BLOCKCHAIN NO DESENVOLVIMENTO DE UMA APLICAÇÃO BASEADA NO USO DE SMART CONTRACTS PARA CRIAÇÃO DE IDENTIFICADORES ÚNICOS PESSOAIS

Gustavo Roberge Warmling[1],Ana Cláudia Garcia Barbosa[2]

Resumo: A falta de exploração e testes existentes em relação aos diferentes casos de uso para as tecnologias geradas ao entorno da *blockchain* é o fator motivador para o presente trabalho e, com base nisso o autor visa proporcionar uma nova perspectiva, utilizando a visão descentralizada das aplicações nativas dessa nova era de desenvolvimento. São utilizados os princípios das redes *blockchain*, fazendo uso de sua confidencialidade, proteção e abrangência global, para criar uma plataforma que seja capaz de produzir e autenticar identificadores pessoais sem depender de uma entidade governamental centralizadora, resultando em uma plataforma capaz de criar, validar e demonstrar identificadores pessoais únicos, ligados ao endereço público da carteira de criptomoedas do usuário. O presente estudo serve como uma demonstração de conceito, não tendo foco em sua aplicação real e na relação plataforma e usuário, mas sim de apresentar o potencial dessa tecnologia emergente, explorando os seus desafios, possibilidades e aplicações dentro da área selecionada. A aplicação apresentou resultados satisfatórios e demonstrou ser possível e proveitoso o uso da *blockchain* no ramo de identificação pessoal, abrindo também a discussão para novas implementações dessa tecnologia emergente e pouco explorada. Mesmo não sendo o foco do estudo, foi possível visualizar a existência de uma barreira de aplicação em grupos de usuário sem conhecimento prévio sobre a *blockchain*.

Palavras-chave: blockchain; ethereum; smart contracts; visão descentralizada; identificadores pessoais; blockchain para criação de identificadores.

ABSTRACT: The lack of exploration and existing tests regarding the different use cases for the technologies generated around blockchain is the motivating factor for the present work and, based on this, the author aims to provide a new perspective, using the decentralized vision of the applications native to this new era of development. The principles of blockchain networks are used, making use of their confidentiality, protection and global reach, to create a platform that is able to produce and authenticate personal identifiers without relying on a centralizing government, resulting in a platform that is able to create, validate and demonstrate unique personal identifiers linked to the public address of the user's cryptocurrency wallet. The present study serves as a demonstration of concept, not focusing on its actual application and the relationship between platform and user, but rather to present the potential of this emerging technology, exploring its challenges, possibilities, and applications within the selected area. The application presented satisfactory results and demonstrated that it is possible and profitable to use blockchain in the field of personal identification, also opening the discussion for new implementations of this emerging and little explored technology. Even though it was not the focus of the study, it was possible to visualize the existence of an application barrier in user groups without prior knowledge about blockchain

Keywords: blockchain; ethereum; smart contracts; decentralized view; personal identifiers; blockchain for identifier creation.

1 INTRODUÇÃO

Existe um movimento sociocultural global referente à convergência da realidade física com a digital, reorganizando o dia à dia dos indivíduos para um novo, e único, modo de vida integrado à tecnologia. Surge então a necessidade de que a identidade física e a digital também se unam, gerando um modelo de identidade que aumente a segurança e a privacidade daqueles que o usam (SIMONS, 2018).

Ao fazer parte desse novo mercado de trabalho, no setor de desenvolvimento de *software*, agora remoto e global, o autor teve a possibilidade de vivenciar dificuldades relacionadas à quantidade de identificadores de identidade. Nessa experiência foi possível detectar uma lacuna relacionada à falta de um

identificador global e independente, que possibilite o reconhecimento do indivíduo não levando em consideração o seu país de origem e assegurando sua privacidade e segurança.

No mundo da tecnologia da informação, pelo menos uma vez num ciclo de poucos anos emerge uma nova tecnologia que parece ser uma resposta a todos os problemas e o início de uma nova era dourada. Desde 2016, esta tecnologia tem sido a *blockchain* (ZĪLE; STRAZDIŅA, 2018). A maioria dos tópicos de pesquisa atuais sobre *blockchain*, e sua utilização junto aos contratos inteligentes, concentra-se em questões de linguagem de programação, segurança e privacidade, enquanto a proliferação da utilização de *blockchain* e seus contratos também apresentam um novo horizonte de aplicações diversificadas possíveis (ZHENG et al., 2020).

Uma *blockchain* é um livro-razão, registro de escrituras com a finalidade de coletar e registrar dados cronológicos de transações, digital, que armazena publicamente transações após realizar a verificação das mesmas através de *nodes*, pontos de conexão dentro de uma rede. Cada transação é validada pelos *nodes* e são asseguradas por uma função de *hash*, ou seja, um código criado a partir de um bloco de dados criptografado. Uma transação é ligada pelo seu valor de *hash* de transação anterior. Uma vez adicionada à cadeia de bloqueio, ninguém pode modificá-la ou alterá-la, mas esta pode ser vista abertamente, trazendo transparência e segurança ao sistema (MOHANTA; PANDA; JENA, 2018).

Um contrato inteligente é um código executável que age na *blockchain* para facilitar, operar e fazer cumprir os termos de um acordo entre partes não confiantes. Pode ser pensado como um sistema que libera bens digitais a todas ou algumas das partes envolvidas, uma vez cumpridas as regras pré-definidas. Em comparação com os contratos tradicionais, os contratos inteligentes não dependem de uma terceira parte de confiança para operar, resultando em baixos custos de transação. Diferentes redes *blockchain* podem ser utilizadas para desenvolver contratos inteligentes, mas o Ethereum é a mais comum. (ALHARBY; MOORSEL, 2017)

Neste contexto, o presente trabalho visa empregar os conceitos das redes *blockchain*, utilizando-se de sua privacidade, segurança e globalização, na criação de uma plataforma capaz de gerar e validar identificadores pessoais não atrelados à um governo centralizador. Este servirá como uma prova de conceito, não visando explorar

os desafios de aplicação real, da plataforma, mas apresentar o potencial desta tecnologia emergente.

Os objetivos específicos consistem em: assimilar a necessidade de um novo identificador digital; integrar os conceitos de *blockchain* à identidade digital; investigar a possibilidade de uso da *blockchain* para gerar uma nova identificação; desenvolver uma aplicação utilizando a tecnologia *blockchain* e a possibilidade de uso dessa tecnologia no setor de identificação pessoal.

2 TRABALHOS CORRELATOS

O trabalho intitulado ”Identificação digital baseada em *blockchain*: Um conceito disruptivo no ciberespaço.”, realizado por Batista, Dias e Silva, da Universidade Federal de Goiás (UFG), e publicado no V simpósio internacional de inovação em mídias interativas, em 2018, teve como objetivo apresentar uma nova padronização do comportamento dos indivíduos no mundo digital, baseado em blockchain, bem como analisar as possibilidades de sua aplicação, partindo do conceito de reputação digital chegando, até mesmo, em incentivos financeiros e identidade autêntica.

O caso de uso analisado baseia-se no cadastro, do usuário, dentro de uma plataforma, esse tendo a posse das chaves privadas e públicas. Essa capaz de marcar os conteúdos digitais de seu interesse, enquanto aquela será utilizada para estabelecer a autenticidade do conteúdo assinado. A assinatura digital somente será validada após a inserção do seu bloco à blockchain (BATISTA; DIAS; SILVA, 2018).

Sendo o propósito do trabalho apenas explicar e analisar uma das possíveis aplicações da tecnologia *blockchain* para a criação de identificadores digitais, o trabalho obteve resultado satisfatório ao analisar a aplicação proposta. A blockchain se mostrou uma alternativa interessante para solucionar as problemáticas de confiabilidade, não necessitando de um intermédio ou de autoridades centrais, além de, também, se mostrar interessante para outros setores como o financeiro e o governamental (BATISTA; DIAS; SILVA, 2018).

O artigo “Uso Não Financeiro de *Blockchain*: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos”, desenvolvido por Costa, Faustino, et al., no centro de informática da Universidade

Federal da Paraíba (UFPB) teve como motivação a necessidade de proteção aos documentos de âmbito acadêmico.

Nesse artigo foi proposto a construção de uma plataforma, que servirá como uma prova de conceito, com foco em ser escalável e agnóstica, para realizar o armazenamento e, posteriormente, a verificação da autenticidade de documentos digitais vindos do setor acadêmico, combinando técnicas de blockchain junto a certificação digital e preservação digital (LIRA, 2018).

Foi conquistado, com a finalização do projeto, a criação de um novo ambiente com o intuito de dar suporte ao protótipo gerado. Nesse é possível autenticar e preservar os documentos digitais acadêmicos. Também foi analisado a existência de potencial para outras organizações educacionais, sendo elas públicas ou privadas, adotarem a plataforma desenvolvida. Além de ser explanado que a infraestrutura deste pode, também, apoiar a criação de outros diferentes tipos de serviço relacionados à autenticação e preservação de documentos em ambiente virtual (DELOITTE, 2018).

O estudo ”*Blockchain-Based Privacy-Preserving Vaccine Passport System*”, em português, Sistema de Passaporte de Vacina, preservador de privacidade, baseado em blockchain, realizado por Cao, Chen e Cao, publicado em 2022 na *Hindawi Security and Communication Networks*, Baseado em *Blockchain*, propõe um novo sistema de passaporte de vacinas para controle e prevenção de doenças contaminosas.

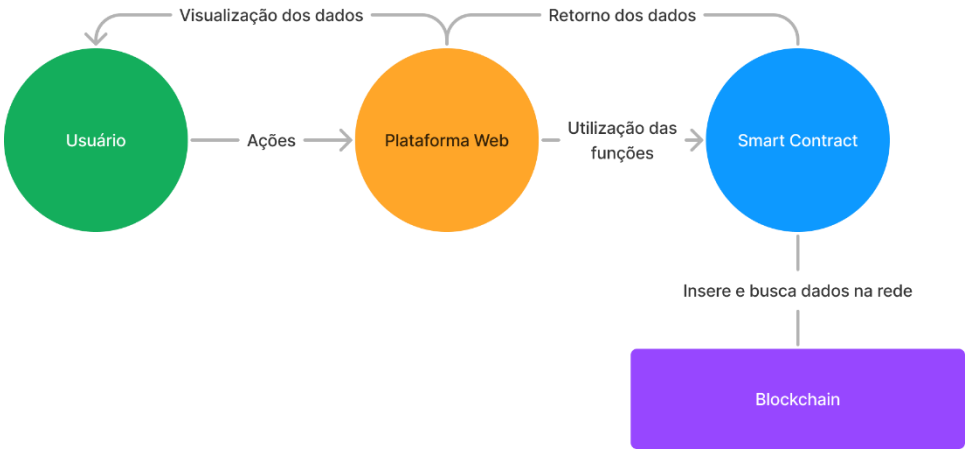
Propondo então um sistema de dupla blockchain, garantindo segurança e escalonamento de forma global, para validação e gerenciamento dos passaportes e vacinas inseridos. As ferramentas de criptografia utilizadas, como por exemplo credenciais anônimas, garantem que os usuários não exponham nenhuma informação privada na hora de utilizar-se de seu passaporte de vacinas e, da mesma forma, garante segurança ao órgão fiscalizador que irá validar as vacinas aplicadas, podendo tomar medidas de segurança especificas para cada vacina não cadastrada. (CAO; CHEN; CAO, 2022)

Após finalização, conclui-se que o estudo conseguiu realizar melhoras no sistema de validação, de forma global, dos indivíduos. Além de conseguir manter o enfoque inicial de não expor dados pessoais e sensíveis dos usuários. (CAO; CHEN; CAO, 2022)

3 MATERIAIS E MÉTODOS

O desenvolvimento de uma aplicação capaz de criar e validar identidades digitais utilizando blockchain consistiu numa pesquisa aplicada com base tecnológica, de categoria descritiva e de estudo bibliográfico. O sistema teve como objetivo a criação de um contrato inteligente capaz de gerar identidades com identificadores únicos e, posteriormente, validar esses identificadores para a visualização das identidades criadas, o usuário utilizará a aplicação através de uma interface web *front-end*.

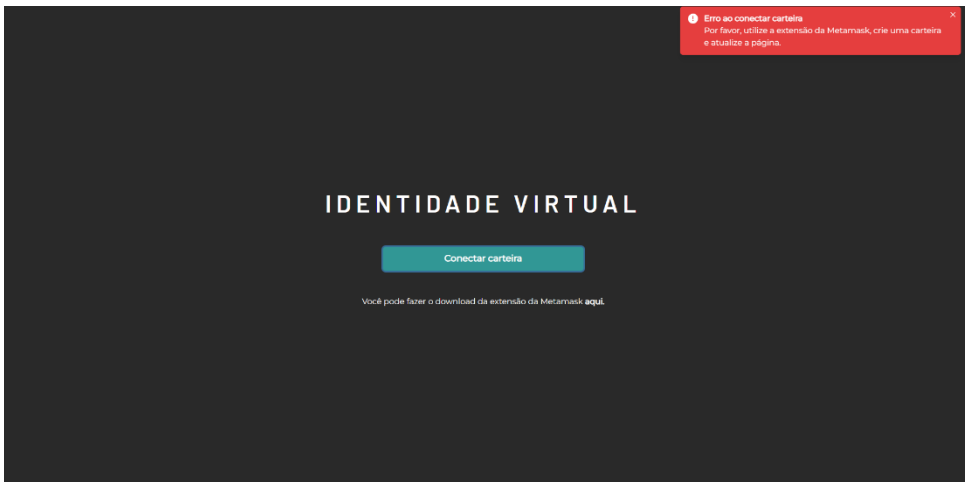
Figura 1 – Fluxo de uso do sistema de identidade digital



Fonte: elaborado pelo autor (2023).

Como demonstrado na imagem, a arquitetura do sistema é constituída por uma plataforma web, que é responsável por ser o intermédio entre as ações do usuário e o contrato inteligente, bem como pela disposição dos dados requisitados para visualização. O contrato é então responsável por realizar as ações do usuário dentro da *blockchain*, gerando as identidades e posteriormente realizando a busca por seu código único, este sendo o identificador pessoal, e retornando os dados para a plataforma web. Para não se opor às ideias descentralizadoras das *blockchain*, foi necessário, também, a utilização de uma estratégia *peer-to-peer*, ou seja, sem intermédio terceiro, para o armazenamento de arquivos dos usuários, utilizados nas identidades.

Figura 2 – Interface disponibilizada ao não encontrar carteira vinculada.



Fonte: elaborado pelo autor (2023).

Como é necessário que o usuário se conecte à plataforma utilizando sua carteira gerada pela MetaMask, foram desenvolvidas interfaces que auxiliam o usuário caso não seja encontrada a aplicação da metamask ou caso a carteira ainda não tenha sido vinculada à plataforma, como demonstrado na figura 2.

3.1 Aplicação web

Para realizar as interações com a *blockchain*, necessárias para o cumprimento dos objetivos propostos na pesquisa, desenvolveu-se um *smart contract* capaz de realizar a criação, busca e exclusão de blocos de dados, sendo esses blocos intitulados, no presente trabalho, de identidade digital.

Como plataforma para o desenvolvimento do contrato inteligente foi escolhida a Ethereum junto à linguagem Solidity e a biblioteca Hardhat, conjunto de tecnologias comuns dentro da área de *blockchain*.

Além disso foi realizada a publicação do contrato inteligente utilizando a plataforma Alchemy, plataforma de desenvolvimento e publicação voltada à web3, contando com, além dos recursos para publicação, ferramentas de monitoramento e debug dos contratos já publicados. Estas foram utilizadas para medir o tempo médio, em ms, e o custo de gás, unidade de medida utilizada dentro da Ethereum para mensurar o custo computacional envolvido na transação, das requisições realizadas.

A rede utilizada para o teste e publicação foi a Sepolia, rede de teste criada pelo mesmo núcleo de desenvolvedores da Ethereum, nela se fez capaz a mimetização do comportamento real da rede de produção da Ethereum sem a necessidade de investimento de recursos financeiros reais.

A interface disponibilizada para o usuário final, foi construída utilizando linguagem de programação javascript junto a React, biblioteca popular no desenvolvimento de interfaces de usuário para web, mas que também pode ser utilizada para desenvolvimento para dispositivos móveis e de aplicações embarcadas.

3.1.1 Contrato inteligente

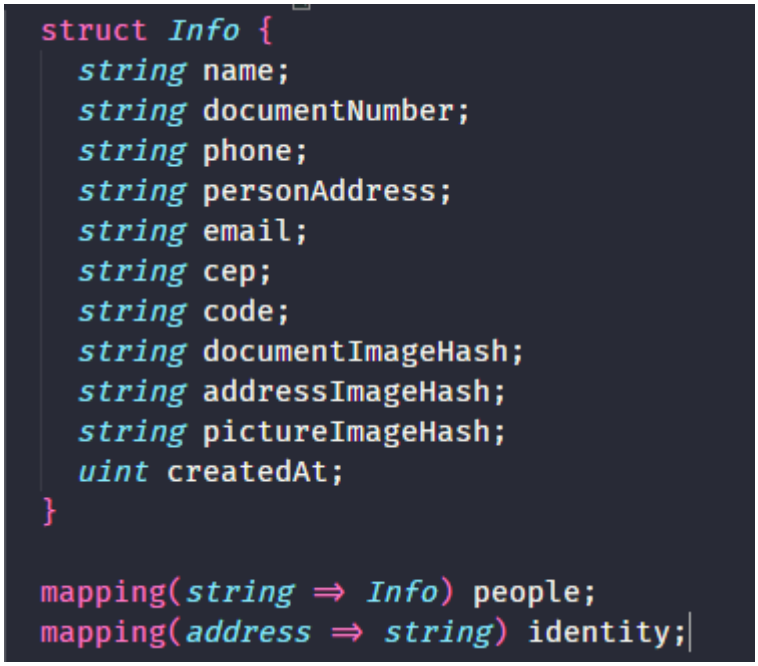
Dentro do contrato foram desenvolvidas e disponibilizadas algumas funções públicas, para que sejam acessadas, utilizando-se da plataforma web, pelos usuários.

A função de criação recebe como parâmetro os dados do usuário e se utiliza de uma função privada para gerar um código de identificação único para cada identidade, além de gerar uma lista interna correlacionando o endereço da carteira conectada ao *front-end* e o seu código único, impedindo que um mesmo endereço dentro da *blockchain* tenha mais de uma identidade na plataforma.

De forma distinta, a função de busca recebe o código anteriormente gerado e valida a sua existência, com a existência verificada, o bloco de informações referente à identidade encontrada é retornado para ser exposto pela interface de usuário.

De forma prática a remoção é possível de ser feita utilizando o código de identidade junto à validação entre endereço solicitante e endereço previamente vinculado ao código, caso a validação se mostre positiva, por igualdade de valores, a identidade é então deletada do sistema. A função de remoção foi desenvolvida somente como prova de funcionamento, não foram levadas em consideração as possíveis regras de negócio relacionadas ao oferecer essa opção ao usuário.

Figura 3 – Estrutura relacional entre endereço e identidade



Fonte: elaborado pelo autor (2023).

No código demonstrado acima está a relação entre endereço da carteira e identidade gerada, este mapeamento está estruturado na forma de lista, com cada linha contendo um *non-fundible token,* popularmente conhecido como *NFT*, sendo este um token único. Essa estrutura é responsável por gerar confiabilidade e privacidade entre plataforma e usuário, fazendo com que o endereço da carteira seja exposto somente ao contrato e não aos outros usuários. A estrutura também facilita a iteração das funções dentro do contrato, realizando buscas de forma performática utilizando-se diretamente da chave índex de cada identidade.

3.1.2 Armazenamento de arquivos

Visando manter-se coerente à proposta de descentralização da aplicação, foi escolhido utilizar o sistema de arquivos IPFS, protocolo e sistema de arquivos distribuído, que possibilita aos usuários armazenar e acessar dados, tais como arquivos, aplicativos e sites, de forma descentralizada.

O objetivo principal dessa tecnologia é estabelecer uma rede global de computadores que assegure conectividade privada, segura e resistente à censura. Em vez de depender de servidores centralizados, o IPFS utiliza uma abordagem peer-to-peer, onde os dados são distribuídos entre os participantes da rede.

Foi escolhido então utilizar a plataforma e biblioteca Pinata, tornando possível não só a criação e armazenamento de arquivos utilizando IPFS, mas também, a utilização de um gateway específico para o retorno dos arquivos.

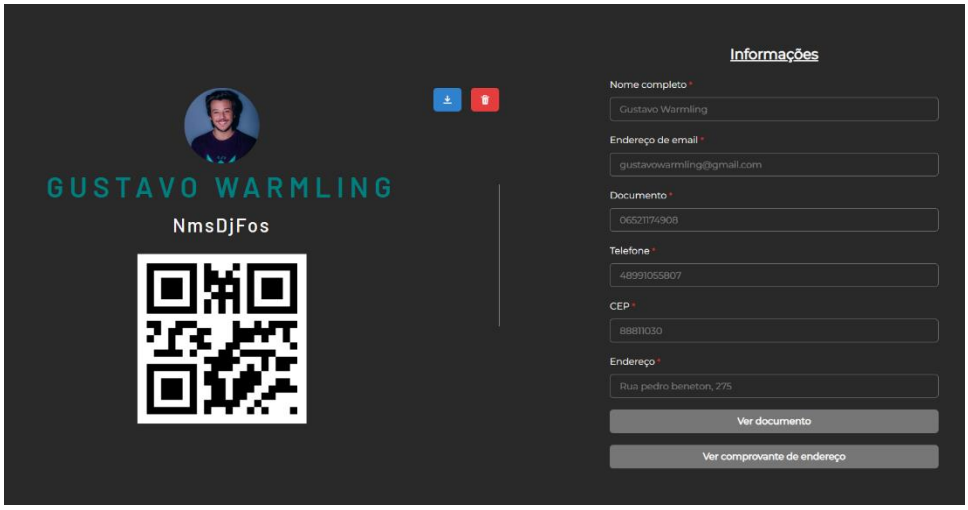
3.1.3 Interface do usuário

De forma primária foi desenhado o esboço da aplicação utilizando-se da aplicação Figma, capaz de gerar protótipos de interface visual, o qual foi utilizado durante todo o desenvolvimento para consulta de fluxo de ações e estilização.

Como já citado no presente artigo, a interface foi desenvolvida utilizando a biblioteca React, fazendo uso de seu ecossistema de componentes. Foi também utilizada a biblioteca de Chakra UI, utilizando-se do seu sistema de componentes pré-desenvolvidos e sua documentação de coloração, medidas e boas práticas para acessibilidade.

Para a conexão entre a interface e o contrato inteligente utilizou-se a biblioteca Ethers, biblioteca compacta e completa que visa ser uma abstração na interação com a Ethereum e seu ecossistema.

Figura 4 – Interface de identidade do usuário



Fonte: elaborado pelo autor (2023).

Como produto da plataforma, como pode ser visualizado na figura acima, foi desenvolvida a interface de identidade do usuário, contendo suas informações, código único de texto e código QR para compartilhamento.

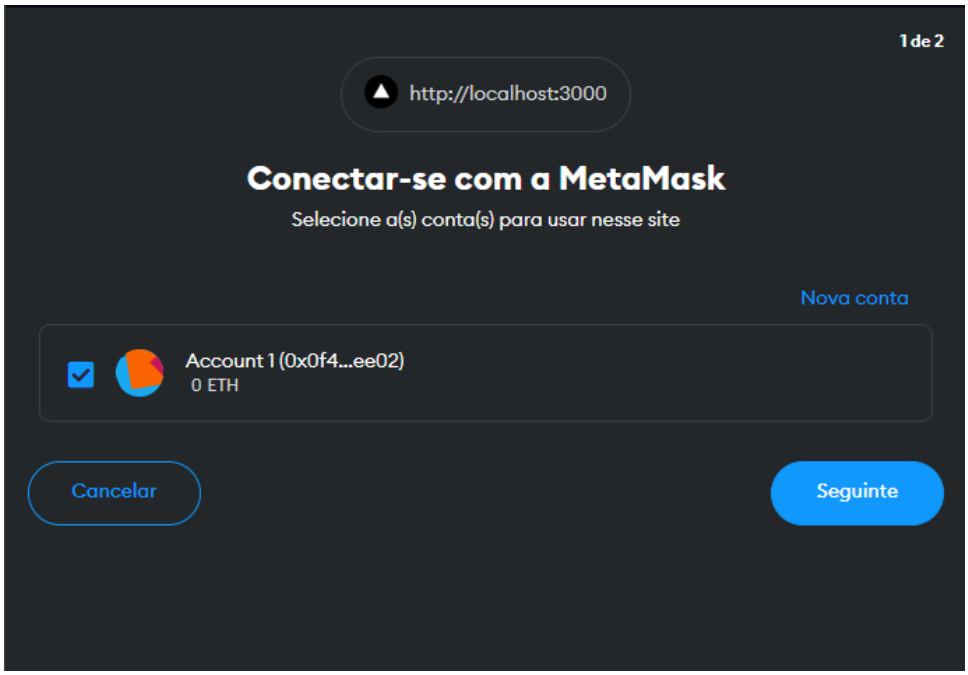
3.2 Carteira de criptomoedas

Para a utilização da plataforma é requisitado que o usuário se conecte utilizando sua carteira de criptomoedas, essa irá conter um endereço único rastreável, capaz de ser endereçada dentro da rede, a conexão é necessária para que todas as ações realizadas dentro da plataforma sejam assinadas pelo endereço do solicitante, ou seja, do usuário. Tornando então capaz a validação de propriedade de cada identidade.

A provedora de carteira escolhida foi a MetaMask, por conta de sua facilidade de uso e integração com a, já citada biblioteca, Ethers. Sua utilização é feita através de um plugin, disponibilizado pela própria desenvolvedora, dentro dele o usuário é capaz de aceitar ou recusar a assinatura de ações, além de também desfrutar da possibilidade de visualizar o custo estimado de gás e de tempo de espera.

O custo das transações é pago diretamente pelo usuário utilizando a moeda de teste SepoliaETH, disponibilizada via Faucet pela já citada Alchemy. Tanto o custo das transações quanto o tempo de espera são estimados mimetizando a rede de produção da Ethereum.

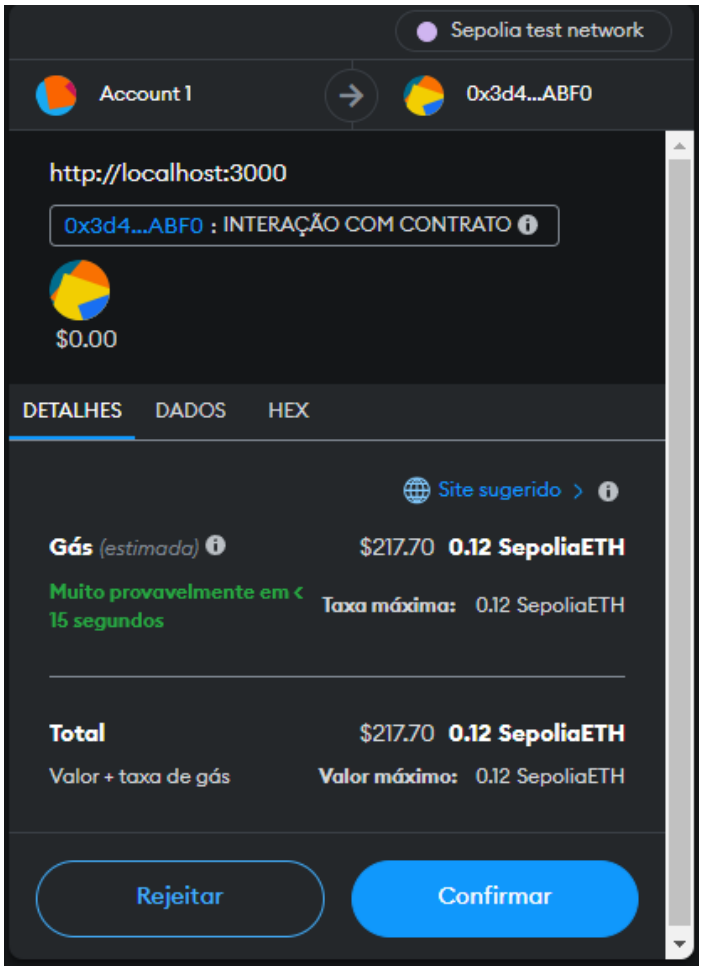
Figura 5 – Fluxo de conexão entre plataforma e Metamask.



Fonte: elaborado pelo autor (2023).

Como demonstrado na figura acima, ao solicitar a conexão, o usuário será exposto ao fluxo de conexão da Metamask, onde poderá selecionar qual endereço, dentro da sua carteira, será vinculado à plataforma, desta forma o seu endereço público da carteira será exposto para a plataforma, que posteriormente utilizará desse endereço para a criação da identidade.

Figura 6 – Tela de aceite da transação para criar uma identidade.



Fonte: elaborado pelo autor (2023).

Na figura 5 está demonstrada a interação que o usuário fará para confirmar ou rejeitar a transação para criação de sua identidade, nessa etapa é possível ver uma estimativa de gás e tempo utilizado, bem como uma estimativa de custo da transação.

3.3 Experimentos

Com a finalidade de cumprir com os objetivos propostos, foi desenvolvida uma rotina de testes e a colocada à prova em 3 diferentes navegadores, sendo eles o Google Chrome, o Firefox e o Brave. Foi utilizado também 3 diferentes faixas de limitação de conexão, configuradas dentro das ferramentas de desenvolvedor de cada navegador, sendo elas: sem limitação; conexão 3g rápida; conexão 3g lenta.

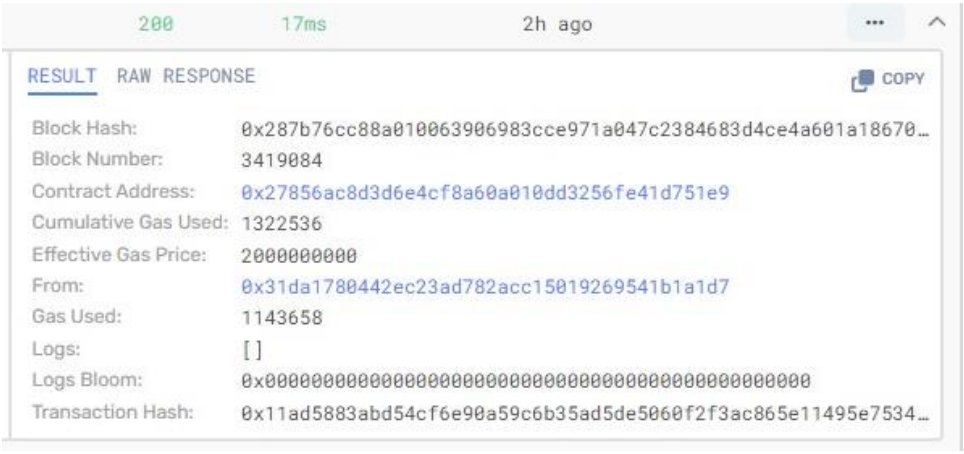
A rotina de testes se baseou no seguinte roteiro: acesso à plataforma sem MetaMask instalada, tendo como resultado esperado a impossibilidade de criar uma identidade; realização do acesso à plataforma com MetaMask instalada e sem identidade vinculada ao endereço da carteira, esperando a possibilidade de criação de nova identidade e a impossibilidade de busca por identidades, realização da criação de nova identidade com sucesso; Acesso à plataforma com MetaMask instalada e identidade criada no passo anterior, esperando a possibilidade de visualizar a própria identidade, além da possibilidade de buscar por outras identidades geradas. Posteriormente ao último passo é realizada a busca por outras identidades previamente geradas, fazendo a validação da função de busca e, por fim, a utilização da função de remoção.

Foi realizado teste do código QR disponibilizado, sendo esse gerado dentro da página de identidade do próprio usuário e disponibilizado para download em formato de jpeg, o arquivo foi então salvo em aparelho celular e apontado para a câmera do computador com a funcionalidade busca por código QR ativa e permissão de uso da câmera habilitada no navegador.

Assim que o código de identidade é validado pela plataforma, sendo esse demonstrado via código QR ou texto, o usuário é redirecionado para a página da identidade requisitada, podendo verificar as informações e documentos cadastrados.

A velocidade e custo das requisições foram analisadas utilizando a plataforma da Alchemy, obtendo acesso aos dados de cada requisição de forma individual, como também, do conjunto de requisições em determinada faixa temporal.

Figura 7 – Recibo de transação.



Fonte: elaborado pelo autor (2023).

Como visto acima, o recibo gerado pela transação e salvo para consulta, dentro da plataforma Alchemy, demonstra as informações cruciais para o entendimento da performance da requisição, é possível destacar as informações de tempo, em ms, código da requisição utilizando a base HTTP, o gás utilizado e o preço do gás no momento da transação. É possível, também, verificarmos informações que garantem segurança à transação, tais como o *hash* do bloco, o número do bloco, o endereço do contrato e o assinante.

4 RESULTADOS E DISCUSSÃO

Mediante os testes realizados pelo autor, a plataforma criada demonstrou, tendo como base a experiência e opinião de uso somente do autor, ter uma interface de simples utilização, rápida e capaz de realizar a criação, visualização e exclusão das identidades com pouca perda de performance em relação à interferência externa, como diferentes conexões e navegadores. Mesmo com a interface simples, é notável também a barreira do conhecimento na tecnologia, visto que é necessário a utilização de uma carteira de criptomoedas, ou seja, o usuário precisa ter conhecimento prévio, prático, do funcionamento da blockchain, para conseguir utilizar as funcionalidades da plataforma.

As ferramentas utilizadas para a criação da plataforma conseguiram suprir a necessidade para a execução do projeto e obtenção do objetivo de gerar a identidade. Porém foi analisada a ausência de necessidade de publicação do contrato

dentro da Amazon *Web Services*, visto que o contrato pôde ser diretamente publicado à rede de testes Sepolia, gerando resultados mais fidedignos à uma aplicação em estado de produção.

Também foi examinada a dificuldade de visualização dos arquivos IPFS, sendo, dos três navegadores testados, somente o Brave consegue fazer a visualização de forma nativa, enquanto o Chrome e o Firefox necessitam de plugins. Além disso demonstrou demora para o carregamento das imagens mesmo utilizando o gateway específico da plataforma Pinata.

Em conformidade ao trabalho desenvolvido por Batista, Dias e Silva (2018) a *blockchain* se mostrou uma proposta interessante, principalmente para sistemas buscando maior confiabilidade e escalabilidade, tendo em vista que não necessita de autoridades centrais para o seu funcionamento.

Também citado por Cao, Chen, Cao (2022) foi confirmada a possibilidade de aumento de privacidade por parte dos usuários, tanto para os usuários utilizando sua identidade quanto para os usuários realizando a validação de identidades, garantindo anonimato para ambas as partes, não expondo nenhuma informação que não esteja cadastrada na plataforma.

Como também analisado em seus respectivos trabalhos Batista, Dias e Silva (2018) e Delloite (2018) foi visto que a tecnologia *blockchain* se mostra viável para além dos propósitos originais dos respectivos trabalhos, podendo ser expandida para novas áreas de atuação, seja na saúde, educação, setores financeiros, setores privados e setores públicos, agregando segurança, privacidade e globalização dos dados.

5 CONCLUSÃO

Com base nos resultados obtidos e no conhecimento teórico adquirido através da pesquisa acadêmica, pode-se concluir que a plataforma desenvolvida utilizando os conceitos da blockchain demonstrou ser promissora. A interface da plataforma mostrou-se utilizável para o desafio proposto, mesmo diante de interferências externas.

No entanto, foi observado que o conhecimento prévio sobre carteiras digitais ainda representa uma barreira para os usuários. Além disso, houve dificuldade

na visualização de arquivos IPFS, exigindo a utilização de plugins específicos em determinados navegadores.

Os estudos anteriores confirmaram que a blockchain é uma proposta interessante para sistemas que buscam confiabilidade e escalabilidade, sem depender de autoridades centrais. Além de demonstrar aumento da privacidade dos usuários. A utilização da blockchain na criação de uma plataforma de identificação pessoal independente e global apresenta um potencial significativo, destacando-se como uma tecnologia emergente capaz de promover avanços no campo da segurança e privacidade, com possibilidade de aplicação em diversos setores.

Para trabalhos futuros sugere-se: analisar a aplicabilidade em ambiente real, testando a aplicação com uma maior gama de usuários, a fim de entender possíveis dificuldades em relação à tecnologia, além de validar regras de negócio, como a transferência de identidade entre carteiras.

REFERÊNCIAS

ALHARBY, Maher; MOORSEL, Aad van. Blockchain-based Smart Contracts: A Systematic Mapping Study. **CoRR**, abs/1710.06372, 2017. arXiv: 1710.06372. Disponível em: <http://arxiv.org/abs/1710.06372>.

BATISTA, Alex Oliveira Abreu; DIAS, Emillie Rebecca Bastos; SILVA, Murilo Borges. Identificação digital baseada em blockchain: Um conceito disruptivo no ciberespaço. pt, p. 14, 2018.

CAO, Yangzhou; CHEN, Jiageng; CAO, Yajun. Blockchain-Based Privacy-Preserving Vaccine Passport System. Edição: Weizhi Meng. **Security and Communication Networks**, Hindawi, v. 2022, p. 4769187, mar. 2022. ISSN 1939-0114. DOI: 10.1155/2022/4769187.

CHEN, Huashan et al. A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses. **ACM Comput. Surv.**, Association for Computing Machinery, New York, NY, USA, v. 53, n. 3, jun. 2020. ISSN 0360-0300. DOI: 10.1145/3391195. Disponível em: <https://doi.org/10.1145/3391195>.

DELOITTE. Picture perfect: A blueprint for digital identity | Deloitte China | Financial Services. en. **Deloitte China**, 2018. Disponível em: <https://www2.deloitte.com/cn/en/pages/financial- services/articles/disruptive-innovation-digital-identity.html>.

LIRA, Jordan et al. Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos, jan. 2018. Disponível em: <https://www.academia.edu/81347209/Uso_N%5C%C3%5C%A3o_Financeiro_de_Blockchain_Um_Estudo_de_Caso_Sobre_o_Registro_Autentica%5C%C3%5C%A7%5C%C3%5C%A3o_e_Preserva%5C%C3%5C%A7%5C%C3%5C%A3o_de_Documentos_ Digitais_Acad%5C%C3%5C%AAmicos>.

MOHANTA, Bhabendu Kumar; PANDA, Soumyashree S; JENA, Debasish. An Overview of Smart Contract and Use Cases in Blockchain Technology, p. 1–4, jul. 2018. DOI: 10.1109/ICCCNT.2018.8494045.

SIMONS, Alex. Decentralized digital identities and blockchain: The future as we see it. en-US. Microsoft 365 Blog, fev. 2018. Disponível em: <https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/>.

ZHENG, Zibin et al. An overview on smart contracts: Challenges, advances and platforms. **Future Generation Computer Systems**, v. 105, p. 475–491, 2020. ISSN 0167-739X. DOI: https://doi.org/10.1016/j.future.2019.12.019.

ZĪLE, Kaspars; STRAZDIŅA, Renāte. Blockchain Use Cases and Their Feasibility. **Applied Computer Systems**, v. 23, p. 12–20, mai. 2018. DOI: 10.2478/acss-2018-0002.