UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

MESTRADO ACADÊMICO EM COMPUTAÇÃO

WAGNER LUIZ BRAGA BEZERRA

UM MODELO DE ARQUITETURA DE SISTEMA DE E-VOTING AUDITÁVEL UTILIZANDO BLOCKCHAIN

QUIXADÁ

2023

WAGNER LUIZ BRAGA BEZERRA

UM MODELO DE ARQUITETURA DE SISTEMA DE E-VOTING AUDITÁVEL UTILIZANDO BLOCKCHAIN

Dissertação apresentada ao Curso de Mestrado Acadêmico em Computação do Programa de Pós-Graduação em Computação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em computação. Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Emanuel Ferreira Coutinho

QUIXADÁ

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B469m Bezerra, Wagner Luiz Braga.
Um modelo de arquitetura de sistema de e-voting auditável utilizando blockchain / Wagner Luiz Braga Bezerra. – 2023.
120 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Campus de Quixadá, Programa de Pós-Graduação em Computação, Quixadá, 2023.
Orientação: Prof. Dr. Emanuel Ferreira Coutinho.

1. blockchains (base de dados). 2. votação eletrônica. 3. auditoria. I. Título.

CDD 005

WAGNER LUIZ BRAGA BEZERRA

UM MODELO DE ARQUITETURA DE SISTEMA DE E-VOTING AUDITÁVEL UTILIZANDO BLOCKCHAIN

Dissertação apresentada ao Curso de Mestrado Acadêmico em Computação do Programa de Pós-Graduação em Computação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em computação. Área de Concentração: Ciência da Computação

Aprovada em: 24 de Novembro de 2023

BANCA EXAMINADORA

Prof. Dr. Emanuel Ferreira Coutinho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Gabriel Antoine Louis Paillard
Universidade Federal do Ceará (UFC)

Prof. Dr. Valdemar Vicente Graciano Neto
Universidade Federal de Goiás (UFG)

Dedico este trabalho à minha amada esposa Beatriz. Uma mulher forte que desperta em mim sentimentos de perseverança. Sua parceria cuidadosa foi essencial para o seguimento deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente à minha mãe, Dulce Braga. Seu amor e apoio têm sido os alicerces que moldaram minha vida de maneira extraordinária. Em cada desafio que enfrentei, você esteve ao meu lado, oferecendo conforto, encorajamento e, acima de tudo, seu amor incondicional. Sua força, compaixão e sabedoria são fontes constantes de inspiração para mim.

Agradeço à minha amada irmã. Em cada passo da minha jornada, seja nas pequenas conquistas do dia a dia ou nos grandes desafios, sua presença encorajadora tem sido uma fonte de apoio inestimável. Saber que tenho alguém tão incrível ao meu lado, sempre torcendo pelo meu sucesso, é verdadeiramente reconfortante. Sua capacidade de celebrar minhas vitórias com alegria genuína e estar lá nos momentos difíceis é um testemunho de nossa irmandade. Sua torcida constante não apenas eleva meu espírito, mas também me inspira a alcançar mais.

Agradeço a pessoa a quem dediquei este trabalho, minha esposa Beatriz. Sinto uma profunda gratidão por ter você ao meu lado como minha esposa e parceira de vida. Sua presença enche minha jornada com alegria, amor e significado, e eu sou eternamente grato por isso. Mais do que minha companheira, você é a luz que ilumina os dias escuros e a razão pela qual cada conquista é mais significativa. Seu cuidado, paciência e compreensão são tesouros que enriquecem minha vida de maneiras indescritíveis.

Agradeço aos meus amigos e colegas, por compartilharmos não apenas momentos de estudo e desafios acadêmicos, mas também momentos de descontração e risos que fizeram dessa jornada uma lembrança tão especial.

Por fim, gostaria de expressar minha sincera gratidão ao meu orientador Emanuel Ferreira Coutinho, por todo o apoio e compreensão que me proporcionou ao longo deste percurso no programa de mestrado. Sua paciência e comprometimento foram fundamentais, especialmente nos momentos em que eu mesmo cogitei desistir. Além de seu papel como orientador acadêmico, agradeço por ser um mentor compassivo, que compreendeu as pressões e desafios pessoais que enfrentei. Sua abertura para ouvir, a disposição para oferecer conselhos e o suporte constante foram além das minhas expectativas.

RESUMO

O surgimento da tecnologia *blockchain*, inicialmente com a criptomoeda *Bitcoin*, trouxe consigo um leque de possibilidades de desenvolvimento de soluções nos mais diversos setores da sociedade. As características da tecnologia garantem diversas vantagens tais como imutabilidade, irrefutabilidade, auditabilidade e transparência. Além disso, por ter a informação replicada em todos os nós da rede, a *blockchain* proporciona descentralização, desintermediação e disponibilidade. A plataforma de *blockchain Hyperledger* oferece *frameworks* como o *Fabric*, que são projetados para atender às necessidades empresariais com redes privadas e permissíveis, garantindo controle e privacidade. Este sistema descentralizado e distribuído encontrou aplicabilidade significativa no âmbito do *e-voting*, oferecendo soluções para questões cruciais, como integridade, autenticação e segurança dos votos. Esse registro é acessível a todos os participantes da rede, garantindo a rastreabilidade e verificabilidade dos resultados eleitorais. A imutabilidade dos dados na *blockchain* assegura que nenhuma informação seja alterada ou adulterada, aumentando a confiança no processo eleitoral. A auditoria é uma técnica de gestão reconhecida que fornece uma visão geral da situação em relação a recursos e serviços específicos dentro de uma organização. No ambiente corporativo existem diversos tipos de auditorias, entre elas a auditoria de sistemas de informação, de modo que não existe um consenso definido na literatura acerca de uma única metodologia para realização de auditoria. Neste trabalho é desenvolvido um estudo acerca da utilização da tecnologia *blockchain* em sistemas de *e-voting* com a inclusão de processos de auditoria simplificados e com baixo ou nenhum custo de implementação. É realizada uma busca do estado da arte para obter uma percepção da produção científica sobre o tema. São realizados experimentos com a plataforma *Hyperledger*. É criada uma aplicação a fim de atestar o funcionamento da arquitetura proposta. Ao final do processo de desenvolvimento é possível concluir que o trabalho atende ao que foi proposto, pois produz avanço da fundamentação teórica, destaca na literatura a crescente produção sobre o tema *e-voting* com o uso da tecnologia *blockchain*, propõe uma arquitetura simples que incorpora um caráter de auditabilidade ao sistema de *e-voting*, realiza uma análise de desempenho realizada com a plataforma *hyperledger*, proporcionando uma compreensão mais aprofundada das características dessa plataforma, por fim validando a possibilidade de criar um sistema completo de *e-voting* utilizando a tecnologia *blockchain* e a plataforma *hyperledger*.

Palavras-chave: blockchains; votação eletrônica; auditoria.

ABSTRACT

The emergence of blockchain technology, initially with the cryptocurrency Bitcoin, has brought with it a range of possibilities for developing solutions in the most diverse sectors of society. The characteristics of the technology guarantee various advantages such as immutability, irrefutability, auditability and transparency. In addition, because the information is replicated in all nodes of the network, blockchain provides decentralization, disintermediation and availability. The blockchain platform Hyperledger platform, offers frameworks such as Fabric, which are designed to meet business needs with private and permissible networks, guaranteeing control and privacy. This decentralized and distributed system has found significant applicability in the realm of e-voting, offering solutions to crucial issues such as the integrity, authentication and security of votes. This record is accessible to all network participants, guaranteeing the traceability and verifiability of election results. The immutability of the data in the blockchain ensures that no information is altered or tampered with, increasing confidence in the electoral process. Auditing is a recognized management technique that provides an overview of the situation regarding specific resources and services within an organization. In the corporate environment there are various types of audits, including information systems audits, so there is no definite consensus in the literature on a single audit methodology. This paper develops a study on the use of blockchain technology in e-voting systems with the inclusion of simplified auditing processes and low or no implementation costs. A state-of-the-art search is carried out in order to gain an insight into scientific production on the subject. Experiments are carried out with the Hyperledger platform. An application is created to test the functioning of the proposed architecture. At the end of the development process, it is possible to conclude that the work meets what was proposed, as it advances the theoretical foundation, highlights in the literature the growing production on the subject of e-voting with the use of blockchain technology, proposes a simple architecture that incorporates an auditability character to the e-voting system, performs a performance analysis using the hyperledger platform, providing a more in-depth understanding of the characteristics of this platform, and finally validates the possibility of creating a complete e-voting system using blockchain technology and the hyperledger platform.

Keywords: blockchain; e-voting; audit.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O advento da tecnologia *blockchain* trouxe um leque de possibilidades. *Blockchain* é uma sequência de blocos que contém um registro completo de transações, como um livro-razão público, apontando a ordem de ocorrência das transações (BHASKAR; CHUEN, 2015). Cada bloco na sequência confirma a integridade do bloco anterior, fazendo um caminho inverso do último para o primeiro bloco da cadeia. Além disso o livro-razão é replicado em todos os nós da rede, garantindo que todos tenham cópias idênticas dos registros. Este processo garante características como transparência, integridade, confiabilidade, autenticidade, segurança, anonimato (XIE *et al.*, 2019).

A tecnologia foi apresentada inicialmente como uma criptomoeda (moeda digital), o Nakamoto (2008), mas suas características permitem que seja aplicada às diversas áreas da sociedade. As oportunidades de pesquisa com *blockchain* estão em amplo crescimento, e uma das aplicações da tecnologia se dá na realização de auditorias. A auditoria é uma técnica de gestão reconhecida que fornece aos gestores um visão geral da situação em relação a recursos e serviços específicos dentro de uma organização (BOTHA; BOON, 2003). Ao realizar uma revisão da literatura nos principais repositórios científicos é possível observar trabalhos que relacionam *blockchain* com auditoria iniciaram em meados passaram a ter maior destaque a por meados de 2014, baseando-se nos resultados das buscas nos 5 repositórios de pesquisa científica utilizados, antes desse período não são encontrados trabalhos neste escopo específico. Os repositórios são ACM Digital Library (MACHINERY, 2023), IEEE (ELECTRICAL; ENGINEERS, 2023), Science Direct (B.V., 2023), Springer (SPRINGER, 2023) e Wiley Online Library (SONS, 2023), durante a busca nestes repositórios é possível observar também que estas pesquisas tem se intensificado, sendo mais de 80% dos trabalhos realizados nos últimos 3 anos.

Diversas aplicações modernas para *blockchain* se dão pela sua associação com outra tecnologia, os contratos inteligentes. O tecnologia dos contratos inteligentes surgiu como um meio de automatização de processos e garantias e foi definida como um protocolo de transação computadorizado que executa os termos de um contrato (SZABO, 1994). A junção de *blockchain* e contratos inteligentes propiciou que diversas plataformas e ambientes de desenvolvimento surgissem para criar inúmeras soluções, inclusive para auditorias. Uma destas plataformas é a Hyperledger.

A plataforma Hyperledger é um ecossistema de desenvolvimento para a tecnologia *blockchain*. Dentro do escopo do Projeto Hyperledger existem outros projetos, sendo *frameworks*

e ferramentas de desenvolvimento que dão base a essas estruturas.

1.1 Motivação

A digitalização tem transformado diversos setores da sociedade, simplificando processos e oferecendo novas oportunidades de interação e participação. Um setor crucial que tem sido impactado é o sistema eleitoral, onde a modernização e a transparência são fundamentais para garantir a democracia (OLIVEIRA; OLIVEIRA, 2020). Nesse sentido, a tecnologia *blockchain* surge37 como uma solução promissora para o desenvolvimento de sistemas de votação eletrônica (*e-voting*) com ênfase na segurança, integridade e auditabilidade (BOUCHER, 2016). A digitalização tem transformado diversos setores da sociedade, simplificando processos e oferecendo novas oportunidades de interação e participação. Um setor crucial que tem sido impactado é o sistema eleitoral, onde a modernização e a transparência são fundamentais para garantir a democracia. Nesse sentido, a tecnologia *blockchain* surge como uma solução promissora para o desenvolvimento de sistemas de votação eletrônica (*e-voting*) com ênfase na segurança, integridade e auditabilidade (HLADKÁ; HERCIG, 2020) (HASSANI; AZMOON, 2019).

O sistema de votação é o alicerce da democracia, assegurando a representatividade do povo e a legitimidade das decisões políticas (OLIVEIRA; OLIVEIRA, 2020). No entanto, os sistemas de votação tradicionais enfrentam desafios consideráveis, como a possibilidade de fraudes, a falta de transparência e a dificuldade em garantir uma auditoria completa. Diante dessas questões, é necessário um avanço tecnológico capaz de aumentar a confiança dos eleitores e permitir uma fiscalização efetiva. A tecnologia *blockchain* desponta como uma solução inovadora e revolucionária. Trata-se de um registro distribuído, imutável e transparente de transações, em que cada nova transação é validada e adicionada como um bloco conectado aos anteriores. Com essa tecnologia, é possível garantir a integridade dos dados e a rastreabilidade de todas as etapas do processo eleitoral (MYAGMAR; SHARMA, 2020).

A arquitetura proposta para o sistema de *e-voting* auditável, baseia-se na tecnologia *blockchain*, que oferece características cruciais para garantir a segurança e a transparência do processo eleitoral. A implementação desse sistema envolve a criação de uma rede de nós distribuídos, nos quais cada nó possui uma cópia do livro-razão da *blockchain*. Essa rede descentralizada elimina a necessidade de uma autoridade central, reduzindo os riscos de manipulação e de ataques maliciosos (STUMPF *et al.*, 2018) (MARQUES; COSTA, 2019) (XIONG *et al.*, 2020).

Um dos principais benefícios do uso da tecnologia *blockchain* no *e-voting* é a capacidade de garantir a integridade dos votos, dadas as características da *blockchain* que garantem integridade dos dados (KHAN *et al.*, 2021). Cada voto registrado na *blockchain* é criptografado e imutável, tornando praticamente impossível a sua alteração ou exclusão. Além disso, a transparência oferecida pela *blockchain* permite que qualquer eleitor ou parte interessada verifique a contagem dos votos e a validade do processo, aumentando a confiança no sistema. Outra vantagem crucial da arquitetura de *e-voting* baseada em *blockchain* é a auditoria abrangente. Através da *blockchain*, é possível rastrear todas as transações e votos, desde a sua origem até o resultado final, garantindo a verificabilidade e a auditabilidade do processo eleitoral. Isso significa que qualquer tentativa de fraude ou manipulação pode ser identificada e corrigida de forma rápida e eficiente, fortalecendo a confiabilidade do sistema e a validade dos resultados (KSHETRI *et al.*, 2018).

No entanto, é importante ressaltar que a implementação bem-sucedida de um sistema de *e-voting* baseado em *blockchain* requer uma cuidadosa análise e consideração de aspectos técnicos, legais e sociais (FEENEY; MACCARTHY, 2019). É necessário desenvolver padrões e regulamentações adequadas, além de garantir a inclusão de todos os eleitores, independentemente do seu nível de familiaridade com a tecnologia. Em suma, a tecnologia *blockchain* tem o potencial de revolucionar o processo eleitoral, oferecendo um ambiente seguro, transparente e auditável para as eleições. A pesquisa e o desenvolvimento nessa área são fundamentais para avançar na direção de sistemas eleitorais mais confiáveis e eficientes, que reflitam verdadeiramente a vontade popular (MOHANRAJ *et al.*, 2020).

1.2 Objetivos

Dentro deste contexto, o objetivo primordial deste trabalho é desenvolver uma arquitetura que permita a criação de sistemas de votação eletrônica auditáveis, utilizando a tecnologia *blockchain* através da plataforma Hyperledger. Esta abordagem visa ser aplicável tanto em ambientes educacionais quanto governamentais.

Para alcançar esse objetivo amplo, são delineados três objetivos específicos essenciais, visando garantir a eficiência e a relevância científica do projeto. O primeiro consiste na identificação de problemas reais presentes em situações de votação, através de uma análise da literatura. Este objetivo busca assegurar que a proposta desenvolvida neste estudo seja capaz de solucionar alguns desses desafios identificados.

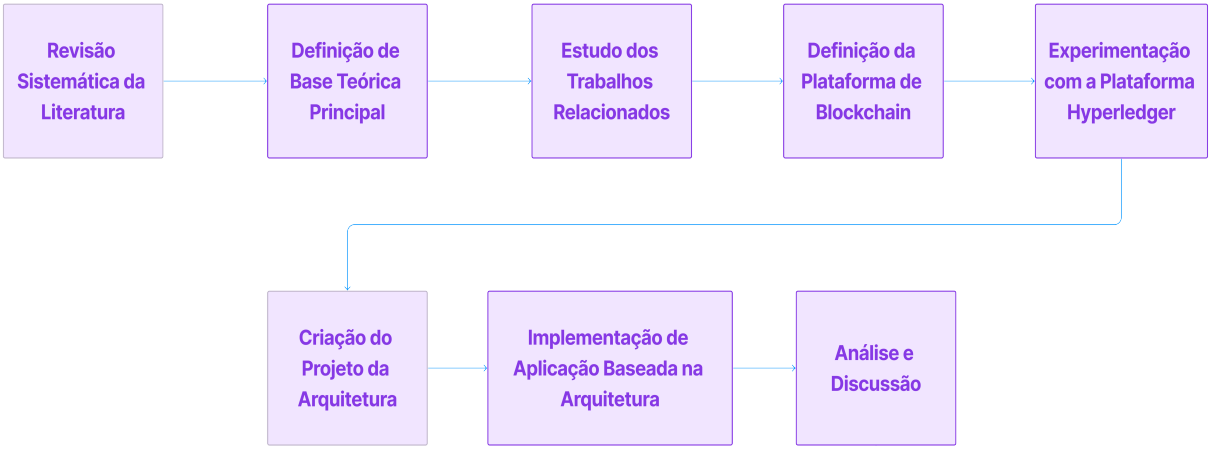
Em seguida, propõe-se um modelo prático e aplicável, utilizando plataformas e tecnologias acessíveis para estudantes, instituições e governos. A ênfase está em escolher tecnologias que possam ser adotadas com baixo ou nenhum custo, visando não somente a praticidade, mas também a contribuição tecnológica ao oferecer uma solução de fácil implementação e uso generalizado.

Por fim, o terceiro objetivo específico é a obtenção de ganhos científicos e tecnológicos, enfatizando a relevância prática e aplicável da solução resultante deste trabalho. Isso implica em criar uma solução que não apenas resolve problemas reais, mas também se destaca pela sua usabilidade e implementação viável em diferentes contextos, contribuindo assim para o avanço do conhecimento na área de votação eletrônica.

1.3 Metodologia

Nesta seção são descritos os passos de condução deste trabalho. O primeiro passo é a condução da revisão sistemática, depois são realizados experimentos com a tecnologia Hyperledger. A seguir é feita a apresentação da proposta e por fim é definido um sistema de validação da arquitetura. Seguidos estes passos, os resultados da pesquisa são comentados para que ao final seja possível definir a conclusão do trabalho. A figura 1 traz uma representação da metodologia deste trabalho.

Figura 1 – Passos da Metodologia.



Fonte: Produzido pelo Autor.

1.3.1 Revisão Sistemática da Literatura

Na realização da revisão sistemática de sistemas de *e-voting* com foco em auditoria utilizando a tecnologia *blockchain* é um processo estruturado que envolve diversos passos para coletar, analisar e sintetizar evidências relevantes de estudos existentes. Em seguida, é necessário estabelecer critérios de inclusão e exclusão para selecionar os estudos que serão analisados. Com os critérios definidos, realiza-se uma busca sistemática em bases de dados acadêmicas, como IEEE (ELECTRICAL; ENGINEERS, 2023) , ACM Digital Library (MACHINERY, 2023), etc. A realização deste mapeamento sistemático da literatura é dividida em três etapas: planejamento, condução e extração de dados.

O principal objetivo da revisão é identificar na literatura trabalhos que tratem de arquiteturas utilizando a tecnologia *blockchain* em sistemas de *e-voting*. Os fatores de comparação destes trabalhos são suas arquiteturas e características, e o contexto a ser observado é o do ambiente acadêmico, corporativo e/ou público governamental, preferencialmente.

1.3.2 Definição de Base Teórica Principal

Outro objetivo da revisão sistemática da literatura é construir uma base teórica acerca das tecnologias utilizadas e dos principais conceitos envolvidos no trabalho. Nesta etapa da metodologia, são definidos quais são os principais conceitos que permeiam o desenvolvimento deste trabalho, bem como através da observação de outros trabalhos, busca-se observar quais os principais autores citados nos referidos temas. A partir daí é desenvolvido um estudo e compilado um resumo que tem como resultado a seção de fundamentação teórica deste trabalho.

1.3.3 Estudo dos Trabalhos Relacionados

Como resultado da busca sistemática em bases de dados acadêmicas, é possível obter um mapeamento dos trabalhos que mais se assemelham ou têm relevância no contexto do trabalho aqui proposto. O objetivo desta etapa é entender melhor as tecnologias que estão sendo utilizadas e o modo como estão sendo desenvolvidas as soluções. A partir deste entendimento busca-se identificar um escopo de trabalho que possa trazer ganho científico, seja pela utilização de uma tecnologia diferente, ou por um novo aspecto da abordagem utilizada na implementação de uma solução, etc.

No desenvolvimento desta proposta de arquitetura, a observação das arquiteturas

propostas em outros trabalhos, ajudou a identificar que existe a necessidade de um modelo de arquitetura simples, mas que seja efetivo. Foi observada a necessidade de um modelo que possa ser utilizado em uma ambiente acadêmico ou governamental, e que este modelo tenha o menor custo possível. Quando a arquitetura proposta já está definida, podemos voltar aos trabalhos relacionados a fim de realizar uma comparação entre esta arquitetura e a de outros trabalhos. Este comparativo permite identificar as vantagens e desvantagens dentre as abordagens observadas e em relação à proposta.

1.3.4 Definição da Plataforma de Blockchain

A fim de atender os objetivos do trabalho e levando em conta o que foi observado na literatura, deve ser definida qual será a plataforma de *blockchain* a ser utilizada. A adequação da utilização da plataforma para o tipo de aplicação que se quer desenvolver, pode ser entendida a partir da observação dos trabalhos relacionados. Considerando, também, o contexto em que a solução proposta deve ser inserida, a plataforma Hyperledger foi definida. Critérios como a disponibilidade gratuita de ferramentas, a possibilidade de instalação em ambiente próprio e a documentação acerca da plataforma, foram cruciais para escolha da plataforma. Outro fator levado em conta é a percepção de que a plataforma Buterin (2022) é a mais utilizada para este tipo de aplicação, o que leva a utilização de uma plataforma diferente como o Hyperledger ter maior possibilidade de ganho científico.

1.3.5 Experimentação com a Plataforma Hyperledger

Para buscar maior entendimento sobre a plataforma Hyperledger e suas ferramentas, outros trabalhos foram desenvolvidos. Instalação de algumas das ferramentas do Hyperledger, comparação de uso com outras plataformas, testes de desempenho, etc. são importantes para definir o melhor caminho para usar o referido *framework* na arquitetura proposta. Os esforços empreendidos resultaram no capítulo 4, bem como no artigo científico *"A Performance Analysis of Hyperledger Fabric: A Perspective of the ISO/IEC 25010 Product Quality Model"* (BEZERRA *et al.*, 2022).

1.3.6 Criação do Projeto da Arquitetura

Na definição e apresentação da proposta de arquitetura, é oferecido um sistema de *e-voting* seguro, transparente e confiável, com características que proporcionam auditoria. Esta definição obedece à critérios que se alinham com os objetivos definidos para o trabalho, como a viabilidade de utilização em ambiente real, o caráter prático da implementação e baixo ou nenhum custo.

1.3.7 Implementação de Aplicação Baseada na Arquitetura

Depois de criado o projeto de arquitetura o próximo passo é comprovar sua viabilidade. Para este trabalho foi criado um sistema de *e-voting* com o objetivo de validar que a arquitetura proposta é funcional. Importante observar que as tecnologias utilizadas para esta validação não geram custo financeiro,ou seja, foi implementado utilizando ferramentas e plataformas gratuitas, o que possibilita o uso desta solução em ambientes com restrições pecuniárias e/ou de infraestrutura.

O sistema criado observa os momentos de auditoria, a utilização de *blockchain*, a simplicidade de implementação. São critérios que advém de características da arquitetura proposta. Por fim são registrados usuários, candidatos, votações e votos, que passam por todo o fluxo proposto na arquitetura e validam sua utilização.

1.3.8 Análise dos Resultados Obtidos

Nesta etapa são discutidos quais os resultados obtidos em cada etapa do processo de desenvolvimento deste trabalho. Esta metodologia permite que os dados coletados, os experimentos realizados, a arquitetura projetada e aplicação criada sejam avaliadas de modo objetivo. Dessa maneira, nesta etapa da metodologia são evidenciados os comportamentos observados e contribuições do trabalho, e discutido o impacto deste trabalho no contexto em que se insere. Dentre os capítulos do trabalho, esta etapa se inicia no capítulo 6.

Ao final do trabalho é feito um resumo das etapas anteriores. Este resumo carrega a impressão do autor sobre o trabalho de modo geral. Também são apresentadas outras contribuições advindas do desenvolvimento do trabalho, desde de estudos tratando do uso da tecnologia *blockchain* de um modo geral até trabalhos que se relacionam diretamente com a solução aqui proposta.

São pontuadas possibilidades de desenvolvimento de trabalhos futuros que sejam diretamente oriundos deste. Há também ideias de trabalhos que não dão continuidade a esta proposta, mas cuja necessidade foi observada no processo de desenvolvimento.

1.4 Contribuições Científicas e Tecnológicas

É possível levantar neste trabalho algumas contribuições científicas e tecnológicas. A primeira contribuição científica pode ser observada na pesquisa para o desenvolvimento da fundamentação teórica e definição dos trabalhos relacionados. É identificada na literatura uma crescente produção acerca do tema *e-voting* utilizando a tecnologia *blockchain*, no entanto, apesar disto nota-se uma carência de um foco específico nas características relacionadas à auditoria, bem como uma carência de modelos que tenham foco nos quesitos de auditabilidade.

Uma proposta de arquitetura simples que traz caráter de auditabilidade ao sistema de *e-voting* é uma outra contribuição científica deste trabalho. Do ponto de vista de aplicabilidade há uma ganho visto que a arquitetura proposta traz uma implementação simples e usual em ambientes reais. Outro caráter de contribuição científica é o reforço das características específicas de auditoria proporcionados pela arquitetura proposta.

Ao implementar a validação da arquitetura é possível identificar uma contribuição tecnológica deste trabalho. Um aplicação web foi desenvolvida para validar que arquitetura proposta é viável. Com interface amigável, a aplicação permite criar usuário e votações, bem como realizar eleições.

Ainda do ponto de vista tecnológico, é possível levantar como contribuição a análise de desempenho realizada com a plataforma Hyperledger permite entender melhor as características da plataforma, o que ajuda a vislumbrar possibilidades de utilização no escopo desta pesquisa, bem como fora deste escopo, visto que a plataforma se mostra robusta e usual.

Por fim, é identificável como principal contribuição desta pesquisa, a validação da possibilidade de criação de um sistema completo de *e-voting* utilizando a tecnologia *blockchain* e a plataforma Hyperledger. Observa-se que todo o sistema foi desenvolvido e validado utilizando tecnologia e infraestrutura que geram baixo ou nenhum custo na sua utilização, sendo dessa forma perfeitamente utilizável em um ambiente de eleição estudantil, por exemplo. Importante levantar que a escolha da plataforma e das tecnologias têm o objetivo de trazer baixo ou nenhum impacto à ambientes que sofram restrições por questões financeiras ou de infraestrutura.

1.5 Estrutura

No Capítulo 2 a seguir é realizada uma fundamentação teórica, de modo a introduzir os principais contextos abordados neste trabalho. No capítulo 3 são apresentados os trabalhos relacionados decorrentes da revisão sistemática da literatura, analisando o estado da arte e fazendo uma comparação entre eles e a proposta deste estudo. Depois disso, no capítulo 4 é descrita a experimentação realizada com a plataforma de *blockchain* Hyperledger, como o objetivo de entender melhor a plataforma, suas vantagens e limitações. No capítulo 5 a arquitetura é projetada e depois apresentada, descrevendo sua estrutura e seus aspectos principais. No capítulo 6 é apresentada a implementação de uma aplicação que valida a utilização da arquitetura proposta neste trabalho. No capítulo 7 são discutidos os resultados para cada etapa do trabalho desenvolvido. Por fim, no capítulo 8 temos a conclusão deste trabalho, mostrando também as limitações deste estudo e os possíveis trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção são tratados os conceitos que são a base para o desenvolvimento deste trabalho. O conceito de auditoria é abordado, desenvolvendo acerca dos tipos de auditoria e sua importância. É realizada uma fundamentação acerca da tecnologia *blockchain*, de sua origem e características. Depois é feita uma explicação acerca de Contratos Inteligentes. Na subseção plataformas de *blockchain* são brevemente apresentadas algumas plataformas conhecidas para desenvolvimento com a tecnologia. Em seguida é feita uma descrição da plataforma Hyperledger, um ambiente de desenvolvimento de *blockchain* amplamente utilizado no meio corporativo e que é utilizado na implementação da infraestrutura deste trabalho. A definição de auditoria, os tipos de auditoria de sistemas e alguns exemplos. Por fim são apresentados os conceitos básicos de *e-voting* e o contexto o qual se insere na literatura.

2.1 Blockchain

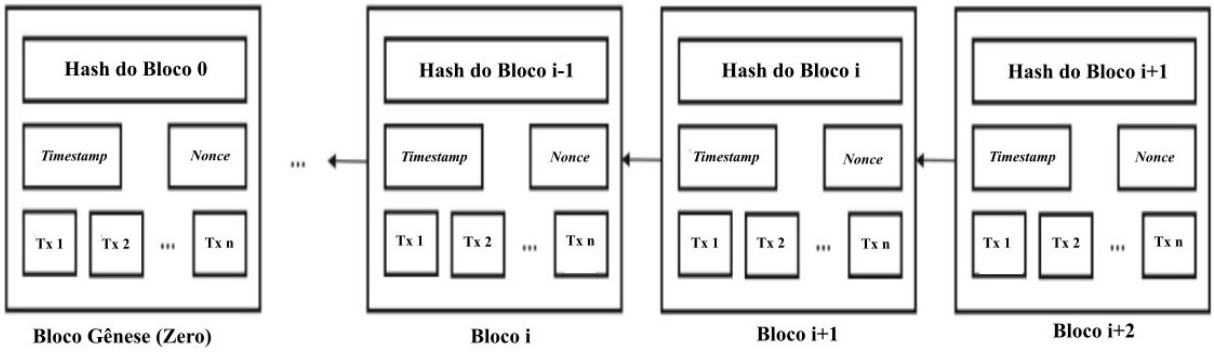
2.1.1 O que é Blockchain?

O termo *blockchain* foi utilizado pela primeira vez em 2008 no trabalho *"Bitcoin: A peer-to-peer eletronic cash system"* de Nakamoto (2008) para tratar de uma tecnologia que, como o próprio nome diz, consiste em uma sequência de blocos (BHASKAR; CHUEN, 2015). Nesta cadeia está contido um registro de transações, dentre outros dados, tal como um livro-razão utilizado na contabilidade. *Blockchain* é basicamente um banco de dados compartilhado imutável, descentralizado e público, que consiste em uma cadeia de pacotes de dados, que são os blocos, onde cada bloco compreende transações múltiplas (NOFER *et al.*, 2017) (XIE *et al.*, 2019).

Ao concluir a gravação dos dados no primeiro bloco da cadeia, chamado bloco gênese ou bloco zero, é processado um *hash* para o bloco. Este *hash* é calculado com base nos dados do bloco, no *timestamp* (data e hora) e no *nonce* (número aleatório de verificação do *hash*), por meio de um algoritmo de *hash* ou prova de trabalho conhecido (JAKOBSSON; JUELS, 1999). O bloco seguinte (bloco um) deve conter além de seus próprios registros a informação do *hash* do bloco zero, que é o seu bloco pai, do mesmo modo o próximo bloco (bloco dois) deve conter além de seus dados o *hash* do bloco anterior (bloco um) que é seu bloco pai. Este processo cria uma cadeia de dependência que faz com que qualquer alteração nos dados de um bloco, provoca uma alteração em seu *hash* e, consequentemente, invalida todos os blocos subsequentes

garantindo a integridade de toda a *blockchain* até o primeiro bloco (BOSU *et al.*, 2019). Os registros são, dessa forma, permanentes, transparentes e imutáveis (THAKKAR *et al.*, 2018). A figura 2 traz uma representação dos blocos de uma *blockchain*.

Figura 2 – Representação dos blocos de uma *blockchain*.



Fonte: adaptado de (NOFER *et al.*, 2017).

Outro fator importante para garantia da integridade é o fato de que cada nó da rede contém uma cópia idêntica deste livro-razão que é a *blockchain*. Através desse processo de replicação dos registros a tecnologia *blockchain* proporciona descentralização de sua operação. As transações são validadas pelos nós membros da rede através de um protocolo de consenso. Um novo bloco é considerado verificado somente após a maioria dos nós membros votar como verdadeiro e confiável usando o protocolo de consenso (BOSU *et al.*, 2019). As novas transações não são automaticamente adicionadas ao livro-razão. Em vez disso, o processo de consenso garante que essas transações sejam armazenadas em um bloco por um certo tempo antes de serem transferidas para o livro-razão. Após este processo, as informações na *blockchain* não podem mais ser alteradas (NOFER *et al.*, 2017).

A implementação de uma *blockchain* exige recursos que muitas vezes geram altos custos. O tamanho do bloco e o tempo gasto para minerá-lo, por exemplo, impactam diretamente no custo, uma vez que este processo requer poder computacional. A mineração é o processo de validação de um bloco em uma *blockchain*, quanto mais poder computacional for necessário para este processo, maior o custo envolvido aplicado em recursos de hardware, energia, etc. Apesar disso, a mineração tem muitos adeptos, pois normalmente estes mineradores são recompensados por fatias do valor agregado ao bloco gerado, como acontece com o Bitcoin que tem sua plataforma focada em transferência de valores financeiros (NAKAMOTO, 2008). A mineração pode afetar todo desempenho do sistema e isto deve ser observado (RIFI *et al.*, 2017).

Determinar que tipo de *blockchain* e qual configuração deve ser utilizada para

determinada solução, tornou-se um obstáculo na tomada de decisões entre fabricantes e arquitetos de sistemas, que são partes interessadas no desenvolvimento destas soluções com a tecnologia. Existem estruturas para auxiliar no entendimento e formulação de projeto técnico e comercial, apesar disso ainda se falha na abordagem do que fazer para verificar a viabilidade de uma solução com *blockchain*, ou que tipo de *blockchain* deve ser implementado se houver esta viabilidade. Considerando as implicações e objetivos destas partes interessadas, ao observar *blockchain* como um componente de software, conclui-se que cada implementação de uma *blockchain* necessita de uma análise cuidadosa de requisitos individuais para cada aplicação (ABREU *et al.*, 2020).

Pode-se definir três tipos de *blockchain*: pública sem permissão, pública com permissão e privada com permissão (PEDERSEN *et al.*, 2019). A *blockchain pública* sem permissão, como o próprio nome sugere, tem como característica principal o fato de qualquer pessoa poder participar da inserção, validação e leitura dos dados, a confiança é construída por meio do algoritmo de consenso, que é respeitado pelos pares da rede sem exceção. A *blockchain* pública com permissão, também chamada híbrida, é uma rede fechada, para nós verificados e confiáveis, onde apenas usuários autorizados podem validar transações e visibilidade dos dados é pública (permitida a todos os usuários). A *blockchain* privada com permissão é a mais restrita, permitindo a leitura, validação e inserção dos dados apenas à usuários específicos dentro da organização (PEDERSEN *et al.*, 2019) (XU *et al.*, 2020).

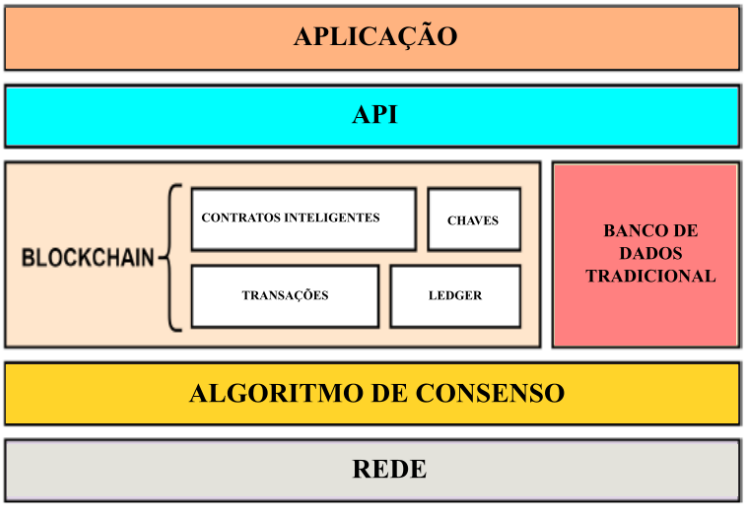
A computação distribuída de um modo geral está sujeita a sofrer problemas relacionados à integridade dos dados, confiança dos nós, incompletude de processos. Com a tecnologia *blockchain* não seria diferente, por isso mecanismos de consenso são utilizados para sanar ou mitigar estas questões.

> O consenso é um problema na computação distribuída em que os nós dentro do sistema devem chegar a um acordo, dada a presença de processos defeituosos ou nós enganosos (BACH *et al.*, 2018).

Diferentes algoritmos de consenso são utilizados em *blockchain* de acordo com o tipo e necessidade do grupo. Em uma *blockchain* pública sem permissão, por exemplos, os dois tipos mais utilizados são a *Proof of Work (PoW)* e a *Proof of Stake (PoS)*. Em uma *blockchain* privada com permissão normalmente é utilizado um *Byzantine Fault Tolerance (BFT)*. Existem diversos mecanismos de consenso, o trabalho de Bach *et al.* (2018) traz uma análise comparativa dos algoritmos citados e mais alguns outros, como *Proof of Importance*, *Ripple Protocol Consensus Algorithm (RPCA)*, *Delegated Byzantine Fault Tolerance (dBFT)*.

A utilização de *blockchain* nas aplicações traz vantagens como transparência, descentralização, segurança, confiabilidade e até mesmo automatização. No entanto o custo de utilização da tecnologia por ser alto, como levantando anteriormente. Dessa forma as arquiteturas com *blockchain* costumam ser construídas de forma híbrida com outras tecnologias de banco de dados, delegando à corrente de blocos o registro de partes sensíveis dos dados. O trabalho de Abreu *et al.* (2020), por exemplo, propõe uma arquitetura a ser utilizada em uma aplicação de registro de certificados em instituições de ensino. A figura 3 traz a representação desta arquitetura.

Figura 3 – Exemplo de arquitetura proposta para aplicação com *blockchain*.



Fonte: adaptado de (ABREU *et al.*, 2020).

Outra parte importante a ser considerada na construção de aplicações utilizando a tecnologia *blockchain*, são os Contratos Inteligentes. Por meio destes contratos é possível realizar automatização de transações e garantir aspectos de regras de negócios em *blockchain*, eles são fundamentados ainda nesta seção.

2.1.2 Estrutura

Dissociada da criptomoeda, a *blockchain* é apenas uma estrutura de dados, ou seja, é uma forma definida de como os dados são unidos e armazenados, muito similar ao banco de dados, porém descentralizada (LEWIS, 2018). Para Viana *et al.* (2020), essa estrutura descentralizada beneficia o sistema em relação à segurança, mas perde em rapidez de processamento, pois todos os nós da rede validam a mesma informação para garantir sua veracidade. A tecnologia *blockchain* pode ser aplicada a quaisquer valores de caráter digital, como por exemplo certificados, contratos,

arquivos ou qualquer outro que se deseje.

Em um *blockchain* devem ser levados em conta as características de rede. Numa perspectiva de alto nível, para Kamienski *et al.* (2005), uma rede *P2P* pode ser considerada uma rede *overlay*, uma vez que funciona como uma rede virtual, formada pela interconexão dos nós (*peers*), executando sobre a infraestrutura de uma rede física. A característica básica de uma rede *P2P* é que existe um grupo de nós com interesses comuns que estão conectados através do mesmo sistema de comunicação. Outras características dessa rede são: (i) os nós são conectados de forma aleatória, não há restrição sobre o número de nós que participam da rede; (ii) a conexão de um nó à rede se estabelece através de outro nó que já pertença à rede; (iii) os nós podem se unir e sair da rede a qualquer momento sem prévio conhecimento dos demais membros.

Não existe unanimidade na definição de uma rede *P2P*, assim a definição acaba sendo dependente do contexto em que a tecnologia é empregada (DETSCH, 2005). De forma geral, entretanto, estabelece-se que redes *P2P* são redes virtuais que funcionam na internet com o objetivo de compartilhar recursos entre os participantes, sendo que, por princípio, não há diferenciação entre os participantes (ROCHA *et al.*, 2004). Uma *blockchain* por definição é composta por uma rede *P2P*, em que cada máquina participante atua como um nó (*peer*) na rede, ou seja, a *blockchain* é uma rede descentralizada com vários nós conectados (SHARPLES; DOMINGUE, 2016), em que os dados armazenados são replicados automaticamente ou com base no comportamento dos usuários na rede *P2P* (XU *et al.*, 2017). A natureza da topologia *P2P* na *blockchain* ajuda a compartilhar os recursos e reduzir os riscos de segurança (ALAMMARY *et al.*, 2019).

Considerando que a confiabilidade da informação é uma característica primordial da tecnologia *blockchain*, surgem alguns fundamentos de segurança da informação que devem ser observados (OLIVEIRA, 2012):

- Disponibilidade: uma informação deve estar disponível para acesso no momento desejado;
- Integridade: o conteúdo da mensagem não deve ser alterado.
- Controle de acesso: o conteúdo da mensagem deve ser acessado somente por pessoas autorizadas;
- Autenticidade: a identidade de quem está enviando a mensagem deve ser garantida;
- Não-repudiação: deve-se prevenir que terceiros neguem o envio e/ou recebimento de uma mensagem;
- Privacidade: deve-se impedir que pessoas não autorizadas tenham acesso ao conteúdo da

mensagem.

Existem duas meotodlogias que são bem comuns ao se falar em criptografia que são os simétricos e assimétricos. A criptografia simétrica baseia-se em dois elementos principais: o algoritmo de cifragem e a chave criptográfica (BARCELOS; MARTINS, 2020). Esse modelo também é caracterizado pela utilização de apenas uma chave tanto para a encriptação da mensagem original, quanto para a decodificação da mensagem encriptada. O principal atributo desta metodologia é a garantia de privacidade, dado que apenas os detentores da chave conseguirão ter acesso à mensagem original (SOUSA, 2019). Uma chave criptográfica é um valor secreto que modifica a saída em um algoritmo de encriptação. Funciona como a fechadura da porta da frente de uma casa, que possui uma série de pinos. Cada um desses pinos possui múltiplas posições possíveis. Quando alguém põe a chave na fechadura, cada um dos pinos é movido para uma posição específica. Se as posições ditadas pela chave são as que a fechadura precisa para ser aberta, ela abre, caso contrário, não.

Na criptografia assimétrica são utilizadas duas chaves, uma pública e outra privada, diferentes e complementares. A chave pública, como o próprio nome insinua, pode estar acessível a qualquer pessoa que deseje se comunicar de modo seguro, porém a chave privada deve ficar em posse somente de cada titular. A chave privada é responsável por decodificar uma mensagem criptografada para ele com a sua respectiva chave pública. Desta maneira, é garantida a confiabilidade da mensagem, desde que a chave privada esteja segura, posto que quem possuir acesso a esta chave terá acesso à mensagem (OLIVEIRA, 2012). A vantagem deste metodologia é a segurança, já que não é necessário e nem prudente compartilhar a chave privada. Por outro lado, a desvantagem é que o tempo de processamento de mensagens neste tipo criptografia é maior que na criptografia simétrica (OLIVEIRA, 2012). Outra aplicação considerada importante por Sousa (2019) da criptografia assimétrica é a geração de assinaturas digitais. Estas são baseadas em sua chave privada e podem ser verificadas por qualquer um que possua a respectiva chave pública.

A criptografia apoia fortemente a *blockchain* para cumprir os requisitos de segurança do sistema e das aplicações (ABREU, 2020). Dentre os recursos mais utilizados, destacam-se as funções *hash* e as assinaturas digitais (GREVE *et al.*, 2018). A assinatura digital no entendimento de Barcelos e Martins (2020), consiste em um processo de inversão do sistema de criptografia assimétrica. O autor assina uma mensagem usando sua chave privada para cifrá-la e ela pode ser decifrada utilizando a chave pública do autor, confirmando sua identidade e reconhecendo que a

mensagem não foi adulterada, uma vez que utiliza funções *hash* no processo. Este metodologia assegura a autenticidade, integridade e não-repudiação da mensagem, entretanto, não assegura sua confidencialidade, pois é decifrada utilizando a chave pública do emissor (OLIVEIRA, 2012).

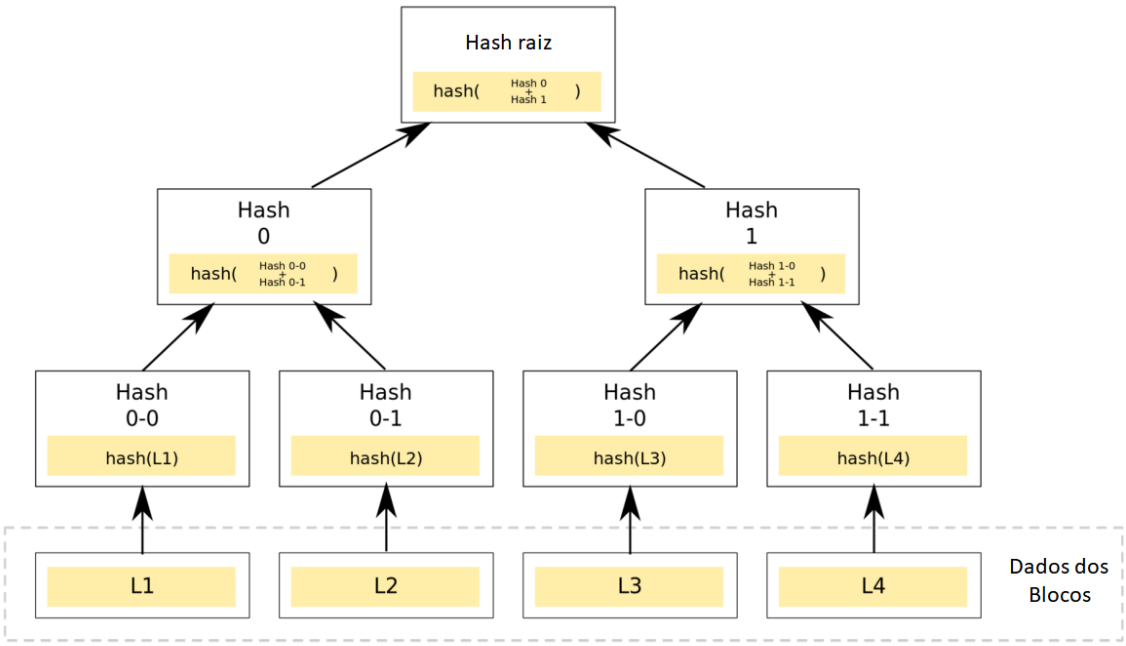
O tipo de criptografia mais empregado de acordo com Sousa (2019), é a função *hash*. Esta técnica encripta uma mensagem de uma maneira tal, que esta não pode retornar ao seu formato original por intermédio de uma função inversa, pelo fato da primeira função ser capaz de gerar um mesmo resultado para diferentes mensagens de entrada. Apesar da mensagem não poder retornar ao seu estado original, a verificação do resultado gerado para uma dada mensagem, é facilmente obtido ao se aplicar a tal mensagem na função *hash*. Já segundo Ishmaev (2017), uma função *hash* é essencialmente uma função matemática que dada uma entrada de dados de qualquer tamanho, produz uma saída de tamanho limitado que pode ser computável com eficiência (em um período de tempo razoável).

Uma árvore de Merkle para Matsumine (2019) é uma árvore binária formada inteiramente por valores de saída de um *hash* criptográfico, tal que cada folha da árvore é rotulada com o *hash* de um bloco de dados correspondente e cada nó que não seja uma folha é rotulado com o *hash* de seus nós filhos. É possível perceber que qualquer alteração em algum dos blocos de dados, produz um valor diferente do valor do *hash* esperado de um bloco íntegro e, devido a sucessão de cálculos de *hash* que se seguem a partir desse primeiro *hash*, todos os níveis superiores seriam afetados e produziriam um valor diferente, consequentemente uma raiz diferente e assim uma árvore de Merkle diferente.

Considerando a Figura 4 que Matsumine (2019) utiliza como exemplo, suponha que se deseja enviar o bloco L4 para o respectivo par da comunicação. Para isso, a árvore de Merkle é construída utilizando os blocos L1, L2, L3 e L4 e então é produzida uma prova para o bloco L4. Esta prova contêm o bloco L4, o *Hash* 1-0 e o *Hash* 0, uma vez que o caminho de L4 até a raiz passa pelo *Hash* 1-1, *Hash* 1 e finalmente chega-se ao *Hash* raiz. O par da comunicação que receberá o bloco L4, tem consigo uma cópia íntegra do *Hash* raiz (calculada a partir de L1 até L4 íntegros e obtida de um terceiro confiável). Após o par receber o bloco L4 junto a sua respectiva prova, o verificador calcula o *hash* de L4 e utilizando *Hash* 1-0 da prova, calcula *Hash* 1 e em posse desse *hash*, utiliza *Hash* 0 da prova para obter *Hash* raiz, o qual será comparado com *Hash* raiz e caso sejam iguais, o bloco L4 é considerado válido, caso contrário ele é descartado.

No contexto do *blockchain*, cada bloco contém um conjunto de transações. Em vez

Figura 4 – Exemplo de uma árvore de Merkle formada a partir dos blocos de dados L1, L2, L3 e L4



Fonte: adaptado de (MATSUMINE, 2019).

de incluir todas as transações diretamente no bloco, as transações são agrupadas em pares e os hashes desses pares são calculados. Esses hashes são então agrupados novamente e seus hashes são calculados. Esse processo continua até que haja apenas um hash raiz, chamado de Merkle root, que representa todas as transações do bloco. A árvore de Merkle é construída de forma que qualquer modificação em uma única transação resulte em uma mudança no hash raiz. Isso significa que, se alguém tentar alterar uma transação em um bloco de uma *blockchain*, o hash raiz será diferente e a alteração será detectada (ANTONOPOULOS, 2017).

2.1.3 Algoritmos de Consenso

Em sistemas de computação distribuídos, um componente, como um servidor, pode aparecer tanto como falho quanto funcional a um sistema de detecção de falhas (BARCELOS; MARTINS, 2020). Estes componentes podem apresentar diferentes sintomas a diferentes observadores, isto é conhecido como “falha bizantina”. É difícil para os outros componentes declararem que o servidor falhou e o desligarem da rede, por que eles primeiramente precisam obter consenso a respeito de qual componente falhou, sendo conhecido como ’falha bizantina’ (DRISCOLL *et al.*, 2004).

Em *blockchain* as transações do livro de registros são verificadas por vários clientes

ou validadores na rede *P2P* da criptomoeda, usando um dos muitos algoritmos de consenso que existem para resolver o problema de confiabilidade em uma rede envolvendo vários nós não confiáveis (BACH *et al.*, 2018). Nesta rede não há nó central que garanta que os registros das transações em nós distribuídos sejam todos iguais. Os nós precisam não confiar em outros. Assim, algumas abordagens são necessárias para garantir que os registros em nós diferentes sejam consistentes (ZHENG *et al.*, 2018).

Sendo um sistema descentralizado, a *blockchain* não precisa de uma autoridade externa. Ao invés disto, ele garante a confiabilidade e a consistência dos dados e das transações através de um mecanismo de consenso (LI *et al.*, 2020b). Isso é feito de forma a evitar o problema do gasto duplo. O gasto duplo é um dos maiores problemas em produtos digitais, que seria um usuário gastar/utilizar/compartilhar duas vezes o mesmo produto. Por exemplo, se existe um arquivo mp3 ou um e-book em um computador, pode-se copiar esse arquivo milhares de vezes livremente e envia-lo para milhares de pessoas diferentes. Para uma moeda digital, a possibilidade de cópia ilimitada significaria uma rápida morte hiperinflacionária (JOSELLI, 2018).

O Bitcoin foi o primeiro sistema de pagamentos eletrônico sem intermediação que se tem notícia (NAKAMOTO, 2008). Para Burgos e Alchieri (2021) problema do gasto duplo diz respeito à incapacidade de se garantir a transferência e a propriedade exclusiva de um artefato digital simultaneamente. O papel-moeda é uma representação física, ou *token* físico, de um determinado valor em uma determinada moeda. Quando é utilizado uma cédula para pagar por algum produto, ou serviço, o valor que ela representa é transferido juntamente com sua posse para o vendedor. Para gastar o valor representado pela mesma cédula mais de uma vez, seria preciso copiá-la, o que é ilegal e passível de detecção devido às tecnologias utilizadas na produção da numeração física. Já a cópia de um artefato digital é indistinguível de seu original, permitindo assim, a circulação indetectável de um número potencialmente ilimitado de cópias do mesmo artefato.

O problema do gasto duplo é comentado por Lucas e Andrea (2019) onde é dito que ele também impossibilitaria a manutenção da moeda, pois o que garante valor ao dinheiro é sua escassez, e então, se todos pudessem multiplicar o dinheiro a seu bel prazer, o sistema monetário seria impraticável. Com isso não haveria mais necessidade em se discutir o valor e consequentemente a necessidade do dinheiro. As criptomoedas, desta forma, não teriam mais valor. Também segundo Lucas e Andrea (2019) as criptomoedas podem ser negociadas entre

os usuários com a utilização da chave pública como espécie de “conta” em que serão retiradas ou recebidas as moedas, mas, podem também, e geralmente são, negociadas em corretoras de câmbio próprias: as *Exchanges*, ambiente no qual podem ser negociadas várias criptomoedas ao preço da moeda do país em que funcionam e são regulamentadas. O problema do gasto duplo é uma das questões que justificam a necessidade de algoritmos de consenso.

Os algoritmos de consenso desempenham um papel fundamental em *blockchain*, assegurando a integridade, segurança e confiabilidade das redes. Eles são responsáveis por determinar como as transações são validadas e como o consenso é alcançado entre os participantes. A necessidade de utilizar algoritmos de consenso em *blockchain* pode ser justificada por várias razões. Em primeiro lugar, esses algoritmos garantem a segurança e a integridade das transações, verificando sua autenticidade e evitando a duplicação ou adulteração de dados. Dessa forma, eles protegem a rede contra ataques maliciosos, como gastos duplos (AMUAIL SHAWN, 2016).

Um algoritmo de consenso em *blockchain* é um mecanismo utilizado para alcançar um acordo entre os participantes da rede sobre o estado do *blockchain*, especialmente em relação à validade das transações e à ordem em que elas são adicionadas ao *blockchain*. Existem diferentes algoritmos de consenso utilizados em *blockchains*, sendo os mais conhecidos o *Proof of Work (PoW)* (NAKAMOTO, 2008), o *Proof of Stake (PoS)* (KING; NADAL, 2012) e o *Delegated Proof of Stake (DPoS)* (LARIMER, 2014a).

O algoritmo *Proof of Work (PoW)* é um mecanismo de consenso utilizado em várias criptomoedas, incluindo o Bitcoin. Ele foi proposto pela primeira vez por Dwork e Naor (1993) como uma medida contra ataques de negação de serviço. Desde então, o *PoW* tem sido amplamente adotado como um método de garantir a segurança e a integridade de um *blockchain* descentralizado. O objetivo do *PoW* é evitar que um adversário malicioso controle a maioria do poder computacional em uma rede e, assim, assuma o controle do processo de validação das transações. Ele requer que os participantes da rede realizem um trabalho computacionalmente intensivo para provar que eles contribuíram para o consenso. A ideia fundamental do *PoW* é que os participantes da rede devem encontrar um valor (conhecido como "nonce") que, quando combinado com os dados de uma transação, produza um resultado *hash* que satisfaça um determinado critério. Esse critério é geralmente definido como encontrar um hash que comece com um número específico de zeros. Encontrar o *nonce* correto requer tentativa e erro, uma vez que o resultado *hash* é imprevisível e não pode ser calculado diretamente. Os participantes da rede precisam realizar cálculos repetitivos, ajustando o valor do *nonce* até que o *hash* produzido

satisfaça o critério definido. Esse processo é intensivo em termos de consumo de recursos computacionais. Uma vez que um participante encontre o *nonce* correto, ele pode enviar a solução para a rede, que verifica se o *hash* satisfaz o critério estabelecido. Se a solução for aceita, o participante é recompensado com uma determinada quantidade de criptomoeda (DWORK *et al.*, 2015).

O *PoW* é considerado seguro porque encontrar o *nonce* correto é um processo difícil, mas a verificação da solução é fácil e rápida. Isso significa que um participante malicioso precisaria de uma quantidade significativa de poder computacional para controlar a rede, tornando o ataque inviável na prática (NARAYANAN *et al.*, 2016).

O algoritmo *Proof of Stake* (PoS) é um protocolo de consenso utilizado em *blockchain* para validar transações e adicionar novos blocos à cadeia de blocos. Ao contrário do algoritmo *Proof of Work* (PoW), que depende da capacidade computacional dos mineradores, o PoS seleciona validadores com base na quantidade de criptomoeda que eles possuem e estão dispostos a "apostar"como garantia. A ideia central do PoS é que os validadores, conhecidos como "stakers"(ou apostadores), devem demonstrar a propriedade de uma certa quantidade de moeda nativa da *blockchain*, conhecida como "token de aposta"ou "token de participação". Em vez de competir pela solução de um problema matemático complexo, como no PoW, os stakers são escolhidos para criar um novo bloco de forma proporcional à quantidade de tokens que possuem e estão dispostos a bloquear. O processo de seleção dos validadores geralmente é determinado por um algoritmo de seleção aleatória ponderada, no qual os stakers com mais tokens têm mais chances de serem selecionados para criar o próximo bloco. Essa seleção aleatória ponderada é projetada para evitar que um único staker com uma grande quantidade de tokens controle todo o processo de validação, proporcionando uma distribuição mais justa do poder de decisão. Existem diferentes variações do algoritmo PoS, como o Delegated Proof of Stake (DPoS), no qual os stakers podem delegar seus direitos de validação a outros participantes na rede, reduzindo a necessidade de manter um nó ativo 24 horas por dia. Outras variantes incluem o *Liquid Proof of Stake* (LPoS), o *Leased Proof of Stake* (LPoS) e o *Bonded Proof of Stake* (BPoS), cada um com suas próprias características e objetivos específicos (BUTERIN, 2016) (ETHEREUM.ORG, 2023b).

Uma das principais vantagens do PoS em relação ao PoW é a eficiência energética. Como não requer poder computacional intensivo, o PoS consome menos eletricidade e, consequentemente, tem menor impacto ambiental. Além disso, o PoS tende a ser mais seguro contra

ataques de 51% (quando um ator malicioso controla a maioria do poder computacional) devido à dispersão do poder de validação. No entanto, assim como qualquer algoritmo de consenso, o PoS também possui desafios e críticas. Alguns argumentam que o PoS pode levar à centralização, pois os stakers com mais tokens têm mais influência na rede. Além disso, a distribuição inicial de tokens e a forma como eles são adquiridos podem afetar a equidade do sistema (ACADEMY, 2023).

O *Delegated Proof of Stake* (DPoS) é um algoritmo de consenso utilizado em algumas criptomoedas e *blockchains*, que foi projetado para oferecer um equilíbrio entre descentralização e eficiência. Ele foi introduzido por Daniel Larimer em 2014 e é usado em plataformas como EOS e Tron. Ele é uma variação do algoritmo *Proof of Stake* (PoS), no qual os participantes da rede, conhecidos como "stakeholders"(detentores de participação), podem delegar sua participação para representantes eleitos, chamados de "block producers"(produtores de blocos) ou "validators"(validadores). Os validadores são responsáveis por criar blocos e validar transações na *blockchain*. Nesse algoritmo, os detentores de participação na rede têm a capacidade de votar nos validadores que desejam eleger. Cada participante pode votar em múltiplos validadores, e a quantidade de votos que cada participante possui é proporcional à quantidade de participação que eles detêm na rede. Com base nos votos dos participantes, os validadores são selecionados periodicamente para serem responsáveis pela criação de blocos e validação das transações. Os validadores mais votados têm mais chances de serem selecionados. Para evitar a centralização de poder, o DPoS utiliza um sistema de rotação dos validadores. A cada rodada, um novo conjunto de validadores é escolhido para produzir blocos. Essa rotação permite que diferentes participantes tenham a oportunidade de participar da validação da rede. Os validadores selecionados são encarregados de criar blocos e adicionar transações à *blockchain*. Cada validador tem um tempo determinado para produzir um bloco. Se um validador não conseguir produzir um bloco dentro desse tempo, ele é substituído por outro validador. Os blocos propostos pelos validadores precisam ser verificados pelos outros validadores da rede antes de serem aceitos. Essa verificação é feita para garantir a integridade e a validade das transações. Em caso de consenso entre a maioria dos validadores, o bloco é adicionado à *blockchain* (LARIMER, 2014b).

O DPoS incentiva os validadores a agirem de forma honesta e apropriada, oferecendo recompensas financeiras na forma de tokens da criptomoeda nativa. No entanto, se um validador for pego agindo de maneira fraudulenta ou maliciosa, ele pode ser penalizado, como ter sua participação confiscada ou ser removido do grupo de validadores (ZHANG *et al.*, 2019).

Na implementação deste trabalho o algoritmo de consenso é gerenciado pela plataforma Hyperledger. Dessa forma, foi definido um protocolo que é mais facilmente configurável na plataforma. O protocolo de consenso *Raft* é um algoritmo de consenso que é projetado para ser simples e fácil de entender. Ele é usado para gerenciar a replicação de logs em servidores. Cada servidor em um*Raft* é um estado de uma máquina de estado que recebe entradas de um log de comandos. O algoritmo de consenso é usado para garantir que todos os servidores concordam nos comandos que estão nos logs (ONGARO; OUSTERHOUT, 2015). O Hyperledger implementa de modo simplificado o protocolo *ETCDRaft*, que é um protocolo baseado inteiramente no protocolo *Raft* (HYPERLEDGER, 2023).

Os algoritmos de consenso são essenciais para manter a descentralização em uma rede *blockchain*. Eles permitem que os participantes cheguem a um acordo sobre o estado da rede sem depender de uma autoridade central. Isso distribui o poder de decisão entre os participantes e evita o controle monopolista. A eficiência e a velocidade também são beneficiadas pelos algoritmos de consenso. Eles são projetados para processar transações de forma rápida e escalável, permitindo um alto volume de transações e reduzindo a latência. Isso é especialmente importante em *blockchains* públicas ou em casos de uso que exigem transações rápidas, como pagamentos ou micropagamentos. Outra função importante dos algoritmos de consenso é a resolução de conflitos. Quando ocorrem disputas, como a criação simultânea de blocos ou transações conflitantes, esses algoritmos estabelecem regras para determinar qual bloco ou transação é considerado válido e deve ser adicionado à *blockchain*. Isso garante a consistência e a coerência da rede (NARAYANAN *et al.*, 2016).

2.1.4 Contratos Inteligentes

Apesar de a tecnologia *blockchain* ter surgido em 2008, o conceito de Contratos Inteligentes *(Smart Contracts)* é mais antigo. Szabo (1994) definiu contratos inteligentes como um protocolo de transação computadorizado que executa os termos de um contrato. Ele propôs transformar cláusulas contratuais comuns, em código e integrá-las em propriedades (hardware ou software) que possam se autoaplicar, de modo a minimizar a necessidade de intermediários confiáveis entre as partes envolvidas na transação, e a ocorrência de exceções maliciosas ou acidentais (SZABO, 1994).

Dentro do contexto da *blockchain*, os contratos inteligentes são um fluxo de valor baseado em certos termos e condições, como contratos no mundo real. A única diferença é

que eles são completamente digitais, significando que um pequeno código é armazenado na *blockchain* (ALHARBY; MOORSEL, 2017). Um contrato inteligente é um agente inteligente, é um programa de computador capaz de tomar decisões quando certas pré-condições são atendidas. A inteligência de um agente depende da complexidade de uma transação para o qual está programado. Os contratos podem ser transações muito simples executadas em segundos e minutos ou transações relativamente complexas e demoradas que envolvem negociações e dezenas de páginas de texto escrito com direitos e obrigações específicos que podem levar horas ou meses para ser concluído. Hoje, os contratos inteligentes se enquadram na categoria de transações relativamente simples (KOLVART *et al.*, 2016).

Contratos inteligentes funcionam como um *script*. Eles têm endereço exclusivo na cadeia de blocos e podem ser acionados endereçando-se uma transação para eles. Estes contratos, quando acionados, executam de forma independente em qualquer nó da rede, de acordo com os dados incluídos na transação (CHRISTIDIS; DEVETSIKIOTIS, 2016). Um contrato inteligente é determinístico, uma mesma entrada sempre resultará em uma mesma saída. Se um contrato não determinístico é implementado, cada nó da rede vai executar de forma independente, isto produzirá resultados diferentes e aleatórios nos diferentes nós da rede, o que impedirá o consenso. Dessa forma, devido à falta do consenso, em *blockchain* não é possível implementar um contrato não determinístico, a própria rede *blockchain* o rejeitará (CACHIN *et al.*, 2016b). A tecnologia *blockchain* chegou a uma nova fase com a implantação de contratos inteligentes. Estes possuem o objetivo de possibilitar a utilização de redes *blockchain* para acordos dinâmicos e com maior confiança na troca de ativos digitais (SWAN, 2015).

Apesar da utilização de contratos inteligentes trazer benefícios para as soluções, existe a necessidade de cuidados em relação a possíveis ameaças ligadas ao uso de contratos inteligentes. Singh *et al.* (2020) levantaram algumas questões e vulnerabilidades enfrentados por contratos inteligentes. A verificação da funcionalidade foi o aspecto de vulnerabilidade mais comum encontrados em contratos inteligentes. Privacidade, segurança, escalabilidade e confiabilidade são outros exemplos de possíveis pontos sujeitos a produzir ações inesperadas ao ser realizados execuções de contratos inteligentes. Além disso, um contrato inteligente que foi inserido na *blockchain* sintaticamente correto, mas com problemas nas regras de negócio, poderá ser executado normalmente, provocando problemas para a aplicação e inserindo dados incoerentes com as regras de negócio e isto deve ser observado antes da implementação, visto que uma vez na *blockchain* não será apagado.

Algumas plataformas são utilizadas para implementação destes contratos inteligentes. Como dito anteriormente aBitcoin de Nakamoto (2008), utilizada para transações financeiras com criptomoeda, foi a primeira delas. A partir disto diversas plataformas e ferramentas foram criadas para desenvolvimento de soluções com *blockchain*. A plataforma de código aberto Ethereum é um exemplo de plataforma para desenvolvimento de *blockchain* descentralizada e que dá suporte a um sistema de computação global. Suas principais características são incorruptibilidade, segurança e é operacionalmente permanente. A ferramenta *Ethereum Virtual Machine* (EVM) é um *blockchain* programável, que permite que desenvolvedores executem programas, utilizando linguagens de alto nível, como *Solidity* que assemelha-se a *Javascript* e *Vyper* que assemelha-se a *Python* (CHEN *et al.*, 2018). Outro exemplo de plataforma é Hyperledger, que é uma iniciativa da *Linux Foundation* para desenvolver um ecossistema de código aberto de desenvolvimento com *blockchain*, dessa forma o Hyperledger é um hub aberto para projetos de *blockchain* de nível empresarial para dar espaço para incubação e amadurecimento em todos os estágios de desenvolvimento e comercialização (DHILLON *et al.*, 2017). Na próxima seção é feita uma descrição desta plataforma.

2.2 Plataformas de Blockchain

Existem diversas plataformas de desenvolvimento com *blockchain* que oferecem diferentes recursos, protocolos de consenso e focos específicos, permitindo que desenvolvedores e organizações possam avaliar as características e definir qual deve atender melhor suas necessidades.

O Bitcoin é a primeira e mais conhecida criptomoeda baseada em *blockchain*. Ela permite transações ponto-a-ponto sem a necessidade de uma autoridade centralizada. A rede Bitcoin é uma plataforma de código aberto que utiliza um protocolo de consenso chamado *Proof-of-Work* (PoW) para validar transações e manter a segurança da rede (PROJECT, 2023).

O Ethereum é uma plataforma de *blockchain* com recursos avançados que permitem a criação e execução de contratos inteligentes. Além de suportar criptomoedas, o Ethereum permite o desenvolvimento de aplicativos descentralizados (DApps) e tokens personalizados. Sua linguagem de programação principal é o Solidity (ETHEREUM.ORG, 2023a).

Hyperledger é um projeto de código aberto hospedado pela *Linux Foundation* que engloba várias plataformas e ferramentas de *blockchain* voltadas para casos de uso empresariais. Diferente do Bitcoin e Ethereum, o Hyperledger não possui uma criptomoeda própria e se

concentra em fornecer estruturas modulares para construir soluções de *blockchain* personalizadas (FOUNDATION, 2023b).

Corda é uma plataforma de *blockchain* de código aberto desenvolvida pela R3. Ela é projetada para atender às necessidades das empresas, permitindo a construção de aplicativos de negócios seguros e interoperáveis. O Corda utiliza um modelo de compartilhamento de dados entre participantes autorizados, enquanto mantém a privacidade e a confidencialidade das informações (R3, 2023).

Stellar é uma plataforma de *blockchain* focada na facilitação de pagamentos rápidos e de baixo custo. Ela permite a emissão e o gerenciamento de ativos digitais personalizados, incluindo moedas fiduciárias, por meio de contratos inteligentes. O Stellar é amplamente utilizado em casos de uso de remessas internacionais e sistemas de pagamentos transfronteiriços (FOUNDATION, 2023c).

NEO é uma plataforma de *blockchain* de código aberto que visa a criação de uma "economia inteligente"digital. Ela permite o desenvolvimento de contratos inteligentes e ativos digitais personalizados. O NEO oferece suporte a várias linguagens de programação populares, como C#, Java e Python, facilitando o desenvolvimento de aplicativos na plataforma (TEAM, 2023).

O EOSIO é uma plataforma de *blockchain* de alto desempenho projetada para aplicativos descentralizados escaláveis. Ela oferece um ambiente de desenvolvimento flexível para a criação de contratos inteligentes e aplicativos descentralizados de alto desempenho. O EOSIO utiliza um modelo de consenso baseado em Delegated Proof-of-Stake (DPoS) (BLOCK.ONE, 2023).

O Cardano é uma plataforma de *blockchain* de terceira geração que combina segurança, escalabilidade e sustentabilidade. Ela utiliza um protocolo de consenso chamado Ouroboros e possui uma abordagem científica em seu design. O Cardano suporta a criação de contratos inteligentes e busca promover a inclusão financeira global (FOUNDATION, 2023a).

O Tron é uma plataforma de *blockchain* voltada para a indústria de entretenimento e conteúdo digital. Ela permite a criação de aplicativos descentralizados e o compartilhamento de conteúdo entre usuários sem intermediários. O Tron possui sua própria criptomoeda chamada TRX e busca descentralizar a indústria de entretenimento tradicional.

O Tezos é uma plataforma de *blockchain* de código aberto que enfatiza a governança descentralizada e a segurança. Ela utiliza um modelo de consenso chamado *Liquid Proof-of-Stake*

(LPoS) e permite a atualização do protocolo sem bifurcações rígidas. O Tezos suporta a criação de contratos inteligentes e incentiva a participação dos detentores de tokens na governança da rede (TEZOS, 2023).

As plataformas mais conhecidas dentre as citadas são a Hyperledger, a Ethereum e a Bitcoin. Cada uma possui suas próprias vantagens e são amplamente adotados em diferentes cenários. A escolha entre Hyperledger, Ethereum e Bitcoin depende dos requisitos específicos do caso de uso e das necessidades da organização que está implementando a tecnologia *blockchain*. Para desenvolvimento deste trabalho, a plataforma Hyperledger foi escolhida uma vez que oferece várias vantagens em relação à Ethereum e ao Bitcoin: Modelo de permissão; Flexibilidade e personalização; Escalabilidade; Eficiência energética; Suporte a contratos inteligentes. A plataforma Hyperledger será melhor descrita na próxima seção

2.3 Hyperledger

A Hyperledger surgiu em junho de 2016 e é uma plataforma de código aberto voltada para o desenvolvimento de soluções baseadas em *blockchain*, desenvolvida pela *Linux Foundation*. Ela foi criada com o objetivo de facilitar a colaboração entre empresas e organizações interessadas em explorar o potencial dessa tecnologia. A tecnologia *blockchain* tem sido amplamente reconhecida como uma inovação disruptiva, com o potencial de transformar setores como finanças, cadeia de suprimentos, saúde, governo e muito mais. No entanto, a implementação de soluções baseadas em *blockchain* pode ser complexa e desafiadora, especialmente em um ambiente empresarial, onde a interoperabilidade, a escalabilidade e a privacidade são fundamentais (CACHIN *et al.*, 2016a). A Hyperledger foi projetada para enfrentar esses desafios, fornecendo um conjunto de *frameworks* e ferramentas que permitem o desenvolvimento e a implantação de redes *blockchain* empresariais personalizadas. Ao adotar uma abordagem modular (*plug-and-play*), a plataforma Hyperledger permite que as organizações escolham e combinem os componentes que adequam-se melhor às suas necessidades específicas.Isto permite que o consenso seja conectável, além de prover serviços de associação exclusivos para diferentes funções do usuário (DHILLON *et al.*, 2017).

Além disso, a Hyperledger oferece um ambiente de colaboração e governança aberto, permitindo que empresas e desenvolvedores trabalhem juntos para criar padrões e boas práticas. Dessa forma, a plataforma busca promover a inovação, acelerar a adoção de *blockchain* e impulsionar o crescimento de aplicativos e soluções baseados nessa tecnologia. Dentro do

escopo do Projeto Hyperledger existem outros projetos, sendo *frameworks* e ferramentas de desenvolvimento que dão base a essas estruturas. Estes projetos vão desde livrarias específicas à ambientes complexos de desenvolvimento.

No Hyperledger os pares da rede *blockchain* realizam descentralização, desintermediação replicação do estado da máquina, para isto vão rodar um protocolo de consenso plugável, com uma implementação de BFT *(Byzantine fault-tolerance)* (CASTRO *et al.*, 1999) específica. O *Fabric* implementa um registro com permissões, portanto contém infraestrutura de segurança para autenticação e autorização, suporta registro de transação por meio de certificados de chave-pública, garante confidencialidade, criptografia.

Em relação às principais plataformas de *blockchain* como por exemplo Bitcoin e Ethereum, a plataforma Hyperledger apresenta vantagens que foram levadas em conta para sua escolha neste trabalho. A Hyperledger utiliza um modelo de permissão, permitindo que as partes envolvidas tenham controle sobre quem pode acessar e participar da rede. Isso é útil para garantir privacidade e governança em redes empresariais e consórcios (CACHIN; VUKOLIĆ, 2017). Também fornece frameworks e ferramentas que permitem a criação de redes de *blockchain* personalizadas para atender às necessidades específicas de uma organização. Isso permite que as empresas adaptem a plataforma às suas próprias regras de negócio, requisitos de desempenho e privacidade (ANDROULAKI *et al.*, 2018).

A rede Hyperledger é projetada para ser escalável e pode lidar com um grande número de transações por segundo. Enquanto a Ethereum e o Bitcoin têm limitações de escalabilidade, a Hyperledger pode ser dimensionada de acordo com os requisitos da rede (ANISIMOV, 2018). A Ethereum e o Bitcoin utilizam algoritmos de consenso baseados em prova de trabalho *(proof-of-work)*, que requerem um alto consumo de energia para validar as transações. A Hyperledger permite diferentes algoritmos de consenso, incluindo aqueles mais eficientes em termos energéticos, como prova de autoridade *(proof-of-authority)* e tolerância a falhas bizantinas *(Byzantine fault tolerance)* (NAKIP; GÜNDÜZ, 2018). Embora a Ethereum seja conhecida por seu suporte a contratos inteligentes, a Hyperledger também oferece essa funcionalidade através do Hyperledger Fabric. Os contratos inteligentes na Hyperledger podem ser escritos em linguagens populares como *javaScript* e permitem a automação de acordos e a execução de lógica de negócios em uma rede *blockchain* (CACHIN *et al.*, 2016a).

Estes contratos inteligentes são chamados de *chaincodes*, são encapsulados em contêineres que rodam no mesmo processo, como um par da rede *blockchain* (CACHIN *et al.*,

2016a). Estas características tornam o Hyperledger Fabric um ambiente de desenvolvimento ideal para testes com contratos inteligentes e aplicações *blockchain*. A figura 5 traz um exemplo de código na linguagem GO *griesemer2009go* implementado para utilização em testes com Hyperledger Fabric. O trecho do código *chaincode* invoca as funções *create* e *query* que, respectivamente, cria registros e os consulta.

Figura 5 – Trecho do *chaincode* na linguagem GO.

```
func (s *SmartContract) Invoke(APIstub shim.ChaincodeStubInterface) sc.Response {

    function, args := APIstub.GetFunctionAndParameters()

    if function == "queryStatePatient" {
        return s.queryStatePatient(APIstub, args)
    } else if function == "initLedger" {
        return s.initLedger(APIstub)
    } else if function == "createStatePatient" {
        return s.createStatePatient(APIstub, args)
    }
    return shim.Error("Invalid Smart Contract function name.")
}
```

Fonte: produzido pelo autor.

Outra ferramenta importante é Hyperledger Caliper (FOUNDATION, 2021), uma ferramenta de *benchmark* para avaliação de desempenho que utiliza uma rede *blockchain*. O Hyperledger Caliper possibilita que um relatório na forma de um arquivo com formato HTML seja gerado a partir do experimento, e se possa observar as métricas em cada etapa da experimentação. A ferramenta pode rastrear métricas como taxa de transferência, latência, transações com sucesso, consumo de recursos de CPU e memória (AMPEL *et al.*, 2019).

É possível observar na literatura,que a plataforma Hyperledger, assim como as ferramentas Hyperledger Fabric e Hyperledger Caliper são utilizadas para implementação e testes em aplicações com *blockchain* para fins de auditoria. Considerando as características desta plataforma e sua aplicação no ambiente corporativo, foi realizada experimentação a fim de estudar características de seu funcionamento. Nas próximas seções essa análise de desempenho é melhor descrita. Para fins de validação da arquitetura proposta neste trabalho é utilizada uma combinação de algumas ferramentas do Hyperledger, mas a ferramenta principal é o Hyperledger Fabric.

O Hyperledger Fabric é uma estrutura de *blockchain* empresarial de código aberto mantida pela *Linux Foundation* e faz parte da iniciativa Hyperledger. Ele fornece uma plataforma

modular e flexível para a criação de redes de *blockchain* privadas, projetadas para atender às necessidades específicas de empresas e organizações. Uma das principais características do Hyperledger Fabric é a sua capacidade de oferecer um consenso flexível. Os participantes de uma rede podem escolher o algoritmo de consenso mais adequado às suas necessidades. O Hyperledger Fabric suporta vários mecanismos de consenso, como o *Practical Byzantine Fault Tolerance (PBFT)* e o *Kafka Orderer*, permitindo maior flexibilidade na seleção do algoritmo de consenso. Outra característica importante é a capacidade de criar modelos de dados privados e públicos. O Hyperledger Fabric permite a criação de canais privados, onde apenas um subconjunto de participantes pode acessar e validar transações. Isso é útil quando certas informações precisam ser mantidas confidenciais entre um grupo específico de participantes, enquanto outras informações podem ser compartilhadas publicamente. O Hyperledger Fabric suporta contratos inteligentes escritos em várias linguagens de programação, como *GO*, *JavaScript* e *Java*. Esses contratos inteligentes são chamados de *"chaincode"* e são executados dentro de contêineres isolados, garantindo a segurança e a escalabilidade do sistema (CONTRIBUTORS, 2023a) (CONTRIBUTORS, 2023b) (CONTRIBUTORS,).

O Hyperledger Fabric suporta dois tipos de bancos de dados de estado de pares: *LevelDB* e *CouchDB*. O Foundation (2023d), que é utilizado neste trabalho, é um banco de dados de estado opcional e alternativo que permite modelar dados no razão como *JSON* e emitir consultas ricas contra valores de dados em vez das chaves. Com o *CouchDB* é possível modelar dados de ativos como *JSON* (CROCKFORD, 2006), para realizar consultas *JSON* complexas.

A identidade e o controle de acesso são aspectos fundamentais do Hyperledger Fabric. Ele oferece recursos avançados de gerenciamento de identidade e controle de acesso. Os participantes podem ser autenticados usando vários métodos, como certificados digitais e provedores de identidade externos. Além disso, é possível definir políticas de acesso granulares para controlar as permissões de leitura e gravação na rede. O Hyperledger Fabric possui recursos poderosos para proteger a privacidade e a confidencialidade das transações. Ele suporta a criptografia de ponta a ponta e o compartilhamento seletivo de informações através de canais privados. Os dados confidenciais podem ser criptografados antes de serem gravados na *blockchain*, garantindo que apenas os participantes autorizados possam acessá-los. O Hyperledger Fabric é amplamente adotado por empresas e organizações em várias indústrias, incluindo finanças, cadeia de suprimentos, saúde e governo. Algumas das organizações que utilizam o Hyperledger Fabric incluem *IBM, Alibaba, Walmart, Maersk*, entre outras (CONTRIBUTORS, 2023a).

Para a construção de API's o Hyperledger contava com uma ferramenta chamada Hyperledger Composer. O Hyperledger Composer foi um projeto pertencente à iniciativa Hyperledger, mantida pela Linux Foundation. Ele era uma ferramenta de desenvolvimento de *blockchain* de alto nível que permitia a criação, implantação e gerenciamento de aplicativos descentralizados (DApps) baseados na tecnologia Hyperledger Fabric (CONTRIBUTORS, 2019).

O Hyperledger Composer fornecia uma camada de abstração para simplificar o processo de desenvolvimento de aplicativos *blockchain*. Com ele, os desenvolvedores podiam criar definições de rede, modelos de dados, lógica de negócios e regras de acesso usando uma linguagem de domínio específica (Domain-Specific Language - DSL) chamada de "Composer Modeling Language". Essa linguagem permitia uma representação fácil e legível dos conceitos do negócio em um ambiente *blockchain*. O motivo da descontinuação do Hyperledger Composer foi anunciado oficialmente em agosto de 2019 pela Linux Foundation. A decisão foi tomada com base em uma análise do ecossistema Hyperledger e das necessidades dos desenvolvedores. O Hyperledger Composer era considerado uma camada adicional de complexidade que não era mais necessária e poderia dificultar a integração de outros componentes do Hyperledger Fabric. A decisão visava incentivar os desenvolvedores a usar as ferramentas nativas do Hyperledger Fabric, como o Chaincode (contrato inteligente) e as APIs do *fabric*, para um desenvolvimento mais direto e eficiente (FOUNDATION,) (CONTRIBUTORS, 2019).

Hoje, o Hyperledger Fabric fornece um arcabouço de ferramentas e funções, além de infraestrutura suficiente para a validação realizada neste trabalho.

2.4 Auditoria

A auditoria é uma técnica de gestão reconhecida que fornece aos gestores um visão geral da situação em relação a recursos e serviços específicos dentro de uma organização. No ambiente corporativo existem diversos tipos de auditorias, entre elas a auditoria de sistemas de informação, de modo que não existe um consenso definido na literatura acerca de uma única metodologia para realização de auditoria. As auditorias são realizadas de formas muito diferentes de acordo com cada organização e necessidade. Em diferentes países, por exemplo, diferentes pré-requisitos se aplicam sobre quem tem permissão para realizar determinados tipos de auditoria, sendo influenciado inclusive pela legislação de cada local (BOTHA; BOON, 2003).

A auditoria, independente de seu tipo, é um processo de controle que gera benefícios no sentido de validar informações antigas, gerar novas informações, realizar diagnósticos, e

proporcionar um *feedback* às partes interessadas (BOTHA; BOON, 2003). Em outras palavras, o principal objetivo de uma auditoria, de sistema de informação inclusive, é formular uma opinião sobre a eficácia e a contribuição de sistemas e recursos para o objetivo da empresa (DEVALE; KULKARNI, 2012).

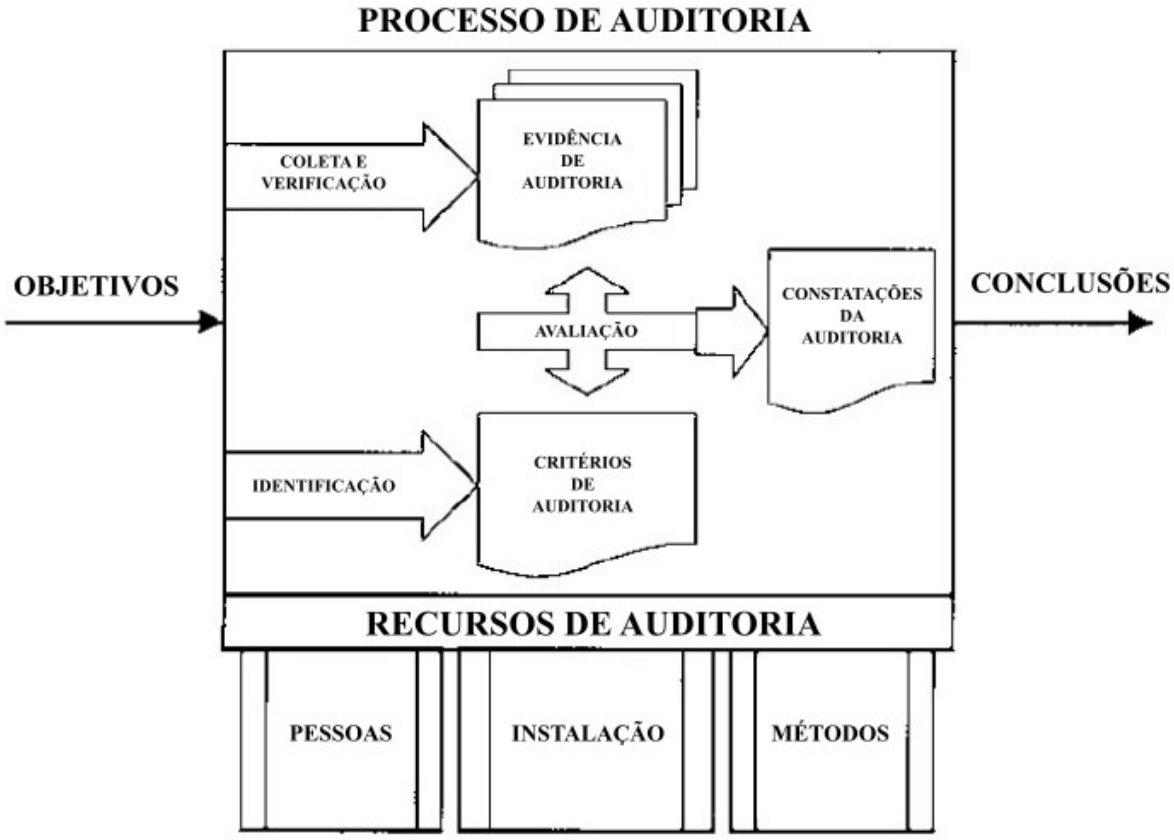
Na área das tecnologias de informação a auditoria de sistemas é uma disciplina essencial que tem como objectivo avaliar e garantir a segurança, integridade e eficiência dos sistemas informáticos de uma organização. Esta prática envolve uma análise sistemática e cuidadosa dos processos, controles e procedimentos implementados nos sistemas, de forma a identificar possíveis falhas, vulnerabilidades e desvios às políticas estabelecidas. As origens da auditoria de sistemas remontam ao surgimento dos primeiros computadores, na década de 1940. À medida que as empresas começaram a adotar a utilização de sistemas informáticos para automatizar as suas operações, tornou-se necessário garantir a fiabilidade e a exatidão das informações processadas pelos computadores. Foi neste contexto que a auditoria de sistemas começou a desenvolver-se. Inicialmente, a auditoria de sistemas estava mais centrada na verificação dos controlos de segurança física dos mainframes e dos procedimentos de salvaguarda e recuperação de dados. À medida que a tecnologia avançava e os sistemas distribuídos proliferavam, a auditoria de sistemas expandiu-se para abranger uma gama mais vasta de aspectos como a segurança lógica, a proteção de dados, a conformidade regulamentar e a governança das tecnologias de informação (SINGH; CHHABRA, 2018) (KAPLAN, 2018).

A evolução da auditoria de sistemas tem acompanhado de perto o crescimento do setor de TI e a crescente dependência das organizações em relação aos sistemas de informação. À medida que os sistemas se tornaram mais complexos e interligados, a auditoria de sistemas tornou-se também mais sofisticada e especializada. Atualmente, a auditoria de sistemas desempenha um papel fundamental para garantir a fiabilidade dos sistemas de informação. Os auditores de sistemas são responsáveis por examinar minuciosamente os processos, infra-estruturas, controles e políticas de segurança implementados numa organização. Utilizam ferramentas e técnicas avançadas para identificar potenciais vulnerabilidades e recomendar melhorias (ALNASSER; GRAY, 2019). As principais áreas de incidência da auditoria de sistemas incluem a identificação e avaliação dos riscos, a revisão dos controlos de acesso e autenticação, a verificação da integridade dos dados, a análise dos registos de eventos, a revisão dos procedimentos de cópia de segurança e recuperação, o cumprimento dos regulamentos de segurança e privacidade, etc (HU *et al.*, 2019). Em suma, a auditoria de sistemas desempenha um papel crucial no mundo das tecnologias

da informação. A sua origem está diretamente relacionada com o aparecimento dos primeiros computadores e com a necessidade de garantir a fiabilidade das informações que estes processam. Ao longo do tempo, a disciplina evoluiu para acompanhar a complexidade dos sistemas e a importância crescente da segurança da informação. A auditoria de sistemas desempenha um papel fundamental na proteção dos ativos e na mitigação dos riscos das organizações num ambiente cada vez mais digital (HALL, 2020).

Alguns padrões foram criados de modo a produzir uma análise de qualidade e padronizar processos de realização deste tipo de auditoria, como a ISO 9001:2000 e a 14001:2004, por exemplo. O trabalho de Bernardo *et al.* (2010), realiza um estudo empírico acerca do modo como são realizadas auditorias internas e externas de sistema. Como resultado, é demonstrado que apesar de não haver uma padrão específico definido para realização das auditorias, a maioria das organizações participantes são auditadas de modo semelhantes, atendendo inclusive a padrões como a ISO 9001:2000 e ISO 14001:2004. A figura 6 traz uma representação das atividades e recursos do processo de auditoria de modo genérico.

Figura 6 – Representação de prática de auditoria de sistemas.



Fonte: adaptado de (KARAPETROVIC; WILLBORN, 2001).

O progresso técnico sempre foi a força motriz fundamental para o desenvolvimento

da auditoria (BOTHA; BOON, 2003). A tecnologia *blockchain*, devido à suas características, tem grande impacto no processo de auditoria, sendo este impacto observado sob dois aspectos: sob o aspecto de demandas de auditoria, e sob o aspectos de metodologia e procedimentos. Do ponto de vista das demandas, avalia-se que a tecnologia *blockchain* levará a uma diminuição significativa das demandas de auditoria, ou mesmo eliminar as necessidades completamente. Outra visão desse mesmo aspecto é que auditoria não será substituída por tecnologia *blockchain*, mas se deverá ser observada do ponto de vista do desenvolvimento. Do ponto de vista de metodologia e procedimentos, a *blockchain* pode melhorar a eficiência da auditoria, reduzindo custos para um mesmo tempo de execução (WANG *et al.*, 2020).

2.4.1 Tipos de Auditoria de Sistemas

A auditoria de sistemas é uma atividade essencial para garantir a segurança, integridade e eficiência dos sistemas de informação de uma organização. Existem vários tipos de auditoria de sistemas que podem ser realizados para avaliar diferentes aspectos dos sistemas de informação. A especificidade de uma auditoria de sistema é dependente dos objetivos da organização a qual se ela se aplica. Dessa forma pode-se observar que existem diferentes tipos de auditoria de sistemas de acordo com a necessidade apresentada (ALNASSER; GRAY, 2019).

A Auditoria de Segurança é um tipo de auditoria que foca na avaliação das medidas de segurança implementadas em um sistema, como *firewalls*, controles de acesso, criptografia e políticas de segurança. O objetivo é identificar vulnerabilidades e falhas de segurança que possam comprometer a confidencialidade, integridade e disponibilidade dos dados (SILVA, 2018). Na Auditoria de Integridade o objetivo é verificar se os dados armazenados no sistema estão completos, precisos e consistentes. É realizada a análise de registros e logs para identificar possíveis inconsistências ou manipulações indevidas dos dados (SILVA, 2017). A Auditoria de Desempenho foca em avaliar a eficiência e o desempenho dos sistemas de informação. São realizadas análises de tempos de resposta, capacidade de processamento e utilização de recursos para identificar gargalos e possíveis melhorias de desempenho (BRONDANI, 2018). A Auditoria de Confiabilidade avalia os controles de segurança e a confiabilidade dos sistemas de informação, garantindo a proteção contra falhas e erros. São analisados os mecanismos de backup, redundância, tolerância a falhas e monitoramento de sistemas (FAVERA, 2018). Esses tipos de auditoria citados são voltados a um critério técnico de tecnologia de informação.

Outros tipos de auditoria de sistemas analisam critérios mais voltados à interdis-

ciplinaridade necessária para se atingir os objetivos da organização ou entidade que utiliza o sistema. A seguir temos alguns tipos que se vinculam a aspectos legais, sociais e de gerencia da organização. A Auditoria de Conformidade, por exemplo, visa avaliar se o sistema está em conformidade com leis, regulamentações e políticas internas e externas estabelecidas pela organização. Isso inclui a verificação de conformidade com padrões de segurança, privacidade de dados e governança de TI (CASTRO, 2019). Na Auditoria de Continuidade de Negócios verifica-se o preparo dos sistemas de informação para lidar com situações de falha ou desastres, garantindo a continuidade das operações de negócio. São avaliados os planos de contingência, backup de dados, procedimentos de recuperação e testes de resiliência (MORAES, 2016). A Auditoria de Privacidade foca na verificação da conformidade com as leis e regulamentações de privacidade de dados. São analisados os processos de coleta, armazenamento e tratamento de informações pessoais para garantir a proteção da privacidade dos usuários (SEGUNDO, 2018). Por fim temos a Auditoria de Acessibilidade onde são verificadas as boas práticas de acessibilidade em sistemas de informação, garantindo que pessoas com deficiência possam utilizar os sistemas de forma igualitária. São analisados critérios como legibilidade, navegabilidade, compatibilidade com tecnologias assistivas e conformidade com padrões de acessibilidade (OLIVEIRA, 2017). Esses são apenas alguns exemplos dos tipos de auditoria de sistemas que podem ser realizados. Cada tipo de auditoria possui suas próprias técnicas, metodologias e critérios de avaliação, dependendo dos objetivos específicos de cada organização e sistema em questão. É importante adaptar a abordagem de auditoria de acordo com as necessidades e particularidades de cada contexto.

2.5 E-Voting

O voto é o pilar central de uma sociedade democrática. Em uma eleição, permite que os cidadãos selecionem seus representantes para administrar a sociedade. Em um referendo, permite que os cidadãos tomem decisões críticas. O voto é considerado um dos métodos mais eficazes para os indivíduos expressarem suas opiniões sobre um determinado assunto. A votação eletrônica refere-se ao uso de computadores ou equipamentos de votação computadorizados para votar em uma eleição (CETINKAYA; CETINKAYA, 2007).

O objetivo de introduzir a computação eletrônica na votação é aumentar a eficiência da cédula tradicional em papel sem comprometer a segurança, a privacidade ou os requisitos legais existentes. A questão que vem antes de cada documento de votação eletrônica na literatura é quais são os requisitos (WANG *et al.*, 2017).Chaum foi pioneiro na noção de votação eletrônica

e então muitos protocolos foram propostos (CHAUM, 1981). O primeiro protocolo prático de votação eletrônica para eleições em grande escala é o de Fujioka *et al.* (1992). A verificabilidade foi introduzida pela primeira vez neste protocolo, no entanto, requer mais envolvimento do eleitor e a precisão pode ser violada, pois a autoridade maliciosa pode adicionar votos se algum eleitor se abster de votar na fase de contagem.

Sistemas de *e-voting* seguros têm sido estudados na literatura há mais de 30 anos desde o trabalho (CHAUM, 1981). Este tópico pode ser considerado como um dos problemas mais difíceis na literatura de segurança. Um sistema de votação eletrônica é um sistema grande e complexo que tem muitas funções, processos. Cada função do sistema não deve ser totalmente confiável. Doravante, qualquer ponto isolado de corrupção pode arruinar o sistema.

A literatura apresenta quatro categorias de *e-voting*, dependendo do nível de segurança, privacidade e confiança que mantêm; essas categorias são *e-commerce*, autoridade de confiança, verificável individualmente e verificável universalmente. No primeiro tipo não há segurança exceto possivelmente nos canais de comunicação. O enchimento de urnas é tolerado, a privacidade do eleitor não é mantida e a adulteração de votos não é impedida. É adequado para site de votação na Internet. Em sistemas de autoridade confiável, os funcionários eleitorais são confiáveis para manter a integridade da eleição, a privacidade do eleitor é mantida e a adulteração de votos é evitada nesses sistemas. Este tipo de sistema de votação é adequado para votação em pequena escala, para a qual o funcionário eleitoral pode ser confiável.

Em sistemas individualmente verificáveis que conduzem o processo de votação eletrônica é seguro, eficiente e eleições privadas são possíveis, a desvantagem deste tipo é que o votante é responsável por garantir que seu voto foi contabilizado na contagem final da eleição, esses sistemas são impraticáveis para eleições cívicas, pois nenhum observador independente pode verificar as eleições.

Na última categoria de votação pela Internet, universalmente verificável, qualquer pessoa pode verificar a eleição sem comprometer a privacidade do eleitor. A provisão deste nível de proteção é difícil. Esses sistemas só podem ser usados para eleições sim ou não devido a contradições entre os requisitos (KAHANI, 2005).

O sistema de votação eletrônica também deve envolver quatro fases: Os eleitores se registram nas autoridades de registro e a lista de eleitores qualificados é compilada antes do dia da eleição, no dia da eleição os eleitores registrados solicitam o voto ou privilégio de voto às autoridades de registro e as autoridades de registro verificam o credenciais daqueles que tentam

votar e só permitem aqueles que são elegíveis e registrados antes. O eleitor vota e, finalmente, as autoridades de contagem contam os votos e anunciam o resultado da eleição (CETINKAYA; CETINKAYA, 2007).

Governos de países já adotam sistemas de votação digital como metodologia oficial para realização de eleições. A Estónia, por exemplo, utiliza a votação eletrônica (*I-Voting System*) desde 2005 . A base deste sistema é um cartão de identificação nacional dado a todos os seus cidadãos. Esses cartões são arquivos criptografados, identificam exclusivamente o proprietário e podem ser usados para assinar documentos, serviços bancários e assim por diante (BARNES *et al.*, 2016).

No Brasil temos um sistema de votação eletrônico que é usado em larga escala desde 1996, nas eleições municipais (SILVA *et al.*, 2021). A segurança das urnas eletrônicas tem sido um tema recorrente no cenário político brasileiro. Existem questionamentos e debates sobre a segurança dessas urnas, levantando preocupações sobre a possibilidade de fraude e manipulação dos resultados eleitorais. Um dos principais questionamentos refere-se à origem e à confiabilidade do software utilizado nas urnas eletrônicas. A observação internacional tem desempenhado um papel importante na verificação da segurança das urnas eletrônicas brasileiras. Em diversas eleições, órgãos como a Organização dos Estados Americanos (OEA) e a União Europeia (UE) enviaram missões de observação para acompanhar o processo eleitoral no Brasil. Essas missões têm destacado a confiabilidade do sistema eleitoral e a transparência das eleições brasileiras. Embora existam questionamentos legítimos sobre a segurança das urnas eletrônicas, é importante considerar que o sistema eleitoral brasileiro adota diversas medidas de segurança e passa por constantes auditorias e testes (TSE, 2021b) (TSE, 2021c) (TSE, 2021a).

Levando em conta o contexto da política Brasileira e o avanços na utilização dos sistemas de votação eletrônica e e-voting em outros países, é entendida a necessidade de um estudo que observe uma solução para garantir critérios que possam melhorar estes sistemas através de uma arquitetura de auditamento. No decorrer deste trabalho temos um estudo sistemático que validade a necessidade deste estudo.

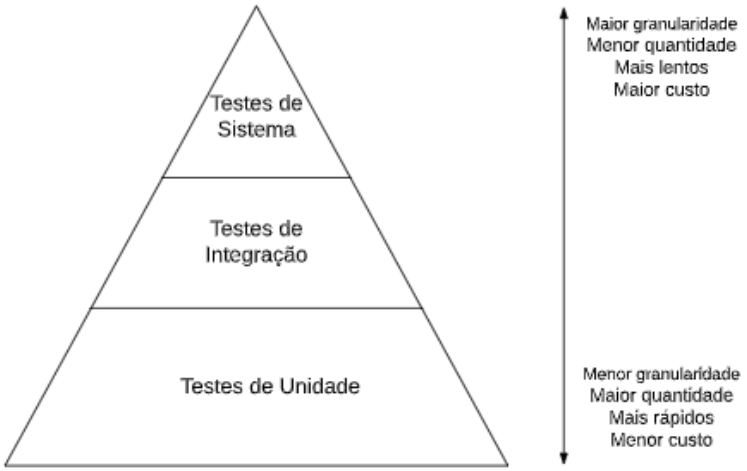
2.6 Qualidade de Software (ISO/IEC 25010)

Produtos de software e sistemas de computador têm muitas partes interessadas, e dentre elas pode-se citar: os desenvolvedores, empresas que adquirem os softwares para revenderem, empresas usuárias do software, pessoas que utilizam o software e até mesmo

pessoas que não utilizam o sistema, mas que podem ser afetadas indiretamente pelo mesmo através de empresas ou outras pessoas. Para garantir valor às partes interessadas a avaliação da confiabilidade deste software tem caráter essencial.

No desenvolvimento de softwares e aplicações, esta confiabilidade é verificada pelas atividades de teste. Mike Cohn (COHN, 2010) propôs uma pirâmide representada na figura 7. Na pirâmide, os testes são divididos em três grupos: testes de unidade, verificam automaticamente pequenas partes de um código; testes de integração, verificam uma transação ou funcionalidade completa; e testes de sistema, simulam uma sessão de uso do sistema em ambiante realístico (VALENTE, 2020). Para este trabalho, observamos o topo da pirâmide, testes de sistema, pois as características de testes de sistema podem ser associadas às características de qualidade definidas pela ISO/IEC 25010 (ISO/IEC, 2011). A qualidade pode ser mensurada e alcançada a partir da sua associação com as metas e objetivos das partes interessadas.

Figura 7 – Pirâmide de testes.

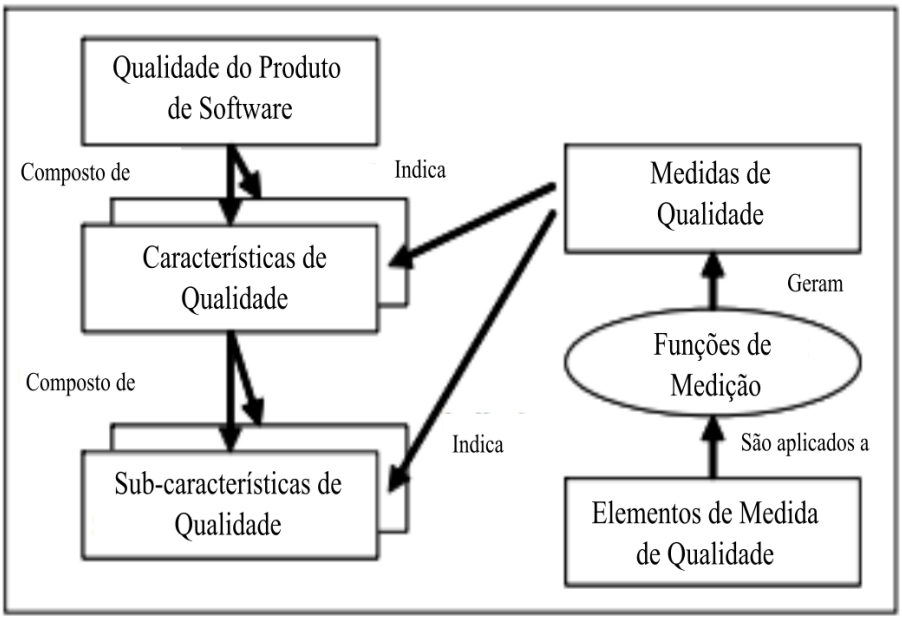


Fonte: (VALENTE, 2020).

As normas estabelecidas na ISO/IEC 25010 descrevem como o software se relaciona com os dados e o impacto que esta relação causa às partes interessadas. Ela surgiu em 2011 com um conjunto de outras normas, derivados da ISO/IEC 9126. Esta norma parte da definição das características do software e estabelece modelos de usuários, e, conforme a necessidade destes usuários, modelos de qualidade específicos. Os modelos de qualidade se dividem em três: modelo de qualidade de produto, modelo de qualidade de dados e modelo de qualidade em uso. Os modelos de qualidade de produto e modelo de qualidade em uso funcionam como uma espécie de lista de verificação para garantir um tratamento abrangente dos requisitos de qualidade e prover uma base para estimar o esforço e atividades consequentes que serão necessários durante

o desenvolvimento dos sistemas. Outras normas, como a ISO/IEC 2502n e a ISO/IEC 15939, apresentam medidas e modelos de medição para serem aplicadas às propriedades de qualidade. A figura 8 exibe a relação entre o modelo de qualidade, as medidas de qualidade e o modelo de medição.

Figura 8 – Modelo de referência de medição de qualidade de produto de software baseado na ISO/IEC 25010:2011



Fonte: (ISO/IEC, 2011).

Neste trabalho apenas o modelo de qualidade de produtos é considerado para avaliação da performance do Hyperledger Fabric. Uma sub-característica do modelo de qualidade do produto é a eficiência de performance, onde são observadas três métricas: comportamento no tempo, grau em que os tempos de resposta e processamento de um sistema atendem aos requisitos; utilização de recursos, grau em que as quantidades e tipos de recursos utilizados por um sistema atendem aos requisitos; e capacidade, grau em que os limites máximos de um produto ou parâmetro do sistema atendem aos requisitos, estes podem incluir o número de itens armazenados, de usuários simultâneos,largura de banda de comunicação, *throughput* de transações e tamanho do banco de dados.

No próximo capítulo são apresentados os trabalhos relacionados decorrentes da revisão sistemática da literatura.

3 TRABALHOS RELACIONADOS

Neste capítulo são apresentados trabalhos que se relacionam diretamente com o tema da pesquisa, relacionando o processo de auditoria à tecnologia *blockchain* do ponto de vista dos sistemas de *e-voting*. O objetivo é dar uma ideia geral sobre o estado da arte. Nesta seção trataremos dos trabalhos que se relacionam diretamente com a pesquisa desenvolvida, estando dessa forma dentro do escopo do estudo das arquiteturas *blockchain* aplicáveis à sistemas de *e-voting*. A fim de captar as informações necessárias foi realizado um mapeamento sistemático da literatura, conforme descrito na metodologia, o resultado se encontra na seção a seguir.

3.1 Revisão Sistemática

Na realização da revisão sistemática de sistemas de *e-voting* com foco em auditoria utilizando a tecnologia *blockchain* é um processo estruturado que envolve diversos passos para coletar, analisar e sintetizar evidências relevantes de estudos existentes. Essa abordagem visa identificar os sistemas de *e-voting* que utilizam a tecnologia *blockchain* para melhorar a auditoria destes sistemas, como foco na observação das arquiteturas descritas. O primeiro passo é formular uma pergunta de pesquisa clara e específica que oriente a revisão. Essa pergunta deve estar alinhada com o objetivo da revisão e direcionar a busca por estudos relevantes. Em seguida, é necessário estabelecer critérios de inclusão e exclusão para selecionar os estudos que serão analisados. Esses critérios podem envolver conferências ou periódicos específicos, períodos de tempo, foco nos sistemas de *e-voting* com tecnologia *blockchain* e auditoria, entre outros. Com os critérios definidos, realiza-se uma busca sistemática em bases de dados acadêmicas, como IEEE Xplore, ACM Digital Library, etc. Utilizando termos de pesquisa relevantes, são obtidos os resultados que serão avaliados em relação aos critérios estabelecidos. Após selecionar os estudos relevantes, realiza-se a extração de dados. Isso envolve criar um formulário ou planilha para registrar informações importantes de cada estudo, como autor, título, ano de publicação, objetivo, metodologia, sistema de *e-voting* analisado, características do sistema *blockchain* utilizado e resultados relacionados à auditoria (BOOTH *et al.*, 2016) (EGGER *et al.*, 2008) (HIGGINS; GREEN, 2019).

A realização deste mapeamento sistemático da literatura é dividida em três etapas: planejamento, condução e extração de dados. O planejamento é descrito nas subseções Objetivos, Questões de Pesquisa, *string* de Busca, Critérios de Inclusão, Critérios de Exclusão e Critérios

de Qualidade. O processo de condução é descrito na última subseção, Condução de Revisão, enquanto a etapa de extração de dados é refletida na seção Resultados. Para realização deste trabalho uma ferramenta importante foi o Parsifal (2022), é uma ferramenta online desenvolvida para apoiar pesquisadores na realização de revisões sistemáticas da literatura no contexto da Engenharia de Software. Pesquisadores distribuídos geograficamente podem trabalhar juntos em um espaço de trabalho compartilhado, projetando o protocolo e conduzindo a pesquisa. A ferramenta baseia-se no trabalho de Kitchenham e Charters (2007) para ditar os passos a serem desenvolvidos na revisão sistemática.

O principal objetivo desta revisão é identificar na literatura trabalhos que tratem de arquiteturas utilizando a tecnologia *blockchain* em sistemas de *e-voting* e definir quais os pontos mais relevantes pára fins de auditoria nesses trabalhos. Definir qual o tipo de arquitetura mais utilizado para auditoria de sistemas de votação utilizando a tecnologia *blockchain*. Identificar o ganho de utilização das arquiteturas com *blockchain* em relação às tradicionais. Atingir este objetivo que é mais geral, será crucial para desenvolvimento de uma perspectiva atual e positiva relacionada ao escopo da pesquisa.

É importante levantar que para atingir este objetivo geral, objetivos mais específicos, relacionados com os passos da revisão, são definidos de modo natural. Um dos primeiros é a definição do escopo da busca. Foi designada uma população de aplicações, serviços ou sistemas de *e-voting*, observando sua existência e suas características. Deve-se considerar o critério de intervenção que é o fato de, necessariamente, estes sistemas utilizarem a tecnologia *blockchain* de alguma forma. Os fatores de comparação destes trabalhos são suas arquiteturas e características, e o contexto a ser observado é o do ambiente acadêmico, corporativo e/ou público governamental, preferencialmente. Responder todas as perguntas de pesquisa de modo claro e conciso também é um desta revisão, bem como definir os melhores trabalhos através dos filtros estabelecidos em todos os critérios do estudo.

3.1.1 Questões de Pesquisa

A fim de nortear o estudo foram desenvolvidas algumas perguntas de pesquisa, dessa forma, a partir das mesmas, pode-se desenvolver o contexto onde se encaixa o estudo em relação ao estado da arte atual. As perguntas vão de um contexto mais geral até algo mais específico com foco nas características das soluções e principalmente nas arquiteturas.

A primeira pergunta de pesquisa geralmente é feita em todas revisão sistemática

da literatura, "Qual o estado da arte de arquiteturas de *blockchain* aplicadas à sistemas de *e-voting* para fins de auditoria?". Pode-se dizer que responder esta pergunta é algo que se realiza naturalmente a partir das respostas às outras perguntas de pesquisa. Em seguida levantam-se questionamentos mais específicos, os quais requerem uma análise mais minuciosa de cada trabalho. A segunda e a terceira perguntas visam esclarecer qual o benefício da utilização da tecnologia *blockchain* em detrimento das tecnologias de bancos de dados tradicionalmente utilizadas: "Em sistemas de votação quais as diferenças entre arquitetura com *blockchain* e arquitetura tradicional, segundo relatado nos trabalhos?", "Quais as maiores vantagens de utilização da tecnologia *blockchain* nas arquiteturas, conforme relatado nos trabalhos?". A quarta e a quinta pergunta levantam questões relativas às plataformas de desenvolvimento de *blockchain*, considerando que cada plataforma tem características específicas foi questionado "Quais as plataformas mais utilizadas para testes das arquiteturas?"e "Em trabalhos comparativos, utilizando arquiteturas de sistemas de *e-voting* com a tecnologia *blockchain* para fins de auditoria, quais plataformas de *blockchain* apresentam melhor desempenho?". Considerando que a ideia deste estudo é proporcionar uma perspetiva de uso real destas soluções, levanta-se uma questão de pesquisa importante tanto no mundo corporativo como nas instituições públicas e governos, "Existem estudos que tratem o custo de utilização da tecnologia *blockchain* em sistemas de *e-voting*? Se sim, qual o impacto deste custo para estes estudos?".

Por fim, considerando que este trabalho é parte de um ideia de pesquisa e desenvolvimento colaborativa, que visa dar perspectiva suficiente para produção de uma solução que possa, também, ser utilizada em um ambiente governamental, mesmo que em pequena escala, foi questionado "de que modo sistemas de *e-voting* utilizando a tecnologia *blockchain* impactam governos e/ou instituições governamentais?". A ultima pergunta de pesquisa não foca exatamente no escopo das característica de arquitetura *blockchain* para os sistemas, no entanto tem relevância acadêmica, visto que sistemas de *e-voting* de um modo geral estão sendo comumente utilizados por governos e instituições governamentais.

3.1.2 String de Busca

A definição da *string* de busca foi um trabalho minucioso,com base na definição de repositórios acadêmicos com reconhecimento internacional na área da Tecnologia da Informação. Foram cinco repositórios no total: "ACM Digital Library (http://portal.acm.org)", "IEEE Digital Library (http://ieeexplore.iel Library (https://onlinelibrary.wiley.com)". Em primeiro momento

foi realizada uma busca utilizando a *string* de busca *"Blockchain AND e-voting AND Audit"*, no entanto o resultado das buscas nas bases de dados foi insatisfatório, gerando uma quantidade mínima de trabalhos. O segundo passo foi aumentar escopo da busca, retirou-se da *string* a palavra *"Audit"*, resultando em um total de 4648 trabalhos. Após análise dos trabalhos obtidos através da segunda *string* de busca, ficou claro que uma quantidade considerável destes trabalhos apenas mencionava os termos da busca, ou então tratava os temas de maneira independente, ou até mesmo eram trabalhos meramente informativos que não aprofundavam suficiente nos temas a fim de que se pudesse obter as características e informações requeridas neste estudo. Dessa forma definiu-se uma terceira *string* de busca e esta foi utilizada neste estudo.

A *string* de busca definida, a qual proporcionou os trabalhos que passaram pelos critérios da revisão sistemática da literatura, foi *"Allintitle: Blockchain AND e-voting"*. O termo *"Allintitle"* no início da *string* faz com que a busca realizada capture apenas trabalhos onde os termos da busca, neste caso *"Blockchain AND e-voting"*, constem no seus referidos títulos. Considera-se que se o termo está no título, ele é tema do estudo, dessa forma não corre-se o risco de buscar trabalhos que apenas mencionem os termos. Outro fator proporcionado por esta definição da *string* é o fato de que obrigatoriamente, os trabalhos vão ter os dois termos da busca como tema do estudo, e esta relação favorece o estudo aqui proposto. No total foram 79 trabalhos, considerando os 5 repositórios, no *"IEEE Digital Library"* estão hospedados 40 trabalhos, pouco mais da metade dos trabalhos. Os trabalhos passaram pelos critérios de inclusão, exclusão e qualidade que são descritos nas próximas subseções.

3.1.3 Critérios de Inclusão

Os critérios de inclusão em uma revisão sistemática da literatura são, basicamente, motivos pré-estabelecidos para que o trabalho seja incluído na pesquisa. Neste trabalho foram definidos critérios a fim de garantir que os trabalhos possuam conteúdo associado ao escopo da pesquisa. São três critérios para inclusão de um trabalho no estudo, onde o mesmo, para ser aceito, deve encaixar-se em um ou mais dos três critérios. São os seguintes: "o trabalho deve apresentar a arquitetura proposta e/ou utilizada na solução", "o trabalho deve apresentar aplicação, serviço ou sistema com aplicabilidade em sistemas de *e-voting* do ponto de vista de auditoria", "o trabalho deve apresentar aplicação, serviço ou sistema que utilize a tecnologia *blockchain*". Trabalhos que se encaixem nos três critérios serão avaliados de modo mais minucioso. Importante destacar que os trabalhos não podem atender a critérios de exclusão, pois mesmo que comportem os três

critérios de inclusão são rejeitados. Dos critérios de exclusão trataremos a seguir.

3.1.4 Critérios de Exclusão

Os critérios de exclusão são critérios de caráter mais prático. Visam eliminar trabalhos que, apesar de tratar do tema, são superficiais ou não têm conteúdo suficiente para ser tidos como relevantes ao estudo. São 5 os critérios de exclusão: "o trabalho possui os termos apenas no título ou resumo", "o trabalho apenas cita os termos da pesquisa, mas não se aprofunda no tema", "o trabalho está escrito em idioma diferente do inglês", "o trabalho possui até quatro páginas", "o trabalho é meramente informativo".

O critério "o trabalho apenas cita os termos da pesquisa, mas não se aprofunda no tema", foi definido após percebe-se que muitos trabalhos não acrescentavam conteúdo do ponto de vista desta pesquisa. Sendo *blockchain* uma tecnologia emergente, muitos dos trabalhos citavam sua capacidade, ou traziam ideia de como trabalhar a tecnologia, da perspectiva de sistemas de *e-voting*, no entanto não traziam soluções bem definidas. Assim foi definido também o critério "o trabalho é meramente informativo", para revistas de tecnologia e outros periódicos informativos, mas que não tem caráter de apresentação de solução. Os outros critérios atendem a necessidades mais práticas como o fato de em 4 páginas não ser o suficiente para apresentar uma solução complexa de arquitetura, ou o fato de estar em idioma diferente do inglês que é conhecidamente a língua padrão para trabalhos na área de tecnologia da informação.

Reitera-se que mesmo atendendo a um ou mais critérios de inclusão, basta que o trabalho atenda a um critério de exclusão e é definido como rejeitado pelo estudo. O próximo passo é tratar os trabalhos aceitos do ponto de vista de qualidade.

3.1.5 Critérios de Qualidade

Dos trabalhos aceitos, são inseridos na condução desta pesquisa apenas os trabalhos que passem pelo crivo da qualidade. Foram definidas perguntas específicas, que levam ao entendimento do trabalho em questão e realiza um ajuste para que apenas trabalhos diretamente relacionados à pesquisa e que atendam às necessidades da mesma se insiram na lista dos trabalhos relacionados. São realizadas oito perguntas, definidas e respondidas pelos autores com base em cada artigo aceito através dos critérios de inclusão e exclusão. São as seguintes:

1. A motivação do estudo está bem embasada?
2. A motivação do estudo está bem justificada?

3. Do ponto de vista de metodologia o trabalho está bem organizado/estruturado?
4. A arquitetura proposta e/ou utilizada no trabalho é apresentada de modo claro e detalhado?
5. Existe um esboço gráfico ou imagem da arquitetura proposta ou utilizada?
6. O trabalho proposto foi testado em ambiente realístico?
7. O trabalho proposto já apresenta um modelo específico *e-voting* que contenha auditoria?
8. O trabalho proposto se relaciona, foi baseado ou foi utilizado por algum governo ou órgão governamental?

As perguntas 1, 2 e 3 atendem especificamente a critérios de metodologia científica, considerando que trabalhos bem motivados, justificados e organizados tendem a apresentar a solução de maneira clara e sem favorecer dubiedades de entendimento acerca da proposta. As perguntas 4, 5 e 6 focam no objetivo principal do estudo, que é o entendimento acerca das arquiteturas do tipo de solução pesquisada. A pergunta 7 é feita a fim de vislumbrar se já existem na literatura estudos no escopo do que se busca realizar a partir desta revisão sistemática. Por fim, considerando o escopo de onde se desenvolve a necessidade desta pesquisa, que é o ambiente *e-voting*, foi decidido como importante entender se governos ou órgãos governamentais utilizam as soluções observadas no estudo, por isso faz-se a pergunta 8. Foi definida uma pontuação para cada resposta positiva (1 ponto), trabalhos que atingem a pontuação superior a 5 pontos passam pelo crivo da qualidade, levando em conta que a pontuação máxima é 8 pontos.

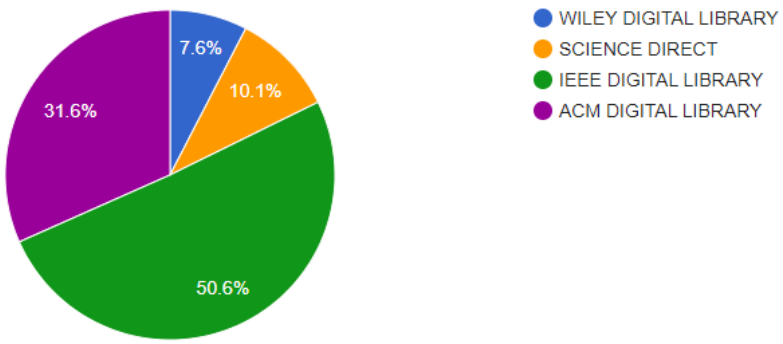
3.1.6 Condução

A pesquisa foi conduzida a partir da definição da *string* de busca, como já relatado, partindo de um total de 79 trabalhos analisados. Após passar por todos os critérios de inclusão, exclusão e qualidade, é determinado que 20 trabalhos devem ser minuciosamente analisados, realizando inclusive a extração dos dados coerentes com a pesquisa aqui realizada. O repositório com a maior quantidade de trabalhos aproveitados na pesquisa foi "IEEE Digital Library"[1]. Seguido por "ACM Digital Library"[2], "Science Direct"[3] e "Wiley Digital Library"[4] respectivamente. O repositório "Springer Link"[5] não apresentou trabalhos compatíveis com a condução desta pesquisa.

Além das perguntas realizadas na tabelas comparativas, outras características dos

[1] http://ieeexplore.ieee.org
[2] http://portal.acm.org
[3] http://www.sciencedirect.com
[4] https://onlinelibrary.wiley.com
[5] http://link.springer.com

Figura 9 – Percentual de estudos aceitos por fontes de pesquisa.



Fonte: (PARSIFAL, 2022).

trabalhos observados na revisão foram observadas. Dentro do escopo do objetivo, um dos critérios observados é o ambiente é que se insere a utilização do sistema de *e-voting*, dando preferência a trabalhos que se insiram no ambiente acadêmico, corporativo e/ou público governamental. Importante destacar que dentre os 20 trabalhos observados após o filtro dos critérios de inclusão, exclusão e qualidade, apenas o trabalho de Goyal e Kumar (2021) se insere no contexto público governamental. É possível verificar que propostas relevantes estão inseridas no ambiente acadêmico como por exemplo o trabalho de Watanavisit e Vorakulpipat (2020). Este primeira percepção já responde a última pergunta de pesquisa "De que modo sistemas de *e-voting* utilizando a tecnologia *blockchain* impactam governos e/ou instituições governamentais?". Aparentemente, apesar de soluções serem utilizadas por governos, do ponto de vista acadêmico o impacto é pequeno, devido ao baixo número de trabalhos aplicados especificamente à este tipo de ambiente.

Na verdade, de um modo geral esta percepção pode ser levada a responder também à primeira pergunta de pesquisa "Qual o estado da arte de arquiteturas de *blockchain* aplicadas a sistemas de *e-voting* para fins de auditoria?". A mesma carência de trabalhos se aplica ao escopo específico de auditoria para os sistemas de *e-voting*. As arquiteturas de *blockchain* para este tipo de sistema, apesar de possuírem características de auditabilidade, não tratam especificamente disto como uma parte específica do sistema, levantando apenas como uma característica da tecnologia. Observa-se que dentro do escopo de auditoria para estes sistemas, não foi possível verificar trabalhos que realizassem testes comparando as plataformas de *blockchain*. Os trabalhos que realizam testes de desempenho, o fazem para validação da solução,, não realizando comparação entre plataformas. Para os principais trabalhos relacionados as maiores vantagens

da utilização de *blockchain* em suas arquiteturas estão ligadas à imutabilidade dos dados e à distribuição dos registros na rede, excluindo a necessidade de um banco de dados centralizado para armazenamento de algumas informações sensíveis.

Na coleta de dados da pesquisa foi possível verificar que existe uma dificuldade de teste das soluções em ambientes reais. Dentre os trabalhos apenas três puderam ser testados dessa forma. Parte dos trabalhos foi implementado utilizando simuladores para simular ambientes realísticos, mas não foram usados em ambiente real. O trabalho de Killer *et al.* (2020), por exemplo, tem todo o aparato para uso em ambiente real, no entanto não o faz. Todavia é possível perceber que tanto em ambiente real, quanto em simulações a plataforma Buterin (2022) é a mais utilizada para implementação e teste dos sistemas. Outra verificação não realizada na literatura dentro do escopo de sistemas de *e-voting* auditáveis é o de custo de uso dessas soluções. Isto surpreende, pois a plataforma Ethereum oferece fácil acesso a este tipo de informação, sendo a mais utilizada esperava-se encontrar estudos neste contexto. É possível verificar que em sistemas de *e-voting* utilizando a tecnologia *blockchain* há pouca inovação em relação à criação de novas arquiteturas. O que foi possível observar é que a maior parte dos trabalhos utiliza arquiteturas pré-existentes, apenas inserindo a tecnologia *blockchain* no contexto de armazenamento de alguns dados, normalmente os dados mais sensíveis. Considerando o tipo de sistema, espera-se que os dados tratados sejam do tipos sensível, uma vez que podem ser informações pessoais dos eleitores e candidatos, bem como o próprio voto. O comportamento se confirma para a maior parte dos trabalhos. Um total de 75% dos trabalhos observados no estudo tratam de dados sensíveis.

3.2 Resultados da Revisão Sistemática

Como resultado da revisão sistemática, espera-se identificar na literatura trabalhos que tratem de arquiteturas utilizando a tecnologia *blockchain* em sistemas de auditoria de votação, como já levantado nos objetivos. No entanto a coleta de dados permite que outras conclusões possam ser tiradas, além das esperadas. Nesta seção busca-se demonstrar as informações pertinentes ao trabalho obtidas na extração de dados, para que possam ser posteriormente discutidas. Ou seja, aqui são apresentados os trabalhos relacionados propriamente ditos.

Algumas informações específicas de cada trabalho são definidas para fins de alinhamento entre os trabalhos, de modo a observá-los de maneira uniforme. São o título do trabalho, o objetivo e o resumo da metodologia; além disso são levantados alguns questionamentos para

fins de mapeamento. As perguntas são objetivas:

1. O trabalho propõe um novo tipo de arquitetura?
2. A arquitetura proposta e/ou utilizada foi aplicada em ambiente real?
3. A arquitetura proposta e/ou utilizada trata de dados sensíveis?
4. Quais os tipos de informações armazenadas na *blockchain*?
5. Uma aplicação, aplicativo ou site foi construída com base na proposta?
6. A solução proposta interage diretamente com o usuário?
7. Quais os tipos de usuários?
8. Quem são os *stakeholders*?
9. Qual o público alvo do trabalho?
10. Se existem clientes específicos, de que tipo seriam?

Acredita-se que com essas perguntas, possa-se vislumbrar a aplicação das soluções estudadas nesta pesquisa de ponto de vista amplo, alcançando inclusive o entendimento do uso no meio corporativo e governamental, se houver.

Para fins de melhor observação dos questionamentos e respostas, dividiu-se os questionamentos objetivos, cujas as respostas são "Sim"ou "Não", em duas tabelas, analisando diferentes aspectos dos trabalhos.

A tabela 1 faz uma comparação dos trabalhos observando as respostas para as perguntas 1 e 5. A ideia desta comparação é visualizar o caráter inovativo do trabalho estudado, verificando se houve a criação de uma nova aplicação e de um novo modelo de arquitetura.

Tabela 1 – Comparação dos trabalhos observando as respostas para as perguntas 6, 2 e 3 da etapa de extração de dados.

Trabalho	**Uma aplicação, aplicativo ou site foi construída com base na proposta?**	**Propõe novo tipo de arquitetura?**
(KHAN *et al.*, 2020)	Não	Não
(KHAN *et al.*, 2021)	Não	Não
(DHULAVVAGOL *et al.*, 2020)	Não	Sim
(GUPTA *et al.*, 2021)	Não	Sim
(KILLER *et al.*, 2020)	Não	Sim
(HOSSAIN *et al.*, 2019)	Não	Não
(WATANAVISIT; VORAKULPIPAT, 2020)	Sim	Sim
(GOYAL; KUMAR, 2021)	Sim	Sim
(GAO *et al.*, 2019)	Não	Não
(CADIZ *et al.*, 2021)	Sim	Não
(QU *et al.*, 2020)	Não	Não
(AL-MADANI *et al.*, 2020)	Sim	Não
(SUYITNO *et al.*, 2020)	Não	Não
(ALVI *et al.*, 2020)	Não	Sim
(ABUIDRIS *et al.*, 2021)	Não	Não
(ROSASOORIA *et al.*, 2020)	Sim	Sim
(PRAMULIA; ANGGOROJATI, 2020)	Sim	Sim
(CHEEMA *et al.*, 2020)	Não	Sim
(RATHEE *et al.*, 2021)	Não	Não
(LI *et al.*, 2020a)	Não	Não
(SENGUPTA *et al.*, 2021)	Não	Sim
(NIWA; MENDES, 2019)	Sim	Sim

Fonte: Produzido pelo autor.

Uma conclusão que pode ser tirada rapidamente da observação desta tabela é que apenas quatro trabalhos propõem uma aplicação, aplicativo ou site ao mesmo tempo que propõe um novo tipo de arquitetura. Ou seja, apenas estes quatro trabalhos atendem a um critério completo de inovação, tendo em vista que os outros 16 trabalhos observados não propõem novo tipo de arquitetura ou não propõem nenhum tipo de sistema, ou até mesmo ambas as opções. Os quatro trabalhos citados devem ser tratados de maneira mais minuciosa ainda nesta subseção, são os seguintes: *"Learning Citizenship in Practice with SchoolVote System: A Participatory Innovation of Blockchain e-Voting System for Schools in Thailand"* Watanavisit e Vorakulpipat (2020), *"Sustainable E-Infrastructure for Blockchain-Based Voting System"* Goyal e Kumar (2021), *"E-voting on blockchain using solidity language"* Rosasooria *et al.* (2020) e *"Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask"* Pramulia e Anggorojati (2020).

A tabela 2 faz uma comparação dos trabalhos observando as respostas para as perguntas 5 e 6. Aqui a comparação traz uma caráter focado na usabilidade da solução. É observado a interação da solução com usuário, a sua usabilidade em ambiente real e se os dados tratados são do tipo sensível.

Aqui as primeira conclusões mostram que dos cinte trabalhos selecionados apenas cinco não tratam de dados sensíveis, isto leva a crer que para este tipo de solução de *blockchain* aplicadas à sistemas de *e-voting* em sua maioria os dados são vistos como sensíveis. Observando os trabalhos pode-se reiterar esta afirmação, visto que os dados pessoais de usuários e escolhas de votos são pode definição dados sensíveis, salvo exceções.

Outro fato que chama a atenção é a pouca validação destes trabalhos em ambientes reais. Em apenas três dos vinte trabalhos, as soluções são testadas em ambiente real. Dessa forma, mesmo tendo a maioria das soluções capacidade de interação direta com o usuário, na maior parte dos trabalhos observados isto não é feito. Alguns trabalhos se destacam, pois atendem a todos os critérios de comparação, ou seja, respondem positivamente a todas as perguntas realizadas nas duas tabelas comparativas.

São definidos como principais trabalhos relacionados, os que respondem positivamente a todos os questionamentos das tabelas comparativas.

O trabalho de Watanavisit e Vorakulpipat (2020) apresenta o *"SchoolVote"* que é um sistema de *e-voting* utilizando *blockchain* para escolas na Tailândia. O trabalho propõe um novo de modelo de arquitetura e a partir dele constrói uma aplicação funcional, que interage

Tabela 2 – Comparação dos trabalhos observando as respostas para as perguntas 5 e 1 da etapa de extração de dados.

Trabalho	A solução proposta interage diretamente com o usuário?	Foi utilizada em ambiente real?	Trata de dados sensíveis?
(KHAN *et al.*, 2020)	Sim	Não	Sim
(KHAN *et al.*, 2021)	Não	Não	Sim
(DHULAVVAGOL *et al.*, 2020)	Sim	Não	Não
(GUPTA *et al.*, 2021)	Sim	Não	Sim
(KILLER *et al.*, 2020)	Sim	Não	Sim
(HOSSAIN *et al.*, 2019)	Sim	Não	Não
(WATANAVISIT; VORAKULPIPAT, 2020)	Sim	Sim	Sim
(GOYAL; KUMAR, 2021)	Sim	Sim	Sim
(GAO *et al.*, 2019)	Não	Não	Não
(CADIZ *et al.*, 2021)	Sim	Não	Sim
(QU *et al.*, 2020)	Não	Não	Não
(AL-MADANI *et al.*, 2020)	Sim	Não	Não
(SUYITNO *et al.*, 2020)	Não	Não	Sim
(ALVI *et al.*, 2020)	Não	Não	Sim
(ABUIDRIS *et al.*, 2021)	Não	Não	Sim
(ROSASOORIA *et al.*, 2020)	Sim	Não	Sim
(PRAMULIA; ANGGOROJATI, 2020)	Sim	Sim	Sim
(CHEEMA *et al.*, 2020)	Não	Não	Sim
(RATHEE *et al.*, 2021)	Não	Não	Sim
(LI *et al.*, 2020a)	Não	Não	Sim
(SENGUPTA *et al.*, 2021)	Não	Não	Não
(NIWA; MENDES, 2019)	Sim	Sim	Sim

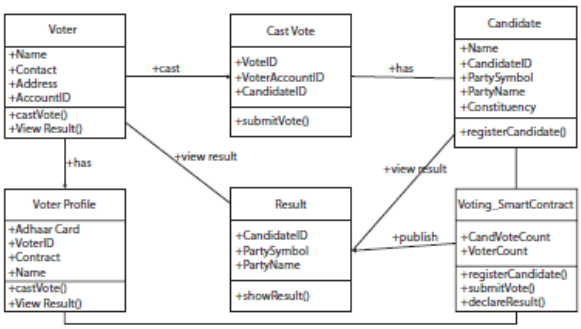
Fonte: Produzido pelo autor.

diretamente com o usuário, foi utilizado em ambiente real e trata de dados sensíveis. Da perspectiva desta revisão, este tipo de trabalho tem grande importância. As características proporcionadas pela tecnologia *blockchain*, como um armazenamento de dados não centralizado que não exija um host ou data center central para armazenar dados, ao passo que possui registros imutáveis é um dos pontos relevantes para fins de auditoria. Observando a metodologia de desenvolvimento da solução proposta no trabalho, pontos relevantes à produção de trabalhos futuros podem ser considerados, como os cinco estágios estabelecidos parta inovação: design, desenvolvimento, validação e teste, implementação e dimensionamento, e por fim avaliação. Esta revisão é o primeiro passo para desenvolvimento de um solução de auditoria para sistemas de *e-voting*, dessa forma, o trabalho de Watanavisit e Vorakulpipat (2020) relaciona-se diretamente com os objetivos desta revisão.

O trabalho de Goyal e Kumar (2021) também tem respostas positivas a todos os questionamentos das tabelas comparativas. Este trabalho é detalhado em relação à sua implementação e casos de uso. Dentre as características da solução que são proveniente do uso de *blockchain* que são relevantes para fins de auditoria estão: exatidão, não é possível que um voto seja alterado, eliminado por qualquer pessoa que não seja o eleitor; privacidade, cada voto é convertido em um hash para privacidade principal; disponibilidade, toda enquete tem um limite de tempo, e qualquer eleitor pode votar dentro do limite. Interessante observar que foi criada uma aplicação web que interage diretamente com usuário, um dos principais ganhos deste trabalho é a descrição das classes na figura 10 e a descrição casos de uso do eleitor para a aplicação na figura 11.

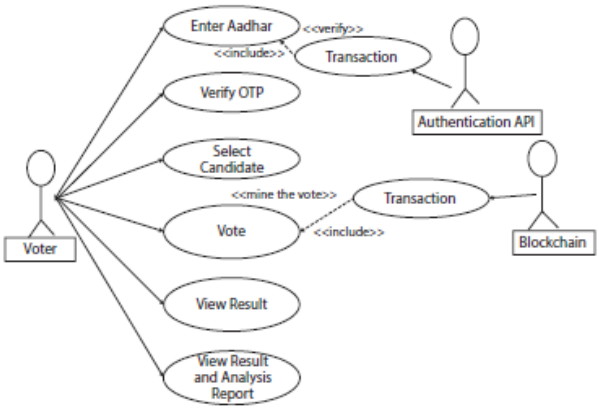
No trabalho de Pramulia e Anggorojati (2020) o ator mais importante é o gerenciador

Figura 10 – Diagrama de classes para sistema de *e-voting*.



Fonte: (GOYAL; KUMAR, 2021).

Figura 11 – Diagrama de caso de uso do eleitor.



Fonte: (GOYAL; KUMAR, 2021).

de cédulas. É responsável por implantar o contrato inteligente na rede *blockchain*, criar proposta de votação, adicionar eleitores, iniciar a votação e encerrar o processo de votação. Para poder realizar todas essas tarefas na rede *blockchain*, um gerenciador de cédulas precisa ter uma conta *blockchain* válida, por exemplo, conta Ethereum neste caso. Apesar de seu nome, ele não armazena informações sobre cédula para satisfazer o princípio do voto secreto na votação. Apenas o nome e o endereço do eleitor são armazenados na rede *blockchain* por meio de contrato inteligente, enquanto as informações de voto são implementadas como modificadores privados. Todo o histórico de transações que envolve o contrato inteligente utilizado neste trabalho pode ser rastreado pesquisando o endereço do contrato. O histórico de transações que envolve o gestor da cédula e qualquer eleitor pode ser rastreado da mesma forma. Esta última característica é a mais relevante do ponto de vista de auditoria. O trabalho também traz uma descrição gráfica da arquitetura de alto nível e do diagrama de fluxo do sistema de *e-voting* proposto como pode-se ver na figura 12

No trabalho de Sengupta *et al.* (2021) é apresentado um framework chamado Pro-Block para a detecção eficiente, segura e confiável de notícias falsas. O modelo ProBlock

implementa um sistema de votação ponderada, calculando uma pontuação com base na interpretação dos especialistas sobre a falsidade de uma notícia. A pontuação dos especialistas é avaliada usando uma abordagem de pontuação dinâmica, levando em consideração estatísticas de carreira e confiança na avaliação de cada especialista. A probabilidade de uma notícia ser genuína é calculada usando o modelo ProBit, e as notícias falsas são removidas do blockchain com base nas avaliações.

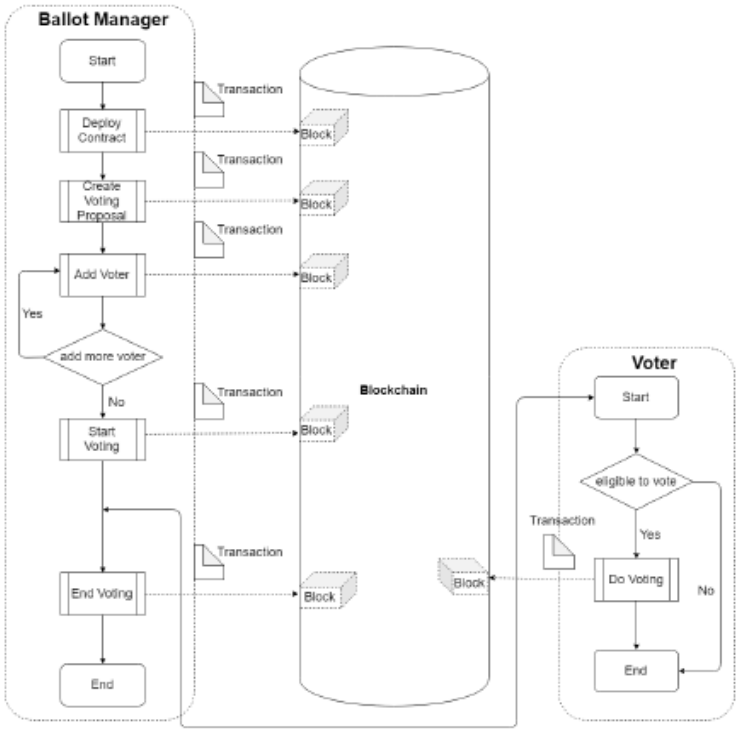
O trabalho de Niwa e Mendes (2019) é o que mais se relaciona com o trabalho aqui proposto. O autor destaca o sistema de voto eletrônico no Brasil, baseado em urnas eletrônicas, apontando suas características, como a necessidade de segurança nas unidades de memória das máquinas para evitar modificações maliciosas. Propõe um sistema de voto eletrônico seguro, eficiente, descentralizado e totalmente auditável, utilizando a tecnologia *blockchain*. A eficiência do trabalho está na velocidade de execução e apuração dos votos, bem como na capacidade de realizar auditorias em tempo real. O sistema proposto é descentralizado, permitindo que órgãos auditores acompanhem os resultados em tempo real, independentemente de sua localização. Observando as perguntas de pesquisa contidas na tabelas acima, este trabalho possui resposta positiva para todas as perguntas. Utilizando a ferramenta GoLedger, algumas etapas da orquestração e implementação da rede blockchain no Hyperledger Fabric são facilitadas. O trabalho aqui proposto tem um enfoque na auditabilidade que o trabalho de **??**) não possui, sendo este o principal diferencial. Além disso a análise de desempenho aqui realizada, a simplicidade e o baixo custo de implementação, permitem uma visão geral acerca do Hyperledger que diferenciam os dois trabalhos.

Durante as pesquisas de trabalho relacionados também foram analisados alguns trabalhos que tem características semelhantes às que são propostas neste trabalho. Dois trabalhos principais se destacam, não são relacionados nas tabelas, pois não utilizam a tecnologia *blockchain*.

O trabalho de Adida (2008) propõe uma nova arquitetura para sistemas de votação, especificamente voltada para votação online e eletrônica. A proposta do *Helios* é inovadora porque visa garantir a segurança, transparência e verificabilidade dos processos eleitorais, mesmo quando realizados de forma digital, algo que não era comum à época de seu lançamento. É possível encontrar na literatura diversos trabalhos que avaliam especificamente o desempenho deste sistema e suas características.

O trabalho Benaloh *et al.* (2012) visa abordar várias preocupações relacionadas à

Figura 12 – Arquitetura de alto nível e do diagrama de fluxo do sistema de *e-voting*.



Fonte: (PRAMULIA; ANGGOROJATI, 2020).

segurança, transparência, auditabilidade e confiabilidade dos sistemas de votação eletrônica. O *STAR-Vote* prioriza medidas de segurança para garantir a integridade e confidencialidade dos votos, além disso incorpora recursos que possibilitam uma auditoria abrangente de todo o processo de votação, desde o registro dos eleitores até a votação e contagem dos votos. Esse sistema integra um rastro em papel ou registro físico de cada voto, permitindo verificação manual e recontagem se necessário, oferecendo também uma forma de verificar eletronicamente os resultados com as cédulas físicas, adicionando uma camada adicional de garantia.

3.3 Comparação Entre os Trabalhos

Nesta seção são destacados os pontos em que o modelo de arquitetura proposto se difere dos principais trabalhos relacionados. São levantadas características importantes para o sistema do ponto de vista de auditoria e realizada uma comparação.

Comparando com o trabalho de Watanavisit e Vorakulpipat (2020) é possível observar que a proposta de utilizar um sistema baseado na *blockchain Hyperledger* é uma vantagem significativa, pois oferece um armazenamento de dados não centralizado, imutabilidade e transparência, elementos cruciais para a integridade e a confiança no processo de votação. O modelo

aqui proposto considera a replicação de registros e o uso do consenso do *Hyperledger*, garantindo confiabilidade e robustez na manutenção dos dados. A ênfase na autenticidade do usuário com um ID único e a conexão segura do usuário ao sistema são aspectos fundamentais para evitar duplicação de votos e garantir a integridade do processo eleitoral.

Comparando com o trabalho de Goyal e Kumar (2021) verifica-se que ambas as propostas fazem uso da *blockchain* para garantir a integridade e a segurança dos votos. No entanto, o uso específico da *blockchain Hyperledger*, pode ser uma vantagem em termos de garantia de confidencialidade dos votos, uma vez que a *Hyperledger* é conhecida por sua segurança e privacidade. A clareza na descrição das classes e casos de uso para a interação do eleitor com a aplicação proporciona uma vantagem em termos de compreensão e implementação eficaz do sistema de votação. Outra vantagem do modelo proposto neste trabalho é a geração de relatórios para auditoria definitiva com referências do bloco da *blockchain* uma vez que fornece maior transparência e verificabilidade do processo de votação.

Na comparação com o trabalho Pramulia e Anggorojati (2020) o trabalho aqui proposto tem vantagem da forma que faz uma consideração explícita da auditoria, com a replicação de registros e o uso do consenso, demonstra um foco claro na transparência e na verificabilidade do processo de votação, o que é uma vantagem significativa.

Relacionando com o sistema descrito no trabalho Adida (2008) a utilização da *blockchain Hyperledger* representa uma evolução em relação a abordagens mais antigas. A *blockchain* oferece maior segurança e transparência devido à sua natureza imutável e descentralizada. A geração de relatório para auditoria definitiva, com o uso de *hashcode* do bloco e referência do bloco, fornece uma vantagem adicional em termos de integridade e verificabilidade dos registros.

Fazendo um paralelo com o trabalho (BENALOH *et al.*, 2012) observa-se que as duas propostas buscam garantir segurança, transparência e auditabilidade no processo de votação eletrônica. No entanto, a escolha da *blockchain Hyperledger* pode oferecer maior confiança na integridade dos dados, pois é projetada para ambientes corporativos e foca em segurança e permissões. A replicação de registros e a aplicação do consenso do *Hyperledger* fornecem uma camada adicional de confiança e confiabilidade no processo de votação, superando as abordagens tradicionais.

As atribuições da plataforma de *blockchain Hyperledger* representam aspectos distintivos que reafirmam a sua natureza transparente e asseguram que o processo de auditoria receba a devida ênfase. Assim, o modelo de arquitetura proposto apresenta uma vantagem distintiva

sobre as demais abordagens, especialmente nos aspectos primordiais dentro do nosso escopo.

3.4 Resultados da Revisão Sistemática

Deve-se rememorar foram definidas perguntas de pesquisa para serem respondidas no decorrer deste trabalho de revisão. Nesta seção são apresentadas as respostas aos questionamentos levantados, o que pode ser obtido como resultado direto da revisão.

3.4.1 Qual o estado da arte de arquiteturas de blockchain aplicadas à sistemas de e-voting para fins de auditoria?

É possível afirmar que as pesquisas demonstram uma crescente adoção e interesse na aplicação da tecnologia *blockchain* nesse contexto, destacando sua capacidade de proporcionar transparência, segurança e integridade aos processos eleitorais. Muitos estudos exploram modelos de arquiteturas *blockchain* adaptados para sistemas de *e-voting*, enfocando aspectos como escalabilidade, privacidade e confiabilidade. Um exemplo disto é o trabalho de (GOYAL; KUMAR, 2021), que é um dos trabalhos relacionados.

A realização de uma busca acerca do estado da arte da área de desenvolvimento de sistemas de auditoria utilizando a tecnologia *blockchain* tem como resultado conclusões que direcionam os esforços para o desenvolvimento de uma pesquisa que traga ganho científico e uma solução aplicável ao mundo real.

3.4.2 Quais são as diferenças entre arquiteturas com blockchain e arquiteturas tradicionais em sistemas de votação, conforme descrito na literatura?

Os estudos indicam que as principais diferenças entre arquiteturas com *blockchain* e as tradicionais em sistemas de votação residem na descentralização, imutabilidade e transparência oferecidas pela *blockchain*. Enquanto os sistemas tradicionais frequentemente dependem de bancos de dados centralizados, as arquiteturas com *blockchain* operam em redes descentralizadas, garantindo uma trilha imutável de registros e maior confiança nas transações realizadas.

3.4.3 Quais são as principais vantagens relatadas na utilização da tecnologia blockchain em arquiteturas de sistemas de e-voting, de acordo com os estudos analisados?

Com base nos trabalhos observados nesta revisão sistemática, é possível afirmar que existem diversas vantagens da tecnologia *blockchain* em sistemas de *e-voting*, incluindo segurança aprimorada devido à criptografia e ao consenso distribuído, transparência nas transações e a capacidade de permitir a verificação pública dos resultados eleitorais sem comprometer a privacidade do voto.

3.4.4 Quais são as plataformas mais frequentemente utilizadas para testes de arquiteturas de sistemas de e-voting com blockchain?

As plataformas mais comuns utilizadas para testes de arquiteturas de sistemas de *e-voting* com *blockchain* conforme os trabalhos observados, incluem Buterin (2022), Contributors (2023a), Block.one (2023), e R3 (2023). Cada uma dessas plataformas oferece diferentes recursos e protocolos que podem ser adaptados para atender às necessidades específicas de sistemas de *voting*. No escopo desta pesquisa é possível afirmar que a plataforma mais utilizada é a Ethereum, seguida pela plataforma Hyperledger.

3.4.5 Em estudos comparativos que utilizam arquiteturas de sistemas de e-voting com blockchain para fins de auditoria, quais plataformas de blockchain demonstram melhor desempenho?

Alguns trabalhos destacam o desempenho superior de plataformas como o Hyperledger Fabric em relação a aspectos como escalabilidade e privacidade, enquanto outros podem enfatizar a flexibilidade e a facilidade de desenvolvimento oferecidas por Ethereum. É observado que as relações de desempenho entre as plataformas de *blockchain* podem alterar-se, a depender do contexto em que a tecnologia está inserida.

3.4.6 Existem estudos que abordam o custo de implementação e utilização da tecnologia blockchain em sistemas de e-voting? Em caso afirmativo, qual é o impacto desse custo nos resultados desses estudos?

Existem estudos que abordam o custo de implementação e utilização da tecnologia *blockchain* em sistemas de *e-voting*.No entanto, como observado já no início da revisão sistemá-

tica, dentro do escopo dos trabalhos observados o tema do custo não é amplamente abordado. Dessa forma identifica-se que existe um espaço na literatura para estudos neste sentido. Por outro lado, de um ponto de vista geral sistemas baseados em *blockchain* podem ter custo de implementação e manutenção maior que os sistemas tradicionais, devido à infraestrutura e protocolos específicos necessários. O impacto financeiro varia conforme o escopo e as características de cada implementação, sendo um ponto de análise crítico em avaliações de viabilidade e adoção dessas soluções (ISMAIL *et al.*, 2022) (ALSHAMSI *et al.*, 2022). Neste trabalho, por exemplo, são utilizadas ferramentas gratuitas para implementação da aplicação. A ideia é garantir que qualquer instituição possa utilizá-la, sem ter preocupação direta com os custos.

Em suma, pode-se observar que as pesquisas realizadas até o momento tem foco principal em aprimoramento dos sistemas já existentes por meio da inserção da tecnologia *blockchain*. Relatos de diferentes tipos de modelagens de associação de bancos de dados relacionais à *blockchain* são comuns à boa parte dos trabalhos. O ponto de entrada de *blockchain* é, normalmente, o registro de parte dos arquivos de log na cadeia. Sobre o protocolo de consenso, pode-se observar que o mais utilizado em sistemas de auditoria é o *Practical Byzantine Fault Tolerance* (PBFT), pois possui duas fases de preparação antes de confirmar a informação a ser registrada na cadeia de blocos.

Realizar uma auditoria é um processo de verificação custoso, visto que além de observar incongruências nos dados, deve-se verificar a confiabilidade destes dados e da informação de quem os produziu. Observando o estado da arte, pode-se concluir que as soluções que utilizam *blockchain* para este fim atacam principalmente o problema de confiabilidade, devido ao rastro deixado na cadeia de blocos. A imutabilidade dos dados traz ganhos do ponto de vista de processos, uma vez que, oferece aos sistemas de auditoria maior eficiência em relação à garantia de integridade dos dados, garantia de não repúdio e confiabilidade da informação em ambiente de controle descentralizado, o que também pode ser relacionado ao consenso da rede *blockchain*.

4 EXPERIMENTAÇÃO COM *BLOCKCHAIN*

Os trabalhos obtidos na busca foram analisados individualmente a fim de formar uma ideia acerca do estado da arte em auditoria com *blockchain*. Foi concluído que muitos dos trabalhos se utiliza da plataforma Hyperledger, para criação da rede *blockchain*. Considerando que a plataforma definida para uso neste trabalho é plataforma Hyperledger foi definida uma experimentação a fim atestar alguns critérios de desempenho que se relacionam com a qualidade do software.

No desenvolvimento de softwares e aplicações, a confiabilidade dos mesmos é verificada pelas atividades de teste. Segundo Cohn (2010) os testes são divididos em três grupos: testes de unidade, verificam automaticamente pequenas partes de um código; testes de integração, verificam uma transação ou funcionalidade completa; e testes de sistema, simulam uma sessão de uso do sistema em ambiante realístico (VALENTE, 2020). Este experimento deve ser um teste de sistema, pois as características de testes de sistema podem ser associadas às características de qualidade definidas em ISO/IEC (2011). A qualidade pode ser mensurada e alcançada a partir da sua associação com as metas e objetivos das partes interessadas. Desse modo, neste experimento é utilizada uma norma ISO como base para realização dos testes e verificação da qualidade da principal ferramenta utilizada neste trabalho, o Hyperledger Fabric.

As normas estabelecidas na ISO/IEC 25010 descrevem como o software se relaciona com os dados e o impacto que esta relação causa às partes interessadas. Ela surgiu em 2011 com um conjunto de outras normas, derivados da ISO/IEC 9126. Esta norma parte da definição das características do software e estabelece modelos de usuários, e, conforme a necessidade destes usuários, modelos de qualidade específicos. De acordo coma ISO/IEC 25010, os modelos de qualidade se dividem em três: modelo de qualidade de produto, modelo de qualidade de dados e modelo de qualidade em uso. Os modelos de qualidade de produto e modelo de qualidade em uso funcionam como uma espécie de lista de verificação para garantir um tratamento abrangente dos requisitos de qualidade e prover uma base para estimar o esforço e atividades consequentes que serão necessários durante o desenvolvimento dos sistemas. Outras normas, como a ISO/IEC 2502n e a ISO/IEC 15939, apresentam medidas e modelos de medição para serem aplicadas às propriedades de qualidade.

Neste trabalho apenas o modelo de qualidade de produtos é considerado para avaliação do desempenho do Hyperledger Fabric. Uma sub-característica do modelo de qualidade do produto é a eficiência de desempenho, onde são observadas três métricas: comportamento

no tempo, grau em que os tempos de resposta e processamento de um sistema atendem aos requisitos; utilização de recursos, grau em que as quantidades e tipos de recursos utilizados por um sistema atendem aos requisitos; e capacidade, grau em que os limites máximos de um produto ou parâmetro do sistema atendem aos requisitos, estes podem incluir o número de itens armazenados, de usuários simultâneos,largura de banda de comunicação, *throughput* de transações e tamanho do banco de dados.

Sob o contexto de auditoria de sistemas de e-voting, a observação dos critérios estabelecidos na ISO/IEC 25010, permite que os auditores observem características da aplicação a fim de atestar sua confiabilidade. Características como tempo de resposta, utilização de recursos, escalabilidade, economia de energia. O teste de desempenho realizado fornece bases para avaliação da confiabilidade da aplicação visto que avalia a plataforma onde o sistema proposto é construído. O modelo de eficiência de desempenho e suas métricas serão observadas nesta seção.

4.1 Metodologia do Experimento

Para esta avaliação, uma máquina virtual foi instanciada na plataforma *Microsoft Azure* executando o sistema operacional *Ubuntu Server 18.02*.A máquina virtual contém duas vCPU's virtuais e 8 GB de memória. O Hyperledger Fabric foi instalado na máquina virtual. Para analisar sua performance utilizou-se o Hyperledger Caliper (FOUNDATION, 2021), uma ferramenta de *benchmark* para avaliação de desempenho em *blockchain*. A rede é composta por três nós, sendo um nó *orderer* (administrador) em uma organização e dois nós comuns (usuários) em outra organização. Para esta análise também foi necessário a implementação de um pequeno contrato inteligente em GO, que no Hyperledger Fabric recebe a nomenclatura de *chaincode*.

Este *chaincode* realiza transações simples com uma função *create*, que insere dados na *blockchain* e uma função *query* que realiza consultas. A cada iteração do experimento, o *chaincode* realiza transações de gravação e consulta na *blockchain*. A informação registrada no bloco não tem relevância para este estudo. Dessa forma, definiu-se um conjunto de informações simples, um objeto e alguns atributos, resultando em 4 valores. Cada transação possui um tamanho de 3,3KB, sendo o tamanho máximo do bloco 33KB, ou seja, 10 transações. O Hyperledger Caliperpossibilita que um relatório na forma de um arquivo com formato HTML seja gerado a partir do experimento, e se possa observar as métricas em cada etapa da experimentação.

De acordo com ISO/IEC 25010 (ISO/IEC, 2011), as sub-características que tratam

da qualidade do software em eficiência de performance são comportamento no tempo, utilização de recursos e capacidade. Para avaliar estas características são observadas as métricas *throughput* (bits por segundo), latência (segundos) percentual de utilização da CPU. Alguns parâmetros são estabelecidos por meio de funções da própria ferramenta de Hyperledger Caliper. As funções utilizadas no experimento são *txduration* e *txnumber*, que correspondem respectivamente a duração das transações e o número de transações. A função *txduration* define por quanto tempo o experimento vai executar tantas transações quanto possível, de acordo com a capacidade do sistema. A função *txnumber* define a quantidade de transações por execução, em um tempo não especificado, de acordo com a capacidade do sistema. A ideia é realizar testes carga a fim de prover um teste de desempenho do Hyperledger Fabric por meio de uma infraestrutura básica.

Utilizando estas funções, o experimento se define em duas etapas. Na primeira etapa são definidos quatro valores de tempo de execução em segundos: 15, 30, 60 e 120. Cinco testes em cada valor de tempo são executados. Na segunda etapa são definidos quatro valores de número de transações por execução: 50, 100, 500 e 1000. Cinco testes em cada valor de número de transações São executados. Ao final das duas etapas, obtém-se 40 resultados. Ambas as etapas foram realizadas utilizando a mesma infraestrutura. Esta infraestrutura é composta pela rede *blockchain* formada por 2 organizações. Em uma das organizações temos em execução o nó *orderer*, responsável pela configuração da rede no Hyperledger Fabric, basicamente um nó controlador. Na outra organização existem em execução 2 nós comuns, aqui chamados *peers*, que são como usuários comuns desta rede *blockchain*. As Figuras 13 e 14 exibem as configurações dos experimentos no Hyperledger Caliper.

Ao final do experimento, as métricas coletadas foram *Throughput*, Latência Média e Utilização da CPU. Os resultados são levantados a partir da divisão da coleta de acordo com os níveis e o cálculo de uma média aritmética dos valores coletados em cada etapa da experimentação. Os resultados obtidos devem ser observados sob a perspectiva de eficiência de performance, definida na ISO/IEC 25010. Para eficiência de tempo é observado o crescimento do número de transações e a resposta no *throughtput*. Para capacidade e utilização de recursos é observado o aumento das transações e o comportamento da latência média em relação ao *trhoughtput* e, também, a utilização de CPU. Realizando esta experimentação é possível atender requisitos de teste de desempenho.

Figura 13 – Configuração do experimento utilizando a função *txduration*.

```
workers:
  type: local
rounds:
  - label: Create
    txDuration: 15
    rateControl:
      type: maximum-rate
      opts:
        tps: 10
        step: 10
    workload:
      module: benchmarks/scenario/createCar.js
  - label: Query
    txDuration: 15
    rateControl:
      type: maximum-rate
      opts:
        tps: 10
        step: 10
    workload:
      module: benchmarks/scenario/queryCar.js
      arguments:
        assets: 10
```

Fonte: Produzido pelo autor.

Figura 14 – Configuração do experimento utilizando a função *txnumber*.

```
workers:
  type: local
rounds:
  - label: Create
    txNumber: 50
    rateControl:
      type: maximum-rate
      opts:
        tps: 10
        step: 10
    workload:
      module: benchmarks/scenario/createCar.js
  - label: Query
    txNumber: 50
    rateControl:
      type: maximum-rate
      opts:
        tps: 10
        step: 10
    workload:
      module: benchmarks/scenario/queryCar.js
      arguments:
        assets: 10
```

Fonte: Produzido pelo autor.

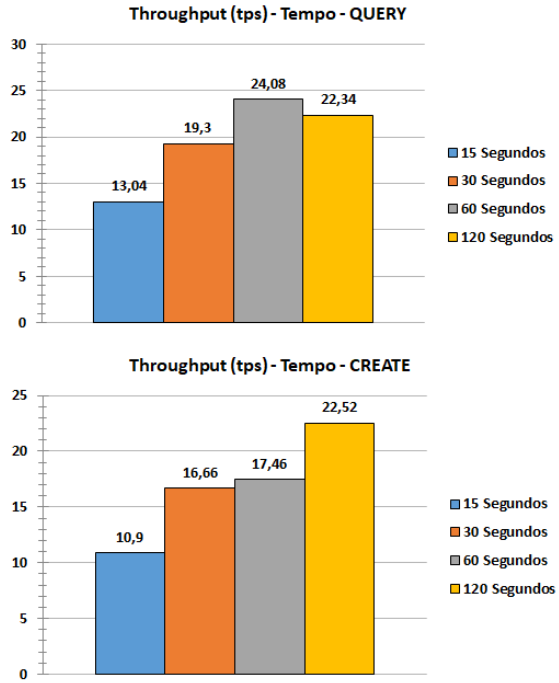
4.2 Resultados do Experimento

Nesta seção são apresentados os resultados obtidos com o experimento. O relatório do *Hypeledger Caliper* fornece as seguintes métricas: número de transações, número de falhas, latência máxima, latência mínima, latência média, *throughput*, utilização máxima de CPU, utilização mínima de CPU, utilização máxima de memória, utilização mínima de memória, tráfego de entrada, tráfego de saída, dados escritos em disco, dados lidos do disco. Para esta

análise são levadas em conta as métricas: *throughput*, latência média e utilização de CPU. Este último é observado apenas na execução da função *create*.

A Figura 15 apresenta gráficos com a métrica *throughput* na primeira etapa do experimento, em função do tempo, para operações de leitura e escrita. É possível observar uma tendência para crescimento do *throughput* quando o tempo aumenta. A mesma tendência pode ser observada na Figura 16, que apresenta gráficos para o *throughput* na segunda etapa do experimento, em função do número de transações, para operações de leitura e escrita. Pode-se observar, no entanto, que na Figura 15, para função *query*, existe um momento de redução do *throughput* no tempo de 120 segundos.

Figura 15 – *Throughput* para valores fixos de tempo.

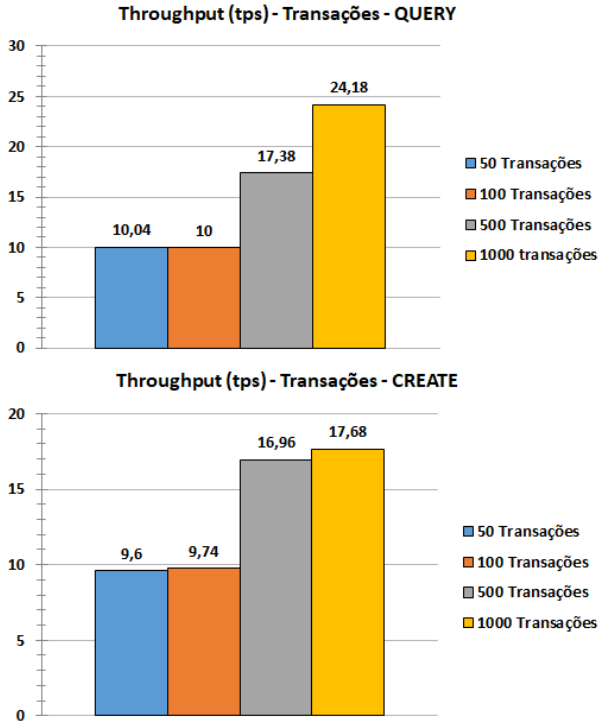


Fonte: Produzido pelo autor.

As Figuras 17 e 18 apresentam gráficos para a latência média nas duas etapas do experimento, para operações de leitura e escrita. Na observação desta métrica é identificada uma variação muito baixa nas duas funções. Apesar disso, para função a *create*, observa-se um crescimento abrupto no experimento com 1000 transações.

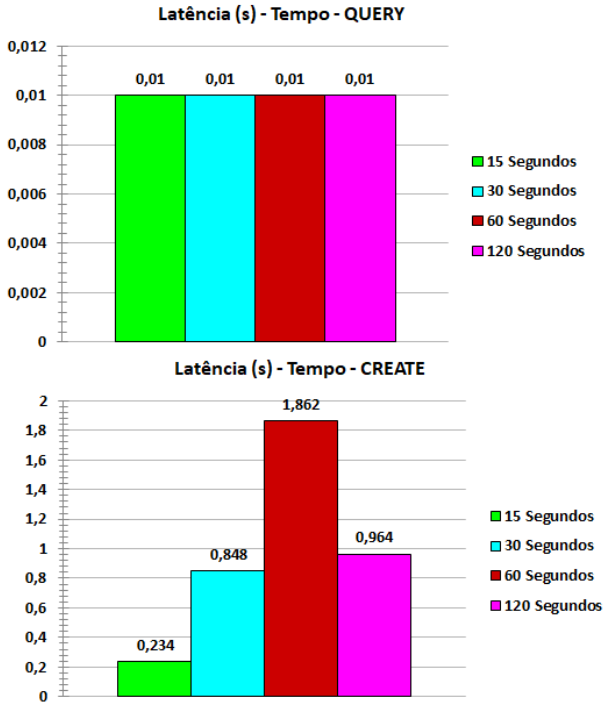
As Figuras 19 e 20 apresentam gráficos para utilização da CPU nos nós da rede *blockchain* implementada. Considerando que os resultados de todos os nós são diretamente proporcionais, neste estudo são considerados apenas os resultados obtidos no nó *orderer*. Nestes gráficos, o comportamento da CPU é como esperado, existindo um aumento da utilização

Figura 16 – *Throughput* para valores fixos de transações.



Fonte: Produzido pelo autor.

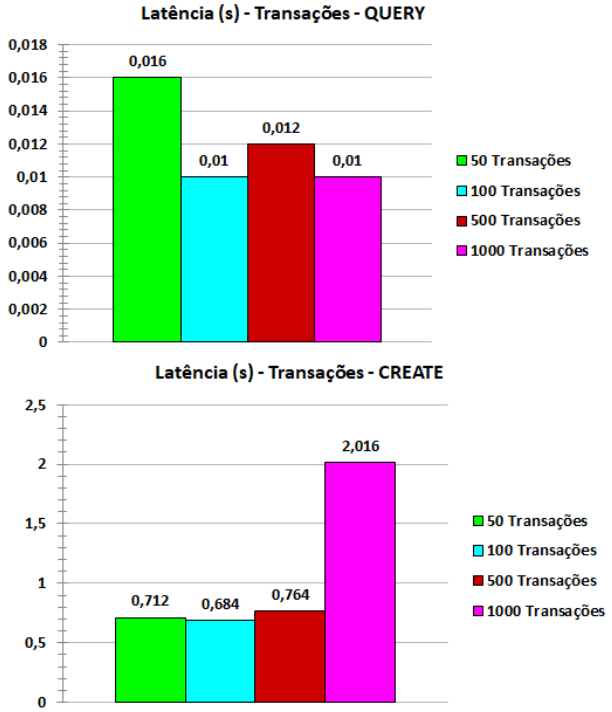
Figura 17 – Latência média para valores fixos de tempo.



Fonte: Produzido pelo autor.

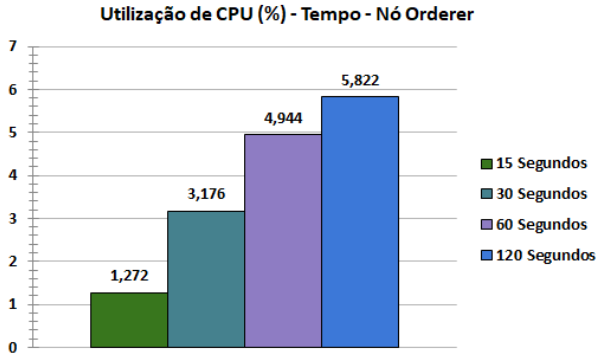
conforme se aumenta o tempo de experimento ou número de transações. O número de transações do experimento aparentemente não chega ao limite da CPU em nenhuma das etapas da experimentação.

Figura 18 – Latência média para valores fixos de transações.



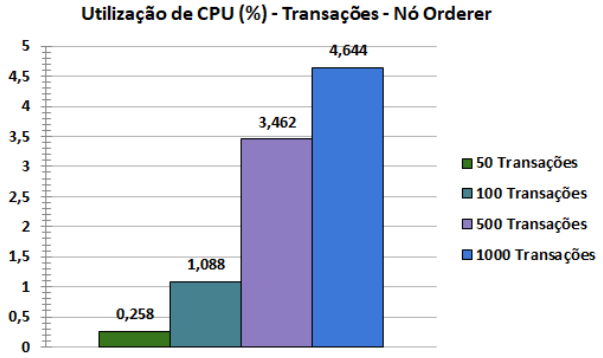
Fonte: Produzido pelo autor.

Figura 19 – Utilização de CPU para valores fixos de tempo.



Fonte: Produzido pelo autor.

Figura 20 – Utilização de CPU para valores fixos de transações.



Fonte: Produzido pelo autor.

4.3 Discussão

Os testes de carga realizados permitem observar o comportamento da ferramenta Hyperledger Fabric. Apenas observando os gráficos é possível perceber que o número de transações impacta diretamente no desempenho da rede, de modo que um maior número de transações nas duas etapas do experimento aumentam o *throughput*, que é a taxa em que os dados são transmitidos em determinado período de tempo. Ou seja, conforme a capacidade da rede, se o número de transações do tipo *create e query* aumenta, é esperado que o *throughput* também cresça. Este comportamento aliado à observação da utilização de CPU demonstra escalabilidade da infraestrutura, uma vez que os recursos são disponibilizados de modo diretamente proporcional ao número de transações.

É possível observar também que quando existe uma elevação do número de transações, em alguns momentos, a latência diminui. A latência é o tempo que o pacote leva para chegar da origem ao destino. Como o *throughput* aumenta conforme o número de transações, é normal que a latência média aumente devido a fatores como congestionamento na rede. No entanto, a latência média em alguns momentos diminui quando o número de transações é maior no experimento. Isto traz a impressão de uma certa escalabilidade da rede, apesar de não haver mudanças na infraestrutura implementada. Isto é observado claramente na Figura 16 na execução da função *create*. Isto também demonstra que um número de transações de valor 1000 reduz o desempenho da rede *blockchain* implementada no experimento, uma vez que conforme observado na Figura 20, a utilização da CPU tem um aumento gradual e proporcional ao número de transações e, como observado na Figura 18, a latência aumenta drasticamente para função *create*. Considerando a perspectiva de qualidade, que é foco deste experimento, é possível observar uma degradação da infraestrutura em função da elevação do número de transações, mesmo sem alcançar o limite de capacidade da rede e da máquina.

Uma aplicação baseada em *blockchain* poderia sofrer uma redução da eficiência de desempenho para função *create*, se implementada no Hyperledger Fabric.Também observa-se que a variação na latência para a função *query* é mínima, podendo ser imperceptível, como fica claro na Figura 17. Isto demonstra que para aplicações que realizem apenas consulta não há degradação da eficiência de desempenho, consequentemente, não há perda de qualidade. Pode-se concluir também, que a função *create*, que realiza gravação de dados, utiliza mais recursos da infraestrutura de rede implementada que a função *query*, que executa apenas consultas.

4.4 Ameaças à Validade do Experimento

Foi conduzido um teste de desempenho de uma infraestrutura de *blockchain*, com funções simples e quantidade de dados relativamente pequenos. Desta forma é possível levantar algumas ameaças à sua validade.

Na experimentação contou-se com uma infraestrutura em pequena escala, com apenas 3 nós, não podendo ser generalizadas. Os resultados obtidos podem não ser replicáveis em uma infraestrutura de maior escala. Outra ameaça é relacionada ao desempenho dos nós, que atendeu aos requisitos necessários à execução do experimento. Deve-se considerar que este desempenho pode não ser suficiente se o número de transações ou o tempo de experimento sofrerem uma brusca elevação.

Também utilizou-se apenas uma plataforma de *blockchain*, no caso o Hyperledger Fabric. Mesmo que o projeto do experimento tenha sido focado Hyperledger Fabric, o estudo pode ser replicado para outras plataformas de *blockchain*, como a *Ethereum*, e comparar os resultados.

Olhando sob a perspectiva de qualidade, esta experimentação é parte de um trabalho ainda em progresso. A ISO/IEC 25010 não é a única que trata de confiabilidade do software e qualidade, outras normas, como as que foram citadas anteriormente, a complementam para realizar a aferição da qualidade.

Dessa forma esta avaliação pode ser considerada superficial para a medição de um sistema *blockchain* como um todo, sob a ótica de diferentes requisitos não funcionais. Além disso, testes de desempenho trazem uma série de requisitos que não foram profundamente observados neste estudo. Tendo em vista que é um estudo inicial acerca do tema, espera-se sanar estas ameaças à validade em trabalhos e experimentos futuros.

5 PROPOSTA DA ARQUITETURA E DA AUDITORIA

Nesta seção apresenta-se uma proposta de arquitetura para um sistema de *e-voting* (votação eletrônica) baseado na tecnologia *blockchain*, com um enfoque especial na auditoria. A proposta visa garantir a transparência, segurança e integridade das eleições, fornecendo um registro imutável de todas as transações relacionadas ao processo de votação. A arquitetura proposta incorpora elementos-chave do *blockchain*, como descentralização, criptografia e consenso distribuído, para assegurar a confiança dos eleitores e a verificabilidade dos resultados. A utilização da tecnologia *blockchain* na votação eletrônica traz diversas vantagens em relação aos sistemas tradicionais. A transparência, segurança e a capacidade de auditoria são características intrínsecas à tecnologia *blockchain* e podem ajudar a solucionar muitos dos desafios enfrentados pelos sistemas de votação convencionais.

5.1 Projeto de Arquitetura

A arquitetura proposta para o sistema de *e-voting* baseado em *blockchain* é composta por três camadas principais: a camada de interface com o eleitor, a camada de processamento de votos e a camada de armazenamento distribuído (FAWAZ *et al.*, 2018) (KAKAR *et al.*, 2018) (KERN; MAUTHE, 2019).

5.1.1 Camada de Interface com o Eleitor

Esta camada é responsável pela interação entre o eleitor e o sistema de *e-voting*. Ela consiste em aplicativos de votação eletrônica que podem ser executados em dispositivos como smartphones, tablets ou computadores. Essa aplicação fornece uma interface amigável ao eleitor, permitindo que ele registre seus votos de forma segura e verificável.

5.1.2 Camada de Processamento de Votos

Nesta camada, os votos registrados pelos eleitores são processados e validados. Os votos são criptografados para garantir a privacidade do eleitor e, em seguida, registrados como transações na *blockchain*.

5.1.3 Camada de Armazenamento Distribuído

A camada de armazenamento distribuído é composta por nós da rede *blockchain* que mantêm uma cópia completa do registro de votos. Essa cópia é atualizada à medida que novas transações de votos são adicionadas à *blockchain*. A descentralização do armazenamento garante a segurança e a resistência a falhas do sistema, uma vez que não há um único ponto de falha.

5.1.4 Auditoria

A auditoria desempenha um papel fundamental na proposta de arquitetura. A utilização do *blockchain* permite que todos os registros de votação sejam imutáveis e publicamente verificáveis. Isso significa que qualquer pessoa pode verificar a precisão e a integridade dos resultados eleitorais, garantindo a confiança no processo. Além disso, é possível realizar auditorias em tempo real durante o processo de votação. Os eleitores podem verificar se seus votos foram registrados corretamente e confirmar se eles foram incluídos na contagem final. Esse nível de transparência fortalece a confiança do eleitorado e reduz as chances de manipulação dos resultados (BHARGAVAN *et al.*, 2016) (KERN; MAUTHE, 2019) (NG; PARTRIDGE, 2020).

5.1.5 Segurança

A segurança é uma preocupação primordial em qualquer sistema de votação eletrônica. Na arquitetura proposta, a criptografia é utilizada para garantir a privacidade do eleitor e a autenticidade dos votos. Além disso, a descentralização e o consenso distribuído do *blockchain* ajudam a prevenir ataques maliciosos, tornando o sistema mais resiliente a tentativas de adulteração. Outras medidas de segurança, como a autenticação dos eleitores por meio de identidades digitais únicas e a adoção de protocolos robustos para proteger a rede contra ataques de negação de serviço, devem ser consideradas na implementação do sistema (KAKAR *et al.*, 2018) (SHRESTHA *et al.*, 2018) (ZENG *et al.*, 2021).

5.1.6 Considerações sobre a proposta

A proposta de arquitetura apresentada, oferece um sistema de *e-voting* seguro, transparente e confiável, com características que proporcionam auditoria. A utilização da tecnologia *blockchain* permite a criação de um registro imutável de votos, fornecendo aos eleitores e à sociedade como um todo a capacidade de auditar os resultados eleitorais. No entanto,

é importante ressaltar que a implementação de um sistema de *e-voting* baseado em *blockchain* requer cuidadosa análise e testes para garantir sua eficácia e confiabilidade.

Em primeiro momento deve-se realizar uma análise detalhada dos requisitos e especificações fornecidos para o sistema de *e-voting* com *blockchain*. Identificar as tecnologias necessárias, incluindo Hyperledger para a *blockchain* e outros componentes relacionados. Feito isto será possível criar a interface de usuário para permitir a conexão ao sistema usando um ID único e credenciais seguras. Implementar o sistema de autenticação para garantir a segurança e a integridade das credenciais dos usuários. Depois disso deve-se desenvolver a funcionalidade que permita a definição de candidatos e a criação de votações. A partir daí o usuário de ter a possibilidade de realizar seu voto no sistema, garantindo a segurança e a integridade do processo de votação.

Em um segundo momento é programada a lógica de processamento de votos, gerando um registro para auditoria periódica com informações sobre o número de usuários que concluíram o processo de votação e uma parcial dos resultados. Incluída nesta lógica deve estar a implementação da funcionalidade que disponibiliza o registro para auditoria simplificada no sistema, permitindo que os usuários analisem as informações relacionadas à auditoria.

O terceiro passo é configurar e implementar os processos relacionados à gravação dos dados na *blockchain*, neste caso, usando Hyperledger. Criar o contrato inteligente e a lógica necessária para compilar as informações e gerar um bloco na *blockchain*.

O quarto passo é programar a geração do relatório para a auditoria definitiva, incluindo o *hashcode* do bloco gerado e a referência do bloco que contém o voto do usuário. No contrato inteligente já são definidas as informações que vão ser registradas na *blockchain*, dessa forma, nesta etapa deve ser definido um meio que garanta que isso pode ser verificado, seja pela própria aplicação ou não.

Por último deve-se implementar o consenso dentro da rede *blockchain* para garantir a confiabilidade dos registros replicados em cada nó da rede. Deve haver um meio de permitir que o usuário verifique a integridade do bloco utilizando o *hashcode* ou a referência do bloco em que está registrado o voto.

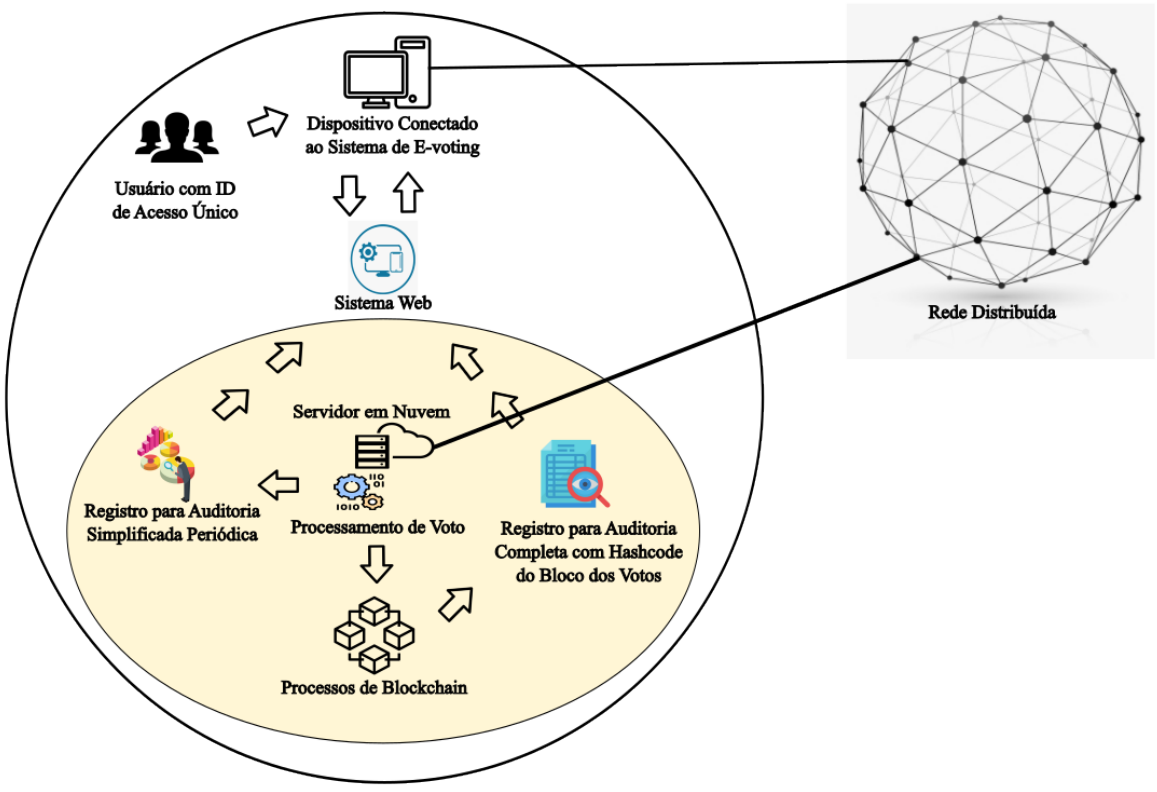
Seguidos estes passos será possível validar a utilização do modelo de arquitetura aqui proposto. Pode-se observar que estes passos, assim como a arquitetura, são definidos no sentido de possibilitar uma certa liberdade de implementação de uma aplicação ou sistema específico para validação. Por outro lado os passos para validação são bem definidos e seguem

uma sequência lógica de modo a garantir que toda a arquitetura seja validada.

5.2 Arquitetura Proposta

A arquitetura proposta tem foco principal na simplicidade e baixo custo de implementação, e capacidade de ser facilmente auditável, a utilização a plataforma Hyperledger promete atender a estes quesitos. Considerando que a aplicação desta arquitetura é qualquer tipo de votação que envolva candidatos ou até mesmo opções de escolha, reforça-se por meio da arquitetura o objetivo final que é prover um caráter de auditoria simplificada, do ponto de vista de experiência do usuário, através dos relatórios, mas com efetiva segurança e transparência garantidas pela *blockchain*. A figura 21 traz uma amostra em alto nível da arquitetura aqui proposta.

Figura 21 – Arquitetura de alto nível proposta neste trabalho.

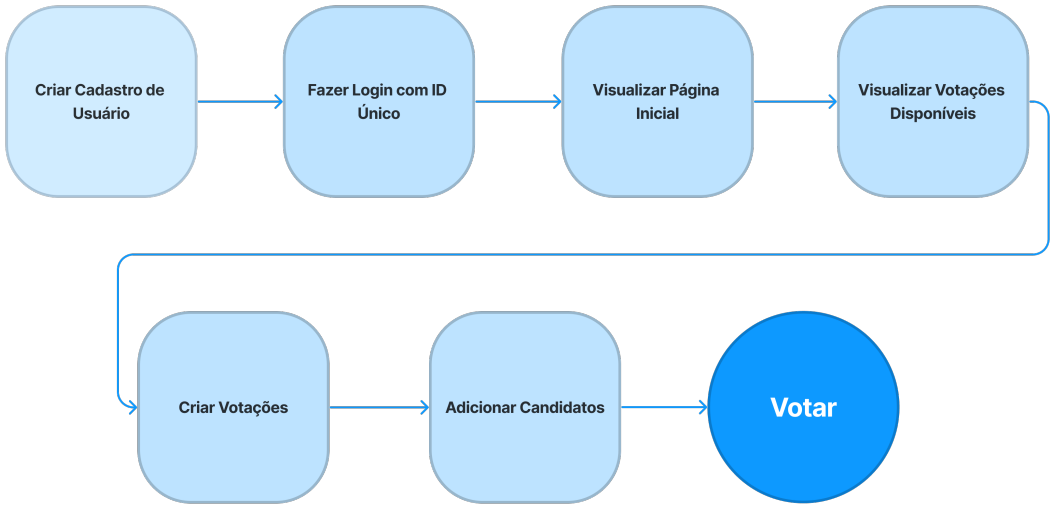


Fonte: Produzido pelo autor.

5.3 Interface do Usuário

A interface do usuário deve ser intuitiva e garantir que seu acesso seja feito através de ID único. Deve ser possível ao usuário adicionar candidatos ou itens a serem escolhidos (opções de escolha) e criar votações com as opções de escolha definidas. O sistema pode conter características diversas, mas o processo de auditoria se inicia no acesso à aplicação com ID único. Em um sistema de *e-voting*, o login com ID é uma medida de segurança que nesta arquitetura visa proteger o sistema contra fraudes eleitorais, como votos duplicados, manipulação de resultados, entre outros. A figura 22 apresenta um fluxograma das ações que devem ser possíveis de executar na interface de usuário para a arquitetura proposta. É importante que além do usuário, cada candidato, cada votação e cada voto possua um ID único.

Figura 22 – Fluxo de ações na interface de usuário até a votação.



Fonte: Produzido pelo autor.

5.4 Processamento de Voto

Realizado o processo descrito no fluxograma deve ocorrer o processamento do voto. Isto nada mais é que o registro das informações do voto. É importante observar, que levando em consideração a arquitetura de alto nível na figura 21, este processamento ocorre do lado servido da aplicação. Feito este processamento do voto já deve ser possível visualizar resultados parciais de votações. O processamento das informações feito nesta etapa, corresponde a outra camada de

auditoria. As parciais de cada votação deve estar disponível em tempo real, o que permite um auditoria periódica, ou seja,deve haver a possibilidade de a qualquer momento ser realizada uma conferência dos votos e resultados das votações.

5.5 Processos de *Blockchain*

Os votos processados, nesta camada da arquitetura devem ser registrados na *blockchain*. Basicamente é gerar uma cópia dos dados processados e gravar na *blockchain*. O protocolo de consenso para a rede *blockchain* deve ser implementado de acordo com a melhor opção para plataforma utilizada. Considerando que neste trabalho a plataforma Hyperledger é utilizada um protocolo de consenso viável seria baseado no protocolo *Raft* (ONGARO; OUSTERHOUT, 2014), que é facilmente implementável na plataforma e atende ao tipo de arquitetura aqui proposta.

Tendo o ambiente *blockchain* configurado, deve-se subir um canal com o protocolo de consenso. Os nós da rede devem ser adicionados ao canal e o contrato inteligente deve ser instalado no canal. A partir daí deve ser feito o registro propriamente dito dos dados na *blockchain*, como interações por meio do contrato inteligente. O consenso e o gerenciamento da geração de blocos deve ser feito pela plataforma.

No *hyperledger fabric* por exemplo, o protocolo *etcdraft* garante o consenso sobre os blocos antes de adicioná-los à *blockchain*. Os detalhes internos do *etcdraft* e da geração de blocos são gerenciados pelo sistema. É possível monitorar a saída dos *containers* do nó *orderer* para visualizar o progresso e verificar se os blocos estão sendo gerados e aceitos pelo consenso.

5.6 Registros Auditáveis

Na arquitetura proposta o registros auditáveis são obtidos em dois momentos: logo após o processamento do voto e logo após o registro dos dados na *blockchain*. A informações que devem estar no registro de cada voto são: ID do usuário, ID da votação, ID do voto e ID do candidato escolhido no voto. Essa informações devem ser armazenadas no banco de dados da aplicação e também na rede *blockchain*. Deve haver um registro único por voto, e a informação da data e hora deste voto deve ser anexada como um dos campos do registro. Para o registro contido na *blockchain*, ao gerar um relatório, o *hashcode* do bloco onde está o registro deve ser informado.

O caráter de auditabilidade destes registros se dá por meio da possibilidade de conferência e comparação dos mesmos em tempo real. Ou seja, sempre que um voto é registrado deve ser adicionado à contagem das votações de imediato, dando a possibilidade de conferência dos resultados parciais e finais das votações a qualquer usuário. Importante observar que cada usuário deve possuir um ID único, como já foi dito. Isto permitirá, em caso de auditamento dos registros, saber os votos de cada usuário, para as devidas conferências, no entanto isto deve ser transparente na aplicação.

5.7 Vantagens e Aspectos Principais

Esta proposta de arquitetura tem como aspecto principal a definição de três pontos de auditabilidade do sistema de votação. O primeiro ponto, como dito anteriormente é o da criação de um usuário, que deve conter um ID único. Isto determina que as ações deste usuário podem ser rastreadas dentro do contexto da aplicação. O segundo ponto é o registro para uma auditoria simplificada periódica, onde é possível dentro do contexto da aplicação acompanhar informações sobre as votações. O último ponto é o registro das informações processadas na aplicação em uma rede *blockchain*

5.7.1 ID único de usuário

Associar um voto a um eleitor específico permite a rastreabilidade, ou seja, é possível verificar como um eleitor votou. Isso pode ser útil em auditorias e verificações de integridade. A associação única de ID a cada eleitor ajuda a evitar que uma pessoa vote várias vezes usando diferentes identidades. Essa é uma medida fundamental para garantir a integridade do processo eleitoral. Também contribui para a segurança do sistema, ajudando a controlar quem pode acessar as funcionalidades de votação. Apenas eleitores autenticados devem ter permissão para votar.Também pode ser visto como uma medida de segurança que visa proteger o sistema contra fraudes eleitorais, como votos duplicados, manipulação de resultados, entre outros. Um sistema de login com ID facilita a manutenção de uma lista de eleitores, garantindo que apenas eleitores registrados tenham acesso ao processo de votação.

Do ponto de vista de funcionalidade, pode permitir uma experiência personalizada para o eleitor, mostrando informações específicas relacionadas à sua jurisdição, candidatos ou outras questões relevantes.

5.7.2 Registro Para Auditoria Simplificada Periódica

Observando a etapa onde é possível obter um registro para uma auditoria simplificada periódica e considerando que este período de acompanhamento pode ser em tempo real, é possível elaborar que permitir que os eleitores, candidatos e observadores acompanhem o progresso da votação contribui para a transparência do processo eleitoral, aumentando a confiança dos participantes no sistema. Ao monitorar os votos em tempo real, é possível identificar rapidamente qualquer problema técnico. Isso permite uma resposta imediata para corrigir problemas e garantir a integridade do processo.

Outro benefício do acompanhamento em tempo real é a possibilidade de aumentar o engajamento do eleitor, proporcionando uma experiência interativa e informativa. Eleitores podem ver como seus votos contribuem para os resultados gerais, o que pode incentivar a participação. Além disso pode facilitar a identificação de atividades suspeitas, como tentativas de manipulação do sistema, ataques cibernéticos ou comportamentos anômalos. Isso ajuda a prevenir fraudes e a proteger a integridade da eleição. A eficiência do processo eleitoral pode ser melhorada, uma vez que essa característica permite uma resposta rápida a eventos inesperados, ajustes de logística e otimização do fluxo de votação. Após o encerramento da votação, é possível fornecer dados valiosos para análises pós-eleição. Isso pode incluir padrões de votação, participação eleitoral e outras métricas que ajudam na compreensão do processo eleitoral.

5.7.3 Registros dos Dados na Blockchain

O registro dos dados dos votos em uma *blockchain*, dadas as características da tecnologia é caracterizado principalmente pela imutabilidade dos dados. Uma vez que um voto é registrado em um bloco, é praticamente impossível alterar ou apagar esse registro. Isso ajuda a proteger contra a manipulação de votos. Todos os votos registrados na *blockchain* são visíveis para os participantes da rede. Isso proporciona transparência ao processo eleitoral, permitindo que os eleitores, candidatos e outros interessados verifiquem os resultados e a integridade do sistema.

A *blockchain* utiliza algoritmos criptográficos para garantir a segurança dos dados. Isso inclui a proteção contra ataques cibernéticos e a garantia de que apenas usuários autorizados possam acessar e alterar os registros. Considerando que é uma rede distribuída em vários nós, o risco de ataques direcionados a um único ponto de falha é mitigado.

Contratos inteligentes podem ser incorporados para automatizar e garantir a execução de regras específicas do processo eleitoral. Isso inclui a contagem de votos, verificação de elegibilidade e outras operações programáveis. A combinação de imutabilidade, transparência e segurança criptográfica contribui para a redução significativa de fraudes e manipulações no sistema de *e-voting*. Por fim, a capacidade de rastrear cada voto na *blockchain* simplifica as auditorias pós-eleição. As autoridades eleitorais e outras partes interessadas podem revisar o registro completo de votos para verificar a precisão e a legitimidade dos resultados.

E importante ressaltar que a arquitetura proposta atende ao objetivo geral proposto, bem como aos objetivos específicos. No decorrer deste trabalho será apresentado um protótipo que visa validar a utilização da arquitetura, observando os critérios estabelecidos nos objetivos.

6 APLICAÇÃO *E-VOTING* SYSTEM

Nesta seção é apresentada uma validação da utilização da arquitetura proposta. Para esta validação foi implementada uma aplicação de *e-voting* com a arquitetura proposta na seção anterior. Para atingir um dos objetivos específicos deste trabalho, que visa possibilitar o uso desta solução em ambientes com restrições pecuniárias e/ou de infraestrutura, as ferramentas e *frameworks* utilizadas são de utilização gratuita.

6.1 Máquina Virtual e Blockchain

Para criação da rede foi utilizada a *Google Cloud Platform* (LLC, 2023), que proporciona créditos gratuitos aos novos usuários. Dentro da plataforma foi criada uma instância de máquina utilizando o sistema operacional Ubuntu 20.04.6 LTS GNU/Linux (LTD., 2023). A máquina conta com 7,7Gb de memória ram, 30Gb de memória de armazenamento, processador Intel(R) Xeon(R).

Figura 23 – Característica Gerais da Instância.

Fonte: Produzido pelo autor.

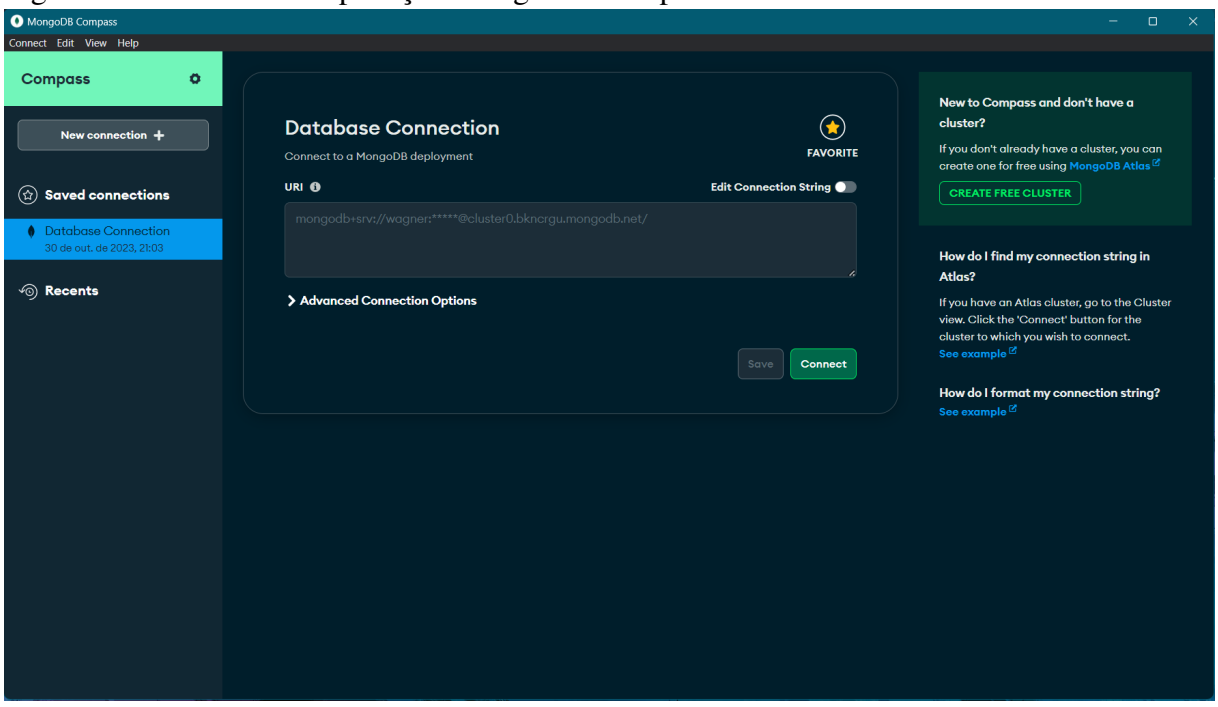
A plataforma Hyperledger é configurada nesta máquina. Dessa forma a rede *block-*

chain é simulada nesta máquina, contendo 3 nós onde em um é executado o *orderer*, responsável pela configuração da rede no Hyperledger, e nos outros são executadas as organizações com *peers*, que são como usuários comuns desta rede *blockchain*.

6.2 Gerenciamento de Dados

No desenvolvimento da aplicação de *e-voting* foi definido o MongoDB como sistema de gerenciamento de banco de dados. A plataforma *MongoDB Atlas* (MONGODB, INC.,) foram armazenadas informações não relacionadas à *blockchain*, como detalhes do usuário e dados de votação antes que sejam processados e registrados na *blockchain*. É uma escolha popular para aplicações modernas devido à sua escalabilidade e flexibilidade no armazenamento de dados. A utilização em baixa escala é possível de modo gratuito através das ferramentas disponibilizadas pela plataforma. O MongoDB Compass, por exemplo, permite a criação de um banco de dados por meio de um *cluster* mantido em nuvem, sendo necessário apenas um cadastro na plataforma (CHELLAPPAN *et al.*, 2020). A imagem 24 traz a interface da aplicação MongoDB Compass.

Figura 24 – Interface da Aplicação MongoDB Compass.

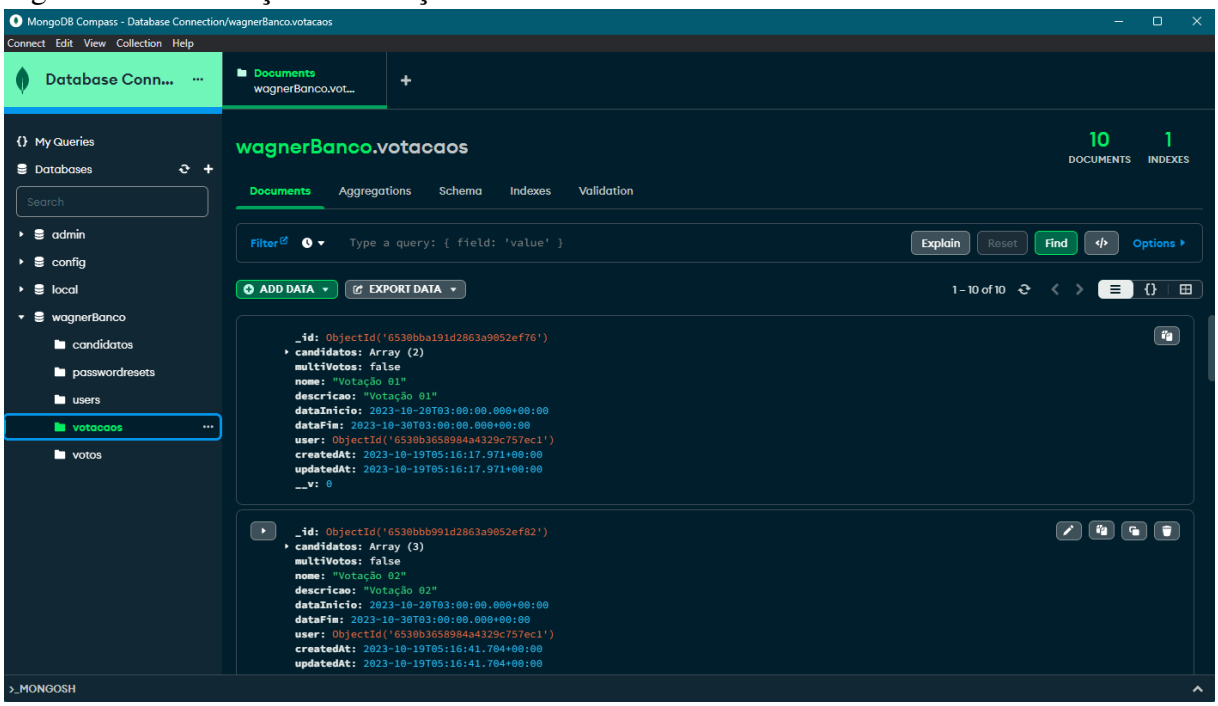


Fonte: Produzido pelo autor.

Depois de todo o processo de votação as informações das votações são exportadas para um arquivo no formato JSON (JavaScript Object Notation - Notação de Objetos JavaScript) (CROCKFORD, 2006). Os dados deste arquivos são inseridos no arquivo de *deploy* do contrato

inteligente na rede *blockchain* contida na instância. A imagem 25 mostra como estão organizadas a informações de votação no banco de dados.

Figura 25 – Informações de votação no Banco de Dados.



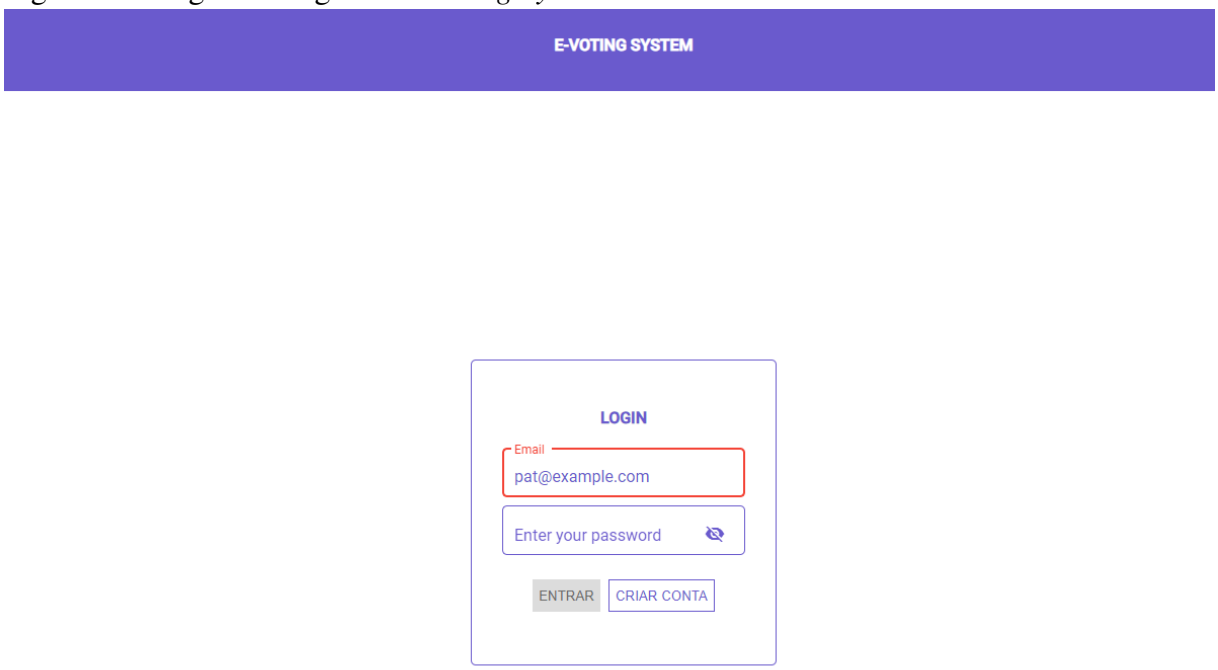
Fonte: Produzido pelo autor.

6.3 Interface da Aplicação

A interface do usuário foi desenvolvida utilizando o *framework* Angular (GOOGLE,), que permite a criação de interfaces web interativas e dinâmicas. Angular é uma escolha popular para aplicações *front-end* robustas e escaláveis. O servidor (*back-end*) foi implementado usando *Node.js* (Node.js Foundation,), um ambiente de execução JavaScript (ECMA, 2023) do lado do servidor que permite a construção de aplicativos escaláveis e de alta performance. O servidor *Node.js* nesta aplicação é responsável por: receber as requisições dos usuário; gerenciar a lógica de negócios, como processamento de votos e interação com a *blockchain*; comunicar-se com o MongoDB para armazenar informações não relacionadas à *blockchain*. Para o usuário é possível criar um cadastro contendo e-mail e senha, para garantir o login seguro na aplicação.

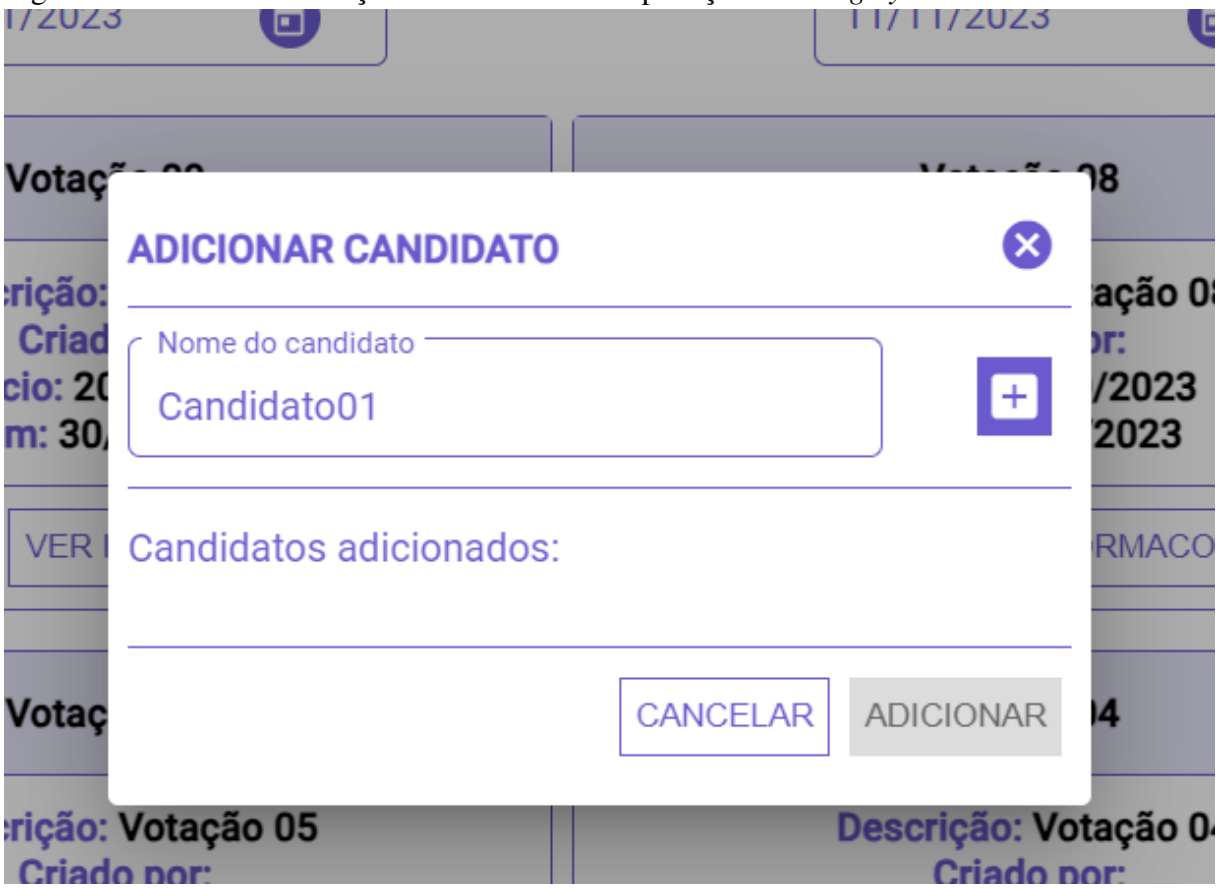
Depois de criar o cadastro e realizar a entrada na aplicação, o usuário administrador poderá adicionar novos candidatos e criar novas votações. A figura 27 traz a interface da adição de novos candidatos da aplicação, enquanto a figura 28 traz a interface de adição de nova votação onde o usuário administrador pode criar uma nova votação.

Figura 26 – Página de login do *E-voting System*.



Fonte: Produzido pelo autor.

Figura 27 – Interface de adição de candidatos da aplicação *E-voting System*.



Fonte: Produzido pelo autor.

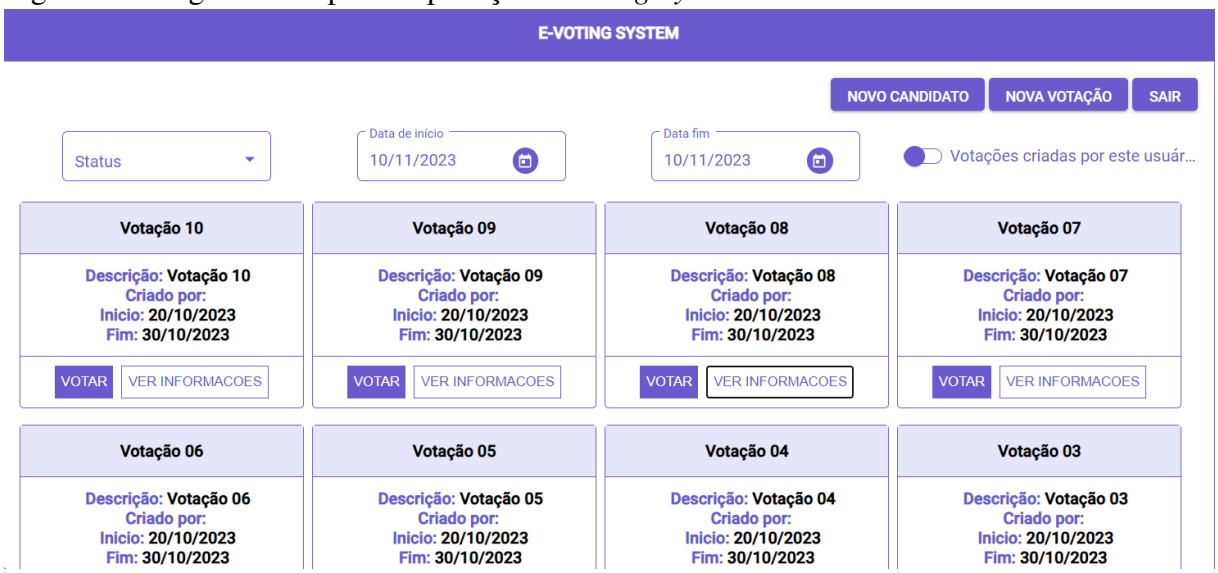
Figura 28 – Interface de adição de nova votação da aplicação *E-voting System*.

Fonte: Produzido pelo autor.

É possível a todos os usuários visualizar as votações já existentes na página principal da aplicação. Para o suário comum, a interface apresentada é a mesma que para o usuário administrador, com exceção dos botões de adicionar novo candidato e nova votação, que não estão visíveis para o usuário comum. Qualquer usuário poderá votar nas votações já criadas. A figura 29 traz a interface da página principal da aplicação, a figura 30 mostra a interface de votação onde o usuário registra o voto em uma votação disponível.

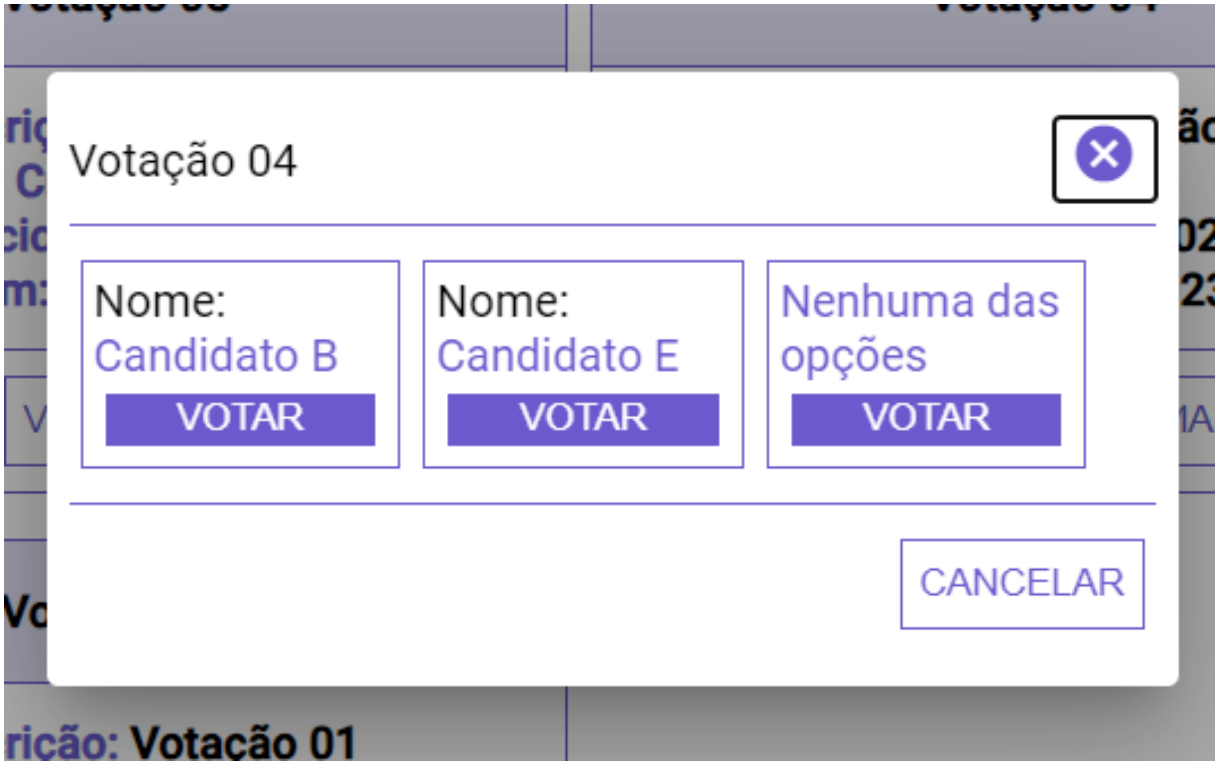
Após o usuário votar na interface *Angular*, o *back-end Node.js* processa o voto, gerando um registro para a auditoria simplificada periódica, que nesta aplicação web é representado por um modal que surge ao clicar-se em um botão de visualização. Este registro contém informações sobre a votação, como o número de pessoas que votaram e uma parcial do resultado da votação. Do ponto de vista da arquitetura proposta, esta seria uma primeira etapa de auditamento, visto que a parcial das votações podem ser acompanhadas em tempo real. A imagem 31 mostra a aplicação no momento em que surge o modal.

Figura 29 – Página Principal da aplicação *E-voting System*.



Fonte: Produzido pelo autor.

Figura 30 – Interface de votação da aplicação *E-voting System*.

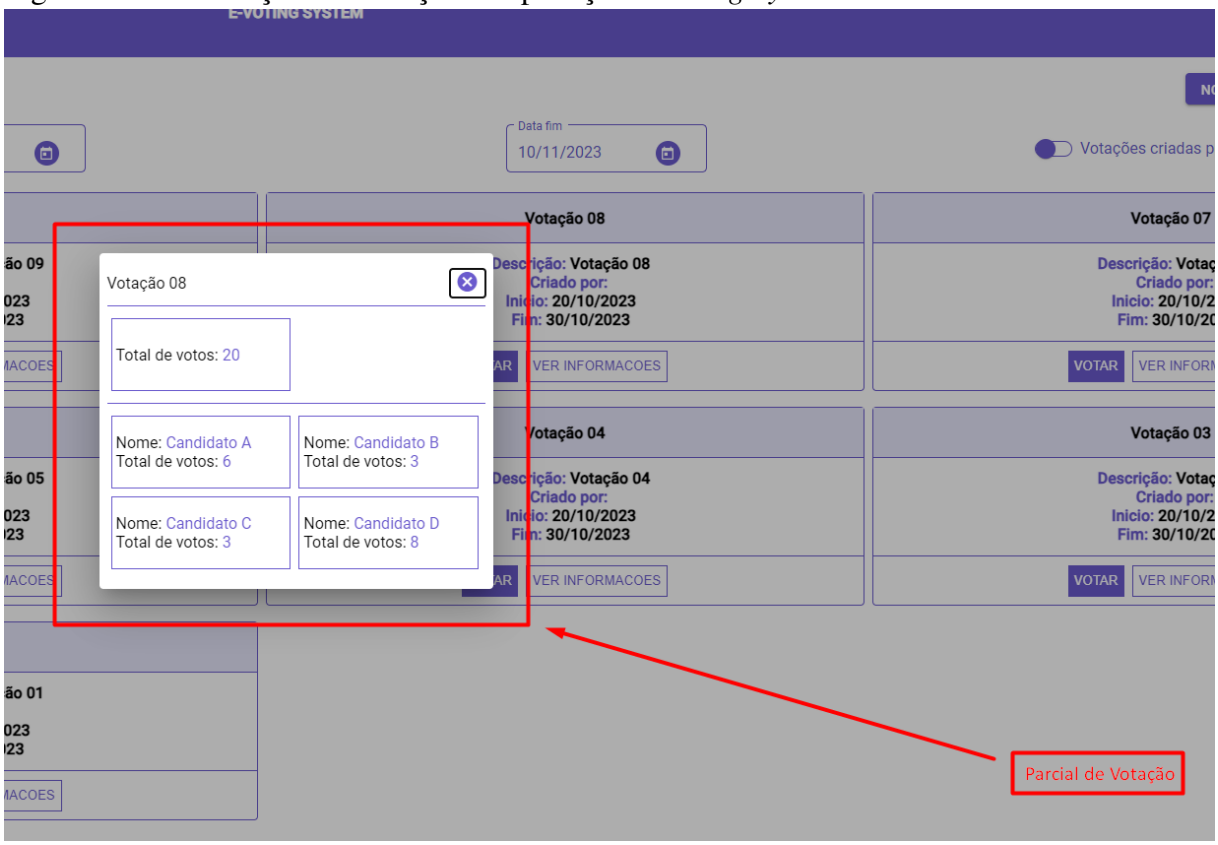


Fonte: Produzido pelo autor.

6.4 Contrato Inteligente

O Contrato Inteligente, como dito anteriormente, são programas autônomos que executam a lógica de negócios na *blockchain* (SZABO, 1994). Nesta validação foram desenvolvidos usando Hyperledger Fabric. Conforme já explicado em uma seção anterior, o Hyperledger Fabric oferece uma arquitetura modular e permite o desenvolvimento de aplicativos *blockchain*

Figura 31 – Informações de votação na aplicação *E-voting System*.



Fonte: Produzido pelo autor.

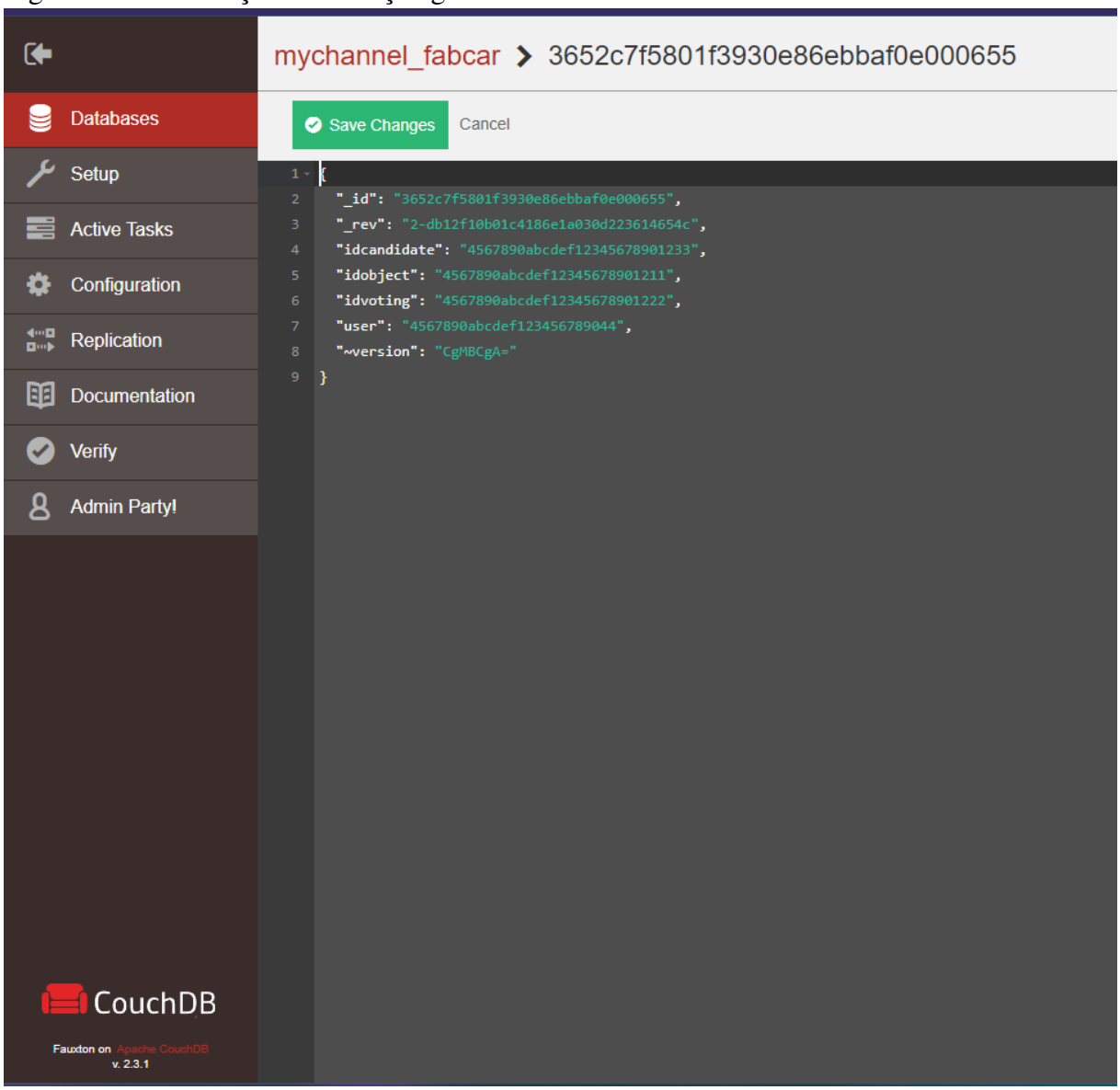
permissionados. A rede Hyperledger Fabric é composta por nós que armazenam uma cópia dos registros da *blockchain*. A configuração da rede, o modelo de consenso e a implantação dos contratos inteligentes são gerenciados pela Hyperledger. O método *chaincodeInvoke()* do contrato inteligente criado para esta solução recebe como parâmetro as informações da votação conforme exportado pelo Sistema de Gerenciamento de Banco de Dados definido. A partir daí o registro das informações já está feito na *blockchain*.

O ciclo de vida da aplicação criada para esta validação se encerra quando é possível visualizar os dados gravados na *blockchain*, o que representa a segunda etapa de auditoria proposta na arquitetura. Por meio do Hyperledger Fabric isto é possível. A figura 32 mostra o registro de um voto gravado na *blockchain*, é possível visualizar por meio do canal aberto proporcionado pela utilização do Hyperledger Fabric.

6.5 Configuração do Experimento

Para validar a arquitetura e por conseguinte a aplicação desenvolvida, dois critérios foram observados: o primeiro é a verificação dos registros para auditoria periódica simplificada

Figura 32 – Informações de votação gravadas na *blockchain*.



Fonte: Produzido pelo autor.

e definitiva estão sendo armazenados e gerados corretamente, de acordo com a interação do usuário; o segundo critério é a certificação de que a rastreabilidade dos votos na *blockchain* é precisa.

Para o primeiro critério, a observação do banco de dados da aplicação, em comparação como os resultados dos votos obtidos na interface do usuário garante mostra que o registro está acontecendo da maneira correta. Para o segundo critério, o registro na *blockchain* também deve ser observado. Considerando que não foi construída uma *API* para realizar integração direta entre o banco de dados da aplicação e a *blockchain* no *framework* Hyperledger, a inserção dos dados na *blockchain* é realizada diretamente no *chaincode* do Hyperledger.

Para haver geração de dados com caráter de aleatoriedade foi criado um questionário

Tabela 3 – Tabela de votações e candidatos possíveis

Votação	Candidatos Possíveis
01	**A, B**
02	**C, D, E**
03	**A, C, D**
04	**B, E**
05	**B, C, D**
06	**A, B, D, E**
07	**C, E**
08	**A, B, C, D**
09	**B, C, E**
10	**A, D, E**

Fonte: Produzido pelo autor.

com dez perguntas e cinco possíveis respostas. Cada pergunta por ter diferentes quantidades de respostas dentre as cinco respostas possíveis. O questionário foi respondido por 20 participantes de diferentes grupos de pessoas no contexto profissional e pessoal do autor deste trabalho. Cada pergunta foi transformada em uma votação dentro do escopo da aplicação, onde cada possível resposta (opção de resposta) é representada por um candidato. A tabela 3 mostra como ficaram as votações definidas a partir do questionário.

O mesmo processo foi realizado em relação aos votos. Os votos realizados nos formulários foram replicados na aplicação, resultando em um total de 199 registros. A interface fornece o resultado de cada votação como é possível visualizar na figura 30. No entanto para o processo de validação é preciso garantir que o registro do voto esteja replicado fielmente na interface gráfica da aplicação e no banco de dados. Dessa forma foi criada uma consulta que recebe como parâmetros o ID da votação e os ID's dos Candidatos e retorna o a quantidade de vezes que esses ID's aparecem nos registros. Dessa forma é possível verificar através do ID da votação o total de votos, e dos ID‘s dos candidatos a quantidade de votos que eles receberam. No código fonte 1 é possível visualizar um exemplo de consulta aos registros do banco de dados.

É estabelecida uma conexão com o MongoDb em um servidor, que neste caso é local. O banco de dados "mydb"é selecionado, em seguida são definidas variáveis para representar ID's de votação e candidatos. O próximo passo é a contagem do número de documentos na lista "votos"através do "idVotacao", depois, conta o número de documentos onde o ID do candidato é igual a "idCandidatoA"e faz o mesmo para "idCandidatoB". Por fim, o resultado é impresso no console, mostrando a quantidade de ocorrências de voto para cada ID, e depois fecha a conexão com o banco de dados.

Código-fonte 1 – Consulta de votos no banco de dados

```
var MongoClient = require('mongodb').MongoClient;
var url = "mongodb://localhost:27017/";
MongoClient.connect(url, function(err, db) {
  if (err) throw err;
  var dbo = db.db("mydb");
  var idVotacao = "IDVotacao";
  var idCandidatoA = "IDCandidatoA";
  var idCandidatoB = "IDCandidatoB";
  dbo.collection("votos").countDocuments({idVotacao:
     idVotacao}, function(err, countVotacao) {
    dbo.collection("votos").countDocuments({idCandidato:
       idCandidatoA}, function(err, countCandidatoA) {
      dbo.collection("votos").countDocuments({idCandidato:
         idCandidatoB}, function(err, countCandidatoB) {
        console.log("IDVotacao ocorre " + countVotacao + "
           vezes.");
        console.log("IDCandidatoA ocorre " +
           countCandidatoA + " vezes.");
        console.log("IDCandidatoB ocorre " +
           countCandidatoB + " vezes.");
        db.close();
      });
    });
  });
});
```

Fonte: Produzido pelo autor.

No código fonte 2 é possível visualizar um exemplo de consulta aos registros na *blockchain*. O código define uma função assíncrona chamada "countVotes"que recebe três ID's como parâmetros. A função configura o caminho para o arquivo de conexão, lê o conteúdo, define o caminho para a carteira e recupera a identidade do usuário "appUser". Em seguida, cria

uma instância do gateway, conecta-se à rede Hyperledger Fabric e obtém o contrato. A função realiza transações de consulta no contrato para obter a contagem de votos para ID's específicos de votação e candidatos. Os resultados são exibidos no console, e mensagens de erro são tratadas se ocorrerem durante a execução. No final, a função é chamada com argumentos específicos ('IDVotacao', 'IDCandidatoA', 'IDCandidatoB').

Código-fonte 2: Consulta de votos na *blockchain*

```
{const { Gateway, Wallets } = require('fabric-network');
const fs = require('fs');
const path = require('path');
async function countVotes(idVotacao, idCandidatoA,
   idCandidatoB) {
    try {
        const ccpPath = path.resolve(__dirname, '..', '..',
            'test-network', 'organizations', '
           peerOrganizations', 'org1.example.com', '
           connection-org1.json');
        const ccp = JSON.parse(fs.readFileSync(ccpPath, '
           utf8'));
        const walletPath = path.join(process.cwd(), 'wallet
           ');
        const wallet = await Wallets.newFileSystemWallet(
           walletPath);
        const identity = await wallet.get('appUser');
        if (!identity) {
            console.log('An identity for the user "appUser"
                does not exist in the wallet');
            console.log('Run the registerUser.js
               application before retrying');
            return;
        }
        const gateway = new Gateway();
        await gateway.connect(ccp, { wallet, identity: '
           appUser', discovery: { enabled: true,
           asLocalhost: true } });
        const network = await gateway.getNetwork('mychannel
           ');
        const contract = network.getContract('fabcar');
```

```
20          const countVotacao = await contract.
               evaluateTransaction('queryVotes', idVotacao);
21          const countCandidatoA = await contract.
               evaluateTransaction('queryVotes', idCandidatoA);
22          const countCandidatoB = await contract.
               evaluateTransaction('queryVotes', idCandidatoB);
23          console.log(`IDVotacao ocorre ${countVotacao} vezes
               .`);
24          console.log(`IDCandidatoA ocorre ${countCandidatoA}
                vezes.`);
25          console.log(`IDCandidatoB ocorre ${countCandidatoB}
                vezes.`);
26      } catch (error) {
27          console.error(`Failed to evaluate transaction: ${
               error}`);
28          process.exit(1);
29      }
30  }
31  countVotes('IDVotacao', 'IDCandidatoA', 'IDCandidatoB');
```

Fonte: Produzido pelo autor.

Tabela 4: Resultados das votações.

Votação	Total de Votos	Vencedor da Votação
01	20	A = 11 votos
02	19	C = 9 votos
03	20	D = 10 votos
04	20	E = 11 votos
05	20	B = 9 votos
06	20	E = 7 votos
07	20	E = 11 votos
08	20	D = 8 votos
09	20	B = 10 votos
10	20	E = 8votos

Fonte: Produzido pelo autor.

6.6 Resultados

Realizando a experimentação espera-se alguns resultados. O primeiro é uma confirmação de que os registros para auditoria estão sendo armazenados corretamente na aplicação. Isso é demonstrado pela correspondência entre os dados exibidos na interface de informações de votação e os registros consultados no banco de dados. Deve-se verificar a coerência e a precisão das informações armazenadas.

Outro resultado esperado é a confirmação da precisão na rastreabilidade dos votos na *blockchain*. Para isto verifica-se que os registros para auditoria periódica simplificada e definitiva estão sendo armazenados e gerados corretamente, de acordo com a interação do usuário.POr meio da visualização da interface de informações da votação, é possível ver todos os dados de cada votação. Ao comparar com os registros contidos no banco de dados, obtidos através de consultas como o exemplo contido no código fonte 1, foi verificado que o comportamento acontece como esperado, o registros são idênticos.

Em relação à certificação de que a rastreabilidade dos votos na *blockchain* é precisa, a confirmação é feita de dois modos. De modo simples, é possível visualizar na interface do Apache CouchDB (FOUNDATION, 2023d) que fica disponível através de configuração do Hyperledger. Já foi observado na imagem 32 o registro de um voto na *blockchain* por meio da visualização da interface do Apache CouchDB. O outro modo é utilizando-se de um consulta como a exemplificada no código fonte 2.

A tabela mostra os resultados obtidos na interface da aplicação, na consulta ao banco de dados e na consulta à *blockchain*.

Os resultados obtidos na observação da aplicação são idênticos aos obtidos na

consulta aos registros do banco de dados. A consulta aos registros da *blockchain* também são idênticos. A análise conjunta desses métodos de verificação oferece uma confirmação abrangente da integridade dos votos. A aplicação cumpre os critérios de auditoria, armazenamento correto dos votos e rastreabilidade na *blockchain*, o que reforça a confiança na precisão e segurança do sistema de *e-voting* baseado em Hyperledger. Esses resultados indicam um processo robusto de verificação e validação, promovendo transparência, segurança e confiabilidade no sistema de votação eletrônica.

Analisando o resultados obtidos com aplicação criada, é possível fazer um paralelo entre esta etapa do trabalho e a etapa de experimentação com *blockchain* contida no capitulo 4. Existe um interseção necessária entre as duas etapas, que é a utilização da tecnologia da platafroma Hyperledger. É possível observar que nestas duas etapas do trabalho são abordados aspectos cruciais da aplicação da tecnologia Hyperledger em contextos distintos, sendo o primeiro voltado para a validação de uma aplicação de votação e o segundo para a análise de desempenho da infraestrutura subjacente. Essa abordagem complementar fornece uma visão abrangente sobre como o Hyperledger é implementado e avaliado em cenários práticos, abordando tanto a funcionalidade específica da aplicação quanto a eficácia operacional da infraestrutura subjacente.

6.7 Análise do *E-voting System* e dos Experimentos com *Blockchain*

A experimentação realizada na plataforma Hyperledger, além dos resultados observados no capítulo 4, traz um panorama do arcabouço de ferramentas de desenvolvimento disponibilizadas pela plataforma. Apesar de o experimento ser em pequena escala, por meio da plataforma Hyperledger é possível criar uma infraestrutura complexa de *blockchain*. No desenvolvimento da experimentação é possível observar que as funções e ferramentas do Hyperledger são altamente configuráveis e que pode ser integradas em ambientes de testes ou ambientes reais. Além disso o *framework* disponibilizado pela plataforma proporciona meios de avaliação das soluções implementadas sem a necessidade de utilização de ferramentas externas para muitas métricas.

O objetivo de um melhor entendimento do Hyperledger Fabric foi alcançado. No entanto, o tamanho da infraestrutura utilizada no experimento traz o risco de que os resultados obtidos possam não ser replicáveis em uma infraestrutura de maior escala. Esta avaliação pode ser considerada superficial para a medição de um sistema *blockchain* como um todo, sob a ótica de diferentes requisitos não funcionais.

Por outro lado os testes de carga realizados permitem observar o comportamento da ferramenta Hyperledger Fabric. A verificação da escalabilidade da infraestrutura configurada na plataforma Hyperledger é um ponto positivo desta experimentação, visto que sistemas de *e-voting* podem ou não ser robustos dependendo do escopo de sua utilização.

Juntando a característica de escalabilidade ao fato de poder ser utilizada sem custo em uma infraestrutura própria, é possível afirmar que a plataforma Hyperledger possui capacidade de ser utilizada em uma abordagem de sistema de *e-voting* utilizando a tecnologia *blockchain*.

6.8 Considerações Sobre a Proposta e Validação

A arquitetura proposta neste trabalho foi projetada a partir da observação do estado da arte sobre sistemas de *e-voting* utilizando a tecnologia *blockchain*. A explicitação de três pontos de auditabilidade é um diferencial em relação aos trabalhos relacionados. O modelo de arquitetura definido dá liberdade de utilização de diferentes plataformas de *blockchain*, uma vez que o algoritmo de consenso utilizado não impacta nas características de auditabilidade.

O modo como está definida, também proporciona que tudo seja implementado em uma infraestrutura própria, o que gera uma economia custos e a possibilidade de aproveitamento de recursos. Isto é essencial para sua utilização no contexto de instituições governamentais e estudantis.

Na validação, todas as partes da arquitetura proposta foram implementadas. É possível fazer uma ligação dos três pontos de auditabilidade com as telas e *features* da aplicação criada. Todas as etapas da implementação da aplicação de validação resultam em registros equivalentes. É possível afirmar que a aplicação implementada valida a arquitetura proposta.

No decorrer do desenvolvimento deste trabalho foram percebidos benefícios da utilização da arquitetura conforme os critérios estabelecidos. Em primeiro lugar a definição da plataforma Hyperledger Fabric para instalação do contrato inteligente, permitiu que fosse utilizada uma infraestrutura gratuita. No decorrer do trabalho a rede *blockchain* emulada tanto na própria máquina do autor, em primeiro momento, quanto em uma máquina virtual comum da plataforma *Google Cloud* (LLC, 2023).Máquina virtual esta que foi instanciada utilizando créditos gratuitos, ou seja, sem nenhum custo financeiro. Além disso a plataforma Hyperledger possui uma robusta documentação, tanto descritiva quando instrutiva.

Outro benefício da arquitetura proposta observado durante a execução do trabalho, é que a simplicidade de sua implementação, permite que seja validada por diferentes tipos de

sistemas de *e-voting*. Além disso o processo de auditoria nos três pontos definidos no trabalho, parte sempre de um processo de conferência simples.

Quanto a dificuldades percebidas, é possível levantar que os processos de configuração de uma *blockchain* no *framework* Hyperledger é extenso. A dificuldade desta configuração também se dá pelo fato de serem necessárias a instalação e configuração de aplicativos externos antes de tratar da *blockchain*. Aplicativos como *docker* (INC, 2023), por exemplo, deve estar instalado e configurado para que se possa instalar e executar o Hyperledger Fabric.

Considerando os resultados consistentes e a confirmação abrangente da integridade dos votos obtidos na aplicação de votação eletrônica baseada em Hyperledger, aliada à análise de desempenho da infraestrutura, é evidente que o trabalho realizado apresenta uma contribuição significativa no campo de sistemas de votação eletrônica. A utilização da tecnologia Hyperledger não apenas valida a segurança e transparência da aplicação de votação, mas também destaca a importância de uma infraestrutura eficiente e escalável para suportar tais sistemas. A interseção entre a validação da aplicação e a análise de desempenho proporciona uma abordagem holística que fortalece a confiança na implementação prática dessa tecnologia em cenários sensíveis, como eleições eletrônicas. Dessa forma, o trabalho não apenas aborda questões técnicas, mas também oferece insights valiosos para o avanço e aprimoramento de sistemas de votação eletrônica baseados em *blockchain*.

6.9 Ameaças à Validade e Limitações da Pesquisa

Limitações e ameaças à validade deste trabalho foram observadas durante a condução deste trabalho. Nesta seção elas serão descritas.

Em relação à revisão sistemática da literatura, uma ameaça a validade é a probabilidade de que trabalhos dentro do escopo desta pesquisa estejam sendo ignorados, caso estejam disponíveis em repositórios que não foram analisados. Outra possível ameaça à validade é o período de busca, durante a produção deste trabalho, algum trabalho relacionado a esta pesquisa pode ser publicado sem que seja verificado em tempo hábil.

Tratando-se dos experimentos realizados com a plataforma, que indicam que o Hyperledger é escalável e viável para aplicação da arquitetura proposta, uma possível ameaça à validade é o fato de que a infraestrutura utilizada é limitada a três nós. Apesar de ser atestada a escalabilidade da plataforma, os resultados obtidos no experimento, podem não ser equivalentes aos obtidos quando a infraestrutura for muito maior. O fato de os experimentos não trazerem

comparativos entre o Hyperledger e outras plataformas de *blockchain* e outra ameaça à validade do ponto de vista das plataformas.

Sobre a validação implementada, a principal ameaça à validade é a não implementação de uma API que faça a ligação direta entre a aplicação e a *blockchain*. Como explicado anteriormente, o registro dos dados obtidos pela interação com a aplicação na rede *blockchain* é feito através de métodos no contrato inteligente. Isto pode enfraquecer as características de auditabilidade que são próprias do uso de *blockchain*. Dessa forma levanta-se ainda, que aplicação deveria propiciar a interação diretamente com a plataforma de *blockchain*, possibilitando a utilização em ambiente real e a consequente inserção de um volume de dados muito maior. Sobre o volume de dados, inclusive, dado a baixa quantidade de dados não é possível garantir escalabilidade da plataforma no contexto da aplicação, por isso também não é possível garantir o mesmo comportamento observado nos experimentos quando o volume de dados inserido for muito maior que volume de dados inseridos na experimentação realizada.

Ainda sobre a validação, uma outra ameaça à validade é o fato de que os usuários participantes que geraram as votações não interagiram diretamente com a aplicação. Dessa forma não foi possível validar a aplicação, tampouco a arquitetura, do ponto de vista de usabilidade e confiança no processo de votação. Isto se resolveria com a utilização da aplicação em ambiente real, o que não foi possível realizar de maneira direta.

7 CONCLUSÕES

É possível afirmar que o trabalho proporciona contribuições científicas e tecnológicas. A pesquisa contribui inicialmente para o avanço da fundamentação teórica e definição dos trabalhos relacionados, destacando-se na literatura a crescente produção sobre o tema *e-voting* com o uso da tecnologia *blockchain*. Contudo, é notável a falta de enfoque específico nas características relacionadas à auditoria, assim como a ausência de modelos centrados nos requisitos de auditabilidade.

Outra contribuição do trabalho é uma proposta de arquitetura simples que incorpora um caráter de auditabilidade ao sistema de *e-voting*. Do ponto de vista da aplicabilidade, a arquitetura proposta oferece benefícios, pois sua implementação é simples e prática em ambientes reais. A validação da arquitetura apresenta outra contribuição tecnológica, evidenciada pela criação de uma aplicação web que verifica a viabilidade da arquitetura proposta. Com uma interface amigável, a aplicação possibilita a criação de usuários, a realização de votações e a condução de eleições.

No âmbito tecnológico, destaca-se a contribuição da análise de desempenho realizada com a plataforma Hyperledger, proporcionando uma compreensão mais aprofundada das características dessa plataforma. Isso não apenas auxilia na visão de possibilidades de utilização no escopo da pesquisa, mas também fora desse escopo, pois a plataforma demonstra ser robusta e aplicável.

Por fim, a contribuição científica principal desta pesquisa é a validação da possibilidade de criar um sistema completo de *e-voting* utilizando a tecnologia *blockchain* e a plataforma Hyperledger. O sistema desenvolvido e validado utiliza tecnologia e infraestrutura de baixo ou nenhum custo, tornando-se ideal para ambientes, como eleições estudantis, que possam ter restrições financeiras ou de infraestrutura. Além disso, destaca-se como contribuição científica o reforço das características específicas de auditoria proporcionadas pela arquitetura proposta.

Toda a arquitetura foi definida observando o objetivo geral que é criar uma abordagem para criação de sistemas de *e-voting* auditáveis utilizando a tecnologia *blockchain*, utilizando um ambiente próprio, proporcionado pela plataforma Hyperledger, de modo a ser utilizável em ambientes estudantis e governamentais. Os objetivos específicos também foram observados e alcançados. Pode-se afirmar que um problemas do mundo real foram tratados, uma vez que a arquitetura proposta foi validada trazendo uma sistema perfeitamente utilizável no mundo real. Toda a validação foi realizada sem nenhum custo financeiro, o que proporciona que seja

facilmente replicável por estudantes, instituições, governos. Todos os passo definidos foram seguidos de modo a garantir o cumprimento dos objetivos.

7.1 Publicações Obtidas

Nesta seção são apresentadas breves descrições de trabalhos produzidos em parceria com colegas no período de desenvolvimento desta pesquisa, e que foram submetidos à publicação em conferências e periódicos. Estes trabalhos são fruto de estudos realizados com o objetivo de obter maiores conhecimentos acerca de tecnologias e suas aplicações, e tem foco principalmente na tecnologia *blockchain*, sendo inclusive complementares em muitos aspectos. Existem ainda outros trabalhos em fase de submissão, que não são citados por não terem tido aceitação até o momento. A lista a seguir descreve os trabalhos realizado em grupos de pesquisa onde houve participação no desenvolvimento de trabalho de colegas:

- *Um Estudo Preliminar das Relações entre Características de Blockchain e a Aplicação na Sociedade* (COUTINHO *et al.*, 2020): este trabalho tem como objetivo iniciar os estudos sobre as relações e impactos de *blockchain* sobre a sociedade, seja por beneficiar-se de suas características, seja por aplicações nas mais diversas áreas. Aplicou-se um questionário *online* com pessoas que já conhecem *blockchain* sobre aspectos da sociedade, em seguida fez-se uma análise qualitativa para compreensão do resultado;
- *Uma Análise Inicial sobre a aplicação de Blockchain na Sociedade* (COUTINHO *et al.*, 2021): este trabalho tem como objetivo apresentar um estudo inicial sobre as relações e impactos de *blockchain* na sociedade. É feita uma pesquisa na literatura e um questionário online;
- *Avaliando Custos de Contratos Inteligentes em Aplicações Blockchain por meio de Ambientes de Simulação* (COUTINHO *et al.*, 2020): este trabalho tem como objetivo apresentar uma simulação do uso de contratos inteligentes em um ambiente de *blockchain*, para se ter uma visão do consumo dos recursos financeiros na execução das operações;
- *Analyzing a Blockchain Application for the Educational Domain from the Perspective of a Software Ecosystem* (ABREU *et al.*, 2022): este trabalho apresenta uma discussão sobre uma aplicação de domínio educacional sob a ótica SECO que utiliza recursos de blockchain para tratar certificados de alunos de instituições de ensino superior;

A lista a seguir descreve os trabalhos realizados pelo no decorrer do desenvolvimento do trabalho aqui proposto":

- *Oportunidades de Pesquisa em Blockchain em Tempos de Pandemia* (BEZERRA *et al.*, 2020): o objetivo este trabalho é discutir oportunidades de pesquisa em *blockchain*. Consiste na identificação de oportunidades de pesquisa que em tempos de pandemia possam beneficiar-se de *blockchain* e realização de uma busca geral por trabalhos que ressaltem essas oportunidades;
- *A Performance Analysis of Hyperledger Fabric: A Perspective of the ISO/IEC 25010 Product Quality Model* (BEZERRA *et al.*, 2022): neste trabalho são definidas métricas de medição de qualidade para uma blockchain implementada no hyperledger fabric. Para isso foi utilizado o hyperledger caliper para observar as métricas sob a perspectiva da ISO/IEC 25010.

7.2 Trabalhos Futuros

Existe uma perspectiva de continuação deste trabalho que promete não apenas sanar as ameaças a validade que foram levantadas, como gerar novos trabalhos sejam extensão deste ou que se relacionem com este do ponto de vista de utilização das tecnologias. Alguns trabalhos futuros que pode ser desenvolvidos são enumerados a seguir:

- Implementação de API para conexão direta ente a aplicação e a *blockchain*;
- Aumento do escopo de busca em outro repositórios de busca, realizando uma pesquisa mais ampla de modo a resultar em um *survey*;
- Implementação de de estrutura mais robusta na plataforma *blockchain hyperledger*. Ao invés de emular uma rede completa, construir de fato uma rede completa e robusta, realizar testes de carga observando os parâmetros estabelecidos na ISO/IEC 25010 e outras ISOs que tratam de qualidade e confiabilidade de software;
- Ampliar as *features* da aplicação criada e disponibilizar em um ambiente real por um período determinado a fim de verificar o comportamento da aplicação e as impressões dos usuários em relação ao sistema.

REFERÊNCIAS

ABREU, A. W.; COUTINHO, E. F.; BEZERRA, W.; MAIA, D.; GOMES, A. N.; SANTOS, I. Analyzing a blockchain application for the educational domain from the perspective of a software ecosystem. In: SBC. **Anais do III Workshop sobre as Implicações da Computação na Sociedade**. [S.l.], 2022. p. 85–92.

ABREU, A. W. d. S. **Uma abordagem baseada em blockchain para armazenamento e controle de acesso aos dados de certificados de alunos do ensino superior**. Dissertação (Mestre em Computação) – Universidade Federal do Ceará, Quixadá-CE, 2020.

ABREU, A. W. S.; COUTINHO, E. F.; BEZERRA, C. I. A blockchain-based architecture for query and registration of student degree certificates. In: **Proceedings of the 14th Brazilian Symposium on Software Components, Architectures, and Reuse**. [S.l: s.n], 2020. p. 151–160.

ABUIDRIS, Y.; KUMAR, R.; YANG, T.; ONGINJO, J. Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding. **Etri Journal**, Wiley Online Library, [S.l.], v. 43, n. 2, p. 357–370, 2021.

ACADEMY, B. **Proof of Stake (PoS) and Proof of Work (PoW) Explained**. [S.l: s.n], 2023. Disponível em: https://academy.binance.com/pt/articles/proof-of-work-vs-proof-of-stake. Acesso em: 14 de jun. de 2023.

ADIDA, B. Helios: Web-based open-audit voting. In: **USENIX/ACCURATE Electronic Voting Technology Workshop**. [S.l: s.n], 2008.

AL-MADANI, A. M.; GAIKWAD, A. T.; MAHALE, V.; AHMED, Z. A. Decentralized e-voting system based on smart contract by using blockchain technology. In: IEEE. **2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)**. [S.l.], 2020. p. 176–180.

ALAMMARY, A.; ALHAZMI, S.; ALMASRI, M.; GILLANI, S. Blockchain-based applications in education: A systematic review. **Applied Sciences**, Multidisciplinary Digital Publishing Institute, [S.l.], v. 9, n. 12, p. 2400, 2019.

ALHARBY, M.; MOORSEL, A. V. Blockchain-based smart contracts: A systematic mapping study. **arXiv preprint arXiv:1710.06372**, [S.l.], 2017.

ALNASSER, Y.; GRAY, G. L. An exploratory study of is auditors' cognitive representations of the systems development life cycle (sdlc). **Journal of Information Systems**, [S.l.], v. 33, n. 2, p. 1–24, 2019.

ALSHAMSI, M.; AL-EMRAN, M.; SHAALAN, K. A systematic review on blockchain adoption. **Applied Sciences**, MDPI, [S.l.], v. 12, n. 9, p. 4245, 2022.

ALVI, S. T.; UDDIN, M. N.; ISLAM, L. Digital voting: A blockchain-based e-voting system using biohash and smart contract. In: IEEE. **2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)**. [S.l.], 2020. p. 228–233.

AMPEL, B.; PATTON, M.; CHEN, H. Performance modeling of hyperledger sawtooth blockchain. In: IEEE. **2019 IEEE International Conference on Intelligence and Security Informatics (ISI)**. [S.l.], 2019. p. 59–61.

AMUAIL SHAWN, J. N. D. J. S. **The Blockchain**: A guide for legal and business professionals. [S.l.]: LegalWorks, 2016.

ANDROULAKI, E.; BARGER, A.; BORTNIKOV, V.; CACHIN, C.; CHRISTIDIS, K.; CARO, A. D.; ENYEART, D.; FERRIS, C.; LAVENTMAN, G.; MANEVICH, Y. *et al.* **Hyperledger Fabric**: A distributed operating system for permissioned blockchains. [S.l: s.n], 2018.

ANISIMOV, M. **Hyperledger Performance and Scalability**. [S.l:s.n]: arXiv preprint arXiv:1807.02963, 2018.

ANTONOPOULOS, A. M. **Mastering Bitcoin**: Unlocking digital cryptocurrencies. [S.l.]: O'Reilly Media, 2017. Disponível em: https://github.com/bitcoinbook/bitcoinbook. Acesso em: 10 de ago. de 2022.

BACH, L. M.; MIHALJEVIC, B.; ZAGAR, M. Comparative analysis of blockchain consensus algorithms. IEEE, New York, NY, USA **Conference** [...], 2018. Disponível em: https://ieeexplore.ieee.org/abstract/document/8400278. Acesso em: 10 de ago. de 2022.

BARCELOS, F. A.; MARTINS, J. V. d. L. **Aplicabilidade da blockchain no sistema de eleição departamental da UTFPR campus Ponta Grossa**. Monografia (TCC) – Universidade Tecnológica Federal do Paraná, Ponta Grossa - Paraná, PR, 2020, 2020.

BARNES, A.; BRAKE, C.; PERRY, T. Digital voting with the use of blockchain technology. **Team Plymouth Pioneers-Plymouth University**, [S.l.], 2016.

BENALOH, J.; BYRNE, M.; KORTUM, P.; MCBURNETT, N.; PEREIRA, O.; STARK, P. B.; WALLACH, D. S. Star-vote: A secure, transparent, auditable, and reliable voting system. **arXiv preprint arXiv:1211.1904**, [S.l.], 2012.

BERNARDO, M.; CASADESUS, M.; KARAPETROVIC, S.; HERAS, I. An empirical study on the integration of management system audits. **Journal of Cleaner Production**, Elsevier, [S.l.], v. 18, n. 5, p. 486–495, 2010.

BEZERRA, W. L. B.; GOMES, A. N.; COUTINHO, E. F.; SOUZA, C. P. d.; MAGALHAES, R. P.; VASCONCELOS, D. R. d. A performance analysis of hyperledger fabric: A perspective of the iso/iec 25010 product quality model. In: **Proceedings of the 11th Euro American Conference on Telematics and Information Systems**. [S.l: s.n], 2022. p. 1–8.

BEZERRA, W. L. B.; MAIA, D. J. H.; ABREU, A. W.; COUTINHO, E. F. Oportunidades de pesquisa em blockchain em tempos de pandemia. **Revista Sistemas e Mídias Digitais (RSMD)**, [S.l.], v. 5, n. 1, jul. 2020.

BHARGAVAN, K.; DELIGNAT-LAVAUD, A.; FOURNET, C.; GOLLAMUDI, A.; GONTHIER, G.; KOBEISSI, N. *et al.* Formal verification of smart contracts: Short paper. In: SPRINGER. **International Conference on Principles of Security and Trust**. [S.l.], 2016. p. 528–547.

BHASKAR, N. D.; CHUEN, D. L. K. Bitcoin mining technology. In: **Handbook of digital currency**. [S.l.]: Elsevier, 2015. p. 45–65.

BLOCK.ONE. **EOSIO**. 2023. Disponível em: https://eos.io/. Acesso em: 14 de jun. de 2023.

BOOTH, A.; SUTTON, A.; PAPAIOANNOU, D. **Systematic Approaches to a Successful Literature Review**. [S.l.]: Sage, 2016.

BOSU, A.; IQBAL, A.; SHAHRIYAR, R.; CHAKRABORTY, P. Understanding the motivations, challenges and needs of blockchain software developers: A survey. **Empirical Software Engineering**, Springer, [S.l.], v. 24, n. 4, p. 2636–2673, 2019.

BOTHA, H.; BOON, J. **The information audit**: principles and guidelines. [S.l.]: Walter de Gruyter GmbH & Co. KG, 2003.

BOUCHER, P. N. **What if blockchain technology revolutionised voting?** [S.l.]: EPRS: European Parliamentary Research Service, 2016.

BRONDANI, A. L. **Auditoria de sistemas: teoria e prática**. [S.l.]: Novatec Editora, 2018.

BURGOS, A.; ALCHIERI, E. Um estudo sobre o uso de replicação máquina de estados paralelas na implementação de blockchains. In: XXII WORKSHOP DE TESTES E TOLERÂNCIA A FALHAS. Uberlândia, MG **Anais** [...], 2021. p. 57–70.

BUTERIN, V. **A proof of stake design philosophy**. [S.l: s.n], 2016.

BUTERIN, V. **Ethereum Whitepaper**. 2022. Disponível em: https://ethereum.org/en/whitepaper/. Acesso em: 09 de ago. de 2022.

B.V., E. **Science Direct**. 2023. Disponível em: https://www.sciencedirect.com/. Acesso em: 10 de nov. de 2023.

CACHIN, C. *et al.* Architecture of the hyperledger blockchain fabric. In: CHICAGO, IL. **Workshop on distributed cryptocurrencies and consensus ledgers**. [S.l.], 2016. v. 310, n. 4.

CACHIN, C.; SCHUBERT, S.; VUKOLIĆ, M. Non-determinism in byzantine fault-tolerant replication. **arXiv preprint arXiv:1603.07351**, [S.l.], 2016.

CACHIN, C.; VUKOLIĆ, M. Hyperledger: A permissioned blockchain framework. In: SPRINGER. **Annual International Conference on the Theory and Applications of Cryptographic Techniques**. [S.l.], 2017. p. 1–18.

CADIZ, J. V.; MARISCAL, N. A. M.; CENIZA-CANILLO, A. M. An empirical analysis of using blockchain technology in e-voting systems. In: IEEE. **2021 1st International Conference in Information and Computing Research (iCORE)**. [S.l.], 2021. p. 78–83.

CASTRO, F. A. d. **Auditoria de sistemas de informação**. [S.l.]: Juruá Editora, 2019.

CASTRO, M.; LISKOV, B. *et al.* Practical byzantine fault tolerance. In: **OSDI**. [S.l: s.n], 1999. v. 99, n. 1999, p. 173–186.

CETINKAYA, O.; CETINKAYA, D. Verification and validation issues in electronic voting. **Electronic journal of e-government**, [S.l.], v. 5, n. 2, 2007.

CHAUM, D. L. Untraceable electronic mail, return addresses, and digital pseudonyms. **Communications of the ACM**, ACM New York, NY, USA, [S.l.], v. 24, n. 2, p. 84–90, 1981.

CHEEMA, M. A.; ASHRAF, N.; AFTAB, A.; QURESHI, H. K.; KAZIM, M.; AZAR, A. T. Machine learning with blockchain for secure e-voting system. In: IEEE. **2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)**. [S.l.], 2020. p. 177–182.

CHELLAPPAN, S.; GANESAN, D.; CHELLAPPAN, S.; GANESAN, D. Mongodb features and installation. **MongoDB Recipes: With Data Modeling and Query Building Strategies**, Springer, [S.l.], p. 1–24, 2020.

CHEN, G.; XU, B.; LU, M.; CHEN, N.-S. Exploring blockchain technology and its potential applications for education. **Smart Learning Environments**, SpringerOpen, [S.l.], v. 5, n. 1, p. 1–10, 2018.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. **Ieee Access**, Ieee, [S.l.], v. 4, p. 2292–2303, 2016.

COHN, M. **Succeeding with agile**: Software development using scrum. [S.l.]: Pearson Education, 2010.

CONTRIBUTORS, T. H. C. **Hyperledger Composer Documentation**. 2019. Disponível em: https://hyperledger.github.io/composer/latest/. Acesso em: 15 de jun. de 2023.

CONTRIBUTORS, T. H. F. **Hyperledger Fabric GitHub Repository**. Disponível em: https://github.com/hyperledger/fabric. Acesso em: 15 de jun. de 2023.

CONTRIBUTORS, T. H. F. **Hyperledger Fabric**. 2023. Disponível em: https://www.hyperledger.org/use/fabric. Acesso em: 15 de jun. de 2023.

CONTRIBUTORS, T. H. F. **Hyperledger Fabric Documentation**. 2023. Disponível em: https://hyperledger-fabric.readthedocs.io/. Acesso em: 15 de jun. de 2023.

COUTINHO, E.; BEZERRA, W. B.; MAIA, D. Um estudo preliminar das relações entre características de blockchain e a aplicação na sociedade. In: SBC. **Anais do V Workshop sobre Aspectos Sociais, Humanos e Econômicos de Software**. [S.l.], 2020. p. 116–120.

COUTINHO, E. F.; BEZERRA, W. L. B.; MAIA, D. Uma análise inicial sobre a aplicação de blockchain na sociedade. In: SBC. **Anais do II Workshop sobre as Implicações da Computação na Sociedade**. [S.l.], 2021. p. 45–56.

COUTINHO, E. F.; MAIA, D. J. H.; BEZERRA, W. L. B.; ABREU, A. W. dos S. Avaliando o custo de contratos inteligentes em aplicações blockchain por meio de ambientes de simulação. In: SBC. **Anais do II Workshop em Modelagem e Simulação de Sistemas Intensivos em Software**. [S.l.], 2020. p. 56–65.

CROCKFORD, D. **JSON: The fat-free alternative to XML**. [S.l: s.n], 2006.

DETSCH, A. **Uma arquitetura para incorporação modular de aspectos de segurança em aplicações peer-to-peer.** Dissertação (Mestre em Computação Aplicada) – Universidade do Vale do Rio do Sinos, São Leopoldo, RS, 2005.

DEVALE, A.; KULKARNI, R. A review of expert system in information system audit. **International Journal of Computer Science and Information Technologies (IJCSIT)**, Citeseer, [S.l.], v. 3, n. 5, p. 5172–5175, 2012.

DHILLON, V.; METCALF, D.; HOOPER, M. Blockchain enabled applications. **Apress, Berkeley, CA**, Springer, [S.l.], v. 72, 2017.

DHULAVVAGOL, P. M.; BHAJANTRI, V. H.; TOTAD, S. Blockchain ethereum clients performance analysis considering e-voting application. **Procedia Computer Science**, Elsevier, [S.l.], v. 167, p. 2506–2515, 2020.

DRISCOLL, K.; HALL, B.; PAULITSCH, M.; ZUMSTEG, P.; SIVENCRONA, H. The real byzantine generals. In: IEEE. **The 23rd Digital Avionics Systems Conference (IEEE Cat. No. 04CH37576)**. [S.l.], 2004. v. 2, p. 6–D.

DWORK, C.; GOLDBERG, A.; NAOR, M. The blockchain as a byzantine agreement. **Cryptology ePrint Archive**, [S.l.], v. 2015, p. 1019, 2015.

DWORK, C.; NAOR, M. Pricing via processing or combatting junk mail. In: SPRINGER. **Annual International Cryptology Conference**. [S.l.], 1993. p. 139–147.

ECMA, I. **ECMAScript Language Specification**. 2023. Disponível em: https://www.ecma-international.org/ecma-262/XX.X/. Acesso em: 09 out. 2023.

EGGER, M.; SMITH, G. D.; ALTMAN, D. G. **Systematic Reviews in Health Care**: Meta-analysis in context. [*S. l.*]: John Wiley & Sons, 2008.

ELECTRICAL, I. I. of; ENGINEERS, E. **IEEE Digital Library**. 2023. Disponível em: https://www.ieee.org/. Acesso em: 10 de nov. de 2023.

ETHEREUM.ORG. **Ethereum**. 2023. Disponível em: https://ethereum.org/. Acesso em: 14 de jun. de 2023.

ETHEREUM.ORG. **Proof of Stake**. 2023. Disponível em: https://ethereum.org/pt/developers/docs/consensus-mechanisms/pos/. Acesso em: 15 de jun. de 2023.

FAVERA, E. C. D. **Auditoria de Sistemas: Enfoque Prático**. [S.l.]: Editora Brasport, 2018.

FAWAZ, A.; CHOUMAN, M.; ALAZAB, M.; LIAO, H.; HU, J. Blockchain-based e-voting system: A systematic review. **IEEE Access**, IEEE, [S.l.], v. 6, p. 11580–11592, 2018.

FEENEY, L. M.; MACCARTHY, B. L. Auditability requirements for e-voting systems. In: IEEE. **2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)**. [S.l.], 2019. p. 165–169.

FOUNDATION, C. **Cardano**. 2023. Disponível em: https://www.cardano.org/. Acesso em: 14 de jun. de 2023.

FOUNDATION, H. **Hyperledger**. 2023. Disponível em: https://www.hyperledger.org/. Acesso em: 14 de jun. de 2023.

FOUNDATION, S. D. **Stellar**. 2023. Disponível em: https://www.stellar.org/. Acesso em: 14 de jun. de 2023.

FOUNDATION, T. A. S. **Apache CouchDB**. 2023. Disponível em: https://couchdb.apache.org/. Acesso em: 10 de nov. de 2023.

FOUNDATION, T. L. **Hyperledger Composer Retirement Announcement**. Disponível em: https://www.hyperledger.org/blog/2019/08/30/hyperledger-composer-retirement. Acesso em: 15 de jun. de 2023.

FOUNDATION, T. L. **Hyperledger Caliper**. 2021. Disponível em: https://www.hyperledger.org/use/caliper. Acesso em: 15 de jun. de 2023.

FUJIOKA, A.; OKAMOTO, T.; OHTA, K. A practical secret voting scheme for large scale elections. In: SPRINGER. **International Workshop on the Theory and Application of Cryptographic Techniques**. [S.l.], 1992. p. 244–251.

GAO, S.; ZHENG, D.; GUO, R.; JING, C.; HU, C. An anti-quantum e-voting protocol in blockchain with audit function. **IEEE Access**, IEEE, [S.l.], v. 7, p. 115304–115316, 2019.

GOOGLE. **Angular Documentation**. Disponível em: https://angular.io/docs. Acesso em: 09 out. 2023.

GOYAL, M.; KUMAR, A. Sustainable e-infrastructure for blockchain-based voting system. **Digital Cities Roadmap: IoT-Based Architecture and Sustainable Buildings**, Wiley Online Library, [S.l.], p. 221–251, 2021.

GREVE, F.; SAMPAIO, L.; ABIJAUDE, J.; COUTINHO, A. A.; BRITO, I.; QUEIROZ, S. Blockchain e a revolução do consenso sob demanda. In: MINICURSOS DO SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS. Porto Alegre, RS **Simpósio** [...]: Sociedade Brasileira de Computação, 2018.

GUPTA, S.; GUPTA, A.; PANDYA, I. Y.; BHATT, A.; MEHTA, K. End to end secure e-voting using blockchain & quantum key distribution. **Materials Today: Proceedings**, Elsevier, [S.l.], 2021.

HALL, J. A. **Information Technology Audit and Assurance**. [S.l.]: Cengage Learning, 2020. 537-580 p.

HASSANI, M.; AZMOON, H. Enhancing the security of e-voting systems using blockchain technology: A review. In: IEEE. **2019 1st International Conference on Computer Science and Engineering (UBMK)**. [*S. l.*], 2019. p. 421–426.

HIGGINS, J. P. T.; GREEN, S. **Systematic Reviews and Meta-Analysis**: A step-by-step guide. [*S. l.*]: Wiley, 2019.

HLADKÁ, E.; HERCIG, T. E-voting systems: A comprehensive literature review. In: SPRINGER. **EAI/Springer Innovations in Communication and Computing**. [S.l.], 2020. p. 149–163.

HOSSAIN, S. S.; ARANI, S. A.; RAHMAN, M. T.; BHUIYAN, T.; ALAM, D.; ZAMAN, M. E-voting system using blockchain technology. In: INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY (IRJET). **Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications**. [S.l.], 2019. p. 113–117.

HU, Q.; HARTONO, E.; CAI, L. A. The impact of the timing of it audits on financial reporting quality: Evidence from audit fees and financial misstatements. **International Journal of Accounting Information Systems**, [S.l.], v. 35, p. 100410, 2019.

HYPERLEDGER. **Configuring and operating a Raft ordering service**. [S.l: s.n], 2023. Disponível em: https://hyperledger-fabric.readthedocs.io/en/latest/raft_configuration.html. Acesso em: 10 de nov. de 2023.

INC, D. **Docker**. 2023. Disponível em: https://www.docker.com/. Acesso em: 10 de nov. de 2023.

ISHMAEV, G. Blockchain technology as an institution of property. **Metaphilosophy**, [S.l.], v. 48, n. 5, p. 666–686, 2017.

ISMAIL, A.; TOOHEY, M.; LEE, Y. C.; DONG, Z.; ZOMAYA, A. Y. Cost and performance analysis on decentralized file systems for blockchain-based applications: State-of-the-art report. In: IEEE. **2022 IEEE International Conference on Blockchain (Blockchain)**. [S.l.], 2022. p. 230–237.

ISO/IEC. **ISO-IEC 25010**: 2011 systems and software engineering-systems and software quality requirements and evaluation (square)-system and software quality models. [S.l.]: ISO, 2011.

JAKOBSSON, M.; JUELS, A. Proofs of work and bread pudding protocols. In: **Secure information networks**. [S.l.]: Springer, 1999. p. 258–272.

JOSELLI, M. Blockchain e games. **SBGAMES**, [S.l.], v. 17, p. 1–11, 2018.

KAHANI, M. Experiencing small-scale e-democracy in iran. **The Electronic Journal of Information Systems in Developing Countries**, Wiley Online Library, [S.l.], v. 22, n. 1, p. 1–9, 2005.

KAKAR, Z.; LEE, M.; KIM, D. **Blockchain-based secure electronic voting system**. [S.l: s.n], 2018. 2947 p.

KAMIENSKI, C.; SOUTO, E.; ROCHA, J.; DOMINGUES, M.; CALLADO, A.; SADOK, D. Colaboraçao na internet e a tecnologia peer-to-peer. In: XXV CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO–SBC2005. São Leopoldo, RS **Proceedings** [...], 2005. v. 25.

KAPLAN, J. M. **Audit Considerations for Information Systems**. [S.l.]: CRC Press, 2018. 177-188 p.

KARAPETROVIC, S.; WILLBORN, W. Audit system: concepts and practices. **Total Quality Management**, Taylor & Francis, [S.l.], v. 12, n. 1, p. 13–28, 2001.

KERN, A.; MAUTHE, A. Blockchain for electronic voting: A survey. **IEEE Access**, IEEE, [S.l.], v. 7, p. 17470–17482, 2019.

KHAN, K. M.; ARSHAD, J.; KHAN, M. M. Investigating performance constraints for blockchain based secure e-voting system. **Future Generation Computer Systems**, Elsevier, [S.l.], v. 105, p. 13–26, 2020.

KHAN, K. M.; ARSHAD, J.; KHAN, M. M. Empirical analysis of transaction malleability within blockchain-based e-voting. **Computers & Security**, Elsevier, [S.l.], v. 100, p. 102081, 2021.

KILLER, C.; RODRIGUES, B.; MATILE, R.; SCHEID, E.; STILLER, B. Design and implementation of cast-as-intended verifiability for a blockchain-based voting system. In: **Proceedings of the 35th Annual ACM Symposium on Applied Computing**. [S.l.]: [ACM Digital Library], 2020. p. 286–293.

KING, S.; NADAL, S. **PPCoin**: Peer-to-peer crypto-currency with proof-of-stake. [S.l: s.n], 2012. Disponível em: https://github.com/ppcoin/ppcoin/wiki/PPCoin-paper. Acesso em: 10 de ago. de 2022.

KITCHENHAM, B.; CHARTERS, S. **Guidelines for performing systematic literature reviews in software engineering**. [S.l.]: Citeseer, 2007.

KOLVART, M.; POOLA, M.; RULL, A. Smart contracts. In: **The Future of Law and etechnologies**. [S.l.]: Springer, 2016. p. 133–147.

KSHETRI, N.; VOAS, J.; PARK, J. H. Blockchain-enabled e-voting. **IT Professional**, IEEE, [S.l.], v. 20, n. 3, p. 30–37, 2018.

LARIMER, D. **Delegated Proof-of-Stake (DPoS)**. [S.l.]: BitShares Blog, 2014.

LARIMER, D. **A New Kind of Blockchain: Delegated Proof of Stake**. [S.l.]: BitShares Blog, 2014.

LEWIS, A. **The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them**. [S.l.]: Mango Media Inc., 2018.

LI, H.; LI, Y.; YU, Y.; WANG, B.; CHEN, K. A blockchain-based traceable self-tallying e-voting protocol in ai era. **IEEE Transactions on Network Science and Engineering**, IEEE, [S.l.], v. 8, n. 2, p. 1019–1032, 2020.

LI, X.; JIANG, P.; CHEN, T.; LUO, X.; WEN, Q. A survey on the security of blockchain systems. **Future Generation Computer Systems**, Elsevier, [S.l.], v. 107, p. 841–853, 2020.

LLC, G. **Google Cloud Platform**. 2023. Disponível em: https://cloud.google.com/. Acesso em: 10 de nov. de 2023.

LTD., C. **Ubuntu**. 2023. Disponível em: https://ubuntu.com/. Acesso em: 14 de jun. de 2023.

LUCAS, R. A. F.; ANDREA, C. M. **A regulamentação das criptomoedas como meio garantidor de segurança jurídica**. [S.l: s.n], 2019.

MACHINERY, A. for C. **ACM Digital Library**. 2023. Disponível em: https://dl.acm.org/. Acesso em: 10 de nov. de 2023.

MARQUES, J. R.; COSTA, C. Blockchain as a solution for secure and transparent e-voting systems. In: SCITEPRESS-SCIENCE AND TECHNOLOGY PUBLICATIONS. **Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering**. [S.l.], 2019. p. 317–324.

MATSUMINE, V. S. M. **Uma implementação do esquema de multi-assinaturas MuSig no cenário m-de-n com árvores de Merkle e suas aplicações ao bitcoin**. Monografia (TCC) – Universidade de Brasília, Brasília, DF, 2021, 2019.

MOHANRAJ, G.; GOPI, S.; SUNDARAM, S. Blockchain based secure e-voting system with auditability. In: IEEE. **2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)**. [S.l.], 2020. p. 413–417.

MONGODB, INC. **MongoDB Documentation**. [S.l.]. Disponível em: https://docs.mongodb.com/. Acesso em: 09 out. 2023.

MORAES, C. d. **Auditoria de Sistemas de Informação**. [S.l.]: Elsevier Brasil, 2016.

MYAGMAR, S.; SHARMA, R. Blockchain-based e-voting system for secure and auditable elections. In: IEEE. **2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)**. [S.l.], 2020. p. 1–6.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, [S.l.], p. 21260, 2008.

NAKIP, M.; GÜNDÜZ, D. Energy efficiency in blockchain systems. In: IEEE. **2018 26th Signal Processing and Communications Applications Conference (SIU)**. [S.l.], 2018. p. 1–4.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. Bitcoin and cryptocurrency technologies: a comprehensive introduction. **Princeton University Press**, [S.l.], 2016.

NG, I. C.; PARTRIDGE, C. Blockchain for e-voting: A systematic literature review. **Government Information Quarterly**, Elsevier, [S.l.], v. 37, n. 1, p. 101436, 2020.

NIWA, H.; MENDES, C. Sistema de voto eletrônico utilizando a blockchain. **Cadernos do IME-Série Informática**, [S.l.], v. 43, n. 2, p. 55–69, 2019.

Node.js Foundation. **Node.js Documentation**. Disponível em: https://nodejs.org/en/docs/. Acesso em: 09 out. 2023.

NOFER, M.; GOMBER, P.; HINZ, O.; SCHIERECK, D. Blockchain. **Business & Information Systems Engineering**, [S.l.], v. 59, n. 3, p. 183–187, Jun 2017.

OLIVEIRA, E. d. **Auditoria de Sistemas: Uma Abordagem Prática**. [S.l.]: Érica, 2017.

OLIVEIRA, R. L. B. G. de; OLIVEIRA, J. V. M. de. A democracia como direito fundamental do ser humano. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, [S.l.], v. 16, n. 16, 2020.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital [Revista online]**, [S.l.], v. 31, p. 11–15, 2012.

ONGARO, D.; OUSTERHOUT, J. In search of an understandable consensus algorithm. In: USENIX THE ADVANCED COMPUTING SYSTEMS ASSOCIATION. **2014 USENIX annual technical conference (USENIX ATC 14)**. [S.l.], 2014. p. 305–319.

ONGARO, D.; OUSTERHOUT, J. The raft consensus algorithm. **Lecture Notes CS**, [S.l.], v. 190, p. 2022, 2015.

PARSIFAL. **Parsifal: An online tool designed to support researchers to perform systematic literature reviews.** 2022. Disponível em: https://parsif.al/. Acesso em: 01-06-2022.

PEDERSEN, A. B.; RISIUS, M.; BECK, R. A ten-step decision path to determine when to use blockchain technologies. **MIS Quarterly Executive**, Indiana University, [S.l.], v. 18, n. 2, p. 99–115, 2019.

PRAMULIA, D.; ANGGOROJATI, B. Implementation and evaluation of blockchain based e-voting system with ethereum and metamask. In: IEEE. **2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)**. [S.l.], 2020. p. 18–23.

PROJECT, B. **Bitcoin**. 2023. Disponível em: https://bitcoin.org/. Acesso em: 14 de jun. de 2023.

QU, W.; WU, L.; WANG, W.; LIU, Z.; WANG, H. A electronic voting protocol based on blockchain and homomorphic signcryption. **Concurrency and Computation: Practice and Experience**, Wiley Online Library, [S.l.], p. e5817, 2020.

R3. **Corda**. 2023. Disponível em: https://www.corda.net/. Acesso em: 14 de jun. de 2023.

RATHEE, G.; IQBAL, R.; WAQAR, O.; BASHIR, A. K. On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities. **IEEE Access**, IEEE, [S.l.], v. 9, p. 34165–34176, 2021.

RIFI, N.; RACHKIDI, E.; AGOULMINE, N.; TAHER, N. C. Towards using blockchain technology for ehealth data access management. In: IEEE. **2017 fourth international conference on advances in biomedical engineering (ICABME)**. [S.l.], 2017. p. 1–4.

ROCHA, J.; DOMINGUES, M.; CALLADO, A.; SOUTO, E.; SILVESTRE, G.; KAMIENSKI, C.; SADOK, D. Peer-to-peer: Computaçao colaborativa na internet. In: MINICURSOS DO XXII SIMPOSIO BRASILEIRO DE REDES DE COMPUTADORES (SBRC 2004). Gramado, RS **Proceedings** [...], 2004.

ROSASOORIA, Y.; SAON, S.; ISA, M. A. M.; YAMAGUCHI, S.; AHMADON, M. A. *et al.* E-voting on blockchain using solidity language. In: IEEE. **2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE)**. [S.l.], 2020. p. 1–6.

SEGUNDO, P. R. S. **Auditoria de sistemas e tecnologia da informação**. [S.l.]: Editora Atlas, 2018.

SENGUPTA, E.; NAGPAL, R.; MEHROTRA, D.; SRIVASTAVA, G. Problock: a novel approach for fake news detection. **Cluster Computing**, Springer, [S.l.], v. 24, p. 3779–3795, 2021.

SHARPLES, M.; DOMINGUE, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In: SPRINGER. **Adaptive and Adaptable Learning: 11th European Conference on Technology Enhanced Learning**. [S.l.], 2016. p. 490–496.

SHRESTHA, R.; CHANG, V.; GHIMIRE, L. Blockchain-based e-voting system: A survey and an application of consensus algorithm. **Journal of Grid Computing**, Springer, [S.l.], v. 16, n. 4, p. 565–583, 2018.

SILVA, J. C.; OLIVEIRA, P.; SOUZA, R. **Auditoria de Sistemas de Voto Eletrônico**: Estudo de caso no brasil. [S.l.], 2021.

SILVA, P. S. F. d. **Auditoria de sistemas de informação**. [S.l.]: Atlas, 2018.

SILVA, R. A. C. d. **Auditoria de Sistemas e Governança de TI**. [S.l.]: Brasport, 2017.

SINGH, A.; PARIZI, R. M.; ZHANG, Q.; CHOO, K.-K. R.; DEHGHANTANHA, A. Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. **Computers & Security**, [S.l.], v. 88, p. 101654, 2020.

SINGH, R. K.; CHHABRA, M. Evolution of it auditing: A comparative study. **Journal of King Saud University-Computer and Information Sciences**, [S.l.], v. 30, n. 4, p. 430–439, 2018.

SONS, I. J. W. . **Wiley Online Library**. 2023. Disponível em: https://onlinelibrary.wiley.com/. Acesso em: 10 de nov. de 2023.

SOUSA, T. M. P. d. **Votechain, uma solução mais segura, acessível e inovadora para as eleições, implementada com a tecnologia Blockchain**. Dissertação (B.S. thesis) – Universidade Federal do Rio Grande do Norte, 2019.

SPRINGER. **Springer**. 2023. Disponível em: https://www.springer.com/br. Acesso em: 10 de nov. de 2023.

STUMPF, F. P.; BECK, R.; ABECK, S. Blockchain technology for secure and auditable voting systems. In: SCITEPRESS-SCIENCE AND TECHNOLOGY PUBLICATIONS. **2018 15th International Joint Conference on e-Business and Telecommunications (ICETE)**. [S.l.], 2018. p. 29–40.

SUYITNO, D.; ALADHIRUS, B. R.; WARDHANI, R. W. Design and implementation of smart card based secure key storage the blockchain e-voting application. In: IEEE. **2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)**. [S.l.], 2020. p. 259–264.

SWAN, M. **Blockchain**: Blueprint for a new economy. [S.l.]: "O'Reilly Media, Inc.", 2015.

SZABO, N. **Smart Contracts**. 1994. Disponível em: http://bit.ly/2Yc9vjb. Acesso em: 21 mar. 2022.

TEAM, N. **NEO**. 2023. Disponível em: https://neo.org/. Acesso em: 14 de jun. de 2023.

TEZOS. **Tezos**: aself-amendingcrypto-ledger. 2023. Disponível em: https://tezos.com/. Acesso em: 14 de jun. de 2023.

THAKKAR, P.; NATHAN, S.; VISWANATHAN, B. Performance benchmarking and optimizing hyperledger fabric blockchain platform. In: IEEE. **2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)**. [S.l.], 2018. p. 264–276.

TSE. **Missões de Observação Eleitoral no Brasil**. 2021. Disponível em: https://www.tse.jus.br/o-tse/observacao-eleitoral/no-brasil. Acesso em: 10 jun. 2022.

TSE. **Relatório de Segurança do Teste Público de Segurança (TPS) das Urnas Eletrônicas**. 2021. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/relatorios-de-seguranca/relatorios-de-seguranca-das-urnas-eletronicas. Acesso em: 10 jun. 2022.

TSE. **Teste Público de Segurança das Urnas Eletrônicas**. 2021. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/teste-publico-de-seguranca. Acesso em: 10 jun. 2022.

VALENTE, M. T. Engenharia de software moderna. **Princípios e Práticas para Desenvolvimento de Software com Produtividade**, [S.l.], v. 1, p. 24, 2020.

VIANA, C.; BRANDAO, A.; DIAS, D.; CASTELLANO, G.; GUIMARAES, M. de P. Blockchain para gerenciamento de prontuários eletrônicos. **Revista ibérica de sistemas e tecnologias de informação**, Associação Ibérica de Sistemas e Tecnologias de Informacao, [S.l.], n. E28, p. 177–187, 2020.

WANG, K.; ZHANG, Y.; CHANG, E. A conceptual model for blockchain-based auditing information system. In: **Proceedings of the 2020 2nd International Electronics Communication Conference**. [*S. l.*]: ACM Digital Library, 2020. p. 101–107.

WANG, K.-H.; MONDAL, S. K.; CHAN, K.; XIE, X. A review of contemporary e-voting: Requirements, technology, systems and usability. **Data Science and Pattern Recognition**, [S.l.], v. 1, n. 1, p. 31–47, 2017.

WATANAVISIT, S. T.; VORAKULPIPAT, C. Learning citizenship in practice with schoolvote system: A participatory innovation of blockchain e-voting system for schools in thailand. **Proceedings of the 2020 9th International Conference on Educational and Information Technology**, ACM Digital Library, [S.l.], p. 254–258, 2020.

XIE, J.; TANG, H.; HUANG, T.; YU, F. R.; XIE, R.; LIU, J.; LIU, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. **IEEE Communications Surveys & Tutorials**, IEEE, [S.l.], v. 21, n. 3, p. 2794–2830, 2019.

XIONG, Y.; LIU, Y.; ZOU, D.; LU, R. Secure and auditable e-voting system based on blockchain. In: IEEE. **Proceedings of the 19th International Symposium on Parallel and Distributed Computing (ISPDC)**. [S.l.], 2020. p. 1–8.

XU, X.; WEBER, I.; STAPLES, M.; ZHU, L.; BOSCH, J.; BASS, L.; PAUTASSO, C.; RIMBA, P. A taxonomy of blockchain-based systems for architecture design. **2017 IEEE International Conference on Software Architecture (ICSA)**, IEEE, New York, NY, USA, p. 243–252, 2017.

XU, Y.; ZHANG, C.; WANG, G.; QIN, Z.; ZENG, Q. A blockchain-enabled deduplicatable data auditing mechanism for network storage services. **IEEE Transactions on Emerging Topics in Computing**, IEEE, [S.l.], 2020.

ZENG, W.; WANG, J.; YANG, J.; LIN, X. An e-voting system based on consortium blockchain and smart contract. **Concurrency and Computation: Practice and Experience**, Wiley Online Library, [S.l.], v. 33, n. 15, p. e6369, 2021.

ZHANG, S.; LI, K.; CAO, Z. Consensus algorithms in blockchain: A survey. **Journal of Computer Science and Technology**, [S.l.], v. 34, n. 1, p. 185–214, 2019.

ZHENG, Z.; XIE, S.; DAI, H.-N.; CHEN, X.; WANG, H. **Blockchain challenges and opportunities: A survey**. [S.l.], 2018. v. 14, n. 4, 352–375 p. Disponível em: https://allquantor.at/blockchainbib/pdf/zheng2018blockchain.pdf. Acesso em: 10 de ago. de 2022.