UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
SISTEMAS DE INFORMAÇÃO

Bruno Daniel Elias

Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino

Florianópolis
2023

Bruno Daniel Elias

Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino

Trabalho de Conclusão de Curso submetido ao Curso de Graduação em Sistemas de Informação do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito para obtenção do título de Bacharel em Sistemas de Informação.
Orientador: Lucas Machado da Palma, Me.
Coorientador: Prof. Jean Everson Martina, Dr.

Florianópolis
2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Elias, Bruno Daniel
Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino / Bruno Daniel Elias ; orientador, Lucas Machado da Palma, coorientador, Jean Everson Martina, 2023.
70 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Tecnológico, Graduação em Sistemas de Informação, Florianópolis, 2023.

Inclui referências.

1. Sistemas de Informação. 2. Blockchain. 3. Autenticação. I. da Palma, Lucas Machado. II. Martina, Jean Everson. III. Universidade Federal de Santa Catarina. Graduação em Sistemas de Informação. IV. Título.

Bruno Daniel Elias

Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo curso de Graduação em Sistemas de Informação.

Florianópolis, 2023.

Prof. Álvaro Junio Pereira Franco, Dr.
Coordenador do Curso

Banca Examinadora:

Lucas Machado da Palma, Me.
Orientador
Universidade Federal de Santa Catarina

Prof. Jean Everson Martina, Dr.
Avaliador
Universidade Federal de Santa Catarina

Gabriel Estevam de Oliveira, Me.
Avaliador
Universidade Federal de Santa Catarina

Johann Westphall, Me.
Avaliador
Universidade Federal de Santa Catarina

Este trabalho é dedicado à todos que me apoiaram durante minha trajetória e nunca duvidaram da minha capacidade de superar todos os desafios.

RESUMO

Atualmente, o Ministério da Educação (MEC) é responsável por autenticar cada processo executado pelas instituições de ensino no Brasil. No entanto, surge uma oportunidade de descentralizar essa responsabilidade, permitindo que as universidades participantes autentiquem e aprovem os processos com base nas regras definidas pelo MEC. A tecnologia Hyperledger Fabric é apresentada como uma solução promissora para alcançar essa descentralização. Com base nessa proposta, o MEC iniciou um projeto em parceria com o Laboratório de Segurança em Computação (LABSEC) da Universidade Federal de Santa Catarina (UFSC). O objetivo é desenvolver um modelo que utilize blockchain e contratos inteligentes no registro de instituições de ensino superior. No entanto, há um problema a ser abordado: a autenticação e identificação dos estudantes na rede. Para resolver essa questão, o presente trabalho propõe a criação de um protótipo de interface gráfica web que permita aos estudantes se autenticarem e utilizarem o sistema desenvolvido pelo LABSEC. O protótipo deve ser acessível em qualquer máquina com um navegador e conexão à internet. Além disso, o meio de autenticação utilizado será o gov.br, que já está integrado a várias tecnologias no Brasil, para autenticar e identificar os estudantes que desejam acessar a rede blockchain. A fim de facilitar o processo e fornecer uma melhor experiência ao usuário, a interface gráfica foi desenvolvida utilizando o framework ReactJS seguindo o Design System do Governo Brasileiro. Após a coleta e análise dos dados, foi possível calcular a média e o intervalo das notas obtidas no questionário SUS (System Usability Scale). A média do SUS Score foi de aproximadamente 89 pontos, indicando uma boa avaliação da usabilidade da aplicação. Esse resultado reflete a percepção positiva dos participantes em relação à facilidade de uso, eficiência e satisfação geral com a autenticação na rede Blockchain via gov.br e a interface gráfica da aplicação. A análise do intervalo das notas mostrou uma variação de 12,5 pontos, indo de 82,5 a 95 pontos. Essa variação indica que, embora a avaliação geral seja positiva, houve diferenças na percepção dos participantes. Essas diferenças podem ser atribuídas a diversos fatores, como familiaridade com a autenticação do gov.br, experiência prévia com interfaces similares e preferências individuais.

Palavras-chave: Autenticação. Blockchain. Estudantes. Ministério da Educação.

ABSTRACT

Currently, the Ministry of Education (MEC) is responsible for authenticating each process performed by educational institutions in Brazil. However, an opportunity arises to decentralize this responsibility, allowing the participating universities to authenticate and approve the processes based on the rules defined by the MEC. Hyperledger Fabric technology is presented as a promising solution to achieve this decentralization. Based on this proposal, MEC started a project in partnership with the Computer Security Laboratory (LABSEC) of the Federal University of Santa Catarina (UFSC). The objective is to develop a model that uses blockchain and smart contracts in the registration of higher education institutions. However, there is a problem to be addressed: the authentication and identification of students on the network. To resolve this issue, the present work proposes the creation of a web graphical interface prototype that allows students to authenticate themselves and use the system developed by LABSEC. The prototype must be accessible on any machine with a browser and internet connection. In addition, the means of authentication used will be gov.br, which is already integrated with various technologies in Brazil, to authenticate and identify students who wish to access the blockchain network. In order to facilitate the process and provide a better user experience, the graphical interface was developed using the ReactJS framework following the Design System of the Brazilian Government. After data collection and analysis, it was possible to calculate the mean and range of scores obtained in the SUS (System Usability Scale) questionnaire. The SUS Score mean was approximately 89 points, indicating a good assessment of the application's usability. This result reflects the positive perception of the participants regarding the ease of use, efficiency, and general satisfaction with authentication on the Blockchain network via gov.br and the application's graphical interface. The analysis of the range of scores showed a variation of 12.5 points, ranging from 82.5 to 95 points. This variation indicates that, although the general evaluation is positive, there were differences in the participants' perceptions. These differences can be attributed to several factors, such as familiarity with gov.br authentication, previous experience with similar interfaces, and individual preferences.

Keywords: Authentication. Blockchain. Students. Ministry of Education.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O termo Blockchain foi introduzido ao mundo no artigo acadêmico *Bitcoin: A peer-to-peer to electronic cash system* (NAKAMOTO, 2008). O artigo apresentou as falhas que os modelos baseados em confiança possuíam mesmo funcionando adequadamente para realizar transações. Além dessas falhas, o autor afirma que a dependência de um terceiro para mediar os problemas que podem vir a ocorrer durante uma transação faz com que aumente os gastos para que essa ação seja realizada.

Diante disso, segundo Nakamoto (2008), o ideal para um sistema eletrônico de transações é uma criptografia baseada em comprovação e não em confiança. Isso permite que duas partes possam realizar transações entre elas sem a necessidade de uma terceira entidade envolvida. Com isso, surge o *Bitcoin*, primeira moeda inteiramente digital utilizada para realizar transações, utilizando assinatura digital, hash e timestamp em conjunto com o protocolo de consenso, para resolver a maior parte dos problemas existentes em um modelo baseado em confiança. Após isso, as tecnologias baseadas em blockchain entraram em ascensão, sendo consideradas uma revolução no quesito financeiro e tecnológico. Essa tecnologia combina os registros de transações em cadeias de blocos em uma rede. Uma rede blockchain pode ser utilizada para prestação de serviços governamentais, facilitando o compartilhamento de informações e a coordenação de processos entre os órgãos do governo. Embora o conteúdo da maioria dos registros governamentais seja público, nesta rede hipotética haveria uma certa complexidade em relação à confidencialidade e privacidade dos dados.

Com base nesses aspectos, diversas redes continuaram surgindo para atender as demandas que apareciam. Entre elas, a rede Ethereum (ETHEREUM, 2014) se destacou, pois surgiu com a ideia de ser muito mais do que um sistema de pagamentos ou apenas uma outra moeda digital. Ela foi desenvolvida para ser uma plataforma descentralizada que consegue executar contratos inteligentes sem ter a interferência de terceiros, isso aumentou a flexibilidade e a funcionalidade de diversos programas que utilizavam tecnologias blockchain. Porém, mesmo com todas essas vantagens, o fato de não ser uma rede blockchain permissionada faz com que muitas empresas não utilizem este tipo de tecnologia por medo da falta de privacidade ou pelo fato de não cobrir o caso de uso desejado.

Para resolver os problemas de confidencialidade e privacidade dos dados, além de aumentar a gama de casos de usos que podem ser atendido pela tecnologia blockchain, surgiu a plataforma Hyperledger Fabric (Hyperledger Foundation, 2020). O Hyperledger Fabric é uma plataforma permissionada e privada que utiliza contratos inteligentes escritos em linguagens atualmente utilizadas pela maioria das empresas, que viram nessa plataforma a possibilidade de entrar finalmente no mundo da blockchain. Isso porque ela tornou possível que empresas privadas e até mesmo públicas pudessem utilizar a rede dentro do seu próprio escopo sem se preocupar em seus dados privados estarem visíveis aos outros.

Eventualmente, o Ministério da Educação (MEC) encontrou uma oportunidade de melhorar seu sistema de autenticação, pois diversos processos burocráticos são realizados por ele

ao longo do ano. Isso porque somente o MEC é responsável por autenticar cada processo realizado pelas instituições de ensino brasileiras. Por exemplo, todo diploma emitido por uma entidade precisa do aval do MEC para ser considerado autêntico. Logo, a tecnologia da Hyperledger Fabric consegue fazer com que essa responsabilidade seja descentralizada para todas as universidade que fizerem parte da rede, isso fará com que cada entidade tenha que validar, autenticar e aprovar cada processo com base nas regras definidas pelo MEC, tornando o trabalho do Ministério da Educação menos burocrático, mais rápido e seguro. Para solucionar alguns dos principais problemas em Instituições de Ensino Superior, no artigo: Blockchain and smart contracts for higher education registry in Brazil (PALMA et al., 2019), é sugerido a criação de um novo modelo que utiliza blockchain e contratos inteligentes em Instituições de Ensino Superior. Essa proposta faz com que seja possível a autenticação de cada processo por entidades que fazem parte da rede. O MEC viu o modelo como promissor e iniciou um projeto com o Laboratório de Segurança em Computação (LABSEC) da Universidade Federal de Santa Catarina (UFSC), dando sequência ao trabalho sugerido pelo artigo. Porém esse modelo não abrange a parte de autenticação e identificação de um estudante na rede e qual a melhor maneira de realizar esse processo.

Diante desses fatores, este trabalho tem como finalidade realizar a autenticação do estudante, bem como identificá-lo na rede. Contudo, o modelo em questão necessita que o usuário tenha algum conhecimento prévio nas tecnologias usadas para conseguir se integrar. Logo, será desenvolvido um protótipo de interface gráfica web que possibilitará ao estudante se autenticar e fazer uso do sistema iniciado pela equipe do LABSEC em qualquer máquina que tenha um navegador e acesso a internet. Além disso, para que seja possível autenticar e identificar o estudante que quer acessar a rede blockchain, pretende-se utilizar o meio de autenticação gov.br pois este já está integrado com diversas tecnologias presentes no Brasil. Contudo, é necessário criar uma interface para que o usuário final não fique perdido diante de todos esses processos, para isso será utilizado o framework ReactJS (React, 2013) que facilita a criação de interfaces gráficas no meio de desenvolvimento web.

1.1 OBJETIVOS

Para facilitar a organização deste documento e o entendimento do escopo do trabalho a ser desenvolvido esta seção foi subdividida em: 1.1.1 Objetivos gerais, apresenta o escopo do projeto de forma genérica; 1.1.2 Objetivos específicos, esclarece de forma mais precisa resultados esperados através do desenvolvimento deste trabalho.

1.1.1 Objetivo Geral

Este trabalho tem como objetivo geral o desenvolvimento de um protótipo de interface gráfica com usuários de uma rede Blockchain focada no Ensino Superior que facilitará a in-

teração do usuário com o sistema, além disso propõe-se a realização de um levantamento das alternativas para identificação e autenticação do estudante nesta rede.

1.1.2 Objetivos Específicos

- Definir a alternativa para identificação e autenticação de usuários que mais se adequa ao cenário de múltiplos estudantes de diferentes IES.
- Testar a usabilidade do protótipo de interface gráfica web utilizando o SUS (*System Usability Scale*).
- Contribuir com a literatura atual relacionada a aplicações web que utilizam Blockchain, principalmente Blockchains privadas.

1.2 METODOLOGIA

Em uma primeira etapa, foi utilizado o método de leituras exploratórias com foco nas tecnologias a serem utilizadas no projeto, esta etapa consistiu em realizar um estudo para entender os conceitos de Criptografia e Segurança relacionados a Blockchain, além de realizar uma fundamentação teórica para a plataforma HyperLedger Fabric (Hyperledger Foundation, 2020), que possui características específicas em relação ao seu funcionamento numa rede Blockchain. O principal objetivo desta etapa é abranger o conhecimento sobre como prover a autenticação e identificação de usuários numa rede Blockchain de ensino e sobre protocolos de comunicação web para então definir a melhor maneira de realizar os objetivos do projeto. Os resultados desta etapa podem ser encontrados neste documento.

Em sequência, antes de iniciar o desenvolvimento do protótipo, foram localizados projetos com temas semelhantes ao proposto neste trabalho para identificar o estado da arte. Aplicações de cunho acadêmico relacionadas ao tema deste trabalho foram utilizadas como uma base estrutural para o desenvolvimento do protótipo. Esta etapa tem como objetivo identificar o que há de mais novo no mercado e na literatura, e utilizar isso para deixar o resultado mais atual possível para o usuário final. Nos casos de tecnologias novas descobertas, foi realizado uma etapa de estudos focada no entendimento e na absorção de conhecimentos relacionados às novas ferramentas. Logo após, o autor buscou entender conceitos de usabilidade e como aplica-los no protótipo a ser desenvolvido.

Após o protótipo ter sido concluído, foi realizado uma nova etapa com o intuito de avaliar o nível de usabilidade do protótipo. Nesta etapa, o responsável utilizou a metodologia System Usability Scale (BROOKE, 1986), que trata de calcular a efetividade, eficiência e satisfação do sistema em questão. Foi utilizado um questionário de dez perguntas, no qual as respostas servem como parâmetro para identificar se a aplicação web analisada está ou não em conformidade com o que o usuário espera.

2 CONCEITOS FUNDAMENTAIS

Este capítulo introduz ao leitor os conceitos necessários para entender como funcionam as tecnologias deste trabalho e os motivos de serem utilizadas.

2.1 CRIPTOGRAFIA E SEGURANÇA

Esta seção tem como objetivo apresentar os principais conceitos de criptografia e segurança utilizados para realizar a autenticação e identificação de um usuário numa rede Blockchain.

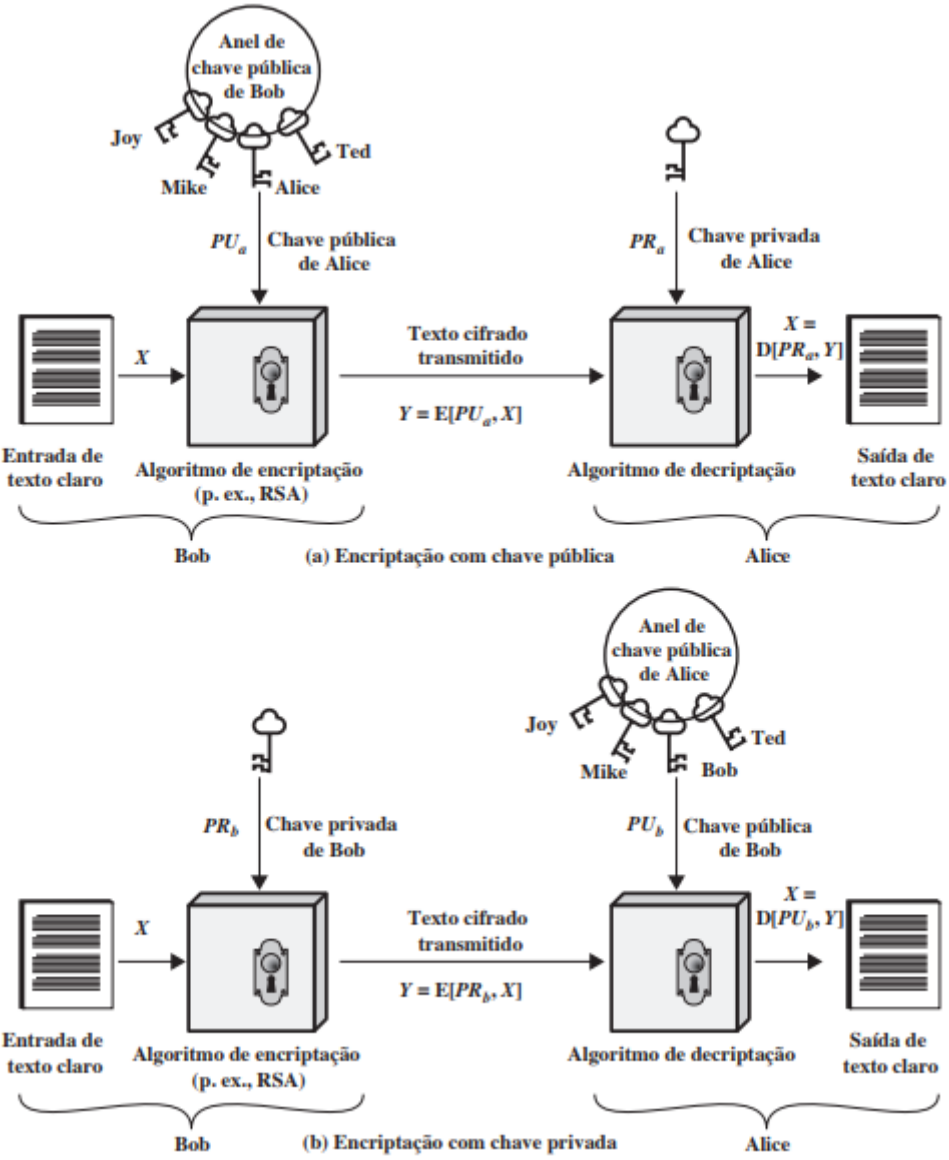
2.1.1 Criptografia de Chave Pública

Segundo Stallings (2006), a criptografia de chave pública se difere das demais, pois é baseada em funções matemáticas ao invés de substituição e permutação. Fora isso, a criptografia assimétrica utiliza duas chaves separadamente, diferente da simétrica que utiliza apenas uma chave. O que pode induzir um aumento de eficácia em certos pontos como confidencialidade e autenticação. A criptografia de chave pública tomou proporções maiores diante da tentativa de amenizar os principais problemas vistos nas criptografias simétricas. Um deles é a distribuição de chaves, que necessita de um compartilhamento prévio de uma chave entre ambas as partes envolvidas ou fazer o uso de um centro de distribuição de chaves. Além disso, um outro problema bem recorrente nas criptografias simétricas está relacionado com as assinaturas digitais. Com a atual digitalização de grande parte dos documentos em papel, é necessário um método que garanta a satisfação de todas as partes envolvidas na troca de mensagem, certificando que ela foi enviada por certa pessoa.

Diante disso, ainda segundo Stallings (2006), os algoritmos assimétricos possuem duas chaves, a pública e a privada, uma primeira para realizar a encriptação e uma segunda para realizar decriptação, relacionada à primeira matematicamente. Desse modo, é muito difícil um invasor conseguir determinar qual é a chave privada, mesmo tendo o conhecimento do algoritmo de criptografia que está sendo usado e da chave pública. Podemos considerar duas chaves A e B, nesse caso o algoritmo pode usar a chave A tanto para realizar a encriptação ou decriptação e utilizar a chave B para fazer o inverso (ver figura 1). Além das duas chaves, o algoritmo de criptografia assimétrica também possui outros elementos como o texto claro, que é a mensagem antes de ser encriptada, o texto cifrado, que é a mensagem após a encriptação, o algoritmo de encriptação, que transforma o texto claro, e o de decriptação, que a partir do texto cifrado e da chave correspondente recupera o texto claro original.

Com base nisso, um algoritmo de criptografia assimétrica começa gerando o par de chaves, uma pública e outra privada. A chave pública pode ser revelada, enquanto somente a privada é guardada apenas pelo dono do par, afirma Stallings (2006). Quando uma parte A deseja enviar uma mensagem para uma parte B ela encripta usando a chave pública de B,

Figura 1 – Criptografia Assimétrica



Fonte: (STALLINGS, 2006).

ao receber a mensagem ela é decriptada utilizando a própria chave privada de B, desse modo, apenas o destinatário B consegue decriptar a mensagem, pois é o único que tem conhecimento da chave privada correspondente (ver figura 1).

Stallings (2006) acredita que utilizando a lógica da criptografia assimétrica podemos resolver o problema de autenticação presente na criptografia simétrica. Um usuário pode utilizar sua chave privada para encriptar uma mensagem e, desse modo, somente esse usuário poderia ter encriptado essa mensagem, tornando a mensagem inteira uma assinatura digital. Além de que, a encriptação da mensagem em si não garante integridade. O dado pode ser alterado e decriptado com a chave pública do autor, igualmente. Nesse caso, não há como saber qual era o texto claro anterior a isso para comparar. Seria possível verificar a integridade caso o texto em

claro fosse enviado junto ou, mais comumente, o hash da mensagem assinado.

2.1.2 Algoritmo RSA

O algoritmo RSA (*Rivest-Shamir-Adleman*), segundo Stallings (2006), se trata de uma cifra de bloco no qual ambos os textos, claro e cifrado, são inteiros entre 0 e n-1, com n sendo gerado a partir da multiplicação de dois primos. Comumente, o tamanho do n é 1024 bits ou 309 dígitos decimais, ou seja, n é menor que 2^{1024}. Neste algoritmo, cada texto claro é encriptado em blocos com valores binários menores ou iguais a $log_2(n)+1$, sendo que a encriptação e decriptação com este algoritmo, considerando M como o texto claro e C o texto cifrado, se dá por $C = M^e mod n$ e $M = C^d mod n = (M^e)^d mod n = M^{ed} mod n$. Diante disto, tanto o emissor quanto o receptor precisam conhecer o valor de n, porém o emissor conhece o valor de e e somente o receptor conhece o valor de d, assim podemos considerar o RSA como um algoritmo de encriptação assimétrica tendo a chave pública como PU = *(e,n)* e a chave privada como PR = *(d,n)*.

2.1.3 Funções Hash Criptográficas

Segundo Stallings (2006), uma função hash se trata de uma função normal que aceita uma mensagem M de tamanho variável como entrada e gera uma saída, h = H(M), com tamanho fixo. Para o quesito aplicações de segurança, o tipo de função hash a ser analisado é a criptográfica. Pois com ela é computacionalmente inviável ser alvo de ataques, como força bruta, para identificar o dado mapeado para o hash. Em funções hash, no geral, a entrada é composta de um inteiro de tamanho variável e o valor do tamanho da mensagem. Esses campos de tamanho são considerados medidas de segurança pois aumentam a dificuldade que um invasor tem ao tentar recriar a mensagem com o mesmo valor de hash.

Funções hash criptográficas são muito utilizadas na autenticação de mensagens para realizar a verificação da integridade dessas mensagens trocadas. Ainda segundo Stallings (2006), ao utilizar essas funções, o valor delas passa a ser considerado um resumo da mensagem. Podemos considerar que, durante uma troca de mensagens, um emissor calcula um valor de hash para a mensagem e transmite ambos, o valor hash e a mensagem ao receptor. O receptor realiza o mesmo cálculo de hash sobre a mensagem e compara com o valor de hash recebido. Se o valor não coincidir, o receptor saberá que algo foi alterado durante o processo. Dito isso, um resumo criptográfico precisa ser bem protegido, pois se um invasor conseguir alterar o conteúdo de uma mensagem ele não deve conseguir modificar o valor hash a fim de realizar ataques a integridade dos dados.

No geral, a autenticação de mensagens é feita com base no MAC (*Message Authentication Code*), que são usados compartilhando uma chave secreta entre todas as partes envolvidas na troca de mensagens. Diante disso, Stallings (2006) informa que, uma função MAC recebe como entrada uma chave secreta e o conteúdo da mensagem, com isso, produz o valor de hash

que é associado a mensagem. Em casos da mensagem ter que ser decriptada, a mesma função MAC é aplicada sobre o texto cifrado e o resultado comparado com o valor MAC associado. Outro uso das funções hash criptográficas são nas assinaturas digitais, que se assemelham muito com o processo realizado pelas funções MAC. Porém, nesse caso, o valor do hash da mensagem passa a utilizar a chave privada do usuário na encriptação, com isso qualquer um que conhecer a chave pública pode verificar o conteúdo da mensagem porém apenas quem conhecer a chave privada pode alterar o conteúdo da mesma.

2.1.3.1 Requisitos e Medidas de Segurança

Será utilizado o valor de hash como h = H(A), sendo A a pré-imagem de h, e se em um caso de $A \neq B$ tiver H(A) = H(B), é chamado de colisão. Porém uma colisão é totalmente indesejável nas funções de hash pois é necessário que elas garantam a integridade dos dados. Com isso, segundo Stallings (2006), se o tamanho do hash, dado como n bits e o tamanho da mensagem como b bits, sendo b > n, o total de mensagens possíveis será de 2^b e o total de valores hash possíveis de 2^n. Diante disso, se a intenção for distribuir de modo uniforme cada valor hash, serão 2^{b-n} pré-imagens.

Levando em consideração os requisitos de segurança, definidos por Stallings (2006), para uma função hash ser considerada segura ela deve ter tamanho de entrada variável e tamanho de saída fixo, além de ter que ser relativamente fácil de calcular qualquer valor de A informado. Com isso, uma função hash segura precisa ser resistente a pré-imagem, ou seja, deve ser inviável gerar uma mensagem dado o código hash, e resistente a segunda pré-imagem, no qual não deve ser possível encontrar uma outra mensagem com o mesmo valor de hash da mensagem atual. Porém, se uma função tiver apenas essas medidas citadas anteriormentes ela ainda é considerada uma função hash fraca, para ser considerada forte ela deve ser resistente a colisão, ou seja, deve ser inviável, considerando $A \neq B$, encontrar um H(A) = H(B).

2.1.4 Assinaturas Digitais

Ao falar em assinaturas digitais, em geral, se refere a autenticação de uma mensagem que protege ambas as partes envolvidas contra um invasor. Considerando o emissor A e o receptor B, a partir do momento em que A envia uma mensagem não-autenticada para B é possível que B crie uma mensagem diferente e afirme que o envio veio de A, ou A pode negar que enviou tal mensagem diante da possível fraude de B. Ambos os cenários podem ser solucionados pela assinatura digital, afirma Stallings (2006), pois ela tem como características verificar o autor e a data e hora. Além de poder ser lida por terceiros a fim de resolver certas disputas.

Uma assinatura digital, segundo Stallings (2006), precisa necessariamente ser um padrão de bits dependente da mensagem que esta sendo assinada, usando algum dado, que é exclusivo do emissor, para impedir falsificações. Além disso, essas assinaturas devem ser fácil de produzir, reconhecer e verificar sua autenticidade. Diante destes requisitos, deve ser

possível guardar uma cópia dessa assinatura, levando em consideração detalhes técnicos como armazenamento. Porém, deve ser computacionalmente inviável realizar uma falsificação dessa assinatura. Numa assinatura digital em que apenas estão envolvidos o emissor e o receptor, a confidencialidade da mensagem pode ser dada pela encriptação da mensagem com adição da assinatura e chave secreta. Porém, a segurança desse método depende da segurança que o emissor atribuiu a chave secreta, podendo deixar ela vulnerável a ataques de terceiros.

2.1.5 Certificados X.509

Os certificados X.509 fazem parte do diretório X.500 que, segundo Stallings (2006), se referem a um servidor que mantém um banco de dados com informações dos usuários. Os X.509 tem como base o uso da criptografia de chave pública e assinaturas digitais, junto com a recomendação do uso do Algoritmo RSA. O eixo desses certificados se da pela chave pública associada a cada usuário, o certificado é criado por uma CA (*Certification Authority*) e armazenado no diretório por ela mesma ou por um outro usuário. A CA assina cada certificado com sua chave privada, desse modo, se a chave pública corresponder a um usuário o mesmo pode verificar se o certificado emitido pela CA é válido.

Cada certificado possui campos que permitem seu funcionamento e validação (ver figura 2). Diante disso, qualquer usuário com a chave pública da CA que emitiu o certificado pode verificar a chave pública do usuário e nenhuma CA pode modificar o certificado sem ser descoberta.

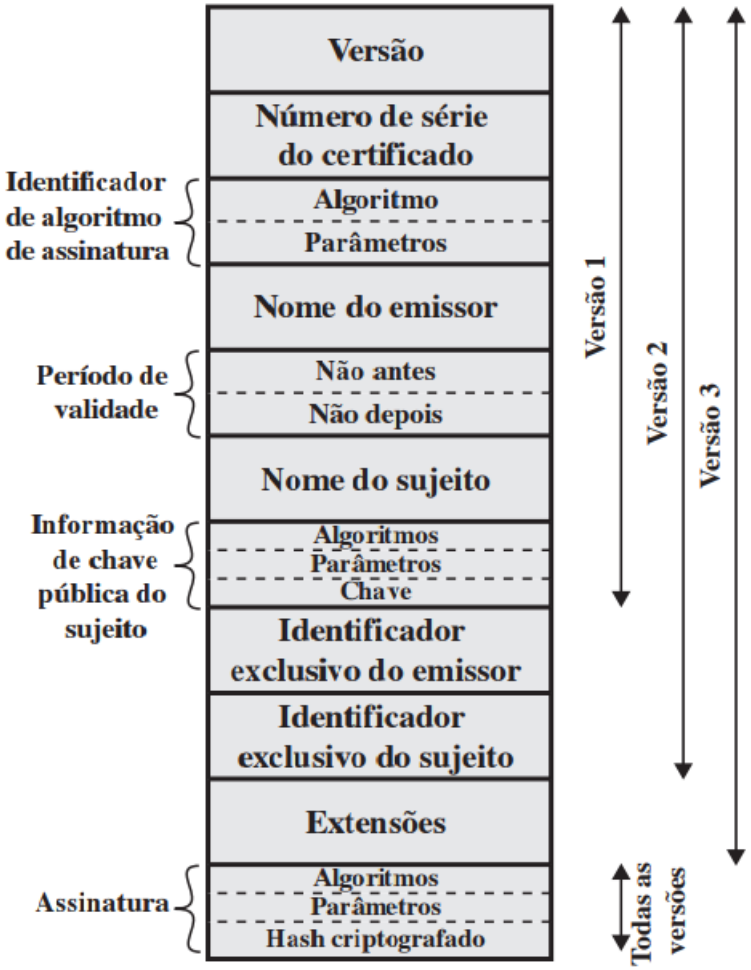
Essas chaves públicas fornecidas a cada usuário, ainda segundo Stallings (2006), devem ser seguras no quesito integridade e autenticidade, para se obter confiança nos certificados associados a elas. Com isso, em alguns casos é mais vantajoso que haja mais de uma CA fornecendo chaves públicas aos usuários, porém todos esses certificados gerados por várias CAs ainda precisam aparecer no diretório X.500 e cada usuário precisa saber como eles estão relacionados para poder acessar a chave pública de algum outro usuário. O X.509 propõe que cada certificado esteja relacionado em forma de uma hierarquia, distinguindo-se entre certificados diretos, que são certificados de certa CA gerados por outras CAs, e certificados reversos, que são certificados gerados por uma CA e certificados por outras CAs.

Em certos casos, com a chave privada do usuário ou o certificado da CA sendo comprometidos, é permitido realizar a revogação do certificado em questão fazendo com que a CA tenha que manter uma lista de certificados revogados ou CRL (*Certificate Revocation List*) que mantém o nome do emissor e data que foi revogado, juntamente com o número de série de cada certificado que é o suficiente para torná-lo identificável.

2.1.6 Infraestrutura de Chave Pública

Uma infraestrutura de chave pública ou PKI (*Public-Key Infrastructure*), segundo Stallings (2006), pode ser definida como um conjunto de elementos necessários para manusear

Figura 2 – Conteúdo de um Certificado X.509

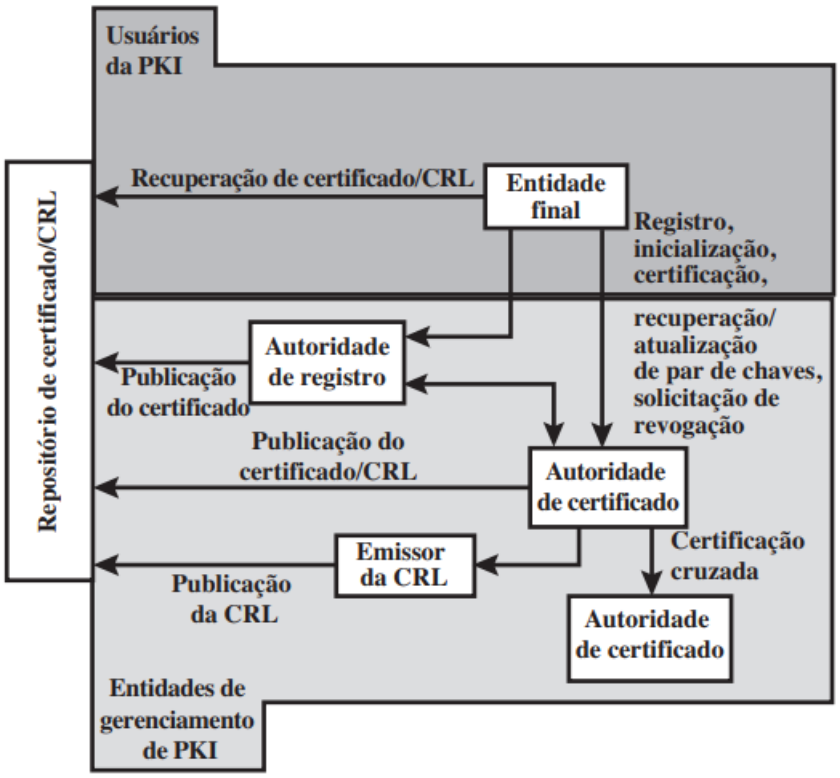


Fonte: (STALLINGS, 2006)

certificados digitais baseados na criptografia assimétrica. Diante disso, surgiu o grupo PKIX (*Public-Key Infrastructure X.509*) que propõe um modelo formal de infraestrutura baseada nos certificados X.509 (ver figura 3). O modelo arquitetônico proposto por esse grupo, utiliza as CAs, citadas anteriormente na seção de certificados X.509, para emitir os certificados e as RAs (*Register Authority*) como componente opcional para administrar o regristro das entidades finais que são qualquer os sujeitos atribuídos a um certificado de chave pública.

O mesmo grupo PKIX, ainda segundo Stallings (2006), identificou certas funções que necessitam estar nos protocolos de gerenciamento. Dentre elas está a função de registro que faz com que um usuário passe a ser reconhecido por uma CA começando o processo de alistamento em uma PKI. Logo após vem o processo de inicialização que instala alguns materiais da chave que se relacionam com as chaves armazenadas em outro local da infraestrutura. Com isso, começa a parte de certificação que é basicamente o processo no qual a CA emite o certificado para a chave pública relacionada ao usuário. Os pares de chaves, no geral, podem ser usados para prover suporte durante a criação e verificação de uma assinatura digital. Porém eles

Figura 3 – Infraestrutura de Chave Publica X.509



Fonte: (STALLINGS, 2006)

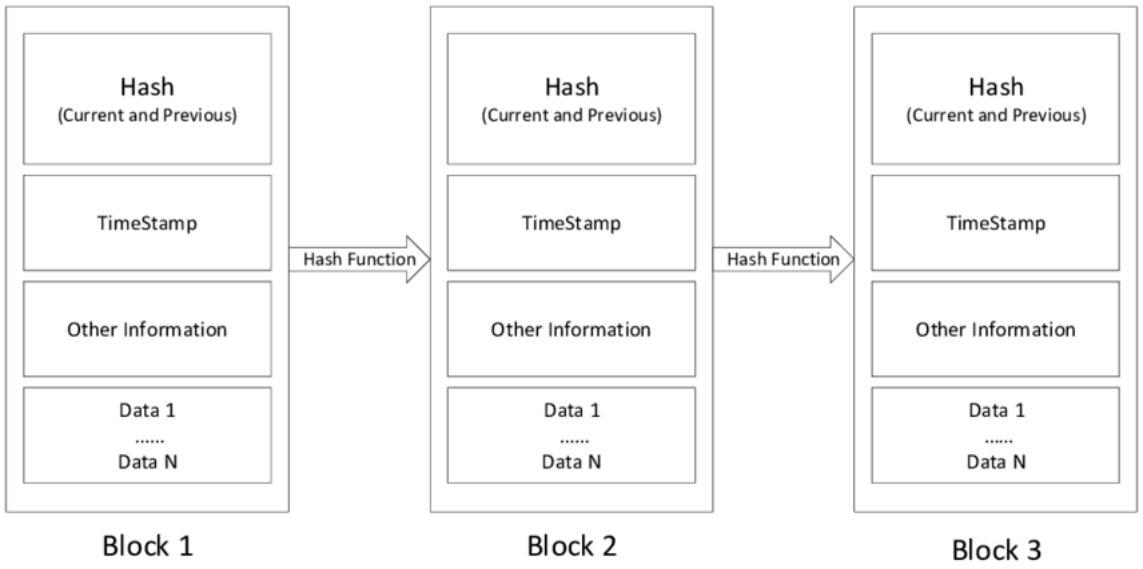
precisam ser atualizados quando o tempo de vida do certificado expirar, tornando necessária uma revogação do certificado. Essa revogação, ao ser solicitada por um usuário, é enviada a CA responsável que analisa a situação anormal, porém essa revogação não acontece só quando o certificado expira, ela pode ser solicitada em casos de comprometimento da chave privada ou troca de nome.

2.2 BLOCKCHAIN

O termo blockchain refere-se a uma tecnologia que é capaz de suportar a verificação de transações entre múltiplas partes, além de conseguir executar e gravar essas transações, combinando criptografia e gerenciamento de dados numa mesma rede. Cada blockchain, segundo Xu, Weber e Staples (2019), é composta por uma *ledger*, que corresponde a uma lista encadeada de blocos (ver figura 4). Nessa *ledger*, cada bloco contém um conjunto de transações realizadas na rede, um valor hash, um endereço do bloco anterior e um *timestamp* que contém o momento em que o bloco foi criado. Nesse caso, quando um dado é enviado, um protocolo chamado de consenso é executado diversas vezes para decidir quais dos dados anexar a *ledger*. Esse protocolo de consenso, em geral, envolve vários participantes, e seu conceito é aplicável a uma ampla variedade de modelos computacionais. Porém como muitos estão envolvidos, os participantes maliciosos podem gerar algumas falhas na rede. Pois as *ledgers* exigem a capacidade de realizar

consenso recorrente devido à sua longa vida útil para adicionar um fluxo de transações na rede.

Figura 4 – Estrutura de uma rede blockchain.



Fonte: (JOSHI; HAN; WANG, 2018).

Uma transação é criada pelos nós, que são responsáveis por verificar a integridade das transações e adicionar novos blocos na rede. Os dados de uma blockchain são replicados entre diversos nós e distribuídos geograficamente. Com isso, segundo Turkanović et al. (2018), podemos pensar numa blockchain como um banco de dados distribuído que preserva de forma segura e irrevogável uma cadeia de dados empacotados em blocos selados. Em que cada novo bloco contém uma referência ao conteúdo do bloco anterior (geralmente se trata de um valor de hash). No entanto, as informações são organizadas em transações de acordo com a estrutura especificada do blockchain e, em seguida, são criptografadas. O dado é protegido usando o processo de criptografia de chave pública, que também garante confiabilidade, irreversibilidade e não repudiabilidade. As redes blockchain podem ser divididas em pública não permissionada ou privada permissionada. Numa blockchain pública todos os dados estão disponíveis e são transparentes para o público porque esse tipo de blockchain não possui permissionamento, ou seja, qualquer pessoa pode ingressar na rede como um nó novo e realizar transações ou acessar o histórico de transações sem a necessidade de solicitar autorização. No entanto, para proteger o anonimato de um participante, alguns componentes do blockchain podem ser criptografados. Uma blockchain privada, por outro lado, permite que apenas nós selecionados se juntem à rede devido seu permissionamento. Isso faz com que pareça uma rede distribuída, mas centralizada, que fornece controle de acesso e identidade em todos os níveis da rede. Evitando muitas fraudes pois as transações são assinadas pelos participantes e não são todos que possuem permissão para adicionar algum dado na rede.

Dentro desse aspecto, ainda segundo Turkanović et al. (2018), um processo de consenso distribuído se trata de diversas partes da rede blockchain que devem concordar com o estado do *ledger* e, consequentemente, a ordem em que novos blocos devem ser adicionados

ao *ledger*. Diante disso, algumas das técnicas de consenso distribuídas que são utilizadas são Prova de trabalho (PoW), Prova de participação (PoS), Prova de participação delegada (DPoS), Prova de importância, Prova de atividade, Prova de queima, Prova de depósito, entre outras. Os dois métodos mais populares para obter consenso em uma blockchain são PoW e PoS. Com isso, o conceito fundamental por trás dos métodos de consenso distribuído se trata de decidir sobre um *peer* que preparará e selará o bloco mais recente usando dados que ainda não foram validados e compactados.

A fluidez de uma rede blockchain se dá pela coordenação entre as partes durante uma transação. Segundo Jiang, Jones e Javie (2008), convencionalmente essa coordenação é atribuída a um terceiro que provê confiança e facilidade ao processo. Porém, a blockchain apresenta um método diferente para suportar essas transações. Fazendo o uso de tecnologia compartilhada ao invés de confiar todo o processo à um terceiro. Além disso, essa rede funciona muito semelhante a um banco de dados tradicional, podendo ser utilizada para representar apenas transações ou até mesmo dados de um aplicativo. Como exemplo, temos o Bitcoin, primeira moeda digital descentralizada, que possibilitou o uso de cripto-moedas em diversos aplicativos para efetuar pagamentos (XU; WEBER; STAPLES, 2019).

Além disso, é possível armazenar *scripts* como parte de transações numa *ledger*, tornando toda a rede muito mais complexa e permitindo o uso de *smart contracts*. Esses *smart contracts* podem ser utilizados para gerenciar propriedades de ativos, como o Bitcoin, ou até mesmo automatizar e supervisionar certas atividades de uma rede, proporcionando uma ampla variedade de casos de uso para uma blockchain.

2.2.1 Smart Contracts

Os *smart contracts* são códigos de programas de computador que, segundo Herlihy (2019), são implementados em forma de dados na *ledger* da blockchain e executados durante cada transação (Ver Código Exemplo 2.1). Esses códigos possuem o objetivo de reduzir falhas e defeitos dos contratos normais durante todo seu ciclo de vida, desde a negociação até o encerramento. Diante disso, um *smart contract* tem a capacidade de chamar ou transmitir outros contratos que também são registrados na rede porém, uma vez implementado, o código dos *smart contracts* são imutáveis e determinísticos. Esses contratos podem se comportar como um objeto em uma linguagem de programação orientada a objetos, possuindo um estado de longa duração, um construtor para inicializar esse estado e uma ou mais funções para lidar com esse estado.

No geral, os *smart contracts* são utilizados para gerenciar a propriedade de criptoativos da blockchain ou de tokens digitais (e.g., Kudos (SHARPLES; DOMINGUE, 2016)), podendo ocasionalmente serem usados para supervisionar ou até mesmo automatizar certos aspectos. Diante disso, eles podem permitir uma ampla variedade de aplicações, além de especificar um protocolo de comunicação entre várias partes, sendo assim, muito usados nas *dapps*.

```
// Codigo exemplo de um Smart Contract

pragma solidity ^0.8.0;

contract Balance {
  function balance() public returns (uint256){
    return payable(address(this)).balance;
  }
}
```

Listing 2.1 – Código exemplo de um Smart Contract

2.2.2 DAPPs

As aplicações baseadas em uma blockchain utilizam contratos inteligentes para gerenciar algumas funcionalidades e dados essenciais que são imutáveis. Nesses aplicativos os usuários precisam executá-lo localmente, porém toda ação será replicada em todos os nós da rede. Entretanto, segundo Cai et al. (2018), um dos principais problemas são as limitações de desempenho que essas tecnologias blockchain possuem ao atenderem demandas de muitas aplicações, abrindo a possibilidade de diversos problemas com manutenção e segurança operacional.

O back-end de um *dapp*, segundo Xu, Weber e Staples (2019), funciona com uma configuração descentralizada, isso o diferencia dos back-ends de aplicativos padrão, que são executados em um servidor centralizado. Assim como aplicações comuns, os dapps também podem conter código de front-end e interfaces de usuário que se comunicam com seus back-ends por meio de APIs. Com isso, um *dapp* processa e armazena dados centralmente no blockchain utilizando contratos inteligentes. Podemos pensar num *dapp* como um site que utiliza um ou mais contratos inteligentes, sendo assim a principal distinção desses aplicativos para os convencionais é que fazem o uso da blockchain para fornecer os dados e capacidade computacional.

Um dos *dapps* mais famosos é o CryptoKitties (EVANS, 2019) que se trata de um jogo, criado pela Axiom Zen, que possibilita que os usuários negociem, coletem e vendam gatos virtuais. Nesse jogo cada gato é único com seu endereço gravado numa rede blockchain, fazendo com que as transações sejam transparentes e garantidas.

2.3 HYPERLEDGER FABRIC

Com a popularidade das tecnologias blockchain surgiu o interesse em utilizar esta tecnologia em ambientes corporativos, porém os casos de usos que as empresas necessitavam não eram satisfeitos com blockchains públicas, como a Ethereum. Pois muitas empresas necessitavam que os participantes da rede fossem identificáveis e que os dados das transações fossem privados e confidenciais. Diante disso, segundo a Hyperledger Foundation (2020), a Fabric sur-

giu na intenção de ser utilizada por ambientes corporativos, sendo uma blockchain de código aberto. Ela possui uma arquitetura de fácil configuração e altamente modular. Além de suportar contratos inteligentes escritos em linguagens de programação populares no ramo corporativo, possibilitando que diversos projetos sejam desenvolvidos sem a necessidade de treinamentos em novas áreas.

Além desses fatores, ainda segundo a Hyperledger Foundation (2020), o Fabric se difere de outras plataformas pois é permissionada, fazendo com que todos os usuários sejam conhecidos. Possui também um suporte aos protocolos de consenso conectáveis. Esses protocolos utilizam implementação adaptada a suposição de confiança escolhida, permitindo que empresas personalizem a plataforma com base nos seus casos de uso. O Fabric surgiu para atender as diversas demandas empresariais. Para isso é necessário ter os seguintes componentes: um *ordering service* que determina a ordem de múltiplas transações em um bloco, um *membership service provider* que associa as entidades presentes na rede com IDs, uma *P2P gossip service* que é responsável por dispersar as saídas dos blocos e solicitar o serviço aos pares, *smart contracts*, uma *ledger* e uma política de validação. Numa rede que utiliza o Fabric, os *smart contracts* recebem o nome de *chaincode* e permitem a realização de transações mais complexas.

Ademais, uma plataforma Hyperledger Fabric conta com uma organização que representa uma entidade da rede. Para ela entrar numa rede é necessário a aprovação dos já integrantes da mesma. As regras de consenso para que uma organização faça parte de uma rede são definidas pelo *membership service provider* que, juntamente com as organizações já participantes, define quais serão os privilégios atribuidos a nova organização. Outro componente importante de uma Fabric são as Autoridades Certificadoras ou CAs, que são responsáveis por atribuir os certificados aos participantes de uma rede com uma assinatura digital. Juntamente a isso, a chave pública de cada participante é vinculada a seu respectivo certificado, fazendo com que as transações realizadas por elas possuam autenticidade. Pois um terceiro pode validar seu certificado utilizando a chave pública em questão.

3 REVISÃO BIBLIOGRÁFICA

Neste capítulo, foi realizada uma revisão abrangente da literatura disponível sobre o tema deste trabalho. O objetivo principal é examinar e sintetizar os estudos e publicações relevantes, a fim de obter uma compreensão profunda do estado atual do conhecimento na área de interesse. Para isso, será utilizado uma ampla variedade de fontes, incluindo artigos científicos, teses, dissertações e outros materiais relevantes, selecionados de acordo com alguns critérios. A busca por essas fontes foi realizada em duas bases de dados especializadas, a ACM (ACM Digital Library, 2023) e a ScienceDirect (Science Direct, 2023), com o intuito de garantir a abrangência e a confiabiliade da revisão.

3.1 MÉTODO DE PESQUISA

Esta seção é responsável por apresentar o método utilizado para realizar a busca dos trabalhos, as palavras-chaves e seus sinônimos, a query de busca, e por fim os resultados. Primeiro, foi definido um conjunto de perguntas a serem feitas a fim de identificar o que está sendo buscado e encontrar trabalhos que possam ser semelhantes. São elas:

- Qual identificador as blockchains privadas usam para armazenar os dados do usuário?
- Quais dados são relevantes para um estudante numa blockchain privada?
- Quais são os padrões existentes para verificar a autenticidade dos dados extraídos do blockchain privado?

Após isso, foi definido uma tabela com palavras-chaves e seus sinônimos no intuito de organizar melhor a busca pelos trabalhos.

Palavra-chave	**Sinônimo**
blockchain	distributed ledger
student	user
authentication	authorization

Com as palavras-chavres e seus sinônimos, foi definida a query de busca utilizada nesta revisão bibliográfica como sendo a seguinte:

```
("blockchain"OR "distributed ledger") AND ("student"OR "user") AND
("authentication"OR "authorization")
```

Esta query foi aplicada buscando esses termos em todo o documento, ou seja, utilizando a opção *full-text*. Além dessa query, os seguintes parâmetros foram utilizados para filtrar melhor a busca:

- Publicações entre 2018 e 2023.
- Não foram considerados capítulos em livros, apresentações, conteúdo antecipado e *short papers*.
- Não foram considerados trabalhos que propõem autenticação baseada em tecnologias blockchain.
- Apenas os 50 primeiros resultados.
- Ordenados por relevância.
- As bases de dados a serem utilizadas serão: ACM e ScienceDirect

Com base nesses parâmetros, ao executar a query de busca, primeiro foi feito um levantamento de artigos que podiam ser semelhantes realizando uma leitura do título e do resumo, com isso muitos trabalhos não correlatos já foram eliminados. Após isso, foi feito a leitura dos artigos selecionados para ver se de fato tinham relação com o tema deste trabalho.

Ao realizar a revisão, foi observado que grande parte dos trabalhos que se relacionavam ao descrito neste documento utilizavam de uma autenticação baseada em blockchain, que não se correlaciona a este trabalho. Porém, foi escolhido um artigo com autenticação baseada em blockchain, do autor Ezawa et al. (2023), para mostrar as diferenças com este protótipo e o artigo dos autores Abreu, Coutinho e Bezerra (2020), que propõe algo semelhante ao nosso protótipo, todavia sem utilizar de autenticação governamental ou uma interface gráfica. Além de que sua proposta é mais focada nas instituições de ensino e não nos estudantes. Na seção a seguir, apresentaremos os artigos correlatos e suas diferenças com este trabalho.

3.2 A BLOCKCHAIN-BASED ARCHITECTURE FOR QUERY AND REGISTRATION OF STUDENT DEGREE CERTIFICATES

Neste artigo, os autores Abreu, Coutinho e Bezerra (2020) propõem um protótipo que faz o uso da tecnologia blockchain para resolver problemas relacionados à autenticação e segurança de diplomas no contexto do ensino superior. Ele destaca os desafios enfrentados pelas instituições de ensino, como o acesso e segurança dos dados de diplomas, a necessidade de validação sem a intervenção de terceiros, a disponibilidade dos sistemas das instituições para comprovação dos diplomas, o armazenamento seguro dos dados e a prevenção de documentos falsificados. A proposta apresenta uma arquitetura baseada em blockchain que busca fornecer um ambiente com credibilidade e segurança, permitindo a publicação e consulta das informações dos diplomas de estudantes de ensino superior.

Diante disso, o autor menciona que a tecnologia blockchain pode abordar os problemas mencionados de forma mais adequada do que as tecnologias tradicionais, permitindo transações entre partes confiáveis, como as instituições de ensino, estudantes, empresas, governo e outras

instituições de ensino. Ele também destaca que o uso da blockchain pode reduzir os riscos de perda de informações, economizar papel, reduzir custos de gerenciamento e prevenir documentos falsificados. Com isso, o autor descreve uma arquitetura de referência para a blockchain, um protótipo de um aplicativo no domínio educacional que utiliza recursos de blockchain e uma avaliação da solução tanto do ponto de vista técnico quanto do usuário. O texto também menciona que a validação da tecnologia blockchain é baseada na lógica de negócios do registro de diplomas, sendo que toda a interação é realizada por meio de uma interface semelhante a um sistema tradicional.

Para ilustrar a arquitetura proposta, é definido um cenário envolvendo uma instituição de ensino superior privada, e a validação é realizada por dois participantes responsáveis pelo setor de emissão de diplomas da instituição. Os dados educacionais inseridos na blockchain são baseados em um ato administrativo específico do Ministério da Educação do Brasil. O trabalho conclui mencionando que a utilização da tecnologia blockchain pode trazer benefícios significativos para a gestão de dados de diplomas no ensino superior, proporcionando maior segurança, verificabilidade e confiabilidade.

Com isso, pode-se concluir que este trabalho correlato se difere da proposta deste documento. Isso pois, este trabalho especifica o uso de autenticação via gov.br. Isso implica que o protótipo estará aproveitando a infraestrutura de autenticação fornecida pelo governo brasileiro por meio do gov.br, que é um sistema de login único que permite aos usuários acessar vários serviços online do governo com um único cadastro. Além disso, o protótipo utilizará o Design System do Governo Federal, visando aumentar a usabilidade da interface pois todos os elementos visuais já são utilizados em outros sites governamentais.

3.3 BLOCKCHAIN-BASED CROSS-DOMAIN AUTHORIZATION SYSTEM FOR USER-CENTRIC RESOURCE SHARING

Neste artigo, o autor Ezawa et al. (2023) propõe uma arquitetura de autorização em várias áreas utilizando tecnologia blockchain para promover o compartilhamento de dados entre organizações. A arquitetura é baseada no conceito de User-Managed Access (UMA), que permite o compartilhamento flexível de dados entre domínios com controle de acesso personalizável. O artigo aborda a falta de transparência nos sistemas de autorização convencionais, especialmente em sistemas de larga escala como cidades inteligentes. A arquitetura proposta utiliza a tecnologia blockchain para solucionar esse problema, garantindo transparência e integridade no controle de acesso. Além disso, a implementação da arquitetura demonstrou bom desempenho, com tempo de processamento abaixo de 500 ms e pouca variação no tempo de processamento.

Além disso, o autor apresenta várias contribuições significativas. Primeiro, propõe uma arquitetura de autorização em várias áreas que não depende de um único ponto de confiança, permitindo o compartilhamento de recursos entre diferentes domínios sem a necessidade de uma autoridade central. Em segundo lugar, aumenta a transparência e a integridade

no controle de acesso por meio do uso da tecnologia blockchain, possibilitando que os usuários confirmem se o controle de acesso está sendo executado conforme especificado. Terceiro, reduz os custos operacionais de um sistema de autorização, automatizando sua operação por meio da tecnologia blockchain e compartilhando os custos entre várias organizações. Além disso, a arquitetura proposta permite que os proprietários de recursos escolham o sistema de autorização mais adequado para gerenciar seus recursos, centralizando o gerenciamento em diferentes domínios. A implementação da arquitetura foi realizada utilizando Hyperledger Fabric e foi avaliada quanto ao tempo de processamento e tamanho dos dados, apresentando resultados promissores.

Em resumo, o autor propõe uma arquitetura de autorização em várias áreas baseada em blockchain, visando resolver os desafios de transparência e controle de acesso em sistemas de larga escala, como cidades inteligentes. A arquitetura permite o compartilhamento flexível de recursos entre organizações, reduzindo custos operacionais e oferecendo maior transparência e integridade no controle de acesso. Os resultados da implementação demonstram um desempenho satisfatório. Essa abordagem tem o potencial de promover o compartilhamento de dados de forma segura e eficiente no contexto da economia digital. A diferença entre essa abordagem e a autenticação com o GovBr reside no escopo e na aplicação. A autenticação com o login único do GovBr se concentra principalmente na autenticação do usuário, fornecendo um único ponto de acesso aos serviços governamentais. Já a arquitetura proposta no estudo aborda a questão da autorização e do compartilhamento de dados entre organizações em diferentes domínios, utilizando a tecnologia blockchain para garantir a transparência e a integridade do controle de acesso. O login único do gov.br é um sistema confiável e amplamente adotado no contexto brasileiro, o que pode gerar confiança e facilitar a adesão dos usuários. Além disso, o governo tem a responsabilidade de proteger os dados dos cidadãos e, portanto, é esperado que os sistemas governamentais sigam rigorosas medidas de segurança e conformidade.

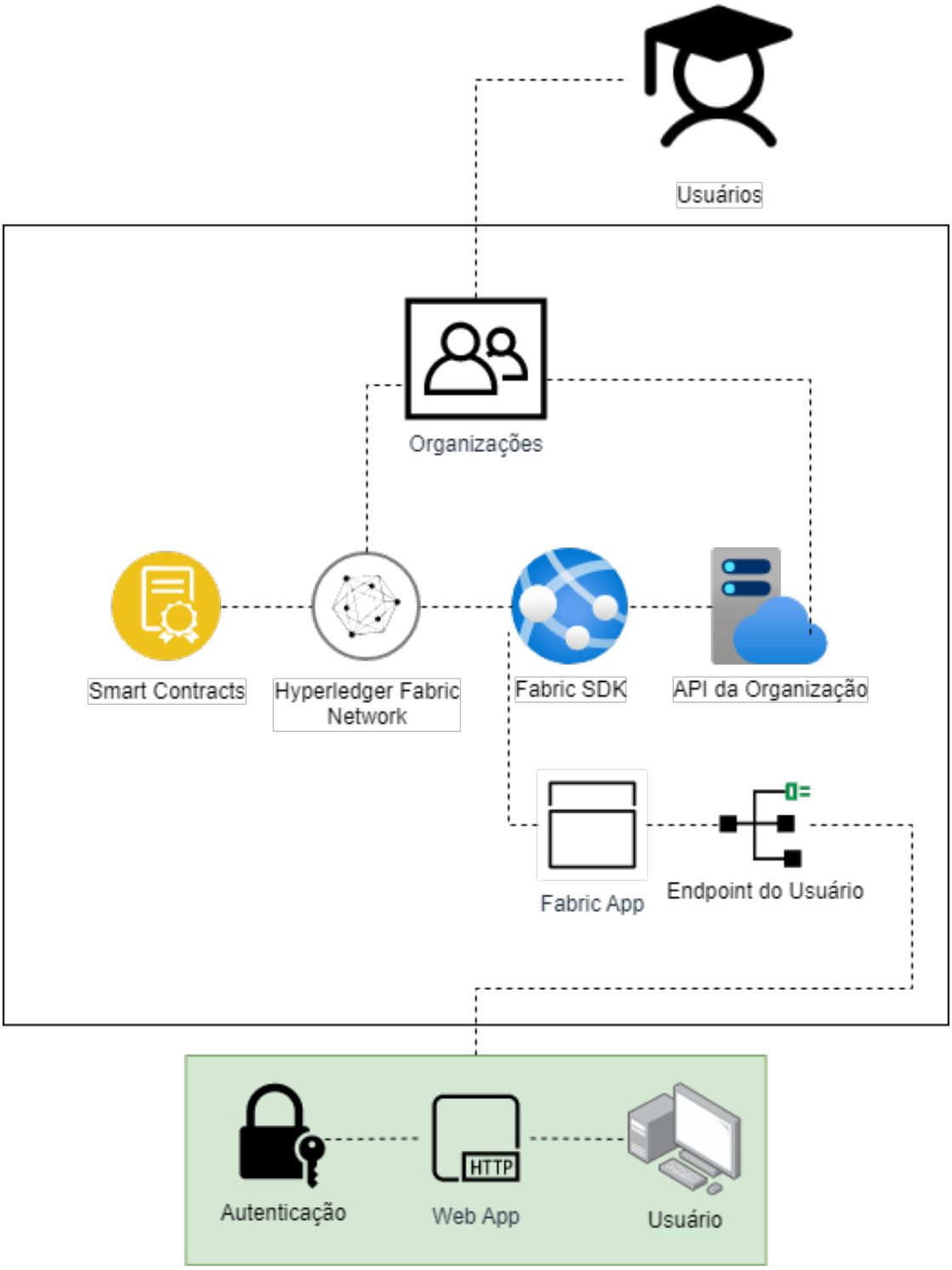
4 PROPOSTA

A proposta deste trabalho se baseia em desenvolver uma aplicação que utiliza as funcionalidades de uma rede Blockchain para possibilitar a interação entre estudantes e instituições de ensino superior. Como base, foi utilizado o projeto Jornada do Estudante, que é mantido atualmente por uma parceria realizada entre o MEC, LABSEC e o Laboratório Bridge, e se trata de uma rede que utiliza a arquitetura blockchain para emitir e controlar certificados digitais das IES. Porém, esse projeto não prevê a interação e autenticação entre estudante e universidades. Com isso, surgiu a possibilidade de desenvolver um novo protótipo que coloque o estudante como um ator primário e utilize de tecnologias para realizar a autenticação do mesmo na rede Blockchain.

Diante disso, o modelo base que foi seguido neste trabalho (Figura 5) tem sua arquitetura composta por: nós das organizações, sendo as organizações e os estudantes inclusos; *smart contracts*, para emitir e controlar os certificados gerados; aplicações responsáveis por conectar os estudantes na rede Blockchain e APIs para que seja possível acessar os métodos providos pelas aplicações. Logo, utilizando este modelo pretende-se desenvolver uma aplicação Web em React.js para realizar a autenticação do estudante e garantir uma interface gráfica para a navegação. Desse modo, é possível que o usuário visualize seus certificados, suas atividades complementares, seus documentos oficiais, entre outros.

A parte destacada de verde claro (Figura 5) demonstra o que foi implementado neste trabalho. Primeiramente foi construído uma API de Autenticação, que autentica o usuário utilizando o Login Único do *gov.br*. Juntamente a isso um protótipo de aplicação web foi construído, utilizando React.js e bibliotecas de interface, visando uma usabilidade de alto nível. Este protótipo tem como responsabilidade integrar o usuário com a rede Jornada do Estudante após ser autenticado.

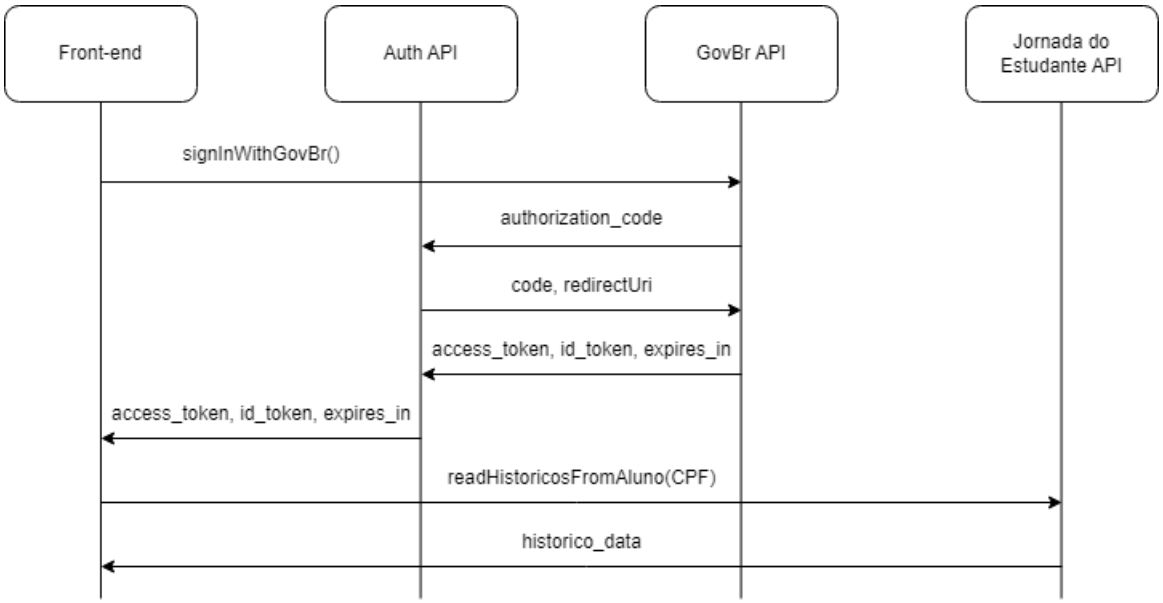
Figura 5 – Modelo Proposto



5 PROTÓTIPO

Neste capítulo, será apresentado o protótipo desenvolvido para a identificação e autenticação de estudantes em uma rede blockchain de ensino (ver figura 6). Para realizar esse desenvolvimento, foi utilizado uma máquina virtual dentro do domínio UFSC com um endereço interno e um endereço externo, para tornar possível a autenticação com a API do Governo Brasileiro. Além disso, a interface do protótipo foi implementada utilizando tecnologias conhecidas no mercado, como Typescript, HTML e CSS. Já as APIs foram implementadas utilizando NodeJS e algumas bibliotecas que facilitam requisições web. Logo após, será apresentado como foi configurado a rede Hyperledger para realizar a integração entre blockchain e servidor web. Por fim, serão destacados alguns problemas e desafios enfrentados durante o desenvolvimento deste protótipo.

Figura 6 – Fluxograma do protótipo



5.1 FRONT-END DA APLICAÇÃO

Nesta seção, apresentaremos o Front-End do nosso protótipo, que busca proporcionar aos usuários uma experiência intuitiva e agradável ao interagir com o sistema. O protótipo foi desenvolvido com base nas melhores práticas de design e usabilidade presentes no guia de UI/UX do Design System GovBr (Governo Brasileiro, 2023), visando fornecer uma interface responsiva, de fácil navegação e com uma estética moderna. Com elementos cuidadosamente dispostos e uma paleta de cores padronizada, o objetivo é criar uma experiência visualmente atraente e com boa usabilidade para os usuários.

5.1.1 Organização do código

A organização do código frontend foi baseada na Folder Architecture do React (WIERUCH, 2017), na qual possui a pasta *components* contém pequenos componentes reutilizáveis que podem ser facilmente combinados para formar páginas e outros elementos de interface de usuário. A estrutura geral de pastas utilizada foi a seguinte:

- /src - Armazena o código-fonte da aplicação e organiza em subpastas de acordo com sua funcionalidade ou tipo.
- /src/@types - Armazena o arquivo 'react.d.ts' que define e fornece tipos para bibliotecas JavaScript de terceiros que não possuem tipos definidos.
- /src/assets - É usada para armazenar recursos que não fazem parte do código da aplicação, mas que são usados em diferentes partes do projeto, como por exemplo imagens e ícones.
- /src/components - Contém os componentes React que compõem as páginas da aplicação.
- /src/pages - É usada para armazenar os arquivos relacionados às páginas da aplicação, em que cada arquivo corresponde a uma rota específica e contém a lógica específica da página.
- /src/styles - Armazena os arquivos de estilo gerais e os temas da aplicação.
- /src/utils - Contém arquivos úteis como funções ou constantes que são usados em diferentes partes do projeto.

5.1.2 Arquivos da raiz do projeto

Essa seção de arquivos da raiz do projeto detalha uma parte essencial do desenvolvimento, a configuração e implantação do sistema como um todo, pois esses são os principais arquivos de configuração do protótipo.

5.1.2.1 Arquivo main.tsx

O arquivo "main.tsx"é responsável por inicializar a aplicação React. Basicamente, ele é o ponto de entrada para a aplicação e é responsável por renderizar o componente principal da aplicação na página. Neste protótipo, o componente App é importado para o main, que o renderiza dentro de um componente StrictMode. O StrictMode é usado para ajudar a identificar problemas potenciais na aplicação e é recomendado para uso durante o desenvolvimento ou em ambientes de testes. Em seguida, o método ReactDOM.createRoot() é usado para criar uma raiz para a aplicação e renderizar o componente App dentro dessa raiz. Essa raiz é criada como um elemento HTML de ID "root", que é exibido na página em que a aplicação é executada.

5.1.2.2 Arquivo app.tsx

O arquivo app.tsx é responsável por criar a função App() que tem como retorno uma estrutura JSX que envolve os componentes React. Primeiramente, ele define o tema padrão para a aplicação usando o componente ThemeProvider e passando o objeto defaultTheme como propriedade, vale ressaltar que nesse protótipo apenas o tema padrão está desenvolvido porém essa estrutura serve para adaptar a aplicação com qualquer tema. Em seguida, a função App() envolve a navegação do aplicativo usando o componente BrowserRouter, que é o responsável por fornecer a navegação baseada em rotas. Dentro do BrowserRouter, o componente Router é renderizado. Por fim, o estilo global é aplicado usando o componente GlobalStyle exportado da pasta /styles.

5.1.2.3 Arquivo Router.tsx

O arquivo Router.tsx define as rotas da aplicação utilizando a biblioteca react-router-dom. Primeiramente, são definidos dois componentes: PublicRoutes e PrivateRoutes, que representam as rotas que serão acessíveis publicamente (sem autenticação) e as rotas que serão acessíveis apenas para usuários autenticados, respectivamente. Dentro de PublicRoutes, há a definição de uma rota através do componente Route que recebe duas props: path que define o caminho da rota e element que define o componente a ser renderizado quando a rota é acessada. Nesse caso, a rota definida é a rota raiz e o componente a ser renderizado é a página SignIn. Em contrapartida, dentro de PrivateRoutes, há a definição do componente Header que será renderizado em todas as rotas privadas formando um template para as páginas privadas. Em seguida, é definida a rota /home que será acessível apenas para usuários autenticados e o componente Home será renderizado quando essa rota é acessada. Por fim, o componente Router é definido como a junção de PublicRoutes e PrivateRoutes. Diante disso, quando a aplicação for carregada, a rota "/"será acessada automaticamente e o componente SignIn será renderizado. Se o usuário fizer o login com sucesso, ele será redirecionado para a rota /home e o componente Header e Home serão renderizados. Se o usuário tentar acessar a rota /home sem estar autenticado, ele será redirecionado automaticamente para a rota raiz.

5.1.3 Páginas da aplicação

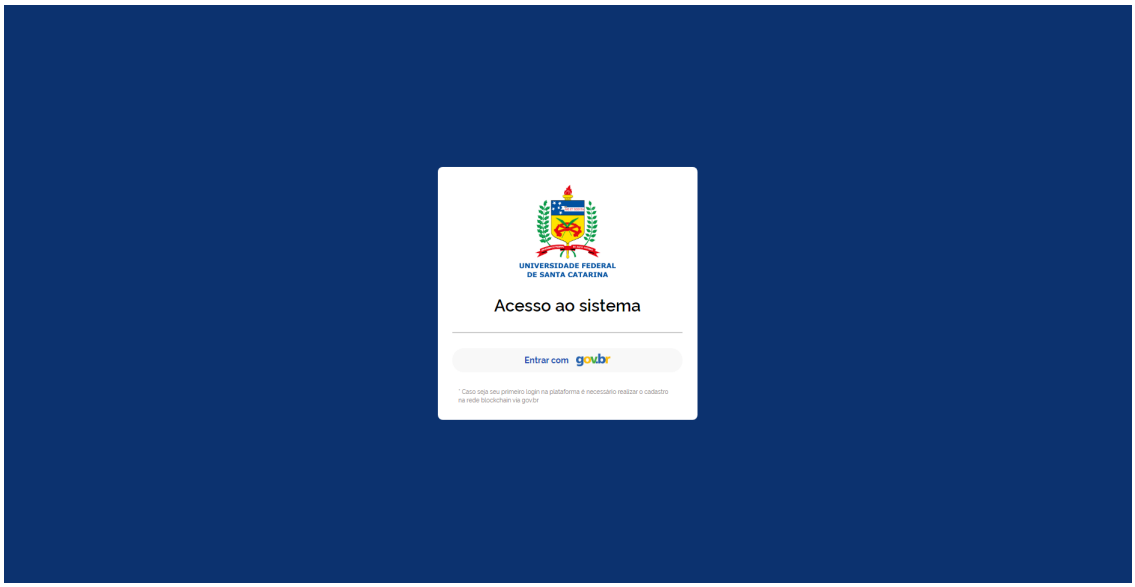
Neste protótipo, o Design System do Governo Brasileiro foi utilizado pois já possui uma boa usabilidade, alta qualidade visual e, como a aplicação faz parte de um Órgão Federal, a padronização das interfaces dos serviços públicos digitais. Além disso, a utilização desse sistema facilita a criação de interfaces, pois o desenvolvedor tem uma orientação do que seguir durante a estilização da aplicação com isso o tempo de desenvolvimento e manutenção da aplicação são reduzidos. Diante disso, o uso do Design System do Governo Brasileiro traz confiabilidade e credibilidade a aplicação pois este sistema segue padrões estabelecidos interna-

cionalmente e é constantemente revisado e atualizado para atender as necessidades dos usuários do serviço público.

5.1.3.1 Página de Login

A página de login (ver figura 7), se baseia em um componente funcional React chamado SignIn, que é responsável por renderizar o botão de acesso a rede blockchain na página raiz da aplicação. A página contém apenas um botão que chama o método de login com o govbr, iniciando todo o processo de autenticação do usuário.

Figura 7 – Página de Login



Ao acionar método handleGovBrSignIn(), um get para a API de autorização do Governo Federal Brasileiro, mais especificamente para a versão de homologação (staging), é realizado. A requisição contém uma série de parâmetros que indicam ao servidor qual é a aplicação que está requisitando autorização, qual é o escopo de acesso requerido, a URI para a qual o servidor deve redirecionar a resposta da requisição, além de um valor nonce e state que são usados para proteger a requisição contra ataques de terceiros mal intencionados.

Os parâmetros da URL são os seguintes:

- responseType: indica o que servidor deve retornar, nesse caso é passado "code"indicando que deve ser retornado um código de autorização em vez de um token de acesso direto.
- clientId: identifica a aplicação que está solicitando autorização, no caso desse protótipo é sistemas.homologacao.ufsc.br.
- scope: define o escopo de acesso requerido, para essa aplicação foi utilizado "openid+ (email/phone) +profile"que inclui informações básicas do perfil do usuário, além de informações de autenticação.

- redirect uri: especifica a URI para a qual o servidor deve redirecionar a resposta da requisição após o usuário autorizar ou negar o acesso, neste protótipo foi utilizado uma rota de redirect para a Api de Autenticação dada por https://govbr.labsec.ufsc.br:3000/redirect.
- nonce: valor aleatório usado para proteger a requisição contra ataques CSRF.
- state: outro valor aleatório usado para proteger a requisição contra ataques CSRF.

Durante essa requisição, uma nova janela no navegador para o serviço de autenticação do governo brasileiro é aberta, na qual o usuário pode colocar seus dados de login e realizar sua autenticação. Devido ao ambiente disponível ser um ambiente de desenvolvimento é necessário cadastrar uma nova conta neste ambiente seguindo as seguintes instruções:

- Inserir o CPF que deseja, deve ser um número de CPF válido.
- Clicar em "Esqueci minha senha"
- Clicar em "Não tenho celular"
- Clicar em "Tentar de outra forma"
- A data de nascimento de qualquer conta do ambiente de desenvolvimento é 01/01/1980
- Nome da mãe de qualquer conta do ambiente de desenvolvimento é MAMÃE
- Criar uma senha e validar com código pelo email ou sms

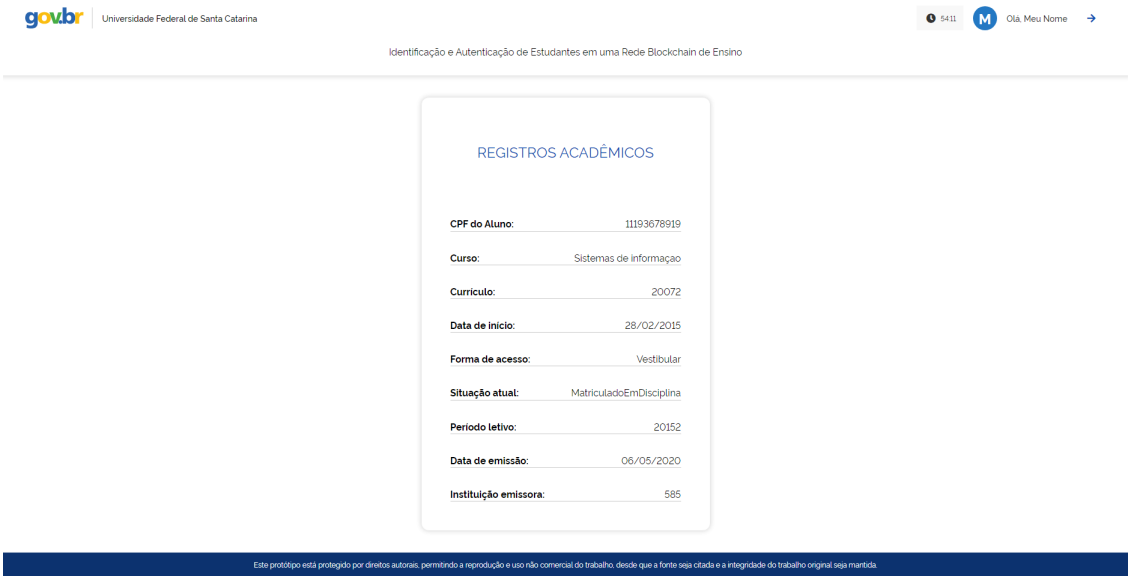
Após isso, a autenticação via GovBr no ambiente de desenvolvimento pode ser realizada normalmente com o CPF e a senha definidos.

5.1.3.2 Página de Home

A página de Home (ver figura 8), se baseia em um componente funcional React, chamado Home, que é responsável por renderizar a página principal da aplicação. Ele importa o hook useLocation() do React Router para coletar os dados vindos pela URL após o redirect de autenticação e a biblioteca jwt-decode para decodificar os tokens de autenticação. Em seguida, define uma interface chamada DecodedIdToken que contém as informações do usuário contidas no token decodificado, como nome, e-mail, CPF e data de expiração. Além disso, esse componente possui uma função chamada handleLogout() que faz uma solicitação ao servidor de autenticação para deslogar o usuário e redirecioná-lo para a página de login caso essas condições sejam verdadeiras: se o tempo de expiração do token é zero ou se o token não está presente.

Nesta página, tambem é realizado a integração com a API do Jornada do Estudante, através do método getHistoricosFromCpf(cpf), o cpf passado é o mesmo recebido pelo token do

Figura 8 – Página de Home



GovBr, que envia uma requisição HTTP para a rota /api/academicRecords/read/readHistoricosFromAluno. Com isso, conseguimos obter diversos dados acadêmicos do usuário autenticado, mostrando ser possível a integração entre GovBr e a Jornada do Estudante.

5.2 API DE AUTENTICAÇÃO

Neste protótipo, foi desenvolvido uma API utilizando Node.js juntamente com o framework Express, para lidar com requisições web, e a biblioteca HTTPS, que permite que os usuários se autentiquem usando o serviço de autenticação SSO (Single Sign-On) do governo brasileiro. Além disso, outras bibliotecas foram utilizadas como, por exemplo, o *fs* que permite ler o arquivo da chave privada e do certificado SSL necessários para usar HTTPS, ou o axios, uma biblioteca HTTP cliente que permite fazer requisições HTTP. Por fim, a biblioteca *jsonwebtoken* que permite criar e verificar JSON Web Tokens utilizados ao longo do código.

5.2.1 Funções da Api

Assim que a Api é iniciada, um middleware para CORS é ativado pois, como não temos acesso ao código da Api do governo brasileiro, é necessário que esse intermediador seja criado para possibilitar solicitações do navegador para o servidor SSO. Além disso, algumas variáveis de configuração foram definidas, como: clientId, clientSecret e redirectUri. Esses valores são usados para autenticar o cliente e redirecioná-lo para o URI especificado na requisição para o servidor SSO.

Em seguida, a rota /redirect é definida, essa é a rota que o servidor usa para redirecionar o usuário para o aplicativo após a autenticação bem-sucedida no GovBr. Neste protótipo, a função criada extrai o código validador e o state passado pela solicitação do Front-End, e

na sequência, faz uma solicitação POST para o SSO para obter o token de acesso e o token de identificação. Nesta solicitação, é necessário que seja definido um cabeçalho com os parâmetros Content-Type sendo um application/x-www-form-urlencoded e Authorization sendo o ClientId:ClientSecret codificado em Base64 com a palavra Basic presente antes da inforação, durante o desenvolvimento foi utilizado o codificador recomendado pela própria documentação do login-único: https://www.base64decode.org/. Além disso, o body da requisição deve ser composto pelos grantType que especifica para o SSO o tipo de autorização, nesse caso é authorizationCode, o código validador para que o SSO possa realizar a autorização, redirectUri para o SSO redirecionar após realizar a autorização. Após isso, a Api recebe os tokens e redireciona o usuário de volta para a página Home do aplicativo com os tokens e o tempo de expiração presentes na URL.

Com isso, o Front-End da aplicação se torna capaz de utilizar os tokens para ter acesso a informações do usuário cadastradas no sistema do governo brasileiro, por exemplo, o token de acesso pode ser usado para acessar recursos sobre a autenticação e o token de identificação para acessar informações sobre o usuário autenticado. Além de que, com o tempo de expiração o Front-End é capaz de desconectar o usuário da aplicação caso o token seja expirado. O padrão do SSO é que cada token dure apenas 60 (sessenta) minutos, ou seja, após esse tempo o usuário terá que se autenticar novamente.

5.3 INTEGRAÇÃO COM A BLOCKCHAIN JORNADA DO ESTUDANTE

No contexto do integração do protótipo com a blockchain, foram adotados alguns comandos e procedimentos para a configuração e execução dos diferentes componentes e serviços envolvidos. Primeiramente, foi necessário executar a rede localmente utilizando um ambiente Docker. Para garantir a limpeza deste ambiente, utilizou-se os seguintes comandos:

- *docker rm -f $(docker ps -a -q) para remover todos os contêineres existentes.*
- *docker system prune -a para limpar as imagens presentes.*

Em seguida, o uso do minifabric permitiu a construção da imagem "labsec/minifab-acadblock"por meio do comando "docker build -t labsec/minifab-acadblock .". Após isso, utilizou-se o comando

- *./minifab up -e true*

para subir a rede com configuração avançada. Posteriormente, os chaincodes foram instalados e inicializados através dos seguintes comandos:

- *./minifab ccup -n decree*
- *./minifab ccup -n XMLog*

- *./minifab ccup -n academicRecords*

Os aplicativos "appacademic"e "appdecree"foram iniciados com os comandos correspondentes:

- *./minifab appacademic*
- *./minifab appdecree*

e os logs podem ser acompanhados através dos comandos:

- *docker logs appacademic -f*
- *docker logs appdecree -f*

Além disso, na pasta raiz do projeto, o comando "docker compose up –build -d"foi utilizado para construir e iniciar os contêineres especificados no arquivo de composição. Os logs dos contêineres "backend-tcc-apiacademic-1"e "backend-tcc-apidecree-1"foram verificados através dos comandos "docker logs backend-tcc-apiacademic-1"e "docker logs backend-tcc-apidecree-1".

Esses procedimentos e comandos são essenciais para a configuração e execução do ambiente de desenvolvimento, garantindo a correta inicialização dos componentes e serviços necessários para o protótipo. O guia do usuário e o guia do desenvolvedor, presentes no repositório da Jornada do Estudante, fornecem informações mais detalhadas sobre esses processos, oferecendo um passo a passo para a configuração e execução do sistema.

5.4 DESAFIOS

Nesta seção, serão abordados os desafios identificados no contexto de autenticação com o GovBr, que precisaram ser superados para garantir a integração da plataforma web com a Api do Governo e a Api da Jornada do Estudante.

5.4.1 Integração com o GovBr

Ao tentar realizar uma requisição para o ambiente staging do SSO do governo brasileiro ocorria um erro de CORS (Cross-Origin Resource Sharing) indicando que a Api GovBr detectou que uma solicitação de recurso (nesse caso um HTML) estaria sendo feita a partir de um site diferente do que o recurso está localizado, sendo assim, para evitar ataques maliciosos, a requisição seria bloqueada. Para evitar esse comportamento, um middleware CORS foi adicionado ao código da Api de Autenticação do protótipo. A função desse middleware é adicionar cabeçalhos de resposta que permitam que um navegador solicite recursos de outro domínio sem bloqueios. O código utilizado adiciona os cabeçalhos "Access-Control-Allow-Origin"e

"Access-Control-Allow-Headers"a resposta do servidor, isso permite que qualquer origem solicite recursos, evitando um erro de Cross-Origin.

Após isso, ao seguir o passo-a-passo detalhado para a integração com o GovBr foram enfrentados alguns problemas, a maioria referente a credenciais. Isso acontece pois, para ter acesso ao ambiente de desenvolvimento do governo é necessário solicitar acesso e encaminhar um plano de integração devidamente preenchido. Diante disso, a UFSC já possui acesso a esse ambiente então foi necessário apenas solicitar que os dados fossem repassados ao autor, entre eles: clientId (chave de acesso do cliente) e a redirectUri (URL que o servidor do governo redireciona após realizar a autenticação), para essa URL funcionar foi necessário que fosse atribuído um endereço externo na máquina virtual hospedada no servidor da UFSC, dado pelo valor "govbr.labsec.ufsc.br", com esse endereço a Api de Autenticação do protótipo poderia rodar no servidor UFSC e ainda assim ser acessada por IPs externos.

Além disso, outro problema enfrentado foi que o ambiente de desenvolvimento do governo brasileiro não aceita a conta que está criada no ambiente de produção, logo seria necessário criar uma nova conta, porém o cadastro de nova conta não existe nesse ambiente. Com isso, um passo a passo teve que ser seguido para conseguir realizar o cadastro no ambiente staging da SSO: Primeiro é necessário que um CPF qualquer seja definido, após isso deve clicar em "Esqueci minha senha"e depois na opção de "Não tenho celular"e, em seguida, "Tentar de outra forma", será aberto uma tela com perguntas de certos dados pré-definidos do ambiente staging, são eles: Data de nascimento como 01/01/1980 e nome da mãe como MAMÃE.

Por fim, foi identificado que a API do GovBr está rodando com o protocolo HTTPS, o que proporciona uma comunicação segura e criptografada entre o cliente e o servidor. No entanto, não estava no escopo deste protótipo a geração de certificados para lidar com protocolo HTTPS de maneira confiável. Dessa forma, foram gerados certificados específicos para testes (OpenSSL Essentials, 2023), a fim de estabelecer essa comunicação segura e confiável no ambiente de desenvolvimento entre os usuários e a API de Autenticação. A geração de certificados HTTPS confiáveis para o ambiente de produção se mostra essencial para garantir a privacidade e a segurança dos dados dos usuários durante o processo de autenticação, reforçando a confiabilidade do sistema como um todo.

5.4.2 Integração com a Jornada do Estudante

Após realizar a autenticação, foi identificada a necessidade de determinar qual dado presente nos tokens do GovBr deve ser utilizado para acessar um usuário na blockchain da Jornada do Estudante. Ao analisar a estrutura dos tokens gerados pelo sistema de autenticação do GovBr, observamos que eles contêm informações relevantes, como o identificador único do usuário e as permissões associadas a ele. Para acessar um usuário específico na blockchain, é crucial identificar o dado correto contido nos tokens que possa ser utilizado como uma chave ou referência para a identificação desse usuário. Essa informação específica do token, que permite a correlação com os registros da blockchain, foi o CPF (Cadastro de Pessoa Física). Ao realizar

uma consulta na blockchain pelo CPF do aluno autenticado, é possível obter diversos dados acadêmicos e, como a Jornada do Estudante só cadastra um aluno quando o histórico do mesmo é registrado e para possuir um histórico é obrigatório ter um CPF, não existe chances de um aluno registrado na blockchain não possuir esse identificador.

Além desse problema, após definir o dado utilizado para realizar buscas na blockchain foi necessário realizar um estudo para definir quais rotas e dados seriam possíveis de obter utilizando o CPF do aluno autenticado. Com isso, foi identificado que os dados do histórico escolar, tais como o nome do curso, a data e a forma de ingresso na instituição, o número do registro do histórico, entre outras informações relacionadas à formação acadêmica do aluno, poderiam ser resgatados. Diante disso, foi possível obter mais informações relacionadas ao curso, a instituição e ao próprio aluno, pois com o CPF é possível conseguir os identificadores de várias entidades da blockchain.

6 TESTE DE USABILIDADE

Esta seção tem como objetivo avaliar a usabilidade e a satisfação dos usuários em relação à autenticação na rede Jornada do Estudante via GovBr e à interface gráfica da aplicação Web desenvolvida para possibilitar a interação entre estudantes e instituições de ensino superior. Para essa avaliação, será utilizado o questionário SUS (System Usability Scale), uma escala de usabilidade rápida e simplificada amplamente utilizada para medir a usabilidade de sistemas e interfaces.

Com isso, espera-se obter dados que permitam aprimorar a aplicação, identificar pontos fortes e áreas de melhoria, bem como compreender a experiência dos usuários ao interagir com a autenticação na rede Blockchain e a interface gráfica desenvolvida. Os resultados deste estudo contribuirão para a evolução da aplicação, visando proporcionar uma melhor experiência aos usuários e promover a interação eficaz entre estudantes e instituições de ensino superior.

6.1 QUESTIONÁRIO SUS

O questionário SUS (System Usability Scale) é uma escala de usabilidade composta por dez perguntas que fornecem uma visão global das avaliações subjetivas de usabilidade. Ele é baseado em uma escala Likert, que consiste em uma série de declarações às quais o respondente indica o grau de concordância ou discordância em uma escala de 1 a 5 pontos.

Para construir esse método de avaliação, segundo (BROOKE et al., 1996), foi montado um grupo de 50 perguntas potenciais para fazerem parte do questionário. Em seguida, dois exemplos de sistemas de software foram selecionados com base na concordância geral de que um era "muito fácil de usar" e o outro era quase impossível de usar, mesmo para usuários altamente habilidosos tecnicamente. Vinte pessoas de um grupo, com ocupações que variavam de secretário a programador de sistemas, classificaram ambos os sistemas em relação as 50 perguntas potenciais do questionário em uma escala de 5 pontos, variando de "concordo totalmente"a "discordo totalmente".

As perguntas que levaram a respostas mais extremas do grupo inicial foram selecionadas, com isso, houve correlações muito próximas entre elas, de ±0,7 a ±0,9. Além disso, essas perguntas foram selecionadas de forma que a resposta comum para metade delas fosse concordância forte e, para a outra metade, discordância forte. Isso foi feito para evitar viés de resposta causado pelo fato de os respondentes não terem que pensar sobre cada declaração; alternando itens positivos e negativos, o respondente é obrigado a ler cada declaração e fazer um esforço para pensar se concorda ou discorda dela.

Dito isso, com o questionário SUS aplicado neste protótipo, pode-se observar que as declarações selecionadas abrangem uma variedade de aspectos da usabilidade do sistema, como necessidade de suporte, treinamento e complexidade. Portanto, possuem um alto nível de validade aparente para medir a usabilidade de um sistema.

6.1.1 Coleta de dados

Para dar início ao experimento, deve ser levado em consideração alguns aspectos: O ambiente utilizado é de desenvolvimento, ou seja, o usuário não conseguirá entrar em sua conta GovBr oficial; A versão utilizada da blockchain Jornada do Estudante é a v1.05, logo, dados presentes em versões mais atualizadas não estarão presentes; O contexto desse trabalho é permitir a integração e autenticação entre a rede blockchain e o GovBr, diante disso, os dados presentes são apenas exemplos do que pode ser mostrado em tela para o usuário; Para ter acesso aos dados o usuário deve ser previamente cadastrado na rede blockchain utilizada.

Com isso, para realizar a etapa de coleta de dados, foi adotado um método que permitiu aos participantes utilizar o protótipo da aplicação em uma máquina disponibilizada pelo autor. Após a interação com o protótipo, os participantes foram entrevistados para responderem às perguntas relacionadas à autenticação na rede Blockchain via GovBr e à interface gráfica.

6.1.1.1 Participantes do experimento

Para definir quais participantes iriam participar do experimento, foi realizado um processo de seleção para identificar pessoas que atendessem aos critérios estabelecidos para este estudo. Os critérios incluem pessoas de 17 a 70 anos, com ensino médio completo, podendo ser estudante ou não. Esses critérios foram definidos visando abranger o teste da aplicação para pessoas que não entendam nada de tecnologia até pessoas que já estão acostumada com esse meio. A amostra é composta por 13 participantes para representar a diversidade dos usuários-alvo da aplicação.

Cada participante foi convidado a utilizar o protótipo da aplicação em um período determinado. Durante essa interação, os participantes tiveram a oportunidade de explorar os recursos da aplicação, realizar a autenticação na rede Blockchain através do GovBr utilizando uma conta teste e navegar pela interface gráfica para acessar informações relacionadas à essa conta.

Após a interação com o protótipo, os participantes foram entrevistados individualmente. Durante a entrevista, as perguntas relacionadas à autenticação na rede Blockchain e à interface gráfica foram apresentadas aos participantes. Com isso, as suas respostas foram anotadas para registro e posterior análise. Além disso, quando necessário, outras observações relevantes sobre a interação dos participantes com o protótipo ou comentários adicionais foram registrados para fornecer contexto adicional à análise dos dados coletados. Segue abaixo os participantes e alguns dados relevantes para análises:

- P1 - Idade: 21 anos; Gênero: Masculino; Nível de escolaridade: Cursando ensino superior; É estudante: Sim;
- P2 - Idade: 19 anos; Gênero: Feminino; Nível de escolaridade: Ensino médio completo; É estudante: Não;

- P3 - Idade: 45 anos; Gênero: Masculino; Nível de escolaridade: Ensino superior incompleto; É estudante: Não;
- P4 - Idade: 37 anos; Gênero: Feminino; Nível de escolaridade: Ensino médio completo; É estudante: Não;
- P5 - Idade: 65 anos; Gênero: Feminino; Nível de escolaridade: Ensino superior completo; É estudante: Não;
- P6 - Idade: 20 anos; Gênero: Feminino; Nível de escolaridade: Cursando ensino superior; É estudante: Sim;
- P7 - Idade: 22 anos; Gênero: Masculino; Nível de escolaridade: Cursando ensino superior; É estudante: Sim;
- P8 - Idade: 23 anos; Gênero: Masculino; Nível de escolaridade: Cursando ensino superior; É estudante: Sim;
- P9 - Idade: 25 anos; Gênero: Masculino; Nível de escolaridade: Ensino superior incompleto; É estudante: Não;
- P10 - Idade: 21 anos; Gênero: Feminino; Nível de escolaridade: Cursando ensino superior; É estudante: Sim;
- P11 - Idade: 17 anos; Gênero: Masculino; Nível de escolaridade: Ensino médio completo; É estudante: Sim;
- P12 - Idade: 28 anos; Gênero: Feminino; Nível de escolaridade: Cursando ensino superior; É estudante: Sim;
- P13 - Idade: 20 anos; Gênero: Masculino; Nível de escolaridade: Cursando ensino superior; É estudante: Sim;

6.1.2 Perguntas do questionário

Nesta seção, serão apresentadas as perguntas que foram utilizadas para capturar a experiência dos participantes em relação à autenticação na rede Blockchain e à interface gráfica do protótipo. Para isso, foi solicitado aos participantes que suas respostas fossem baseadas em suas experiências com a aplicação, visando o máximo de sinceridade, pois essas respostas servem para direcionar melhorias futuras e aprimorar a aplicação, garantindo uma experiência mais satisfatória para os estudantes. Segue abaixo as perguntas utilizadas no questionário aplicado:

- Q1 - Eu acredito que gostaria de utilizar este sistema com frequência.
- Q2 - Eu achei o sistema desnecessariamente complexo.

- Q3 - Eu achei o sistema fácil de usar.
- Q4 - Eu acredito que precisaria de apoio de um especialista para utilizar o sistema.
- Q5 - Eu achei as funções do sistema bem integradas.
- Q6 - Eu achei o sistema confuso de usar.
- Q7 - Eu acredito que a maioria das pessoas aprenderia a utilizar o sistema rapidamente.
- Q8 - Eu achei o sistema muito inconsistente.
- Q9 - Eu me senti confiante usando o sistema.
- Q10 - Eu precisaria aprender muitas coisas novas antes de conseguir utilizar o sistema.

6.1.3 Análise dos resultados

Nesta seção, serão apresentados os detalhes sobre a análise dos resultados obtidos por meio do questionário aplicado aos participantes. Essa análise visa fornecer uma compreensão mais aprofundada da usabilidade e satisfação dos estudantes em relação à autenticação na rede Blockchain e à interface gráfica do protótipo desenvolvido. Esses resultados serão interpretados com o objetivo de identificar pontos fortes e áreas de melhoria do sistema, bem como avaliar a eficácia das funcionalidades implementadas.

Diante disso, serão utilizadas técnicas estatísticas e métodos de análise qualitativa para examinar os dados coletados. A análise quantitativa se baseará em medidas descritivas, como média, desvio padrão e frequência de respostas. Além disso, as respostas qualitativas serão examinadas para identificar padrões, temas comuns e comentários relevantes dos participantes. É importante destacar que a privacidade dos participantes foi preservada durante todo o processo de análise. Sendo assim, todas as informações privadas fornecidas foram tratadas de forma confidencial e utilizadas exclusivamente para fins acadêmicos.

Segundo (BROOKE et al., 1996), a métrica utilizada para medir a usabilidade com base nos dados do questionário é o SUS Score, que é calculado seguindo os seguintes métodos:

- Para as questões Q1, Q3, Q5, Q7 e Q9 a pontuação deve ser substituída de 1, por exemplo, caso o participante informe a pontuação da Q1 como 4, o valor dessa pergunta é 4-1=3.
- Para as questões Q2, Q4, Q6, Q8 e Q10 a pontuação deve ser substituída de 5, por exemplo, caso o participante informe a pontuação da Q2 como 3, o valor dessa pergunta é 5-3=2.
- Para obter o valor do SUS score, deve ser realizado um somatório do valor de cada pergunta e por fim uma multiplicação por 2.5 que resulta em um valor no intervalo de 0 a 100.

-	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score
P1	3	1	5	1	4	1	4	1	5	1	90
P2	4	1	4	1	4	2	4	2	5	2	82.5
P3	3	1	5	1	5	1	4	1	5	2	90
P4	3	1	5	1	4	1	4	1	5	2	87.5
P5	3	2	5	2	5	1	4	1	5	3	82.5
P6	5	1	5	1	5	2	5	2	5	1	95
P7	5	2	5	1	5	2	5	1	5	1	95
P8	4	2	5	1	5	2	4	1	5	1	90
P9	3	1	5	1	5	2	5	2	5	1	87.5
P10	5	2	4	1	5	2	4	1	5	3	85
P11	2	1	4	1	5	2	4	1	5	2	82.5
P12	5	1	5	1	4	1	4	1	5	1	95
P13	4	1	5	1	4	1	4	1	5	1	92.5

Após a coleta e análise dos dados, foram calculadas as médias e o intervalo das notas obtidas no questionário SUS. Neste caso, o SUS Score médio foi calculado em aproximadamente 89 pontos, o que indica uma boa avaliação da usabilidade da aplicação desenvolvida. Essa pontuação reflete a percepção positiva dos participantes em relação à facilidade de uso, eficiência e satisfação geral com a autenticação na rede Blockchain via GovBr e a interface gráfica da aplicação.

Além da média do SUS Score, foi analisado o intervalo das notas obtidas, que varia de 82.5 a 95 pontos. Essa variação de 12.5 pontos indica que, apesar da avaliação geral positiva, houve algumas diferenças na percepção dos participantes. Essas diferenças podem ser atribuídas a diferentes níveis de familiaridade com a autenticação do GovBr, experiência prévia com interfaces similares ou preferências individuais dos participantes.

Com base nesse SUS score médio de 89 pontos, pode-se levantar alguns aspectos que podem ter influenciado nesse alto desempenho como, por exemplo, o uso do Design System do GovBr na aplicação. O uso de um design system reconhecido e amplamente adotado faz com que a aplicação aproveite os princípios e as diretrizes de design estabelecidos, que foram desenvolvidos levando em consideração a usabilidade e a experiência do usuário. Permitindo que seja desenvolvida uma interface mais intuitiva e familiar para os usuários, o que pode ter influenciado positivamente a usabilidade percebida.

Além disso, aproximadamente 77% dos participantes consideraram a aplicação fácil de utilizar, essa resultado pode se dar devido a clareza do fluxo de navegação da aplicação. Junto a isso, pode ser notado que aproximadamente 62% dos participantes escolheram a opção "concordo totalmente"com relação a integração das funcionalidades da aplicação, tal valor pode ser devido as funções intuitivas e eficientes presentes no protótipo.

7 CONCLUSÃO

Este trabalho teve como objetivo desenvolver um protótipo de uma aplicação web para autenticação e integração de uma rede Blockchain de ensino via GovBr, utilizando conceitos de criptografia, segurança e protocolos de comunicação web. Com isso, o trabalho seguiu uma metodologia que envolveu etapas de leituras exploratórias, desenvolvimento do protótipo e avaliação da usabilidade, sendo descartado a avaliação de desempenho. Isso pois, ao começar o desenvolvimento do protótipo, ficou claro que não faria sentido realizar experimentos de desempenho pois esses os resultados desses testes teriam a influência das APIs do Governo Federal e da Jornada do Estudante e não do protótipo em si, caso houvesse a necessidade de criar uma API para acessar os dados da blockchain, o teste de desempenho faria sentido.

O método proposto neste trabalho foi baseado em uma abordagem que integra os conhecimentos sobre criptografia, segurança e usabilidade para criar um sistema de autenticação eficiente e seguro. O ineditismo do método está relacionado à sua aplicação específica em uma rede Blockchain de ensino, com o objetivo de prover a autenticação e identificação dos usuários de forma confiável e transparente. Com esse método, os resultados obtidos no teste de usabilidade, utilizando a metodologia System Usability Scale (SUS), revelou um score médio de aproximadamente 89 pontos, indicando uma boa avaliação da usabilidade da aplicação desenvolvida. Esse resultado reflete a percepção positiva dos participantes em relação à facilidade de uso, eficiência e satisfação geral com a autenticação na rede Blockchain via GovBr e a interface gráfica da aplicação. Além disso, a clareza do fluxo de navegação da aplicação e a integração eficiente das funcionalidades contribuíram para a boa avaliação por parte dos usuários.

No entanto, é importante destacar as limitações deste trabalho. Uma das limitações está relacionada à generalização dos resultados, uma vez que a avaliação da usabilidade foi realizada com um número limitado de participantes e em um contexto específico de aplicação. Além disso, as diferenças na percepção dos participantes indicam que ainda há espaço para aprimoramento da usabilidade da aplicação, considerando as preferências individuais e níveis de familiaridade com a autenticação do GovBr. Outra limitação foi a versão do projeto Jornada do Estudante, o protótipo desenvolvido neste trabalhou utilizou a v1.05, pode ser necessário efetuar alguns ajustes para versões mais recentes.

Diante disso, como trabalhos futuros, sugere-se a descentralização da API de Autenticação criada neste protótipo e a realização de estudos adicionais para aprimorar a usabilidade da aplicação, levando em consideração as preferências individuais dos usuários e explorando possíveis melhorias na interface gráfica. Além disso, é importante buscar formas de expandir a avaliação da aplicação, envolvendo um número maior de participantes e considerando diferentes contextos de uso. Também seria interessante investigar a viabilidade de integrar novas funcionalidades e aperfeiçoamentos para a interface desenvolvida, podendo mostrar mais dados que podem ser úteis para o estudante. Outra questão importante a ser analisada, é a possibilidade de implementar um método de autenticação para a API da Jornada do Estudante, através de uma requisição pelo MEC ou com uma verificação do token GovBr na rota academicRecords, pois

ela não faz nenhum verificação do token obtido neste protótipo.

REFERÊNCIAS

ABREU, A. W. S.; COUTINHO, E. F.; BEZERRA, C. I. M. 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**. New York, NY, USA: Association for Computing Machinery, 2020. (SBCARS '20), p. 151–160. ISBN 9781450387545. Disponível em: https://doi.org/10.1145/3425269.3425285.

ACM Digital Library. **ACM Digital Library - [Acesso em 12-06-2023]**. 2023. Disponível em: https://dl.acm.org.

BROOKE, J. System usability scale (sus): a quick-and-dirty method of system evaluation user information. **Reading, UK: Digital equipment co ltd**, v. 43, p. 1–7, 1986.

BROOKE, J. et al. Sus-a quick and dirty usability scale. **Usability evaluation in industry**, London, England, v. 189, n. 194, p. 4–7, 1996.

CAI, W. et al. Decentralized applications: The blockchain-empowered software system. **IEEE Access**, IEEE, v. 6, p. 53019–53033, 2018.

ETHEREUM, W. Ethereum whitepaper. **Ethereum. URL: https://ethereum. org [Acesso em 29-01-2023]**, 2014.

EVANS, T. M. Cryptokitties, cryptography, and copyright. **AIPLA QJ**, HeinOnline, v. 47, p. 219, 2019.

EZAWA, Y. et al. Blockchain-based cross-domain authorization system for user-centric resource sharing. **Blockchain: Research and Applications**, v. 4, n. 2, p. 100126, 2023. ISSN 2096-7209. Disponível em: https://www.sciencedirect.com/science/article/pii/S2096720923000015.

Governo Brasileiro. **Padrão Digital de Governo - [Acesso em 10-06-2023]**. 2023. Disponível em: https://www.gov.br/ds/home.

HERLIHY, M. Blockchains from a distributed computing perspective. **Communications of the ACM**, ACM New York, NY, USA, v. 62, n. 2, p. 78–85, 2019.

Hyperledger Foundation. **A Blockchain Platform for the Enterprise — hyperledger-fabricdocs main documentation [Acesso em 29-01-2023]**. 2020. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.5/.

JIANG, P.; JONES, D. B.; JAVIE, S. How third-party certification programs relate to consumer trust in online transactions: An exploratory study. **Psychology & Marketing**, Wiley Online Library, v. 25, n. 9, p. 839–858, 2008.

JOSHI, A.; HAN, M.; WANG, Y. A survey on security and privacy issues of blockchain technology. **Mathematical Foundations of Computing**, v. 1, p. 121–147, 01 2018.

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

OpenSSL Essentials. **OpenSSL Essentials - [Acesso em 10-06-2023]**. 2023. Disponível em: https://www.digitalocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs.

PALMA, L. M. et al. Blockchain and smart contracts for higher education registry in brazil. **International Journal of Network Management**, Wiley Online Library, v. 29, n. 3, p. e2061, 2019.

React. **ReactJS**. 2013. Disponível em: https://reactjs.org.

Science Direct. **Science Direct - [Acesso em 12-06-2023]**. 2023. Disponível em: https://www.sciencedirect.com.

SHARPLES, M.; DOMINGUE, J. The blockchain and kudos: A distributed system for educational record, reputation and reward. In: SPRINGER. **European conference on technology enhanced learning**. Cham: Springer International Publishing, 2016. p. 490–496.

STALLINGS, W. **Criptografia e segurança de redes. Princípios e práticas, ch. 6**. U.S.: Pearson Prentice Hall, 2006.

TURKANOVIĆ, M. et al. Eductx: A blockchain-based higher education credit platform. **IEEE access**, IEEE, v. 6, p. 5112–5127, 2018.

WIERUCH, R. **The road to react: Your journey to master plain yet pragmatic react. js**. Berlin: Robin Wieruch, 2017.

XU, X.; WEBER, I.; STAPLES, M. **Architecture for blockchain applications**. U.S.: Springer, 2019.

APÊNDICE A – ARTIGO DA MONOGRAFIA

Identificação e Autenticação de Estudantes em uma Rede Blockchain de Ensino

Bruno Daniel Elias

[1]DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC)

Abstract. *Currently, the Ministry of Education (MEC) is responsible for authenticating each process per- formed by educational institutions in Brazil. However, an opportunity arises to decentralize this responsibility, allowing the participating universities to authenticate and approve the pro- cesses based on the rules defined by the MEC. Hyperledger Fabric technology is presented as a promising solution to achieve this decentralization. Based on this proposal, MEC started a project in partnership with the Computer Security Laboratory (LABSEC) of the Federal Uni- versity of Santa Catarina (UFSC). The objective is to develop a model that uses blockchain and smart contracts in the registration of higher education institutions. However, there is a problem to be addressed: the authentication and identification of students on the network. To resolve this issue, the present work proposes the creation of a web graphical interface prototype that allows students to authenticate themselves and use the system developed by LABSEC. The prototype must be accessible on any machine with a browser and internet connection. In addition, the means of authentication used will be gov.br, which is already integrated with various technolo- gies in Brazil, to authenticate and identify students who wish to access the blockchain network. In order to facilitate the process and provide a better user experience, the graphical interface was developed using the ReactJS framework following the Design System of the Brazilian Govern- ment. After data collection and analysis, it was possible to calculate the mean and range of scores obtained in the SUS (System Usability Scale) questionnaire. The SUS Score mean was approximately 89 points, indicating a good assessment of the application's usability. This re- sult reflects the positive perception of the participants regarding the ease of use, efficiency, and general satisfaction with authentication on the Blockchain network via gov.br and the applica- tion's graphical interface. The analysis of the range of scores showed a variation of 12.5 points, ranging from 82.5 to 95 points. This variation indicates that, although the general evaluation is positive, there were differences in the participants' perceptions. These differences can be attributed to several factors, such as familiarity with gov.br authentication, previous experience with similar interfaces, and individual preferences.*

Resumo. *Atualmente, o Ministério da Educação (MEC) é responsável por autenticar cada processo exe- cutado pelas instituições de ensino no Brasil. No entanto, surge uma oportunidade de des- centralizar essa responsabilidade, permitindo que as universidades participantes autentiquem e aprovem os processos com base nas regras definidas pelo MEC. A tecnologia Hyperledger Fabric é apresentada como uma solução promissora para alcançar essa descentralização.*

Com base nessa proposta, o MEC iniciou um projeto em parceria com o Laboratório de Segurança em Computação (LABSEC) da Universidade Federal de Santa Catarina (UFSC). O objetivo é de- senvolver um modelo que utilize blockchain e contratos inteligentes no registro de instituições de ensino superior. No entanto, há um problema a ser abordado: a autenticação e identificação dos estudantes na rede. Para resolver essa questão, o presente trabalho propõe a criação de um protótipo de interface gráfica web que permita aos estudantes se autenticarem e utilizarem o sistema desenvolvido pelo LABSEC. O protótipo deve ser acessível em qualquer máquina com um navegador e conexão à internet. Além disso, o meio de autenticação utilizado será o gov.br, que já está integrado a várias tecnologias no Brasil, para autenticar e identificar os estudantes que desejam acessar a rede blockchain. A fim de facilitar o processo e fornecer uma melhor experiência ao usuário, a interface gráfica foi desenvolvida utilizando o framework ReactJS se- guindo o Design System do Governo Brasileiro. Após a coleta e análise dos dados, foi possível calcular a média e o intervalo das notas obtidas no questionário SUS (System Usability Scale). A média do SUS Score foi de aproximadamente 89 pontos, indicando uma boa avaliação da usabilidade da aplicação. Esse resultado reflete a percepção positiva dos participantes em rela- ção à facilidade de uso, eficiência e satisfação geral com a autenticação na rede Blockchain via gov.br e a interface gráfica da aplicação. A análise do intervalo das notas mostrou uma variação de 12,5 pontos, indo de 82,5 a 95 pontos. Essa variação indica que, embora a avaliação geral seja positiva, houve diferenças na percepção dos participantes. Essas diferenças podem ser atri- buídas a diversos fatores, como familiaridade com a autenticação do gov.br, experiência prévia com interfaces similares e preferências individuais.

1. Introdução

O termo Blockchain foi introduzido ao mundo no artigo acadêmico *Bitcoin: A peer-to-peer to electronic cash system* [Nakamoto 2008]. O artigo apresentou as falhas que os modelos baseados em confiança possuíam mesmo funcionando adequadamente para realizar transações. Além dessas falhas, o autor afirma que a dependência de um terceiro para mediar os problemas que podem vir a ocorrer durante uma transação faz com que aumente os gastos para que essa ação seja realizada. Diante disso, segundo [Nakamoto 2008], o ideal para um sistema eletrônico de transações é uma criptografia baseada em comprovação e não em confiança. Isso permite que duas partes possam realizar transações entre elas sem a necessidade de uma terceira entidade envolvida. Com isso, surge o *Bitcoin*, primeira moeda inteiramente digital utilizada para realizar transações, utilizando assinatura digital, hash e timestamp em conjunto com o protocolo de consenso, para resolver a maior parte dos problemas existentes em um modelo baseado em confiança. Após isso, as tecnologias baseadas em blockchain entraram em ascensão, sendo consideradas uma revolução no quesito financeiro e tecnológico. Essa tecnologia combina os registros de transações em cadeias de blocos em uma rede. Uma rede blockchain pode ser utilizada para prestação de serviços governamentais, facilitando o compartilhamento de informações e a coordenação de processos entre os órgãos do governo. Embora o conteúdo da maioria dos registros governamentais seja público, nesta

rede hipotética haveria uma certa complexidade em relação à confidencialidade e privacidade dos dados. Com base nesses aspectos, diversas redes continuaram surgindo para atender as demandas que apareciam. Entre elas, a rede Ethereum [Ethereum 2014] se destacou, pois surgiu com a ideia de ser muito mais do que um sistema de pagamentos ou apenas uma outra moeda digital. Ela foi desenvolvida para ser uma plataforma descentralizada que consegue executar contratos inteligentes sem ter a interferência de terceiros, isso aumentou a flexibilidade e a funcionalidade de diversos programas que utilizavam tecnologias blockchain. Porém, mesmo com todas essas vantagens, o fato de não ser uma rede blockchain permissionada faz com que muitas empresas não utilizem este tipo de tecnologia por medo da falta de privacidade ou pelo fato de não cobrir o caso de uso desejado. Para resolver os problemas de confidencialidade e privacidade dos dados, além de aumentar a gama de casos de usos que podem ser atendido pela tecnologia blockchain, surgiu a plataforma Hyperledger Fabric [Hyperledger Foundation 2020]. O Hyperledger Fabric é uma plataforma permissionada e privada que utiliza contratos inteligentes escritos em linguagens atualmente utilizadas pela maioria das empresas, que viram nessa plataforma a possibilidade de entrar finalmente no mundo da blockchain. Isso porque ela tornou possível que empresas privadas e até mesmo públicas pudessem utilizar a rede dentro do seu próprio escopo sem se preocupar em seus dados privados estarem visíveis aos outros. Eventualmente, o Ministério da Educação (MEC) encontrou uma oportunidade de melhorar seu sistema de autenticação, pois diversos processos burocráticos são realizados por ele ao longo do ano. Isso porque somente o MEC é responsável por autenticar cada processo realizado pelas instituições de ensino brasileiras. Por exemplo, todo diploma emitido por uma entidade precisa do aval do MEC para ser considerado autêntico. Logo, a tecnologia da Hyperledger Fabric consegue fazer com que essa responsabilidade seja descentralizada para todas as universidade que fizerem parte da rede, isso fará com que cada entidade tenha que validar, autenticar e aprovar cada processo com base nas regras definidas pelo MEC, tornando o trabalho do Ministério da Educação menos burocrático, mais rápido e seguro. Para solucionar alguns dos principais problemas em Instituições de Ensino Superior, no artigo: Blockchain and smart contracts for higher education registry in Brazil [Palma et al. 2019], é sugerido a criação de um novo modelo que utiliza blockchain e contratos inteligentes em Instituições de Ensino Superior. Essa proposta faz com que seja possível a autenticação de cada processo por entidades que fazem parte da rede. O MEC viu o modelo como promissor e iniciou um projeto com o Laboratório de Segurança em Computação (LABSEC) da Universidade Federal de Santa Catarina (UFSC), dando sequência ao trabalho sugerido pelo artigo. Porém esse modelo não abrange a parte de autenticação e identificação de um estudante na rede e qual a melhor maneira de realizar esse processo.Diante desses fatores, este trabalho tem como finalidade realizar a autenticação do estudante, bem como identificá-lo na rede. Contudo, o modelo em questão necessita que o usuário tenha algum conhecimento prévio nas tecnologias usadas para conseguir se integrar. Logo, será desenvolvido um protótipo de interface gráfica web que possibilitará ao estudante se autenticar e fazer uso do sistema iniciado pela equipe do LABSEC em qualquer máquina que tenha um navegador e acesso a internet. Além disso, para que seja possível autenticar e identificar o estudante que quer acessar a rede blockchain, pretende-se utilizar o meio de autenticação gov.br pois este já está integrado com diversas tecnologias presentes no Brasil. Contudo, é necessário criar uma interface para que o usuário final não fique perdido diante de todos esses proces-

sos, para isso será utilizado o framework ReactJS [React 2013] que facilita a criação de interfaces gráficas no meio de desenvolvimento web.

2. Conceitos Fundamentais

Esta seção introduz ao leitor os conceitos necessários para entender como funcionam as tecnologias deste trabalho e os motivos de serem utilizadas.

2.1. Criptografia de Chave Pública

Segundo [Stallings 2006], a criptografia de chave pública se difere das demais, pois é baseada em funções matemáticas ao invés de substituição e permutação. Fora isso, a criptografia assimétrica utiliza duas chaves separadamente, diferente da simétrica que utiliza apenas uma chave. O que pode induzir um aumento de eficácia em certos pontos como confidencialidade e autenticação. A criptografia de chave pública tomou proporções maiores diante da tentativa de amenizar os principais problemas vistos nas criptografias simétricas. Um deles é a distribuição de chaves, que necessita de um compartilhamento prévio de uma chave entre ambas as partes envolvidas ou fazer o uso de um centro de distribuição de chaves. Além disso, um outro problema bem recorrente nas criptografias simétricas está relacionado com as assinaturas digitais. Com a atual digitalização de grande parte dos documentos em papel, é necessário um método que garanta a satisfação de todas as partes envolvidas na troca de mensagem, certificando que ela foi enviada por certa pessoa.

Com base nisso, um algoritmo de criptografia assimétrica começa gerando o par de chaves, uma pública e outra privada. A chave pública pode ser revelada, enquanto somente a privada é guardada apenas pelo dono do par, afirma [Stallings 2006]. Quando uma parte A deseja enviar uma mensagem para uma parte B ela encripta usando a chave pública de B, ao receber a mensagem ela é decriptada utilizando a própria chave privada de B, desse modo, apenas o destinatário B consegue decriptar a mensagem, pois é o único que tem conhecimento da chave privada correspondente.

2.2. Funções Hash Criptográficas

Segundo [Stallings 2006], uma função hash se trata de uma função normal que aceita uma mensagem M de tamanho variável como entrada e gera uma saída, h = H(M), com tamanho fixo. Para o quesito aplicações de segurança, o tipo de função hash a ser analisado é a criptográfica. Pois com ela é computacionalmente inviável ser alvo de ataques, como força bruta, para identificar o dado mapeado para o hash. Em funções hash, no geral, a entrada é composta de um inteiro de tamanho variável e o valor do tamanho da mensagem. Esses campos de tamanho são considerados medidas de segurança pois aumentam a dificuldade que um invasor tem ao tentar recriar a mensagem com o mesmo valor de hash.

Funções hash criptográficas são muito utilizadas na autenticação de mensagens para realizar a verificação da integridade dessas mensagens trocadas. Ainda segundo [Stallings 2006], ao utilizar essas funções, o valor delas passa a ser considerado um resumo da mensagem. Podemos considerar que, durante uma troca de mensagens, um emissor calcula um valor de hash para a mensagem e transmite ambos, o valor hash e a mensagem ao receptor. O receptor realiza o mesmo cálculo de hash sobre a mensagem e

compara com o valor de hash recebido. Se o valor não coincidir, o receptor saberá que algo foi alterado durante o processo. Dito isso, um resumo criptográfico precisa ser bem protegido, pois se um invasor conseguir alterar o conteúdo de uma mensagem ele não deve conseguir modificar o valor hash a fim de realizar ataques a integridade dos dados.

2.3. Blockchain

O termo blockchain refere-se a uma tecnologia que é capaz de suportar a verificação de transações entre múltiplas partes, além de conseguir executar e gravar essas transações, combinando criptografia e gerenciamento de dados numa mesma rede. Cada blockchain, segundo [Xu et al. 2019], é composta por uma *ledger*, que corresponde a uma lista encadeada de blocos. Nessa *ledger*, cada bloco contém um conjunto de transações realizadas na rede, um valor hash, um endereço do bloco anterior e um *timestamp* que contém o momento em que o bloco foi criado. Nesse caso, quando um dado é enviado, um protocolo chamado de consenso é executado diversas vezes para decidir quais dos dados anexar a *ledger*. Esse protocolo de consenso, em geral, envolve vários participantes, e seu conceito é aplicável a uma ampla variedade de modelos computacionais. Porém como muitos estão envolvidos, os participantes maliciosos podem gerar algumas falhas na rede. Pois as *ledgers* exigem a capacidade de realizar consenso recorrente devido à sua longa vida útil para adicionar um fluxo de transações na rede.

2.4. Hyperledger Fabric

Com a popularidade das tecnologias blockchain surgiu o interesse em utilizar esta tecnologia em ambientes corporativos, porém os casos de usos que as empresas necessitavam não eram satisfeitos com blockchains públicas, como a Ethereum. Pois muitas empresas necessitavam que os participantes da rede fossem identificáveis e que os dados das transações fossem privados e confidenciais. Diante disso, segundo a [Hyperledger Foundation 2020], a Fabric surgiu na intenção de ser utilizada por ambientes corporativos, sendo uma blockchain de código aberto. Ela possui uma arquitetura de fácil configuração e altamente modular. Além de suportar contratos inteligentes escritos em linguagens de programação populares no ramo corporativo, possibilitando que diversos projetos sejam desenvolvidos sem a necessidade de treinamentos em novas áreas.

3. Trabalhos Relacionados

3.1. A Blockchain-based Architecture for Query and Registration of Student Degree Certificates

Neste artigo, os autores [Abreu et al. 2020] propõem um protótipo que faz o uso da tecnologia blockchain para resolver problemas relacionados à autenticação e segurança de diplomas no contexto do ensino superior. Ele destaca os desafios enfrentados pelas instituições de ensino, como o acesso e segurança dos dados de diplomas, a necessidade de validação sem a intervenção de terceiros, a disponibilidade dos sistemas das instituições para comprovação dos diplomas, o armazenamento seguro dos dados e a prevenção de documentos falsificados. A proposta apresenta uma arquitetura baseada em blockchain que busca fornecer um ambiente com credibilidade e segurança, permitindo a publicação e consulta das informações dos diplomas de estudantes de ensino superior.

Diante disso, o autor menciona que a tecnologia blockchain pode abordar os problemas mencionados de forma mais adequada do que as tecnologias tradicionais, permitindo transações entre partes confiáveis, como as instituições de ensino, estudantes, empresas, governo e outras instituições de ensino. Ele também destaca que o uso da blockchain pode reduzir os riscos de perda de informações, economizar papel, reduzir custos de gerenciamento e prevenir documentos falsificados. Com isso, o autor descreve uma arquitetura de referência para a blockchain, um protótipo de um aplicativo no domínio educacional que utiliza recursos de blockchain e uma avaliação da solução tanto do ponto de vista técnico quanto do usuário. O texto também menciona que a validação da tecnologia blockchain é baseada na lógica de negócios do registro de diplomas, sendo que toda a interação é realizada por meio de uma interface semelhante a um sistema tradicional.

Para ilustrar a arquitetura proposta, é definido um cenário envolvendo uma instituição de ensino superior privada, e a validação é realizada por dois participantes responsáveis pelo setor de emissão de diplomas da instituição. Os dados educacionais inseridos na blockchain são baseados em um ato administrativo específico do Ministério da Educação do Brasil. O trabalho conclui mencionando que a utilização da tecnologia blockchain pode trazer benefícios significativos para a gestão de dados de diplomas no ensino superior, proporcionando maior segurança, verificabilidade e confiabilidade.

Com isso, pode-se concluir que este trabalho correlato se difere da proposta deste documento. Isso pois, este trabalho especifica o uso de autenticação via gov.br. Isso implica que o protótipo estará aproveitando a infraestrutura de autenticação fornecida pelo governo brasileiro por meio do gov.br, que é um sistema de login único que permite aos usuários acessar vários serviços online do governo com um único cadastro. Além disso, o protótipo utilizará o Design System do Governo Federal, visando aumentar a usabilidade da interface pois todos os elementos visuais já são utilizados em outros sites governamentais.

3.2. Blockchain-based cross-domain authorization system for user-centric resource sharing

Neste artigo, o autor [Ezawa et al. 2023] propõe uma arquitetura de autorização em várias áreas utilizando tecnologia blockchain para promover o compartilhamento de dados entre organizações. A arquitetura é baseada no conceito de User-Managed Access (UMA), que permite o compartilhamento flexível de dados entre domínios com controle de acesso personalizável. O artigo aborda a falta de transparência nos sistemas de autorização convencionais, especialmente em sistemas de larga escala como cidades inteligentes. A arquitetura proposta utiliza a tecnologia blockchain para solucionar esse problema, garantindo transparência e integridade no controle de acesso. Além disso, a implementação da arquitetura demonstrou bom desempenho, com tempo de processamento abaixo de 500 ms e pouca variação no tempo de processamento.

Além disso, o autor apresenta várias contribuições significativas. Primeiro, propõe uma arquitetura de autorização em várias áreas que não depende de um único ponto de confiança, permitindo o compartilhamento de recursos entre diferentes domínios sem a necessidade de uma autoridade central. Em segundo lugar, aumenta a transparência e a integridade no controle de acesso por meio do uso da tecnologia blockchain, possibilitando que os usuários confirmem se o controle de acesso está sendo executado conforme

especificado. Terceiro, reduz os custos operacionais de um sistema de autorização, automatizando sua operação por meio da tecnologia blockchain e compartilhando os custos entre várias organizações. Além disso, a arquitetura proposta permite que os proprietários de recursos escolham o sistema de autorização mais adequado para gerenciar seus recursos, centralizando o gerenciamento em diferentes domínios. A implementação da arquitetura foi realizada utilizando Hyperledger Fabric e foi avaliada quanto ao tempo de processamento e tamanho dos dados, apresentando resultados promissores.

Em resumo, o autor propõe uma arquitetura de autorização em várias áreas baseada em blockchain, visando resolver os desafios de transparência e controle de acesso em sistemas de larga escala, como cidades inteligentes. A arquitetura permite o compartilhamento flexível de recursos entre organizações, reduzindo custos operacionais e oferecendo maior transparência e integridade no controle de acesso. Os resultados da implementação demonstram um desempenho satisfatório. Essa abordagem tem o potencial de promover o compartilhamento de dados de forma segura e eficiente no contexto da economia digital. A diferença entre essa abordagem e a autenticação com o GovBr reside no escopo e na aplicação. A autenticação com o login único do GovBr se concentra principalmente na autenticação do usuário, fornecendo um único ponto de acesso aos serviços governamentais. Já a arquitetura proposta no estudo aborda a questão da autorização e do compartilhamento de dados entre organizações em diferentes domínios, utilizando a tecnologia blockchain para garantir a transparência e a integridade do controle de acesso. O login único do gov.br é um sistema confiável e amplamente adotado no contexto brasileiro, o que pode gerar confiança e facilitar a adesão dos usuários. Além disso, o governo tem a responsabilidade de proteger os dados dos cidadãos e, portanto, é esperado que os sistemas governamentais sigam rigorosas medidas de segurança e conformidade.

4. Proposta

A proposta deste trabalho se baseia em desenvolver uma aplicação que utiliza as funcionalidades de uma rede Blockchain para possibilitar a interação entre estudantes e instituições de ensino superior. Como base, foi utilizado o projeto Jornada do Estudante, que é mantido atualmente por uma parceria realizada entre o MEC, LABSEC e o Laboratório Bridge, e se trata de uma rede que utiliza a arquitetura blockchain para emitir e controlar certificados digitais das IES. Porém, esse projeto não prevê a interação e autenticação entre estudante e universidades. Com isso, surgiu a possibilidade de desenvolver um novo protótipo que coloque o estudante como um ator primário e utilize de tecnologias para realizar a autenticação do mesmo na rede Blockchain.

Diante disso, o modelo base que foi seguido neste trabalho tem sua arquitetura composta por: nós das organizações, sendo as organizações e os estudantes inclusos; *smart contracts*, para emitir e controlar os certificados gerados; aplicações responsáveis por conectar os estudantes na rede Blockchain e APIs para que seja possível acessar os métodos providos pelas aplicações. Logo, utilizando este modelo pretende-se desenvolver uma aplicação Web em React.js para realizar a autenticação do estudante e garantir uma interface gráfica para a navegação. Desse modo, é possível que o usuário visualize seus certificados, suas atividades complementares, seus documentos oficiais, entre outros.

Primeiramente foi construído uma API de Autenticação, que autentica o usuário

utilizando o Login Único do *gov.br*. Juntamente a isso um protótipo de aplicação web foi construído, utilizando React.js e bibliotecas de interface, visando uma usabilidade de alto nível. Este protótipo tem como responsabilidade integrar o usuário com a rede Jornada do Estudante após ser autenticado.

5. Protótipo

5.1. Front-End da Aplicação

Nesta seção, apresentaremos o Front-End do nosso protótipo, que busca proporcionar aos usuários uma experiência intuitiva e agradável ao interagir com o sistema. O protótipo foi desenvolvido com base nas melhores práticas de design e usabilidade presentes no guia de UI/UX do Design System GovBr [Governo Brasileiro 2023], visando fornecer uma interface responsiva, de fácil navegação e com uma estética moderna. Com elementos cuidadosamente dispostos e uma paleta de cores padronizada, o objetivo é criar uma experiência visualmente atraente e com boa usabilidade para os usuários.

5.2. Página de Login

A página de login, se baseia em um componente funcional React chamado SignIn, que é responsável por renderizar o botão de acesso a rede blockchain na página raiz da aplicação. A página contém apenas um botão que chama o método de login com o govbr, iniciando todo o processo de autenticação do usuário. Ao acionar método handleGovBrSignIn(), um get para a API de autorização do Governo Federal Brasileiro, mais especificamente para a versão de homologação (staging), é realizado. A requisição contém uma série de parâmetros que indicam ao servidor qual é a aplicação que está requisitando autorização, qual é o escopo de acesso requerido, a URI para a qual o servidor deve redirecionar a resposta da requisição, além de um valor nonce e state que são usados para proteger a requisição contra ataques de terceiros mal intencionados.

5.3. Página de Home

A página de Home, se baseia em um componente funcional React, chamado Home, que é responsável por renderizar a página principal da aplicação. Ele importa o hook useLocation() do React Router para coletar os dados vindos pela URL após o redirect de autenticação e a biblioteca jwt-decode para decodificar os tokens de autenticação. Em seguida, define uma interface chamada DecodedIdToken que contém as informações do usuário contidas no token decodificado, como nome, e-mail, CPF e data de expiração. Além disso, esse componente possui uma função chamada handleLogout() que faz uma solicitação ao servidor de autenticação para deslogar o usuário e redirecioná-lo para a página de login caso essas condições sejam verdadeiras: se o tempo de expiração do token é zero ou se o token não está presente.

5.4. Api de Autenticação

Neste protótipo, foi desenvolvido uma API utilizando Node.js juntamente com o framework Express, para lidar com requisições web, e a biblioteca HTTPS, que permite que os usuários se autentiquem usando o serviço de autenticação SSO (Single Sign-On) do governo brasileiro. Além disso, outras bibliotecas foram utilizadas como, por exemplo, o *fs* que permite ler o arquivo da chave privada e do certificado SSL necessários para usar

HTTPS, ou o axios, uma biblioteca HTTP cliente que permite fazer requisições HTTP. Por fim, a biblioteca *jsonwebtoken* que permite criar e verificar JSON Web Tokens utilizados ao longo do código.

5.5. Funções da Api

Assim que a Api é iniciada, um middleware para CORS é ativado pois, como não temos acesso ao código da Api do governo brasileiro, é necessário que esse intermediador seja criado para possibilitar solicitações do navegador para o servidor SSO. Além disso, algumas variáveis de configuração foram definidas, como: clientId, clientSecret e redirectUri. Esses valores são usados para autenticar o cliente e redirecioná-lo para o URI especificado na requisição para o servidor SSO.

Em seguida, a rota /redirect é definida, essa é a rota que o servidor usa para redirecionar o usuário para o aplicativo após a autenticação bem-sucedida no GovBr. Neste protótipo, a função criada extrai o código validador e o state passado pela solicitação do Front-End, e na sequência, faz uma solicitação POST para o SSO para obter o token de acesso e o token de identificação. Nesta solicitação, é necessário que seja definido um cabeçalho com os parâmetros Content-Type sendo um application/x-www-form-urlencoded e Authorization sendo o ClientId:ClientSecret codificado em Base64 com a palavra Basic presente antes da inforação, durante o desenvolvimento foi utilizado o codificador recomendado pela própria documentação do login-único: https://www.base64decode.org/. Além disso, o body da requisição deve ser composto pelos grantType que especifica para o SSO o tipo de autorização, nesse caso é authorizationCode, o código validador para que o SSO possa realizar a autorização, redirectUri para o SSO redirecionar após realizar a autorização. Após isso, a Api recebe os tokens e redireciona o usuário de volta para a página Home do aplicativo com os tokens e o tempo de expiração presentes na URL.

Com isso, o Front-End da aplicação se torna capaz de utilizar os tokens para ter acesso a informações do usuário cadastradas no sistema do governo brasileiro, por exemplo, o token de acesso pode ser usado para acessar recursos sobre a autenticação e o token de identificação para acessar informações sobre o usuário autenticado. Além de que, com o tempo de expiração o Front-End é capaz de desconectar o usuário da aplicação caso o token seja expirado. O padrão do SSO é que cada token dure apenas 60 (sessenta) minutos, ou seja, após esse tempo o usuário terá que se autenticar novamente.

6. Experimento SUS

O questionário SUS (System Usability Scale) é uma escala de usabilidade composta por dez perguntas que fornecem uma visão global das avaliações subjetivas de usabilidade. Ele é baseado em uma escala Likert, que consiste em uma série de declarações às quais o respondente indica o grau de concordância ou discordância em uma escala de 1 a 5 pontos.

Para construir esse método de avaliação, segundo [Brooke et al. 1996], foi montado um grupo de 50 perguntas potenciais para fazerem parte do questionário. Em seguida, dois exemplos de sistemas de software foram selecionados com base na concordância geral de que um era ”muito fácil de usar” e o outro era quase impossível de usar, mesmo para usuários altamente habilidosos tecnicamente. Vinte pessoas de um

grupo, com ocupações que variavam de secretário a programador de sistemas, classificaram ambos os sistemas em relação as 50 perguntas potenciais do questionário em uma escala de 5 pontos, variando de ”concordo totalmente” a ”discordo totalmente”.

As perguntas que levaram a respostas mais extremas do grupo inicial foram selecionadas, com isso, houve correlações muito próximas entre elas, de ±0,7 a ±0,9. Além disso, essas perguntas foram selecionadas de forma que a resposta comum para metade delas fosse concordância forte e, para a outra metade, discordância forte. Isso foi feito para evitar viés de resposta causado pelo fato de os respondentes não terem que pensar sobre cada declaração; alternando itens positivos e negativos, o respondente é obrigado a ler cada declaração e fazer um esforço para pensar se concorda ou discorda dela.

Dito isso, com o questionário SUS aplicado neste protótipo, pode-se observar que as declarações selecionadas abrangem uma variedade de aspectos da usabilidade do sistema, como necessidade de suporte, treinamento e complexidade. Portanto, possuem um alto nível de validade aparente para medir a usabilidade de um sistema.

6.1. Coleta de dados

Para dar início ao experimento, deve ser levado em consideração alguns aspectos: O ambiente utilizado é de desenvolvimento, ou seja, o usuário não conseguirá entrar em sua conta GovBr oficial; A versão utilizada da blockchain Jornada do Estudante é a v1.05, logo, dados presentes em versões mais atualizadas não estarão presentes; O contexto desse trabalho é permitir a integração e autenticação entre a rede blockchain e o GovBr, diante disso, os dados presentes são apenas exemplos do que pode ser mostrado em tela para o usuário; Para ter acesso aos dados o usuário deve ser previamente cadastrado na rede blockchain utilizada.

Com isso, para realizar a etapa de coleta de dados, foi adotado um método que permitiu aos participantes utilizar o protótipo da aplicação em uma máquina disponibilizada pelo autor. Após a interação com o protótipo, os participantes foram entrevistados para responderem às perguntas relacionadas à autenticação na rede Blockchain via GovBr e à interface gráfica.

6.2. Participantes do experimento

Para definir quais participantes iriam participar do experimento, foi realizado um processo de seleção para identificar pessoas que atendessem aos critérios estabelecidos para este estudo. Os critérios incluem pessoas de 17 a 70 anos, com ensino médio completo, podendo ser estudante ou não. Esses critérios foram definidos visando abranger o teste da aplicação para pessoas que não entendam nada de tecnologia até pessoas que já estão acostumada com esse meio. A amostra é composta por 13 participantes para representar a diversidade dos usuários-alvo da aplicação.

Cada participante foi convidado a utilizar o protótipo da aplicação em um período determinado. Durante essa interação, os participantes tiveram a oportunidade de explorar os recursos da aplicação, realizar a autenticação na rede Blockchain através do GovBr utilizando uma conta teste e navegar pela interface gráfica para acessar informações relacionadas à essa conta.

Após a interação com o protótipo, os participantes foram entrevistados individualmente. Durante a entrevista, as perguntas relacionadas à autenticação na rede Blockchain

e à interface gráfica foram apresentadas aos participantes. Com isso, as suas respostas foram anotadas para registro e posterior análise. Além disso, quando necessário, outras observações relevantes sobre a interação dos participantes com o protótipo ou comentários adicionais foram registrados para fornecer contexto adicional à análise dos dados coletados.

6.3. Perguntas do questionário

Nesta seção, serão apresentadas as perguntas que foram utilizadas para capturar a experiência dos participantes em relação à autenticação na rede Blockchain e à interface gráfica do protótipo. Para isso, foi solicitado aos participantes que suas respostas fossem baseadas em suas experiências com a aplicação, visando o máximo de sinceridade, pois essas respostas servem para direcionar melhorias futuras e aprimorar a aplicação, garantindo uma experiência mais satisfatória para os estudantes. Segue abaixo as perguntas utilizadas no questionário aplicado:

- Q1 - Eu acredito que gostaria de utilizar este sistema com frequência.
- Q2 - Eu achei o sistema desnecessariamente complexo.
- Q3 - Eu achei o sistema fácil de usar.
- Q4 - Eu acredito que precisaria de apoio de um especialista para utilizar o sistema.
- Q5 - Eu achei as funções do sistema bem integradas.
- Q6 - Eu achei o sistema confuso de usar.
- Q7 - Eu acredito que a maioria das pessoas aprenderia a utilizar o sistema rapidamente.
- Q8 - Eu achei o sistema muito inconsistente.
- Q9 - Eu me senti confiante usando o sistema.
- Q10 - Eu precisaria aprender muitas coisas novas antes de conseguir utilizar o sistema.

6.4. Análise dos resultados

Após a coleta e análise dos dados, foram calculadas as médias e o intervalo das notas obtidas no questionário SUS. Neste caso, o SUS Score médio foi calculado em aproximadamente 89 pontos, o que indica uma boa avaliação da usabilidade da aplicação desenvolvida. Essa pontuação reflete a percepção positiva dos participantes em relação à facilidade de uso, eficiência e satisfação geral com a autenticação na rede Blockchain via GovBr e a interface gráfica da aplicação.

Além da média do SUS Score, foi analisado o intervalo das notas obtidas, que varia de 82.5 a 95 pontos. Essa variação de 12.5 pontos indica que, apesar da avaliação geral positiva, houve algumas diferenças na percepção dos participantes. Essas diferenças podem ser atribuídas a diferentes níveis de familiaridade com a autenticação do GovBr, experiência prévia com interfaces similares ou preferências individuais dos participantes.

Com base nesse SUS score médio de 89 pontos, pode-se levantar alguns aspectos que podem ter influenciado nesse alto desempenho como, por exemplo, o uso do Design System do GovBr na aplicação. O uso de um design system reconhecido e amplamente adotado faz com que a aplicação aproveite os princípios e as diretrizes de design estabelecidos, que foram desenvolvidos levando em consideração a usabilidade e a experiência do usuário. Permitindo que seja desenvolvida uma interface mais intuitiva e familiar para os usuários, o que pode ter influenciado positivamente a usabilidade percebida.

Além disso, aproximadamente 77% dos participantes consideraram a aplicação fácil de utilizar, essa resultado pode se dar devido a clareza do fluxo de navegação da aplicação. Junto a isso, pode ser notado que aproximadamente 62% dos participantes escolheram a opção "concordo totalmente" com relação a integração das funcionalidades da aplicação, tal valor pode ser devido as funções intuitivas e eficientes presentes no protótipo.

7. Conclusão

Este trabalho teve como objetivo desenvolver um protótipo de uma aplicação web para autenticação e integração de uma rede Blockchain de ensino via GovBr, utilizando conceitos de criptografia, segurança e protocolos de comunicação web. Com isso, o trabalho seguiu uma metodologia que envolveu etapas de leituras exploratórias, desenvolvimento do protótipo e avaliação da usabilidade, sendo descartado a avaliação de desempenho. Isso pois, ao começar o desenvolvimento do protótipo, ficou claro que não faria sentido realizar experimentos de desempenho pois esses os resultados desses testes teriam a influência das APIs do Governo Federal e da Jornada do Estudante e não do protótipo em si, caso houvesse a necessidade de criar uma API para acessar os dados da blockchain, o teste de desempenho faria sentido.

O método proposto neste trabalho foi baseado em uma abordagem que integra os conhecimentos sobre criptografia, segurança e usabilidade para criar um sistema de autenticação eficiente e seguro. O ineditismo do método está relacionado à sua aplicação específica em uma rede Blockchain de ensino, com o objetivo de prover a autenticação e identificação dos usuários de forma confiável e transparente. Com esse método, os resultados obtidos no teste de usabilidade, utilizando a metodologia System Usability Scale (SUS), revelou um score médio de aproximadamente 89 pontos, indicando uma boa avaliação da usabilidade da aplicação desenvolvida. Esse resultado reflete a percepção positiva dos participantes em relação à facilidade de uso, eficiência e satisfação geral com a autenticação na rede Blockchain via GovBr e a interface gráfica da aplicação. Além disso, a clareza do fluxo de navegação da aplicação e a integração eficiente das funcionalidades contribuíram para a boa avaliação por parte dos usuários.

No entanto, é importante destacar as limitações deste trabalho. Uma das limitações está relacionada à generalização dos resultados, uma vez que a avaliação da usabilidade foi realizada com um número limitado de participantes e em um contexto específico de aplicação. Além disso, as diferenças na percepção dos participantes indicam que ainda há espaço para aprimoramento da usabilidade da aplicação, considerando as preferências individuais e níveis de familiaridade com a autenticação do GovBr. Outra limitação foi a versão do projeto Jornada do Estudante, o protótipo desenvolvido neste trabalhou utilizou a v1.05, pode ser necessário efetuar alguns ajustes para versões mais recentes.

Diante disso, como trabalhos futuros, sugere-se a descentralização da API de Autenticação criada neste protótipo e a realização de estudos adicionais para aprimorar a usabilidade da aplicação, levando em consideração as preferências individuais dos usuários e explorando possíveis melhorias na interface gráfica. Além disso, é importante buscar formas de expandir a avaliação da aplicação, envolvendo um número maior de participantes e considerando diferentes contextos de uso. Também seria interessante

investigar a viabilidade de integrar novas funcionalidades e aperfeiçoamentos para a interface desenvolvida, podendo mostrar mais dados que podem ser úteis para o estudante. Outra questão importante a ser analisada, é a possibilidade de implementar um método de autenticação para a API da Jornada do Estudante, através de uma requisição pelo MEC ou com uma verificação do token GovBr na rota academicRecords, pois ela não faz nenhum verificação do token obtido neste protótipo.

References

Abreu, A. W. S., Coutinho, E. F., and Bezerra, C. I. M. (2020). 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*, SBCARS '20, page 151–160, New York, NY, USA. Association for Computing Machinery.

Brooke, J. et al. (1996). Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7.

Ethereum, W. (2014). Ethereum whitepaper. *Ethereum. URL: https://ethereum. org [Acesso em 29-01-2023]*.

Ezawa, Y., Kakei, S., Shiraishi, Y., Mohri, M., and Morii, M. (2023). Blockchain-based cross-domain authorization system for user-centric resource sharing. *Blockchain: Research and Applications*, 4(2):100126.

Governo Brasileiro (2023). Padrão digital de governo - [acesso em 10-06-2023].

Hyperledger Foundation (2020). A Blockchain Platform for the Enterprise — hyperledger-fabricdocs main documentation [acesso em 29-01-2023].

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260.

Palma, L. M., Vigil, M. A., Pereira, F. L., and Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in brazil. *International Journal of Network Management*, 29(3):e2061.

React (2013). Reactjs.

Stallings, W. (2006). *Criptografia e segurança de redes. Princípios e práticas, ch. 6*. Pearson Prentice Hall, U.S.

Xu, X., Weber, I., and Staples, M. (2019). *Architecture for blockchain applications*. Springer, U.S.