

BAUERLE, N. *What is Blockchain Technology?* 2018. Disponível em: <https://www.coindesk.com/information/what-is-blockchain-technology>. Acesso em: 04.07.2019. Citado na página 37.

BRASIL, G. D. Rastreabilidade e segurança alimentar. *Boletim Técnico-n.º*, v. 91, p. 1–25, 2012. Citado na página 38.

BRESSER-PEREIRA luiz carlos. Crise e recuperação da confiança. *Brazilian Journal of Political Economy*, scielo, v. 29, p. 133 – 149, 03 2009. ISSN 0101-3157. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-31572009000100008&nrm=iso>. Citado na página 27.

CAMPOS, A. *Sistema de segurança da informação*. [S.l.]: Florianópolis: Visual Books, 2007. Citado na página 33.

CHICARINO, V. et al. Uso de blockchain para privacidade e segurança em internet das coisas. *Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC*, 2017. Citado na página 28.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. *IEEE Access*, v. 4, p. 2292–2303, 2016. ISSN 2169-3536. Citado 3 vezes nas páginas 27, 32 e 37.

DAI, W. B-money. *Consulted*, v. 1, p. 2012, 1998. Citado na página 27.

DAVIS, A. *Software Requirements: Objects, Functions, and States*. PTR Prentice Hall, 1993. ISBN 9780138057633. Disponível em: <https://books.google.com.br/books?id=ZJ1QAAAAMAAJ>. Citado na página 42.

ELMASRI, R. *Fundamentals of database systems*. [S.l.]: Pearson Education India, 2008. Citado na página 36.

ELMASRI, R. et al. Sistemas de banco de dados. Pearson Addison Wesley São Paulo, 2005. Citado na página 35.

EUROPEU, P. Conselho. regulamento (ce) n. º 178/2002. *Jornal Oficial da União Europeia.(2002-02-28) Determina os princípios e normas gerais da legislação alimentar, cria a Autoridade Europeia para a Segurança dos Alimentos e estabelece procedimentos em matéria de segurança dos géneros alimentícios*, 2002. Citado na página 38.

FERREIRA, E. et al. Uso de blockchain para privacidade e segurança em internet das coisas. p. 51, 11 2017. Disponível em: <https://sbseg2017.redes.unb.br/wp-content/uploads/2017/04/20171107-SBSeg2017-Livro_de_Minicursos.pdf>. Citado na página 29.

G1, P. *Polícia apreende 14 toneladas de queijo coalho durante operação no Recife*. 2018. Disponível em: <https://g1.globo.com/pe/pernambuco/noticia/2018/09/18/policia-faz-apreensao-de-queijo-coalho-irregular-durante-operacao-no-recife.ghtml>. Acesso em: 22.06.2019. Citado na página 38.

GANDINI, J. A. D.; SALOMÃO, D. P. d. S.; JACOB, C. A segurança dos documentos digitais. v. 11, 2001. Citado na página 34.

GARTNER. *Gartner Says 4.9 Billion Connected "Things"Will Be in Use in 2015*. 2015. Disponível em: <http://www.gartner.com/newsroom/id/2905717>. Acesso em: 20.03.2019. Citado na página 31.

GARTNER. *Gartner Says Global IT Spending to Reach $3.8 Trillion in 2019*. STAMFORD: [s.n.], 2019. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2019-01-28-gartner-says-global-it-spending-to-reach--3-8-trillio>. Acesso em: 11.06.2019. Citado na página 23.

GREVE, F. et al. Blockchain e a revolução do consenso sob demanda. *Livro de Minicursos do SBRC*, v. 1, p. 1–52, 2018. Citado 3 vezes nas páginas 33, 37 e 55.

HARTIKKA, L. A blockchain in 200 lines of code. março 2017. Disponível em: <https://medium.com/@lhartikk/a-blockchain-in-200-lines-of-code-963cc1cc0e54>. Acesso em: 06.06.2019. Citado na página 51.

HUCKLE, S. et al. Internet of things, blockchain and shared economy applications. *Procedia computer science*, Elsevier, v. 98, p. 461–466, 2016. Citado na página 31.

JUNIOR, D. M. M. Segurança da informação: uma abordagem sobre proteção da privacidade em internet das coisas. Tese (Doutorado em Tecnologia da Inteligência e Design Digital) - Programa de Estudos Pós-Graduados em Tecnologia da Inteligência e Design Digital, Pontifícia Universidade Católica de São Paulo, São Paulo, 2018. Citado na página 33.

KAZIENKO, J. F. et al. Assinatura digital de documentos eletrônicos através da impressao digital. Florianópolis, SC, 2003. Citado 2 vezes nas páginas 34 e 56.

KUHNEN, I. A. Análise de sistemas de gerenciamento de banco de dados para armazenamento de dados climáticos. 2016. Citado na página 36.

LIRANI, A. C. Rastreabilidade, uma exigência comercial. *Visão Agrícola, Piracicaba: ESALQ/USP, n*, p. 97–99, 2005. Citado na página 38.

LIU, D. *Blockchain Architecture*. 2019. Disponível em: <https://www.pluralsight.com/guides/blockchain-architecture>. Acesso em: 03.08.2019. Citado na página 28.

LUU, L. et al. Making smart contracts smarter. In: ACM. *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. [S.l.], 2016. p. 254–269. Citado na página 32.

MACHADO, R. T. M. Sinais de qualidade e rastreabilidade de alimentos: uma visão sistêmica. *Organizações Rurais & Agroindustriais*, v. 7, n. 2, 2005. Citado 2 vezes nas páginas 38 e 56.

MARINS, R. L.; MIRANDA, S. H. G. d. Estudo comparativo de sistemas de rastreabilidade em alimentos e métodos para quantificação de seus efeitos. *Agropecuária; resumos*, 2006. Citado na página 39.

MCGEE, J. *e Prusak, L.(1994) Gerenciamento estratégico da informação: aumente a competitividade ea eficiência de sua empresa utilizando a informação como uma ferramenta estratégica*. [S.l.]: Rio de Janeiro, Campus, 1994. Citado na página 33.

MOL, J. *Mais de 13 mil queijos da Canastra são confiscados pela Polícia Federal*. São Roque, MG: [s.n.], 2015. Disponível em: <https://paladar.estadao.com.br/noticias/comida,mais-de-13-mil-queijos-da-canastra-sao-confiscados-pela-policia-federal,10000011587>. Acesso em: 13.06.2019. Citado na página 24.

MORAIS, A. M. d. *Controle de emissão e validação de diplomas digitais utilizando Blockchain*. Dissertação (B.S. thesis) — Brasil, 2019. Citado na página 35.

MORESI, E. A. D. Delineando o valor do sistema de informação de uma organização. *Ciência da Informação*, scielo, v. 29, p. 14 – 24, 04 2000. ISSN 0100-1965. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652000000100002&nrm=iso>. Citado na página 23.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1–9. doi:10.1007/s10838-008-9062-0stem. *Journal for General Philosophy of Science*, v. 39, n. 1, p. 53–67, 2008. ISSN 09254560. Citado 6 vezes nas páginas 23, 24, 27, 28, 37 e 55.

ORIGINALMY. Registro de autenticidade. 2017. Disponível em: <https://originalmy.readthedocs.io/pt_BR/latest/00-apresentacao.html>. Acesso em: 21.06.2019. Citado na página 35.

PRESSMAN, R. *Engenharia de software*. McGraw-Hill, 2006. ISBN 9788586804571. Disponível em: <https://books.google.com.br/books?id=MNM6AgAACAAJ>. Citado na página 41.

PRODANOV, C. C.; FREITAS, E. C. de. *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição*. [S.l.]: Editora Feevale, 2013. Citado na página 25.

RESENDE, E.; LOPES, M. A. Identificação, certificação e rastreabilidade na cadeia da carne bovina e bubalina no brasil. *Lavras: UFLA*, 2004. Citado na página 38.

RUMBAUGH, J.; BOOCH, G.; JACOBSON, I. *The unified modeling language user guide*. [S.l.]: Addison-wesley, 1998. Citado na página 43.

SANTOS, B. P. et al. Internet das coisas: da teoria à prática. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos*, 2016. Citado na página 31.

SCARFONE, K. A.; JANSEN, W.; TRACY, M. *SP 800-123. Guide to General Server Security*. Gaithersburg, MD, United States, 2008. Citado na página 23.

SCHLAPKOHL, K. *What's the difference between a blockchain and a database?* 2019. Disponível em: <https://www.ibm.com/blogs/blockchain/2019/01/whats-the-difference-between-a-blockchain-and-a-database/>. Acesso em: 05.08.2019. Citado na página 37.

SÊMOLA, M. *Gestão da Segurança da Informação: Uma Visão Executiva. Rio de Janeiro: Ed*. [S.l.]: Campus, 2003. Citado na página 33.

SILBERSCHATZ, A. et al. *Database system concepts*. [S.l.]: McGraw-Hill New York, 1997. v. 4. Citado na página 36.

SOMMERVILLE, I. *Engenharia de software*. 8th. ed. São Paulo: Pearson, 2007. Citado na página 41.

SZABO, N. Formalizing and securing relationships on public networks. *First Monday*, v. 2, n. 9, 1997. Citado na página 32.

TANENBAUM, A. S. *Sistemas Distribuídos, princípios e paradigmas*. 2ª. ed. São Paulo: Pearson, 2007. 1 p. ISBN 978-85-7605-142-8. Citado na página 23.

Wang, S. et al. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, p. 1–12, 2019. ISSN 2168-2216. Citado na página 32.

ZHENG, Z. et al. Blockchain challenges and opportunities: A survey. *Work Pap.–2016*, 2016. Citado na página 29.