Carteira de Identidade Digital Auto Soberana com base em Blockchain

TRABALHO DE CONCLUSÃO DO CURSO DE ENGENHARIA DE COMPUTAÇÃO

Gabriel Custodio Oliveira, Gabriel Fuli Valcarce, Lucas Aparecido Candido Sousa, Victor Dias Klebes, Marcel Stefan Wagner

Universidade Anhembi Morumbi

Departamento de Engenharia da Computação

***Resumo* — SSI ou identidade auto soberana surgiu junto a ideia de descentralizar a informação pessoal das corporações, com a conclusão de que todo tipo de dado que pode ser considerado sensível deve ser alocado em um único lugar pelo proprietário dele, conseguindo um maior controle de informações pessoais dentro do tráfego de informações no ciberespaço. A expertise do contexto de SSI, leva uma solução prática e segura para o usuário, utilizando novas tecnologias de ponta, com o propósito de entregar somente o necessário para o consumo. Neste trabalho propõe-se uma carteira de identidade digital para elevar o nível de segurança no compartilhamento de informações pessoais do usuário. Com base no projeto implementado obtivemos como resultado uma carteira que irá armazenar credenciais para validação se uma pessoa está apta para comprar cerveja em uma máquina de vendas automática.**

***Palavras-Chave:* SSI; Identidade soberana; Segurança da Informação.**

I. INTRODUÇÃO

A segurança da informação é uma pauta que vem sendo cada vez mais discutida por grandes corporações em decorrência do avanço tecnológico.

A forma como sites são acessados, provém de um modelo centralizado de informação, é comum que o registro de novas contas seja efetuado a partir de formulários ou de plataformas de *Single Sign On* (Identificadores intermediários), como o Google, Facebook, LinkedIn etc.

O sistema centralizado abre portas para possíveis invasões, uma vez onde a informação centralizada é armazenada em grandes silos de dados que acabam se tornando alvos para grupos de *hackers*, e ficam vulneráveis a vazamentos em grande escala.

No último ano, a um aumento entre 40% e 50% do uso da rede, segundo dados da Agência Nacional de Telecomunicações (Anatel). De acordo com a Akamai, empresa líder em proteção e entrega de experiências digitais, o tráfego global de dados chegou a subir 30% em um único mês ao longo do período.[4]

Aumentando as tentativas de vazamentos de dados durante esse período pandêmico.

O SSI (Identidade alto soberana) promove uma solução descentralizada e criptografada de ponta a ponta, utilizando tecnologia atual de *blockchain,* dessa forma, transcendendo *databases* físicas (silos de informação), fazendo com que os dados transitem entre os nós da malha que compõem a *blockchain*, portanto, a informação compartilhada para o *server side* não fica alocada estaticamente em um ponto físico, como no caso de sistemas centralizados, e sim, apenas na carteira de identidade digital em um banco offline no *client side,* transitando de maneira irrastreável e encriptada á terceiros, armazenando dados em blocos interligados em cadeias. Os dados são cronologicamente consistentes porque não há possibilidade de mudar ou excluir a cadeia sem afetar o consenso da rede.

A abordagem de *SSI*, possibilita o desenvolvimento de um ecossistema mais seguro e confiável para o gerenciamento de identidades, onde seguindo seus princípios, todos os dados retidos pelo usuário serão verificados por um órgão emissor responsável, o que acaba tornando os dados do usuário autênticos e confiáveis para serem utilizados nas mais diversas soluções. Neste quesito, toda informação a ser trafegada deve ser autorizada pelo cliente final para que seja considerada uma transação bem-sucedida.

II. PROBLEMA DE PESQUISA

Segurança frágil no âmbito dos dados, as grandes unidades de armazenamento de dados pessoais e privados, viram alvo de *cyber*-ataques, com intuito de:

- Fins lucrativos;
- Vazamento de dados no tráfego público;
- Chantagens;
- Impactar em processos empresariais;
- Plágios;
- Destruição de banco de dados;
- Processos jurídicos.

Portanto, este trabalho vem com o sentido de responder a seguinte questão:

É possível aprimorar o mecanismo de tráfego de dados sigilosos através de novos conceitos da tecnologia?

Com a tecnologia *SSI*, pode-se ter um controle no gerenciamento de dados pessoais, fornecidos através de uma organização, compartilhando dados escolhidos e somente os dados mínimos para a validação e concluir a transação, podendo declinar o processo no momento da solicitação dos dados, com o controle total de suas informações.

III. OBJETIVOS

A. Objetivos Gerais: Desenvolver uma carteira de Identidade digital para controle de acesso a uma máquina de vendas de bebidas alcoólicas.

B. Objetivos Específicos:

a) Foi utilizado o *Framework Next.js,* para o desenvolvimento de uma carteira capaz de salvar credenciais.
b) Utilizando a tecnologia *Hyperledger Indy,* para a criação de identidades digitais em *blockchain*. [5]
c) Utilizando a biblioteca *Hyperledger Aries* focado na transmissão e armazenamento de credenciais digitais verificáveis.[7]

IV. PESQUISA TEÓRICA

Com o problema de vazamentos de dados no tráfego da web, a oportunidade de fraudes é abundante, alguns bancos de dados são baseados em relacionamentos de negócios e integrações, com isso conquistar a confiança do usuário para informar esses dados, mas com a deficiência na segurança frágil no âmbito dos dados, várias informações pessoais são expostas na internet. [1]

Os sistemas atuais de gerenciamento de identidade digital apontam problemas severos com a segurança, eficiência e privacidade. Uma nova tecnologia chamada *Self-Sovereign Identify* (SSI), completa essa deficiência equipando os usuários com carteiras móveis para gerenciar suas identidades digitais, com o controle dos direitos da identidade, versar e proteger seus dados, com isso, pode-se controlar as informações que vão ser necessárias, por meio de identificadores e chaves de criptografia, tendo em vista a proteção e a integridade dos dados. [2]

O foco principal da tecnologia *blockchain* é fornecer um sistema de confiança descentralizado. Mapeando os problemas sobre a confiança do sistema centralizado, utilizando uma plataforma de aplicação descentralizada, uma identidade autosoberana que engloba os pontos de:

- Credenciais Verificáveis

Representam a declaração feita por um emissor de maneira inviolável respeitando a privacidade, permitindo uma marca d'água digital gerada através de uma combinação de criptografia de chave pública, atribuindo técnicas de prevenção de privacidade evitando correlações, possibilitando a digitalização de credenciais físicas e seleção unitária da informação que deverá ser compartilhada sem expor necessariamente todos os dados da credencial. [3]

A Divulgação seletiva e Prova de conhecimento zero são dois níveis de preservação de privacidade englobados nesse pilar, você pode divulgar apenas atributos unitários de uma credencial, por exemplo, você pode validar a sua idade ao comprar bebidas alcoólicas, sem necessariamente compartilhar outras informações que seriam de fácil acesso em um RG, como o nome, nome dos pais etc.

Fig. 1. Neste exemplo, o governo emite um passaporte a alguém como Credencial Verificável
Fonte: DOCK (2022).

- Identificadores descentralizados.

Os Identificadores Descentralizados (DIDs) permitem uma conexão p2p (peer-to-peer) exclusiva, privada e segura de ponta a ponta.[3]

A fim de destituir os identificadores intermediários como Google, Facebook etc., onde o compartilhamento de nossos metadados fogem do nosso controle, os DIDs podem ser classificados em 2 segmentos, DIDs Públicos e DIDs Privados. Os DIDs Privados são trocados entre 2 partes a fim de criar um canal seguro a acesso de terceiros, ou seja, nenhum terceiro tem acesso mínimo a qualquer tipo de informação provida pela conexão p2p, sendo possível criar quantos DIDs privados quiser, para os mais tipos de relacionamento de informação diferentes; já os DIDs Públicos são para quando um sujeito deseja ser publicamente identificável, como um órgão governamental por exemplo.

Fig. 2 - Cada DID vem com uma ou muitas chaves privadas e públicas.
Fonte: DOCK (2022).

- Ledger (*Blockchain*).

A Ledger a tecnologia por trás dos bancos de dados descentralizados que oferecem controle evolutivo dos dados entre entidades através de comunicação p2p usando algoritmos de consenso que replicam a informação entre nós de rede

Partindo de um conceito de Livro-Razão, onde qualquer informação gravada seria armazenada para sempre e ao mesmo tempo seria correlacionada com uma infinidade de outros Livros-Razão para confirmar a veracidade da informação la escrita através de alguns processos, permitindo que todos na

rede tenham a mesma fonte de verdade sobre a validade das credenciais e de quem atestou a validade dos dados embutida na credencial, sem revelar nenhum dado, utilizando o blockchain para verificar a validade do atestado, realizando as transações de armazenar nenhum dado garantindo a *SSI*.[3]

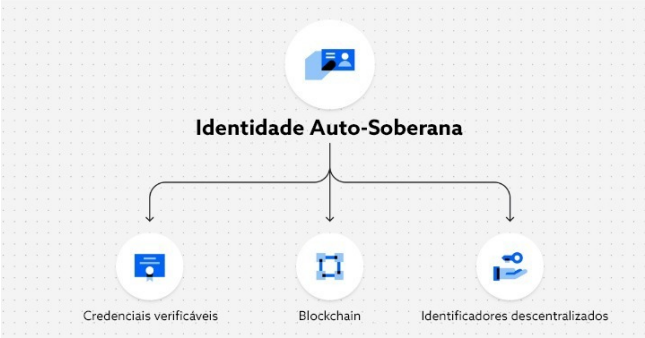

Fig. 3 - Credenciais verificáveis, blockchain, e identificadores descentralizados são 3 pilares da Self-Sovereign Identity.
Fonte: DOCK (2022).

V. METODOLOGIA

Este trabalho apresenta uma pesquisa que busca melhorar o compartilhamento de informações na venda de produtos para maiores.
Foi desenvolvido uma interface que simula a distribuição de dados validados governamentalmente, esses dados são enviados através de um *QR Code* que o mesmo disponibiliza, assim, o APP mobile da carteira digital recebe uma instância de identidade válida que será utilizada para a validação de idade pelo *Nice Beer*, *endpoint* desenvolvido para simulação de uma liberação de vendas de bebidas alcoólicas, ao ler o *QR Code*, é criado um triângulo de confiança, onde se cria uma comunicação com o *Nice Beer* e a API do governo, validando o *token* de idade e entregando um valor booleano, *true* para maior de idade, e *false* para menor.

VI. DESENVOLVIMENTO E RESULTADOS

No primeiro momento, estuda-se a fundo como deve ser feito a comunicação entre os sistemas que posteriormente seriam desenvolvidos, quais os recursos e tecnologias que podem ser utilizadas para a composição do trabalho, a fim de gerar agilidade e dinamismo para as aplicações. Com o escopo em mãos, o design é criado com o intuito de fornecer um ambiente simples e didático, onde público de todas as idades são capazes de usufruir.

Os recursos utilizados na criação do design são:

- *Excalidraw* (Escopo do projeto);
- *Adobe Photoshop* (Criação de imagens);
- *Adobe Illustrator* (Criação de imagens vetorizadas);
- *Figma* (Desenho completo do projeto).

Fig. 4. Logotipos dos *softwares* utilizados no *design*.
Fonte: Autor (2022).

A partir dos desenhos e imagens idealizadas, começa a codificação das três soluções. Utilizando diversas tecnologias de ponta, o desenvolvimento *client-side*, comumente chamado de Front-End, fortalece a percepção de como a dinâmica dos processos resultam. A pesquisa relacionada a utilização de bibliotecas externas possibilitou um grande salto não só no escopo do trabalho, mas nos estudos relacionados à área.

Os recursos utilizados na criação do código são:

- *Visual Studio Code* (IDE para a codificação);
- *XCode* (IDE para a compilação do App / IOS);
- *Expo* (Biblioteca de auxílio para a criação do App);
- *SQL Server* (Banco de dados).

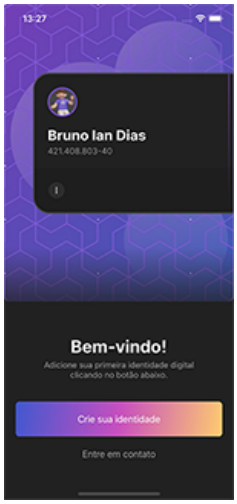

Fig. 5. Primeira impressão do aplicativo já codificado.
Fonte: Autor (2022).

Juntamente ao aplicativo, foi desenvolvido outros dois serviços, um site espelho de um órgão verificador (Gov.br) para fornecer e validar os dados trafegados, e uma solução de venda automática de cervejas (*Nice Beer*), onde por meio dos dados informados, a máquina deverá aprovar ou negar a venda da bebida ao consumidor.

As Linguagens e bibliotecas utilizadas para o desenvolvimento destes projetos são:

- Javascript (Linguagem de programação);
- NextJS (*Framework* de desenvolvimento).

Fig. 6. Logotipos das soluções implementadas em conjunto.
Fonte: Autor (2022).

Trazendo o conceito de um órgão responsável pelos dados autênticos para um ambiente fictício, sabemos que todos possuem informações sigilosas sobre toda a população, como nome, CPF, data de nascimento etc., foi desenvolvido um banco de dados com informações geradas randomicamente, para que seja possível efetuar os testes.

Id	NomeCompleto	CPF	RG	Dt_Nascimento	Sexo
1	Victor Dias Klebes	487.311.098-02	55.168.520-07	2000-06-23 00:00:00.000	M
2	Enrico Tomás das Neves	657.597.128-88	18.876.827-0	1968-07-20 00:00:00.000	M
3	Sueli Maria Catarina Martins	416.958.916-51	37.208.660-3	2004-04-01 00:00:00.000	F
4	Augusto Marcos Marcos da Luz	499.771.284-13	46.532.723-0	1969-01-06 00:00:00.000	M
5	Nair Regina Camila Drumond	085.637.551-96	13.400.096-1	1958-05-15 00:00:00.000	F

Fig. 7. Informações geradas randomicamente e salvas no Banco de Dados (Gov.br).
Fonte: Autor (2022).

Para que o usuário possa adquirir seus dados da aplicação é necessário possuir um cadastro no site do portador e efetuar um login. Neste cenário foi utilizado o Gov.br como exemplo, portanto foi idealizado um ambiente simples para visualizar um *QR Code* a partir de um código em *JSON (Javascript Object Notation)* popularmente conhecido contendo as credenciais. Este código posteriormente é escaneado no aplicativo do SSI utilizando a câmera do celular *smartphone* para gerar a identidade digital, um formulário será automaticamente construído em tela a partir das informações repassadas pelo órgão portador contendo chave e valor com as informações do cliente para que ele possa validar e prosseguir.

Fig. 8. Tela de *Login* (Gov.br).
Fonte: Autor (2022).

Fig. 9. *Qr Code* para criação de credencial (Gov.br).
Fonte: Autor (2022).

Fig. 10. Exemplo de Credencial gerada (Gov.br).
Fonte: Autor (2022).

Vale ressaltar que os dados obtidos são salvos em um *cookie* do próprio smartphone, possibilitando configurar um tempo de expiração ou se preferir até a desinstalação do aplicativo, este recurso é fundamental pois seguindo o intuito do projeto, a empresa portadora do aplicativo SSI não retém nenhum tipo de vínculo com o usuário visa validação podem somente serem conferidos, não podendo ser editados em nenhum momento.

Para este espelhamento do serviço (Gov.br) criaram-se duas tabelas em um banco de dados local, uma contendo dados para efetuar o login no sistema do governo e outra contendo os dados das pessoas cadastradas. Segue abaixo uma foto da estrutura da tabela de registros:

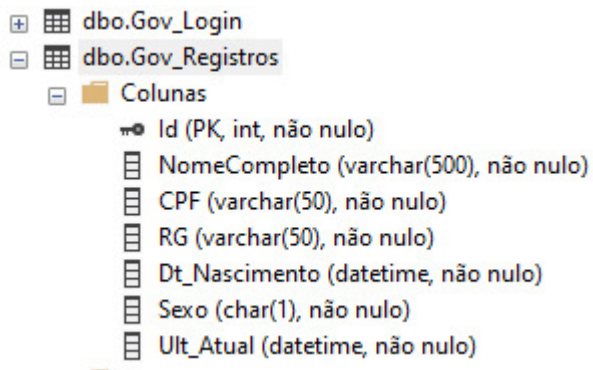

Fig. 11. Estrutura de Tabelas do Banco de Dados (Gov.br).

Fonte: Autor (2022).

Utilizando a mesma tecnologia de *QR Code*, foi criado uma tela para o serviço de venda de cerveja (Nice Beer) como exemplo de uso, onde devemos escanear o código contido em tela.

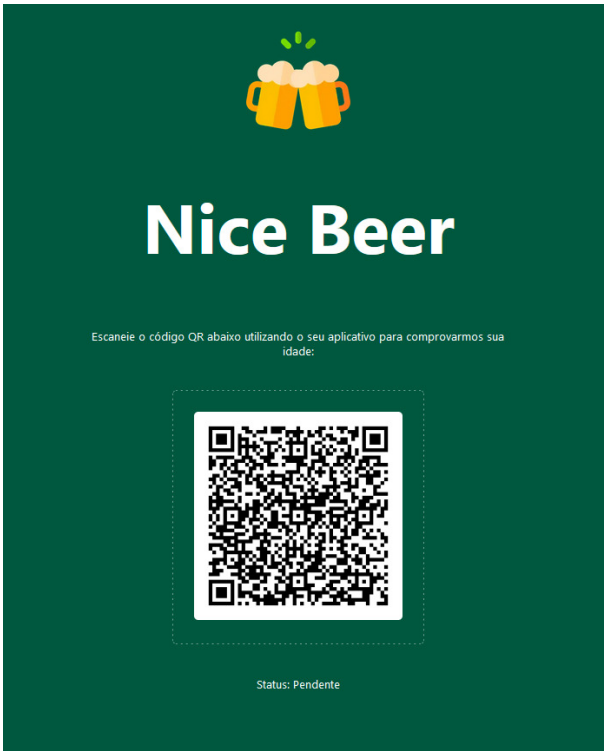

Fig. 11. *Qr Code* para validação de idade
Fonte: Autor (2022).

Este código possibilita à máquina informar quais dados serão necessários para validar a requisição e qual o endereço de URL devemos retornar essas informações, que são passadas para a tela do aplicativo deixando evidente para o usuário as informações que serão repassadas para o serviço a fim de realizar o processo.

```
const configs = {
  serviceName: "Nice Beer",
  postback: "http://homologar.admdeveloper.com.br/Next/api/verify",
  data: ["maiorIdade", "idUser"]
}

useEffect(() => {
  generateQR(JSON.stringify(configs));
}, [])

const generateQR = async text => {
  try {
    const qrcode = await QRCode.toDataURL(text);
    setQrcode(qrcode);
  } catch (err) {
    console.error(err)
  }
}
```

Fig. 12. Codigo de validação de idade
Fonte: Autor (2022).

Caso o portador deseje fornecer os dados solicitados para concluir o processo, o órgão irá utilizar uma rota de API (*Application Programming Interface*) para enviar os dados do portador ao serviço escolhido, então é salvo um histórico de requisições para que posteriormente o usuário consiga rever suas requisições.

VII. CONCLUSÕES

O processo de verificação de identidade e credenciais muitas vezes são preenchidos por informações falsas, com isso, disponibilizando a possibilidade de fraudes de identidades e credenciais.

A compra de bebidas alcoólicas por menores de idade é um problema que vem sendo recorrente há anos, de acordo com a Unifesp cerca de 55,5% dos estabelecimentos comerciais da cidade de Santos, vende bebida alcoólica para menores de 18 anos.[7]

Com isso a carteira de identidade mostrou uma forte e eficaz solução para possibilitar ao indivíduo ter controle total de suas identidades digitais, com verificações mais seguras e confiáveis, pois, a credencial sera imutável para o usuário, porém, o mesmo pode enviar os dados que escolher compartilhar com a máquina de bebidas tornando a informação válida.

À medida que cada vez mais pessoas vão percebendo a importância de um tratamento adequado para impedir a venda de bebidas para menores, o tema ganhará mais importância. Provavelmente ainda teremos um longo caminho para aperfeiçoamento. Esse caminho perpassa modelos de gestão de identidades tais como o de Identidade Auto-Soberana.

No futuro que se aproxima, novas políticas, mecanismos e paradigmas de gerenciamento de dados serão criados, provavelmente novas legislações, conforme passamos mais tempo de nossas vidas no mundo online, paradigmas como a Identidade Auto- Soberana farão parte desse futuro.

REFERÊNCIAS

[1] BUDYNAS, Richard G.; NISBETH, J. Keith. **Elementos de Máquinas de Shigley.** 10ª Edição. McGraw Hill Brasil, 2016.

[2] SARTOR, **Sebastian et al. Love at First Sight**? A User Experience Study of Self-Sovereign Identity Wallets. 2022.

[3] DOCK, Dock.io, **Sign in Self-Sovereign Identity: The Ultimate Guide 2022**. 2022. Disponível em: <https://www.dock.io/post/self-sovereign-identity>. Acesso em 05/2022

[4] BRASILIENSE, Correio Brasiliense, **Estudo aponta 1,6 bilhão de casos de roubo de dados pessoais na internet. Disponível em:<**https://www.correiobraziliense.com.br/brasil/2021/06/4928596-estudo-aponta-16-bilhao-de-casos-de-roubo-de-dados-pessoais-na-internet.html>. Acesso em: 11/2022

[5] Hyperledger Indy Disponível em: <https://indy.readthedocs.io/en/latest/>. Acesso em: 11/2022

[6] Hyperledger Aries Disponivel em: <https://www.hyperledger.org/use/aries>. Acesso em: 11/2022

[7] Uniad Unidade de Pesquisas em Álcool e Drogas. Disponível em: <https://www.uniad.org.br/noticias/pesquisa-da-unifesp-mostra-que-menores-tem-acesso-facil-a-bebidas/>. Acesso em: 11/2022