

Laboratório em Engenharia Informática

19 de Junho de 2021

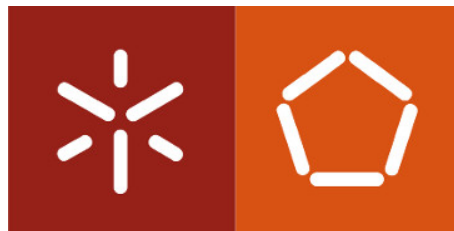
Projeto 66

a83899	André Moraes
a85370	Hugo Matias
a84485	Tiago Magalhães

Orientadores

Professor	José Bacelar Almeida
Professor	José Pina Miranda

Blockchain para a autenticidade de objetos de Luxo



Mestrado Integrado em Engenharia Informática
Universidade do Minho

Conteúdo

1	Introdução	2
2	Problema e objetivos	3
2.1	Análise das soluções existentes	3
2.2	Solução escolhida	3
2.3	Objetivos	4
3	Aplicação Desenvolvida	5
3.1	Arquitetura Geral	5
3.2	Sistema de <i>Back-end</i>	8
3.2.1	Estruturas de dados	9
3.3	Sistema de <i>Front-end</i>	12
3.3.1	Web App	12
3.3.2	App Mobile	19
4	Utilização do Sistema	23
5	Conclusão e Trabalho Futuro	23

Resumo

O trabalho realizado que se encontra a seguir descrito, tem como objectivo o desenvolvimento de uma aplicação que permita o armazenamento de objectos de luxo com recurso à tecnologia *blockchain*. Ao longo do relatório são explicadas também outras tecnologias usadas, a estrutura da aplicação e a sua implementação. Por último, é abordada a forma correcta de utilização do sistema.

KeyWords: *Blockchain*; *Arianee*; Aplicação; Objecto; Armazenar; Sistema.

1 Introdução

Recentemente, a tecnologia *blockchain* tem ganho um relevo e importância que não podem ser ignorados. O conceito de *blockchain* é intuitivamente associado ao conceito de *criptomoeda*, porém, este último é apenas uma das muitas aplicações da tecnologia de *blockchain*.

A área dos objectos de luxo apresenta uma possível aplicação de *blockchain*. Nesta área, é de alta importância o armazenamento seguro imutável deste tipo de objectos, bem como a garantia de autenticidade de um objecto. O trabalho realizado apresenta o uso de uma tecnologia *blockchain* como solução a este problema, garantindo segurança de armazenamento e de identidade com a possibilidade de confirmação de identidade e acesso restrito dos objectos de luxo.

Ao longo deste relatório são assim apresentados os passos efetuados e os recursos utilizados para a estruturação e construção de uma aplicação baseada em *blockchain* que implementa a solução referida acima.

2 Problema e objetivos

Um dos grandes problemas no mercado dos objetos de luxo é a falsificação, estimando-se que 5-9% do volume do comércio global é produção falsificada.[1]

Com este projeto visamos entender como é que a tecnologia, neste caso, a *blockchain*, pode combater esta grande adversidade, por isso inicialmente analisamos o problema e as soluções existentes (e.g., *Arianee* , *Everledger*, *Provenance*)[2, 3, 4]

2.1 Análise das soluções existentes

Após uma análise das 3 soluções propostas, chegamos à conclusão que a *Arianee* é a melhor escolha.

Todas as propostas baseiam-se na certificação dos objetos digitalmente, isto é, pretende-se representar estes objetos através de um certificado servindo como identidade virtual que permite certas propriedades como a sua unicidade, autenticidade e verificação de propriedade.

No entanto a *Everledger* é uma solução focada para um mercado específico e a *Provenance* não é só direcionada a objetos de luxo. Estas duas últimas também não têm uma API pública, enquanto a *Arianee* pretende ser um protocolo *standard* neste meio, permitindo uma maior flexibilidade para adaptar o protocolo aos vários mercados, disponibilizando a sua API

2.2 Solução escolhida

A solução *Arianee* permite resolver os seguintes problemas:

1. A limitação dos certificados físicos.
 - Estes podem ser falsificados mais facilmente;
 - Estão associados a base de dados centralizadas e por isso o acesso é, normalmente, restrito.
2. Limitação dos avaliadores.
 - A única maneira de confirmar a autenticidade de um produto, quando é impossível descobrir a sua origem, é através de um avaliador profissional;

- Normalmente, as pessoas recorrem a especialistas que não têm a capacidade necessária para avaliar. Com a *Ariane*, estas partes encontram-se verificadas pelas marcas na *blockchain*, permitindo ainda que as suas avaliações possam ser guardadas no seus certificados.

3. A prova da compra.

- Devido a utilização de certificados e a natureza dos nodos da *blockchain* verificarem transações, é possível assim ter uma prova de compra válida.

4. Rastreamento de um objeto.

- Entidades como seguradoras, lojas, precisam de recriar a história de um produto e perder inúmeras horas desnecessárias.

Deste modo o certificado *Ariane* vai construir uma confidencialidade indiscutível entre o proprietário e terceiros, devido à *blockchain* ser descentralizada, transparente e inalterável, o que faz com que seja quase impossível falsificar e fácil para qualquer um verificar.

2.3 Objetivos

Após análise do problema é pretendido realizar uma prova de conceito que utilize a tecnologia *Ariane*.

3 Aplicação Desenvolvida

Inicialmente para o projeto foi definida a arquitetura e seus atores com base no protocolo *Ariane*.

3.1 Arquitetura Geral

Para ajudar a perceber melhor, vamos descrever a arquitetura do protocolo *Ariane* por partes:

- ***Brands***: são a fonte de cada certificado. Para estes certificados serem classificados como autênticos, as *Brands* precisam de especificar um conjunto de critérios;
- ***Owners***: são os *end users* dos certificados;
- ***Certificate Management Platform providers*** – possuem os módulos usados pelas *Brands* para criar e gerir certificados na *Blockchain*;
- ***Wallet providers***: possuem a aplicação *mobile/web*, dando aos proprietários acesso ao seus certificados e os dados guardados pelas *brands*. A aplicação da *Wallet* deixa os proprietários importar ou criar um novo endereço *Blockchain* para gerir os certificados;
- ***Nodes***: validam transições relacionadas com o protocolo *Ariane* na *Blockchain*.

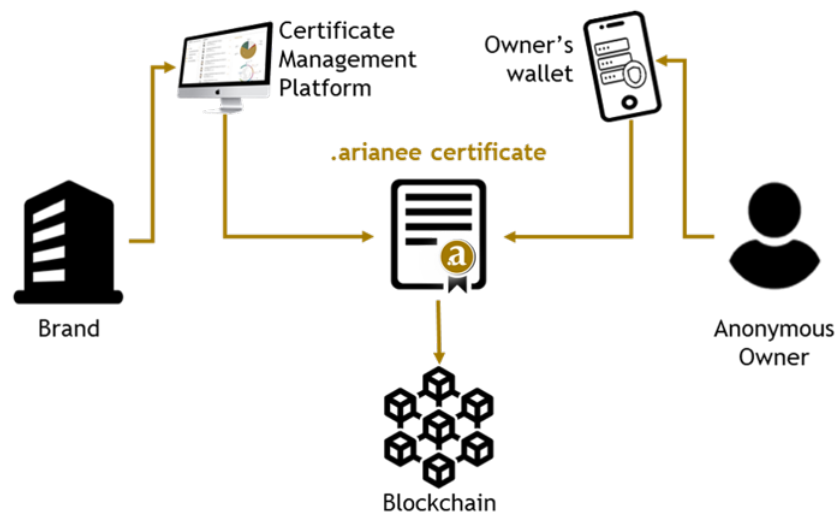


Figura 1: Arquitetura Arianee

Assim o dois grandes atores neste sistema são os utilizadores e as marcas, para isso foi esquematizado os casos de uso destes dois atores do nosso sistema:

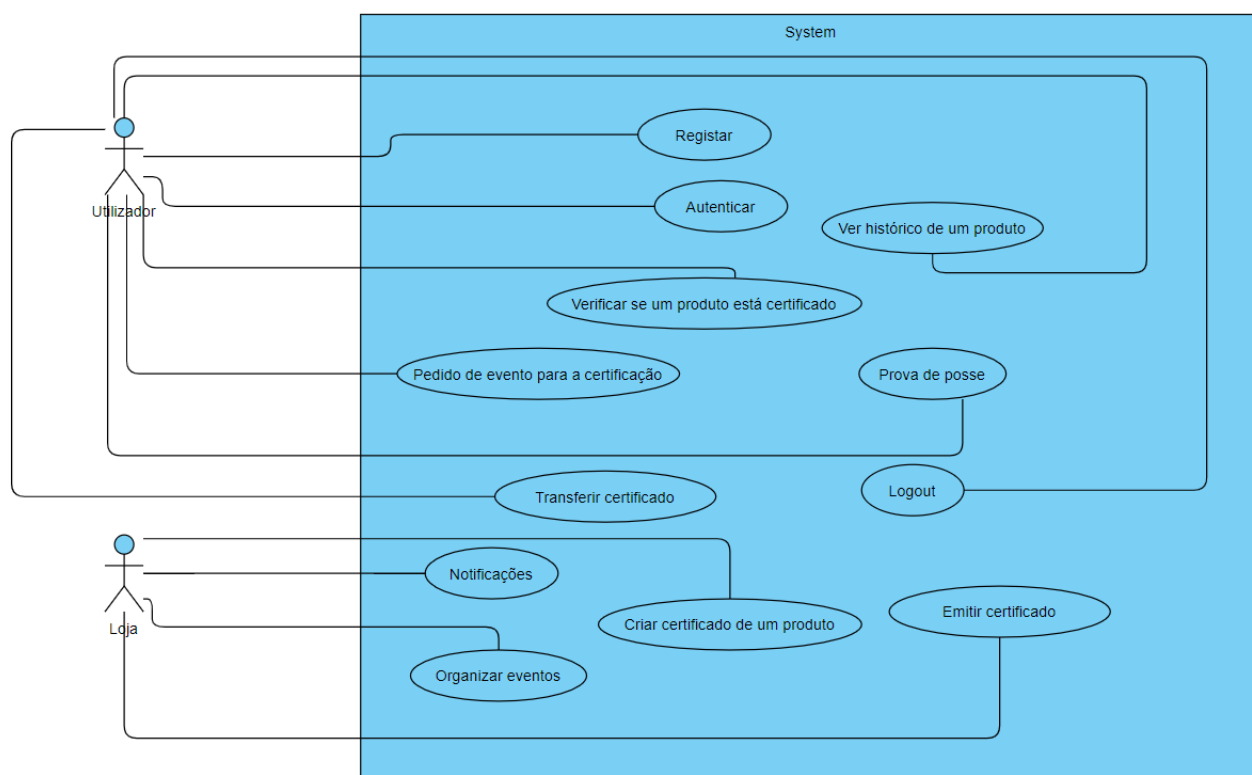


Figura 2: Use Cases

Com base na arquitetura e diagrama anterior foi construído o seguinte sistema:

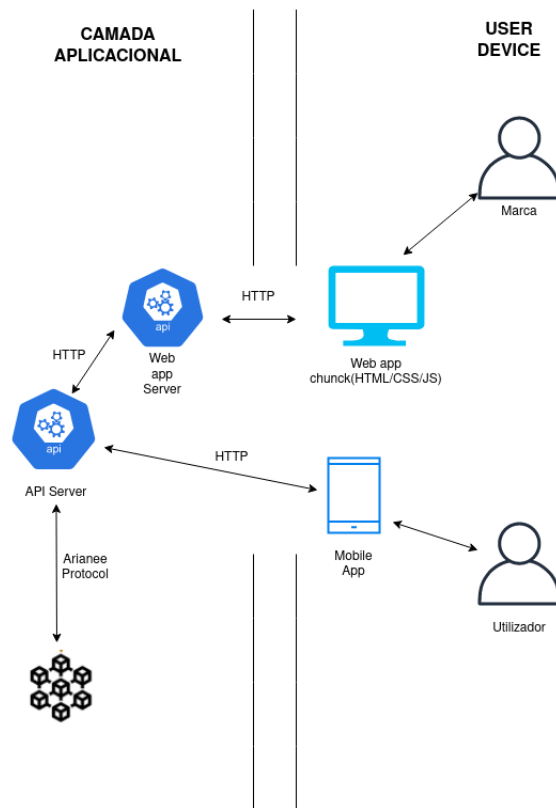


Figura 3: Arquitetura do sistema

Pela figura anterior podemos observar que foram desenvolvidas duas aplicações, uma aplicação *mobile*, em que o utilizador possui uma carteira com os seus produtos e uma aplicação *web*, direcionada apenas para os funcionários de uma loja com produtos.

3.2 Sistema de *Back-end*

Para desenvolvimento do *Back-end* construímos uma REST API, utilizando a *framework express* em *JavaScript* que permite que utilizemos a API da *arianee*, uma vez que está disponível neste linguagem. Neste servidor, todos os pedidos têm de possuir um *token* válido, para que os pedidos feitos possam ser atendidos. Aqui são tratados os pedidos externos vindos das aplicações *mobile* e *web* garantindo comunicação com o protocolo *Ariane*.

3.2.1 Estruturas de dados

As estruturas de dados usadas foram as seguintes, seguindo os *standards* definidos pela *arianee* **Certificado**

Exemplo modelo certificado.

```
{
  "$schema": "https://cert.arianee.org/version1/
  ArianeeProductCertificate-i18n.json",
  "name": "Final",
  "sku": "",
  "gtin": "",
  "brandInternalId": "",
  "category": "object",
  "intended": "",
  "serialnumber": [
    {
      "type": "serialnumber",
      "value": "412421"
    }
  ],
  "subBrand": "",
  "model": "",
  "language": "Portuguese",
  "description": "Ouro 50% Desconto",
  "medias": [
    {
      "mediaType": "picture",
      "type": "product",
      "url": "http://a749ce1c8509.ngrok.io
      /fileStore/1149414_575034622558349_1427378209_o.jpg"
    }
  ],
}
```

```
"attributes":[
  {
    "type":"color",
    "value":"Gold"
  },
  {
    "type":"year",
    "value":"1502"
  }
],
"materials":[
  {
    "material":"gold",
    "pourcentage":"99.9"
  }
],
"size":[
  {
    "type":"weight",
    "value":"0.4",
    "unit":"kg"
  }
],
"manufacturingCountry":"Alemanha",
"facilityId":""
}
```

Evento

Exemplo modelo evento.

```
{
  "$schema": "https://cert.arianee.org/version1/
  ArianeeProductCertificate-i18n.json",
  "id": "640419606",
  "title": "Ouro ",
  "description": "Avaliação",
  "type": "object",
  "attributes": [
    {
      "value": "1400",
      "date": "2021-06-19 01:53:00"
    }
  ],
  "valuePrice": "1400",
  "location": "Esposende"
}
```

Notificação

Exemplo modelo notificação.

```
{
  messageId: 974816790,
  content: {
    '$schema': 'https://cert.arianee.org/version1/
    ArianeeMessage-i18nAlpha.json',
    title: 'Desconto',
    description: 'Ouro 50% Desconto',
    link: 'ourovivo.com'
  }
}
```

3.3 Sistema de *Front-end*

O servidor *front-end* é o responsável por criar as interfaces com as quais o utilizador irá interagir. Decidimos utilizar uma framework *Javascript* para a criação das páginas. Além disso o fato da framework ser desenvolvida em Javascript, facilitou a tarefa de interligação entre o *Frontend*, o *Arianee* e o *Back-end*. Dentro das diferentes frameworks existentes decidimos escolher o **React Native** para aplicação Mobile e o **Express JS** para a aplicação Web.

3.3.1 Web App

Login - Esta é a primeira página apresentada a todos os utilizadores de uma loja. Autenticação é feita através da sua chave privada que foi gerada a quando a criação da conta (Apenas se pode criar contas na Aplicação Mobile)

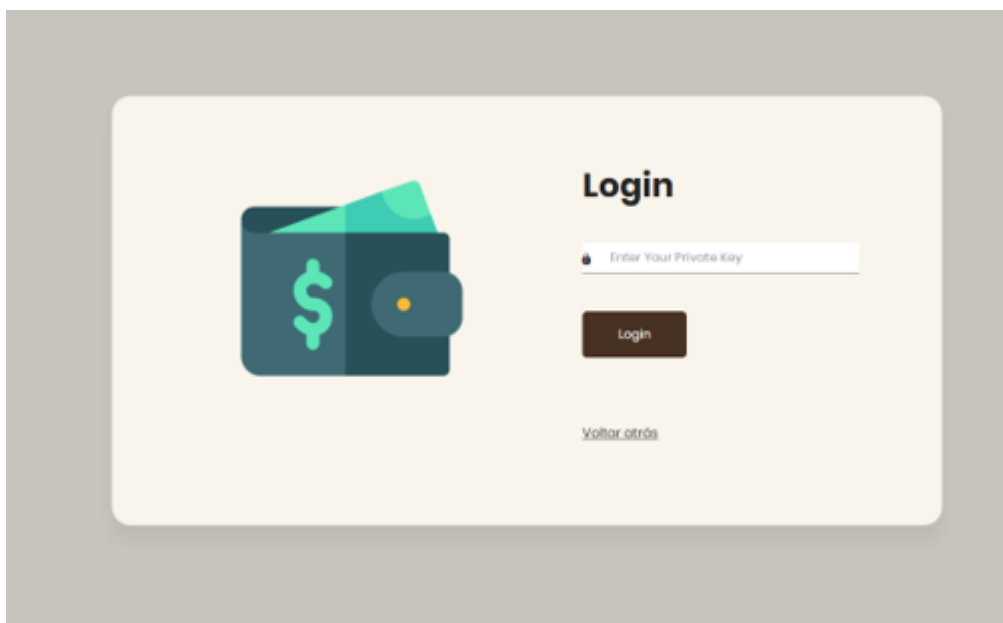


Figura 4: Página Login

Menu - É um menu simples e fácil de perceber o que se entende com esta página. Para a geração de certificados, eventos e/ou notificações, basta carregar nos botões



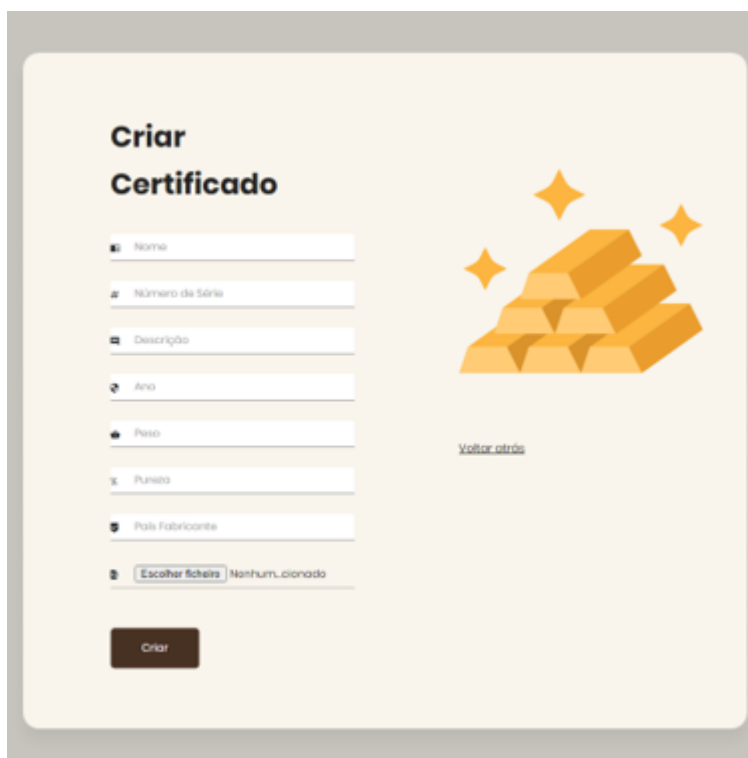
Figura 5: Página Inicial

Menu de Escolha do tipo de Produto - Página responsável por escolher o tipo de produto



Figura 6: Menu para escolher o tipo de certificado

Formulário para um Certificado - Esta é a página para criar um certificado, neste caso, para o ouro. É obrigatório preencher todos os campos e a seleção de uma foto



O formulário, intitulado "Criar Certificado", está dividido em duas colunas. A coluna da esquerda contém sete campos de entrada, cada um com um ícone de campo de texto à esquerda: "Nome", "Número da Série", "Descrição", "Ano", "Peso", "Puroza" e "País Fabricante". Abaixo desses campos, há uma seção com o ícone de uma pasta e o texto "Escolher ficheiros", seguido por "Nenhuma adicionada". Um botão "Criar" está localizado na base da primeira coluna. A coluna da direita apresenta uma ilustração de barras de ouro empilhadas com estrelas amarelas brilhantes. Abaixo da ilustração, há um link "Voltar atrás" em azul.

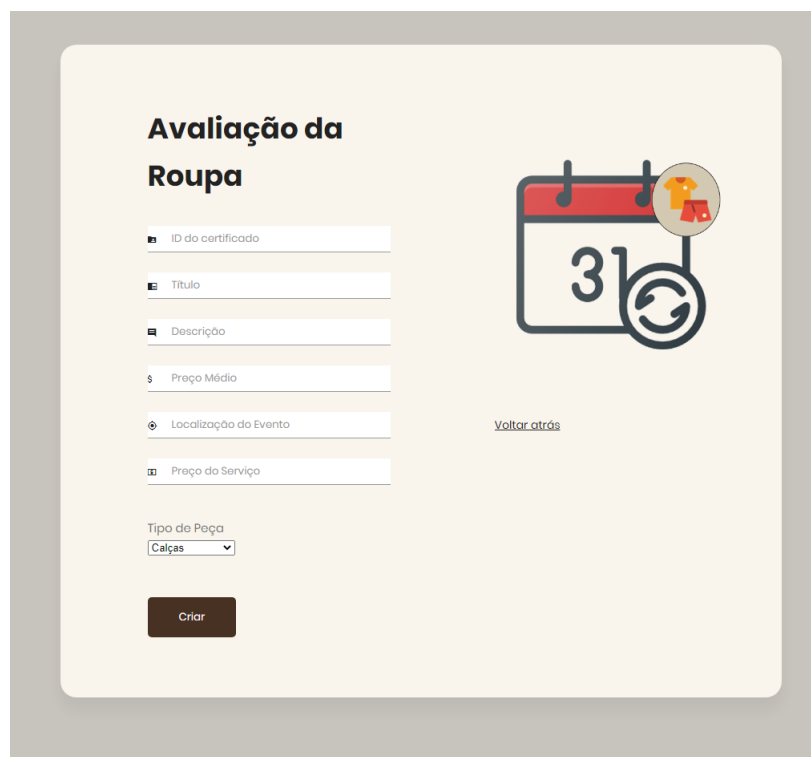
Figura 7: Formulário para o certificado do ouro

Loading - Depois de carregar em Criar, vai ser redirecionado para esta página em que tem de esperar até o certificado estar pronto. Uma vez que o QRCode se apresenta disponível, é só dar *scan* com a Aplicação Mobile



Figura 8: Página de criação do certificado


Evento - Esta é a página para criar um evento, neste caso, para a roupa. É obrigatório preencher todos os campos



The image shows a web form titled "Avaliação da Roupa" (Clothing Evaluation) for creating an event. The form is set against a light beige background with a grey border. It contains several input fields, each with a small icon to its left: "ID do certificado" (ID of the certificate) with a document icon, "Título" (Title) with a document icon, "Descrição" (Description) with a speech bubble icon, "Preço Médio" (Average Price) with a dollar sign icon, "Localização do Evento" (Event Location) with a location pin icon, and "Preço do Serviço" (Service Price) with a tag icon. Below these is a dropdown menu labeled "Tipo de Peça" (Type of Piece) with "Calças" (Trousers) selected. At the bottom left is a dark brown "Criar" (Create) button. On the right side of the form, there is a large illustration of a calendar page showing the number "31", a circular arrow icon, and a small circular inset showing a red shirt and pants. Below this illustration is a link that says "Voltar atrás" (Go back).

Figura 9: Página de criação de um Evento

Notificação - Esta é a página para criar uma notificação. É obrigatório preencher todos os campos

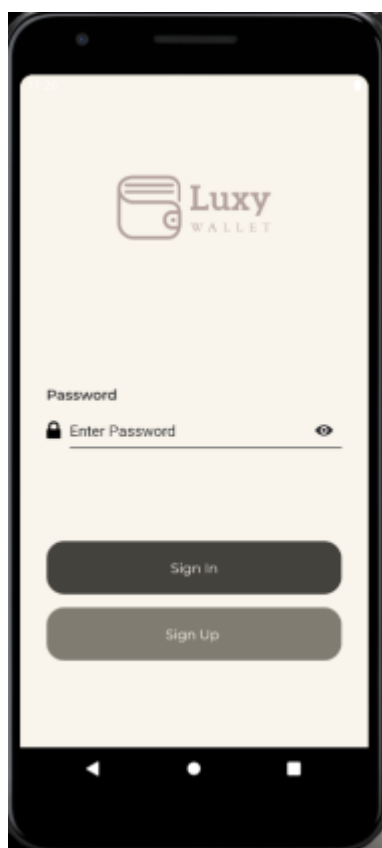


The image shows a web form titled "Notificação" (Notification) on a light beige background. The form contains three input fields: "Título" (Title) with a speech bubble icon, "Descrição" (Description) with a document icon, and "Link" with a chain link icon. Below these fields is a dark brown button labeled "Criar" (Create). To the right of the form is a large illustration of a smartphone with a blue notification bubble and a yellow bell icon. At the bottom right of the form area is a link labeled "Voltar atrás" (Go back).

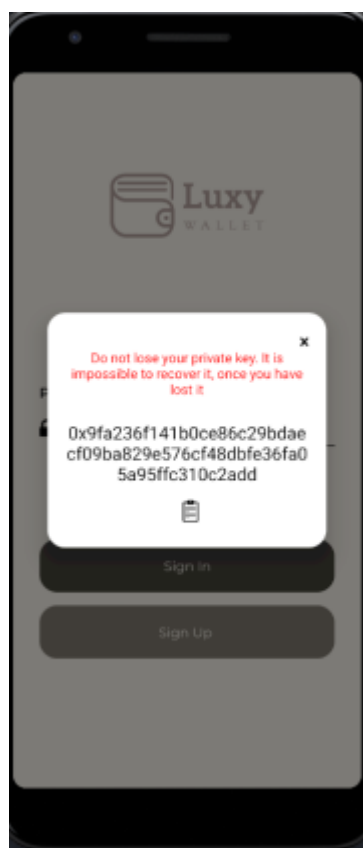
Figura 10: Página de criação de uma notificação

3.3.2 App Mobile

Página Inicial - Esta é a página principal da aplicação quando se inicia. Na **Figura11(a)** temos o Login e se carregarmos no botão *Sign Up* aparece um *pop-up* como podemos ver na **Figura11(b)** com a sua chave privada criada, sendo esta a única forma de ter acesso a sua carteira



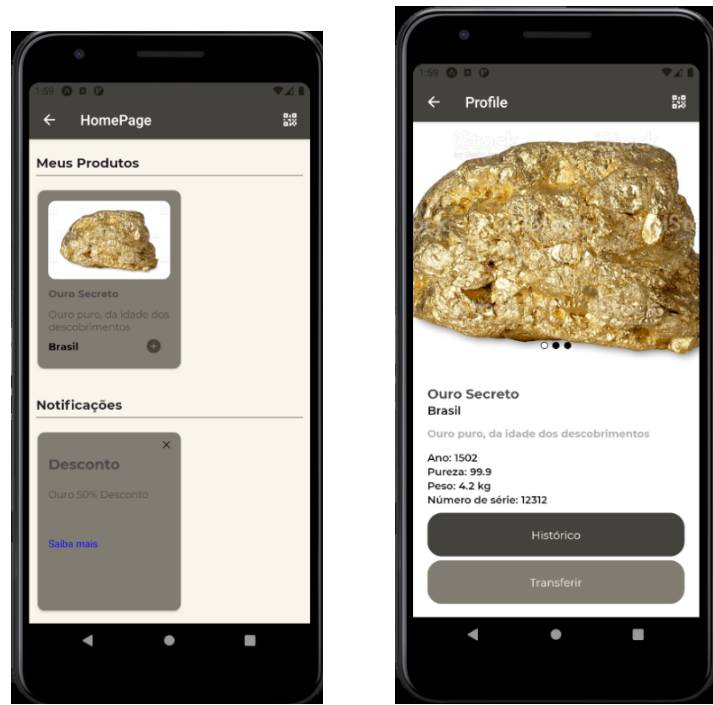
(a) Login



(b) Registo

Figura 11

Homepage & Página de um produto - Página responsável por apresentar todos os produtos e notificações da sua carteira (**Figura12(a)**) e página mais detalhada de um produto (**Figura12(b)**), podendo verificar o seu histórico (**Figura13(a)**) e gerar um QRcode para transferir o produto para outra carteira (**Figura13(b)**).



(a) Homepage

(b) Página de um Produto

Figura 12

Histórico & QRCode - Páginas de histórico de um produto e de geração de um QRCode para a transferência deste para outra carteira.



(a) Histórico de um produto



(b) Geração de QRCode para transferir produto

Scan de um QRCode - Para transferir um produto ou aceitar um evento é preciso dar Scan do QRCode gerado. Para isso temos este *scan* para fazer uso desta funcionalidade.

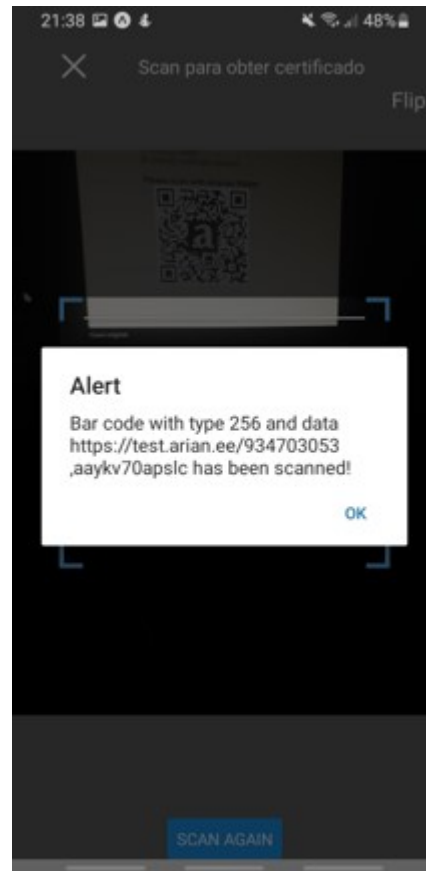


Figura 14: Scan de um QRCode

4 Utilização do Sistema

A utilização do sistema está explicitada no README no nosso [github](#)

5 Conclusão e Trabalho Futuro

Na realização deste projecto tivemos algumas dificuldades iniciais na conexão com a *API* de Arianee em React. Contactamos pessoas que estavam dentro do projeto da Arianee e eles disseram-nos que a *ArianeeJS* não podia ser usada diretamente com o *React Native*. Portanto, tivemos que criar uma API à parte para usarmos o protocolo deles.

Em segundo lugar, tivemos de aprender a trabalhar com *React Native* o que é sempre um pequeno obstáculo, mas nada que não fosse ultrapassável.

O único problema que consideramos não ter ficado resolvido, mas foi arranjado uma maneira de dar a volta temporariamente. Durante o projeto seria útil que os servers estivessem públicos e para isso utilizamos um expositor (**ngrok**) que atuava como uma ponte entre o server local e a internet. Apesar de ser uma solução válida, este método não é, de todo, o ideal. Isso deve-se ao facto de que, de que a cada 2 horas, o ngrok reiniciava e iria atribuir um ip diferente ao serviço local e precisaríamos de alterar dentro do código, este IP.

Finalmente gostaríamos de salientar que, apesar de todas as dificuldades sentidas, estamos satisfeitos com o trabalho desenvolvido pois cumpre todos os requisitos definidos à partida fornecendo uma interface bastante intuitiva a todos os participantes.

No trabalho futuro, existem alguns aspetos que poderiam ser melhorados, como por exemplo alterar os campos dos certificados, permitir escolher a público-alvo das notificações e expandir para mais produtos sem ser roupa e ouro.

Referências

- [1] Brandão, A.M., Gadekar, M. (2019). The Counterfeit Market and the Luxury Goods.
- [2] Arianee. Acedido em Março, em: <https://www.arianee.org/>.
- [3] Everledger. Acedido em Março, em: <https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/>.
- [4] Provenance Blockchain: the solution for transparency in product supply chains. Acedido em Março, em: <https://www.provenance.org/whitepaper>.