



# Blockchain e Seguro Mútuo - com parceria Coover

# Controle do Documento

## Histórico de revisões

Data	Autor	Versão	Resumo da atividade
10/02/2023	Daniel Barzilai, Gabriel Rocha, Gustavo Monteiro, Rodrigo Martins, Thainá Lima e Vitória Rodrigues	1.0	Adição da seção 3 e 4

# Sumário

1. Introdução	5
2. Objetivos e Justificativa	1
2.1. Objetivos	1
2.2. Justificativa	1
3. Análise do Negócio	2
3.1. Contexto da indústria	2
<b>3.1.1. Cinco Forças de Porter</b>	<b>2</b>
3.2. Ferramentas	6
<b>3.2.1. Análise SWOT</b>	<b>6</b>
<b>3.2.2. Matriz de risco</b>	<b>8</b>
<b>3.2.3. Análise de risco</b>	<b>9</b>
<b>3.2.4. Análise Financeira</b>	<b>12</b>
<b>3.2.5. Matriz Oceano azul</b>	<b>13</b>
<b>3.2.6. Value Proposition Canvas</b>	<b>15</b>
4. Análise de Experiência do Usuário	17
4.1. Personas	17
4.2. Jornadas do Usuário e/ou Storyboard.	18
4.3. User Story	19
5. Solução Proposta	23
5.1. Solução	23
5.2. Arquitetura Proposta	23
5.3. Diagrama Macro da Solução	24
5.4. Descrição da Solução	25
5.5. Diagrama de Implantação UML	25
5.6. Diagrama de Sequência de Integração FrontEnd com Smart Contract	27
6. Desenvolvimento e Resultados	29
6.1. Usuário Cliente	29
6.1.1. Descrição	29
6.1.2. Tecnologia adotada	29
6.1.2.1. Carteira MetaMask	29
6.1.2.2. Truffle-cli	29
6.1.2.3. Infura	30
6.1.2.4. Ganache-cli	30
6.1.3. User Stories	30
6.1.4. Prototipação	30
6.1.5. Diagramas	30
<b>6.1.5.2. Diagrama Sequencial - Pedido de Indenização</b>	<b>32</b>

<b>6.1.5.3. Diagrama Sequencial - Reposição de Reserva de Risco</b>	<b>34</b>
6.2. Usuário Administrador	35
6.2.1. Descrição	35
6.2.2. Tecnologia adotada	35
6.2.3. User Stories	35
6.2.4. Prototipação	35
6.2.5. Diagramas	36
6.1.5.2. Diagrama Sequencial - Pedido de Indenização	37
6.3. Avaliação	39
7. Conclusões e Recomendações	41
8. Referências	42
Anexos	43
ANEXO I – Sprint 1	43
ANEXO II – Sprint 2	43
ANEXO III – Sprint 3	44
ANEXO IV – Sprint 5	45

# 1. Introdução

A Coover é uma empresa de pequeno porte, localizada em Vitória, Espírito Santo, e atua na área de seguro para celular e saúde pet.

A Coover detém a licença para seguradoras concedida pela Superintendência de Seguros Privados (SUSEP), mas tenta se posicionar de forma disruptiva em relação a um mercado já consolidado. Quando se trata de seguro, o principal diferencial das grandes empresas é garantir a relação de confiança, por toda sua história no mercado, transmitindo ao cliente sensação de tranquilidade e proteção. Quando se trata de uma seguradora menor, não é tão claramente transmitida para os clientes essa sensação de proteção. Dessa forma, a Coover quer diferenciar suas proposta dentro de mercado com uma regra de negócio diferenciada. Mas como? Para se tornar uma mediadora de seguros, ao invés de uma seguradora tradicional, a proposta é organizar grupos de seguro mútuo. Entre os desafios, estão garantir uma relação de confiança entre pessoas que não se conhecem e viabilizar uma maneira de transmitir essa sensação. Finalmente, será construído um Smart Contract e uma aplicação web3. Dessa forma, nossa solução garantirá confiança através de um contrato autoexecutável e proporcionará uma experiência amigável para novos clientes com uma interface clara e intuitiva.

## 1.1. Parceiro de Negócios

Fabício Vargas Matos, formado em ciência da computação, fundador e CTO da Coover, é o principal stakeholder do projeto de desenvolvimento de software descentralizado utilizando blockchain. Na tentativa de se diferenciar no mercado de seguros, a Coover quer se posicionar como uma mediadora para a formação de grupos de seguro mútuo, mas isso depende da relação de confiança entre desconhecidos que têm o mesmo interesse. Para isso, será construído Smart Contracts que formam o Protocolo de Seguro P2P e aplicação interface web3.

## 1.2. Definição do Problema

### 1.2.1. Problema

O projeto é o primeiro passo para o grande objetivo da Coover: se tornar uma mediadora de seguros, não uma seguradora. Nesse ínterim, será assegurado para a Coover um software descentralizado utilizando blockchain. Assim, será possível para os clientes da Coover participarem de grupos de seguro mútuo, cuja confiança será garantida por Smart Contracts que formam o Protocolo de Seguro P2P.

## 2. Objetivos e Justificativa

### 2.1. Objetivos

A Parceira Coover apresentou uma proposta que visa o desenvolvimento de um de software descentralizado utilizando blockchain e uma aplicação web3. A intenção é permitir a realização e validação de operações em testnet aberto para um modelo simples de seguro peer-to-peer ou grupo de seguro mútuo. Cada grupo criado será uma DAO (Organização Autônoma Descentralizada) no Ethereum, mantendo no próprio smart contract as reservas financeiras.

A proposta da Coover é inovadora e pode trazer muitas vantagens para o mercado de seguros. Ao utilizar a tecnologia blockchain ethereum e a aplicação web3, a Coover propõe a criação de um sistema seguro e transparente para operações de grupos de seguro mútuo.

Essa abordagem permite que cada grupo de mútuo criado seja uma DAO no Ethereum, o que significa que ele é governado pelos próprios membros do grupo, de forma descentralizada e democrática. Além disso, todas as reservas financeiras do grupo serão mantidas no próprio smart contract, garantindo maior transparência e segurança.

### 2.2. Justificativa

A proposta de solução apresentada acima é uma tecnologia blockchain ethereum e a aplicação web3 para criar um sistema inovador e seguro para operações de seguro peer-to-peer ou grupo de seguro mútuo. Essa solução traz diversos potenciais e benefícios para o mercado de seguros.

Em primeiro instância , a solução permite que cada grupo do seguro mútuo criado seja uma DAO, ou seja, os próprios membros do grupo que administram, de forma descentralizada e democrática. Isso garante maior transparência e segurança para as operações realizadas, pois todos os membros têm acesso às informações e podem participar das decisões do grupo.

Além disso, todas as reservas financeiras do grupo serão mantidas no próprio smart contract, garantindo maior transparência e segurança para os usuários. Isso significa que as reservas serão gerenciadas de forma automática e transparente, sem que haja a necessidade de intermediários ou burocracias. Ademais, a solução pode reduzir os custos de operação do seguro, pois, como citado acima, elimina a necessidade de intermediários, além de garantir maior eficiência e transparência para as operações realizadas.

Percebe-se, por conseguinte, que a solução se diferencia por utilizar tecnologia blockchain ethereum e a aplicação web3, tecnologias avançadas e seguras, capazes de garantir a segurança e a transparência das operações realizadas. Portanto, tal solução pode trazer grandes benefícios para o mercado de seguros, tornando-o mais eficiente, transparente e acessível para todos os usuários.

## 3. Análise do Negócio

Para entender melhor os desafios, oportunidades e riscos de uma empresa, diversas ferramentas podem ser utilizadas para ajudar as empresas a se manterem competitivas em relação às outras, em um mercado que muda bastante conforme novas tecnologias surgem. As ferramentas utilizadas neste projeto serão descritas a seguir:

### 3.1. Contexto da indústria

O contexto da indústria é fundamental para a empresa avaliar o mercado em que ela está inserida e assim, elaborar estratégias eficazes para melhorar seus produtos, processos e serviços. Abaixo, está a descrição da análise feita:

#### 3.1.1. Cinco Forças de Porter

Este é um modelo que descreve forças que moldam cada indústria e auxilia a determinar pontos fortes e pontos de atenção do setor analisado, posicionando a solução, de forma estratégica, em relação ao cenário atual do setor.

A seguir serão apresentadas as cinco forças (ameaça de produtos substitutos; ameaça de entrada de novos concorrentes; poder de negociação dos clientes; poder de negociação dos fornecedores e rivalidade entre os concorrentes) do setor de seguros:

##### **Ameaça de Novos Entrantes:**

A facilidade de ingresso de empresas nos setores é uma das variáveis que determinam a ameaça de novos entrantes.

- Big Techs, como Google e Amazon podem ingressar no setor de seguros, na promessa de oferecer mais vantagens e maior eficiência, com o uso de dados e tecnologias de inteligência artificial, para melhorar tomadas de decisão e a personalização de produtos de seguro. Mas é importante destacar questões regulatórias e a proteção de dados, para estabelecer uma confiança e credibilidade com clientes do setor de seguros;
- É importante dizer que existem barreiras significativas para a entrada de empresas no setor de seguros, como a regulamentação, já que o setor de seguros é altamente

regulamentado com licenças para proteger os clientes, e também trazer credibilidade, pois a confiança é um dos aspectos mais importantes para atração de clientes no setor.

- Startups também estão utilizando novos tipos de tecnologia financeira para reservas de investimentos mútuos por meio de um smart contract, com um potencial disruptivo significativo para as empresas tradicionais do setor.

A ameaça de novos entrantes depende de alguns fatores, como regulamentação do mercado, pressão e o espaço ocupados por grandes empresas, a necessidade de um capital significativo para o negócio e a complexidade dos produtos disponibilizados para os clientes. O surgimento e popularidade de tecnologias e empresas de tecnologia financeira podem facilitar a entrada de empresas no setor, aumentando a ameaça de novos entrantes. No caso de seguradoras o risco pode ser considerado médio, por conta das barreiras de regulação que impedem a entrada de empresas sem licença para operar no setor.

### **Ameaça de Produtos ou Serviços Substitutos**

Influenciada pela disponibilidade de alternativas, a relação custo-benefício e os padrões de consumo e preferência dos clientes, a ameaça de produtos ou serviços substitutos é uma análise de indústria importante, pelo impacto nos produtos e serviços oferecidos pelas empresas.

- A tendência crescente de soluções de autosseguro, assim como outras formas de proteção financeira, por meio de investimentos e poupanças, pode aumentar a ameaça de produtos substitutos. Porém, a credibilidade e a percepção de que seguradoras ainda são uma forma mais confiável de proteção ao patrimônio pessoal e empresarial pode reduzir a ameaça de substituição;
- O custo de mudança de produtos de seguradoras pode ser considerado alto, por conta do alto custo para manter os sistemas de gerenciamento dos produtos, onde a mudança pode requerer uma atualização para um preço mais elevado que antes da alteração. Outro aspecto é a regulamentação, que pode afetar diretamente nesse ajuste de produtos, e também o marketing e publicidade, essenciais para divulgar novos produtos.

Mudanças para novos produtos podem trazer benefícios e manter empresas mais competitivas em relação a produtos substitutos, principalmente ao trazer um aspecto



educativo que promova uma mudança de comportamento nos usuários, para entenderem a importância de produtos de uma seguradora, sendo um risco alto no caso das seguradoras, por existirem substitutos de fácil acesso aos usuários, como auto seguros, que são uma forma de proteção do cliente que utiliza seu próprio capital para gerenciar riscos.

### **Poder de Barganha dos Fornecedores**

Este fator é influenciado pela concentração de fornecedores, importância de fornecedores para a empresa, facilidade para mudar para outros fornecedores.

- O custo para se tornar um fornecedor de seguradoras varia com o rigor da regulamentação, que pode criar barreiras para novos fornecedores, dificultando o surgimento de novos fornecedores, aumentando o poder de barganha de fornecedores já existentes;
- Bancos podem ser intermediários entre seguradoras e clientes, possibilitando a oferta de produtos e associações benéficas entre os próprios bancos, as seguradoras e os clientes;
- Seguradoras dependem de outros fornecedores, como consultorias para identificar tendências, peritos para avaliar documentos, entre outros tipos de fornecedores que oferecem atendimentos e promovem melhorias nos produtos e serviços das seguradoras aos clientes;
- Resseguradoras desempenham um papel fundamental para proteger as seguradoras de grandes perdas, permitindo uma gestão de risco associado a grandes quantidades de apólices, evitando grandes perdas financeiras. O poder de barganha das resseguradoras aumenta quando as condições do mercado estão desfavoráveis, e perdas são mais prováveis de acontecer, incentivando o aumento do valor das coberturas de resseguro, ou se tornando mais seletivas quanto às apólices de seguros com cobertura de resseguro.

No setor de seguros, o poder de barganha dos fornecedores pode ser considerado médio, pelo impacto que fornecedores apresentam na influência do preço final dos produtos. Com o aumento dos fornecedores disponíveis e a facilidade de mudança entre os fornecedores, esse poder de barganha pode ser reduzido. Outro fator importante para mitigar o poder de

fornecedores é a diversificação das carteiras de seguro, ou acordos de cooperação entre empresas de seguro, possibilitando um melhor gerenciamento dos riscos.

### **Poder de Barganha dos Compradores**

Os compradores possuem poder de influência sobre as seguradoras através da concentração de compradores, sensibilidade dos clientes sobre preços e o comportamento dos compradores diante das empresas e seus produtos.

- A depender da sensibilidade dos clientes sobre os preços dos produtos e serviços, menor pode ser a variação dos valores dos produtos das seguradoras. Isso também varia de acordo com a percepção da importância do seguro, onde quanto maior a importância e a noção de necessidade, menor a sensibilidade do valor cobrado pelo serviço;
- Mudanças nas condições econômicas, como eventos de recessão econômica ou aumentos na taxa de juros, aumentam a sensibilidade dos clientes aos preços de seguros, incentivando uma procura por alternativas mais acessíveis;
- Autosseguros representam o maior poder de barganha dos consumidores, por eles próprios podendo se proteger cobrindo as próprias despesas de sinistro. Tanto pessoas físicas quanto jurídicas podem fazer preservar capital, controlando os próprios riscos, reduzindo a demanda de seguradoras, mesmo sendo menos eficientes, pela menor experiência sobre gerenciamento de riscos.

O poder de barganha dos compradores pode ser considerado alto, pela sensibilidade em relação aos preços e a possibilidade de produzir o produto de forma autônoma, e também pela influência de mudanças no cenário econômico, afetando diretamente os consumidores e seu poder de compra.

### **Rivalidade entre Concorrentes Existentes**

A rivalidade é uma dimensão importante para as empresas, por afetar diretamente a performance das empresas, disponibilidade e preço dos produtos e serviços oferecidos, pela quantidade de empresas no setor, e a necessidade de diferenciação e diversificação para atrair e fidelizar clientes.

- Seguradoras tendem a apresentar estratégias e produtos semelhantes entre si, incentivando empresas a aplicarem preços mais agressivos, muito mais baixos em relação aos concorrentes, dificultando a implementação de produtos diferenciados mas com o preço mais elevado;
- Por ser um setor com uma alta regulação, essas amarras regulatórias podem aumentar a competição entre as empresas, ao forçar uma padronização que limita a diversificação das empresas ao oferecer produtos e serviços.

No caso do setor de seguros, a concorrência pode ser considerada alta, pela dificuldade na diferenciação de produtos, que afeta diretamente a baixa elasticidade dos preços dos produtos existentes, e a estratégia de divulgação semelhante, que dificulta a diferenciação e a conquista da empresa por clientes.

Assim, a estratégia de especialização de produtos, para alguns tipos de seguros específicos, pode ser interessante para a empresa se destacar e atrair clientes.

O investimento em tecnologias disruptivas, para desenvolver novos produtos e aumentar a segurança e confiança nos processos do seguro, também se mostra interessante para o desenvolvimento e renovação no setor de seguros.

## 3.2. Ferramentas

Ferramentas de análise de negócios possibilitam a coleta, organização e análise de informações importantes para o desenvolvimento de soluções mais eficientes e efetivas para o projeto, podendo aumentar as chances de sucesso.

A seguir serão apresentadas as ferramentas utilizadas neste trabalho, onde cada uma possui objetivos e aplicações específicas:

### 3.2.1. Análise SWOT

Essa ferramenta auxilia na identificação fatores internos e externos da empresa, para desenvolver estratégias mais eficazes, e complementar análises de negócio juntamente com outras ferramentas.

Entre os fatores internos, as forças são características que trazem aspectos positivos da empresa, que a diferenciam de seus concorrentes, usados como vantagem competitiva, e fraquezas trazem pontos a melhorar ou que precisam ser corrigidos, para aumentar a chance de sucesso da empresa.

Já os fatores externos são elementos que a empresa não pode controlar, mas que afetam seu desempenho e sucesso. Ameaças são fatores negativos que podem prejudicar a situação da empresa, podendo indicar tendências negativas. Quando existem fatores externos favoráveis à empresa, são chamados de oportunidades, que podem ser aproveitadas pela empresa.

Forças	Oportunidades
<ul style="list-style-type: none"> <li>• Uso da Tecnologia Blockchain para garantir transparência, segurança e eficiência nos processos;</li> <li>• Possui licença para atuar no setor pelo Órgão Regulador Susep;</li> <li>• Pode oferecer soluções ágeis para cliente, pela automatização de processos e análise de dados;</li> <li>• Diferenciação no setor de seguros, pela diversificação de seus produtos.</li> </ul>	<ul style="list-style-type: none"> <li>• Aumento da presença digital dos clientes pode favorecer a divulgação e entendimento de um novo tipo de solução tecnológica no setor;</li> <li>• Possibilidade de atrair novos clientes interessados em soluções inovadoras de segurança no setor;</li> <li>• Parceria com bancos ou outras empresas financeiras para ampliar a rede de distribuição e oferta de produtos;</li> <li>• O grande desenvolvimento da tecnologia de blockchain pode favorecer parcerias diversas e novas oportunidades de negócio.</li> </ul>
Fraquezas	Ameaças

<ul style="list-style-type: none"> <li>• Falta de experiência e conhecimento no mercado da tecnologia blockchain;</li> <li>• Limitada presença nas mídias sociais;</li> <li>• Risco de queda na confiança dos clientes, se houver problemas técnicos ou de segurança na utilização de uma nova tecnologia;</li> <li>• Alto custo de manutenção e implementação da tecnologia blockchain.</li> </ul>	<ul style="list-style-type: none"> <li>• Entrada de novos competidores que utilizam a tecnologia de blockchain no setor;</li> <li>• Mudanças regulatórias no setor de seguros, que podem restringir ou inviabilizar o uso de tecnologias blockchain nos processos de seguro;</li> <li>• Pouco entendimento das pessoas em relação ao que é Blockchain, reduzindo a confiabilidade na empresa;</li> <li>• Concorrência de outras empresas de proteção financeira, como investimentos.</li> </ul>
---	---

Tabela 1 - Análise SWOT do parceiro de projeto Coover, com a análise de pontos fortes, oportunidades, fraquezas e ameaças.

É importante a empresa investir em campanhas de marketing para aumentar sua presença nas mídias sociais, aproveitando a tecnologia blockchain para aprimorar seus processos e se diferenciar dos concorrentes, promovendo uma maior confiabilidade dos clientes.

As mudanças regulatórias também afetam diretamente o negócio, necessitando manter a empresa sempre atualizada, para possibilitar adequações em tempo hábil.

### 3.2.2. Matriz de risco

Este modelo apresentará os possíveis riscos dentro da produção do MVP. Os riscos são calculados pelo nível de probabilidade e impacto de uma situação caso ocorra, podendo ser Ameaças(Negativo) ou Oportunidades(Positivo).

O link da matriz está indicado ANEXO I -Sprint 1.

### 3.2.3. Análise de risco

Neste capítulo serão apresentados pontos vulneráveis da arquitetura da solução desenvolvida neste projeto, já que através do uso de tecnologias, como computadores e celulares, os dados trafegados por estes aparelhos podem estar suscetíveis a diversas vulnerabilidades, podendo trazer prejuízos aos usuários e à empresa. Por isso, é necessário a implantação de uma Política de Segurança da Informação (PSI), para padronizar processos e minimizar o impacto de ataques aos dados (Castilho e Fonte, 2012).

Com a importância e o valor que os dados representam para as pessoas e instituições, existem cinco características da informação, que leva em conta a relação da natureza do dado, com seu armazenamento e utilização nos sistemas e processos, que são: confidencialidade, autenticidade, integridade, disponibilidade e irretratabilidade (Nakamura, 2011).

Dentre as motivações dos ataques podem variar desde obter lucro através de roubo de criptomoedas e roubo de informações, até utilizar vulnerabilidades do sistema para sabotar a plataforma, e causar danos no sistema como um todo.

Após uma avaliação do projeto e da arquitetura da solução, para elaborar uma análise de risco da segurança da informação, foi determinado a presentes na tabela a seguir:

Tipo de ataque	Probabilidade	Impacto
Página Web vulnerável a acessos que podem sobrecarregar o site e tirar a página do ar.	Média	Médio
Phishing - com a criação de uma página falsa para cadastro dos clientes.	Média	Muito Alto
Packet Capturing - onde pacotes de dados são captados na rede do sistema, e permitindo que o atacante tenha acesso a informações sigilosas.	Alta	Alto
Port Scanning - com acesso de atacantes aos serviços sendo utilizados por um computador, descobrindo quais softwares estão em operação, e explorando as vulnerabilidades destes softwares para invadir o computador.	Média	Alto

	Probabilidade	Impacto
Access control - no qual a falha é associada à permissão que cada endereço possui dentro do contrato.	Média	Alto
Spoofing - em que o atacante se passa por alguém que não é, fraudando os pacotes IP.	Alta	Alto

Tabela 2 - Análise de Riscos de ataques cibernéticos, com tipos de ataques, probabilidade do ataque e o seu impacto no projeto.

### Confidencialidade:

Esta característica se refere à privacidade das informações, e controle de acesso aos dados por usuários, protegendo acessos e ações por usuários sem autorização, mantendo então a confidencialidade.

Violações de confidencialidade podem ocorrer a partir de ataques diretos, para obter acesso a áreas restritas de um sistema, banco de dados, entre outros processos que podem explorar vulnerabilidades da rede de computadores, softwares em funcionamento no sistema, vazamento de informações sensíveis do site, etc.

Alguns dos ataques que podem comprometer a confidencialidade do sistema, é o de phishing, com algum mecanismo que engane o usuário a compartilhar informações por algum meio de comunicação falso. Outros métodos de acesso a dados são Packet Capturing que é o processo de captação de dados diretamente da rede do sistema, Port Scanning já é um mecanismo elaborado de acesso a um computador a partir das portas que são utilizadas por softwares, explorando vulnerabilidades dos próprios softwares.

Outro fator importante para considerar, é o erro humano, como compartilhamento de informações ou processos sigilosos, incluindo a integridade de equipamentos físicos, e unidades de armazenamento, que podem sofrer danos ou serem violados.

Existem várias medidas que podem ser adotadas para proteger a confidencialidade dos dados, como mecanismos de criptografia, para encriptar dados durante o seu trânsito, armazenamento, e uso em processos.

### Vulnerabilidades existentes:

- Vazamento de informações sensíveis do site.
- Softwares utilizados podem apresentar vulnerabilidades.

### **Tipos de ataques:**

- Página Web vulnerável a ataques que podem sobrecarregar o site e tirar a página do ar.
- Phishing, com a criação de uma página falsa para cadastro dos clientes.
- Packet Capturing, onde pacotes de dados são captados na rede do sistema, e permitindo que o atacante tenha acesso a informações sigilosas.

Port Scanning, com acesso de atacantes aos serviços sendo utilizados por um computador, descobrindo quais softwares estão em operação, e explorando as vulnerabilidades destes softwares para invadir o computador.

### **Irretratabilidade:**

A irretratabilidade, também conhecido como não repúdio, consiste no princípio jurídico da irretratabilidade. Resumidamente, a irretratabilidade garante que uma pessoa ou entidade não possa negar a autoria de informações fornecidas, como é o caso de diplomas, certificados e assinaturas digitais.

Na era digital em que vivemos, muitos contratos são feitos virtualmente, portanto, esse pilar da segurança da informação garante ao usuário comprovar o que foi feito, quem fez, o que fez e quando fez, impossibilitando a negação das ações da outra parte.

### **Autenticidade:**

É notável a probabilidade de atacantes provocarem mudanças nas cláusulas do bloco que o *smart contract* está mantido, mudando as regras que regem o contrato mútuo, anteriormente, estabelecido em consenso.

A vulnerabilidade em destaque, corresponde ao *access control*, de acordo com a DASP (Decentralized Application Security Project), pois ataca as falhas em permissões de acesso, que são do criador do contrato. Tal ação ocasiona no incremento ou mudanças nas diretrizes podendo beneficiar uma parte dos envolvidos.

Além disso, outra possibilidade é a quebra da autenticidade no qual atacantes falsificam smart contracts parecidos com aqueles desenvolvidos pelo dono (Coover), enviam o link para



possíveis clientes fazerem parte do grupo de seguro mútuo, e desviam as criptomoedas aplicadas no contrato.

Evidencia-se, conforme regulamentado pela DASP, que essa fragilidade equivale à prática de *spoofing*, visto que, os atacantes podem se passar pela Coover.

### 3.2.4. Análise Financeira

A Análise Financeira é uma ferramenta importante para a tomada de decisões empresariais, pois ajuda a identificar oportunidades de crescimento, pontos fracos na gestão financeira e riscos potenciais. Ela também permite que os gestores avaliem a performance da empresa ao longo do tempo e compreendam como as ações tomadas afetam a saúde financeira da organização.

Nesta análise, dividimos em três seções: Investimento Previsto, Projeções de Custos e Lógica para Alcançar Projeções Financeiras.

#### 1 - Investimento Previsto:

Conforme a informação oferecida pelo cliente, o valor total investido no projeto será de 300 mil reais.

#### 2 - Projeções de Custos:

As projeções de custos e receitas não foram informadas, portanto, para esta análise, será feita uma distribuição do valor total investido em demais requisitos que serão necessários para a realização do projeto.

- Desenvolvimento de contrato inteligente, Web 3.0 e protocolo de seguro blockchain - 35 a 45%;
- Integração com sistemas existentes - 20 a 25%;
- Teste e auditoria - 15 a 20%;
- Marketing e comunicação - 15 a 20%;
- Possíveis imprevistos - 5 a 10%.

A distribuição foi feita por nível de importância das estruturas para o desenvolvimento, teste e conclusão do projeto.

#### 3 - Lógica para Alcançar Projeções Financeiras

### Distribuição com o financiamento

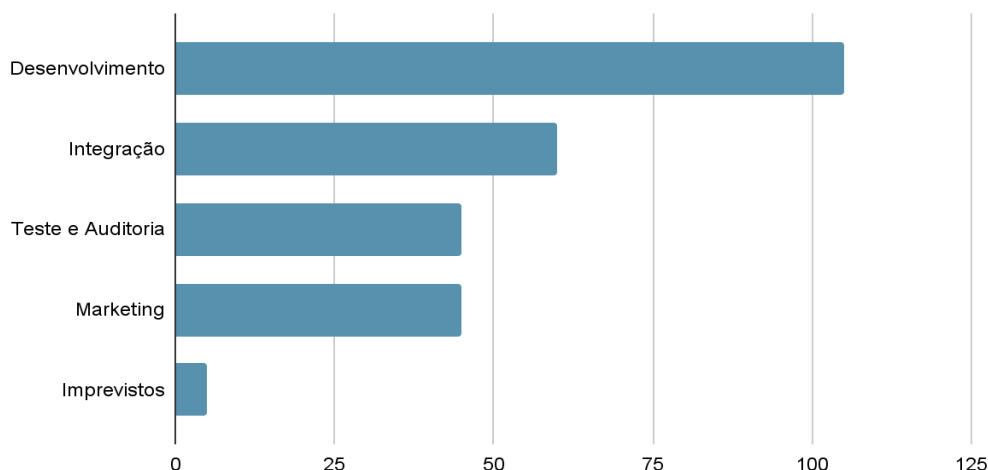


Figura 1 - Gráfico da distribuição com o financiamento

A lógica dita pelo parceiro para alcançar suas projeções financeiras (numericamente não informadas) é o recebimento de investimentos anjos e de debêntures, e por meio das reservas financeiras de usuários da aplicação criada no projeto, que serão armazenadas no contrato inteligente, sendo uma taxa administrativa direcionada para a empresa (Coover).

### 3.2.5. Matriz Oceano azul

A matriz Oceano Azul corresponde ao entendimento de mercados novos e disruptivos. Para melhor compreender a posição da Coover em relação às outras empresas do mercado de seguros, quando relacionados aos fatores essenciais para o bom desenvolvimento do negócio, a matriz foi estruturada, além de possibilitar a visualização gráfica do posicionamento.

Para essa análise, foram utilizadas como comparação outras empresas do mercado de seguro, Porto Seguro e Pier. A Porto Seguro é uma empresa fundada em 1945, na cidade de São Paulo, com o objetivo de se tornar “porto seguro” para as pessoas, assumindo riscos nas mais diversas áreas. Já a Pier, se apresenta no mercado como a primeira seguradora digital do país.

**Eliminar → Zero**

A ação de eliminar está relacionada a enumeração de fatores que podem ser retirados ou melhorados, pois requerem esforço dentro do mercado, mas não possui destaque na Coover. A facilidade de venda é o elemento essencial para aumentar a adoção do público. Na Coover, as etapas de conscientização, interesse, avaliação, experimentação e adoção precisam ser potencializadas, principalmente, quando relacionada ao serviço disponibilizado em Blockchain, tecnologia pouco conhecida e raramente utilizada pelo público geral.

### **Reduzir → Menor**

O padrão de qualidade, nessa observação, é feito com base na adoção da empresa pelo público, além de comentários dos clientes em sites como “reclame aqui”, que reflete a avaliação dos usuários. Para que mais pessoas saibam dos serviços disponibilizados pela Coover, o trabalho de marketing se torna essencial. Entretanto, no atual momento, a Coover, assim como a Pier, é menos conhecida que a Porto Seguros e não domina o “top of mind” da população. O quesito preço é equivalente em todas as empresas, dado que, o valor aplicado na seguradora corresponde à porcentagem do custo agregado ao celular, somado à taxa administrativa.

### **Elevar → Maior que os outros**

A atividade de elevar corresponde ao fator que se destaca na empresa foco da análise e deveria ser otimizado, recebendo maiores investimentos. A praticidade dentro das corporações Coover e Pier são emergentes, principalmente pela digitalização dos serviços. No quesito de segurança, a Coover se destaca na utilização de blockchain para o desenvolvimento de Smart Contracts, sistema seguro, pois não é possível modificar o bloco anterior na rede descentralizada e as regras são imutáveis.

### **Criar → Implementação de ferramentas tecnológicas no procedimento entre segurado e seguradora.**

O entendimento do fator criar é identificar os pontos que estão sendo implementados pelas empresas e são inovadores no mercado. A tecnologia é relativa a utilização do blockchain para armazenamento do smart contract, sendo disruptivo. Já o conforto e comodidade é notório, visto que a Coover mantém os seus serviços com a maior segurança e facilidade, mesmo com uma tecnologia pouco utilizada, estando em contato direto com os clientes.

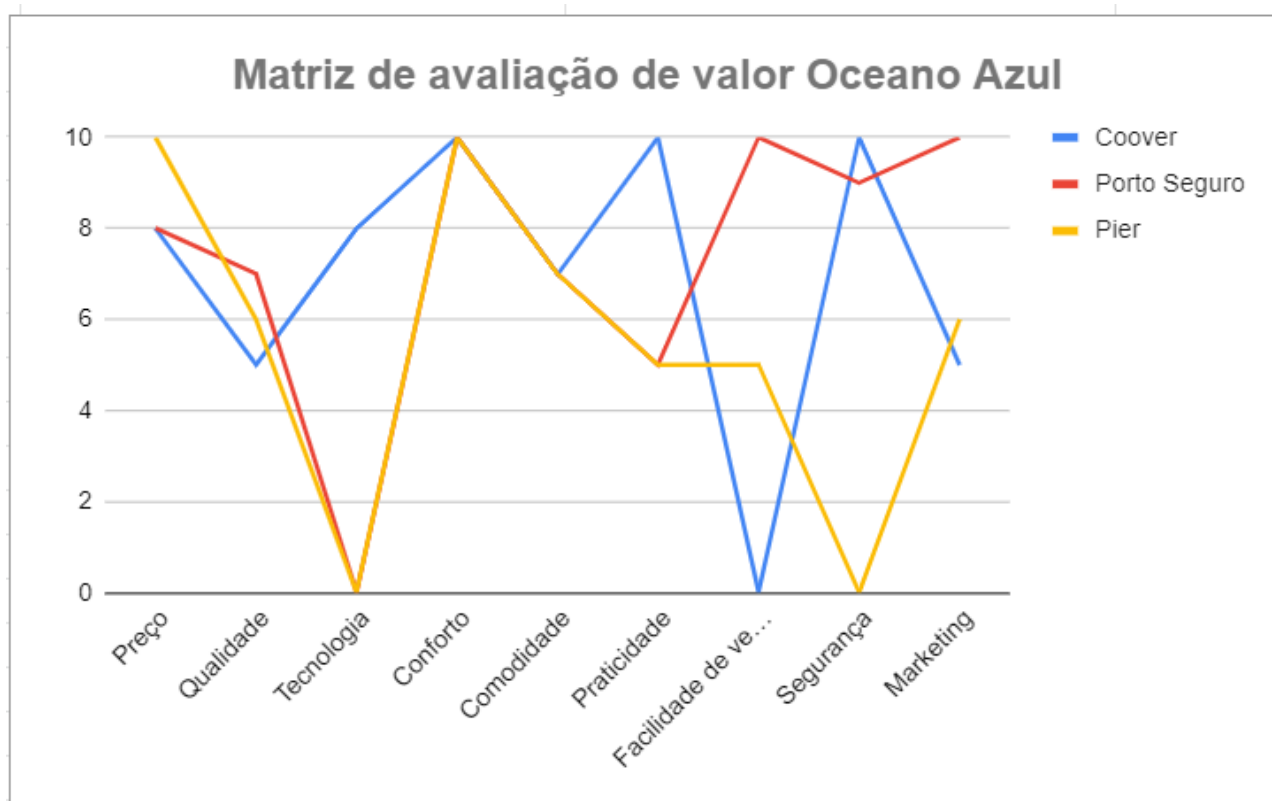


Figura 2 - Gráfico da matriz de avaliação de valor Oceano Azul.

### 3.2.6. Value Proposition Canvas

O "Value Proposition Canvas" é uma ferramenta visual que ajuda as empresas a entender como seus produtos ou serviços criam valor para seus clientes. É composto por duas seções principais:

**Perfil do cliente:** Descreve o segmento de clientes que a empresa visa atender e suas tarefas, dores e ganhos.

**Mapa de Valor:** Descreve como o negócio pretende criar valor para o segmento de clientes, incluindo os produtos e serviços oferecidos, analgésicos, geradores de ganhos e os canais utilizados para atingir o segmento de clientes.

O Perfil do Cliente ajuda as empresas a entender as necessidades, desejos e desafios de seu segmento de clientes-alvo. O Mapa de Valor ajuda as empresas a identificar como criar e

entregar valor que atenda a essas necessidades, abordando as dores do segmento de clientes e gerando ganhos.

Ao usar o Value Proposition Canvas, as empresas podem alinhar suas ofertas com as necessidades do cliente, melhorar suas mensagens de marketing e se diferenciar de seus concorrentes.

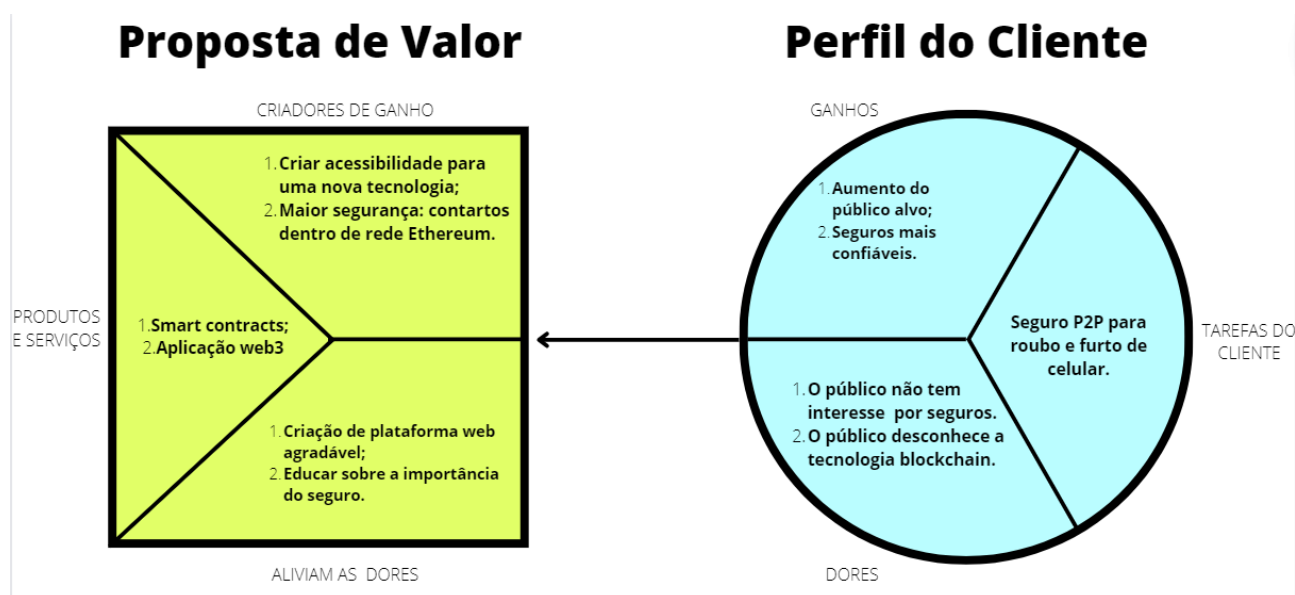


Figura 3 - Canvas de Proposta de Valor de uma solução de Smart Contract em aplicação Web 3.0 para a empresa de seguros Coover.

## 4. Análise de Experiência do Usuário

### 4.1. Personas

A Persona é uma representação humanizada do cliente ideal e é usada para ajudar a equipe de desenvolvimento a compreender melhor as necessidades, desejos e comportamentos de seu público-alvo.

Devido o sistema ser o contato/conexão entre dois públicos alvos, seguradora e cliente, dividimos em duas Personas.

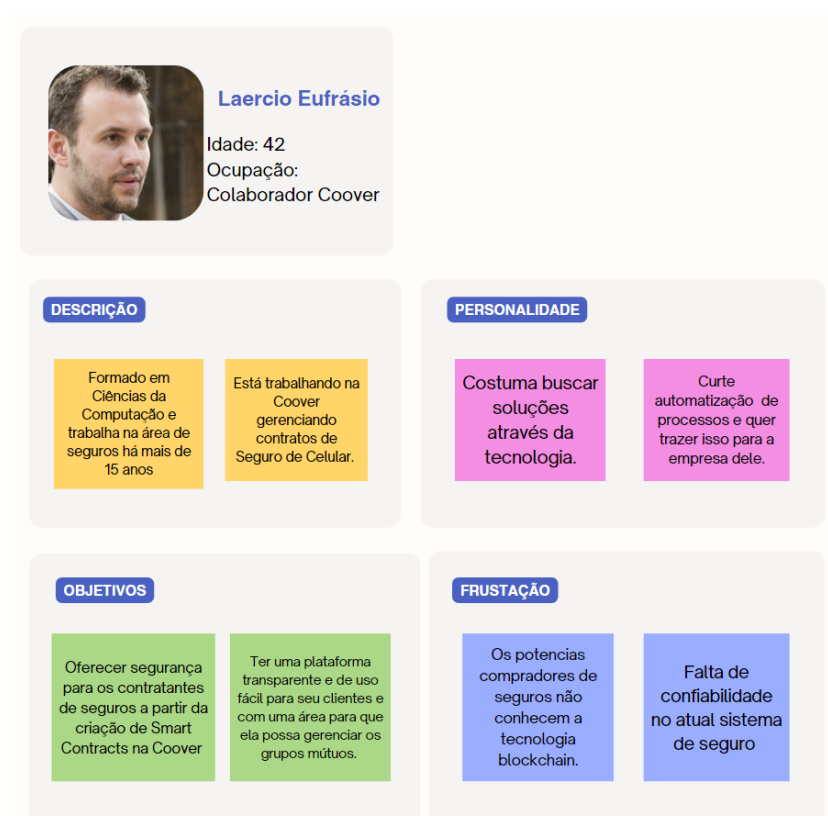


Figura 4 - Laercio Eufrásio, primeira persona desenvolvida, para representar um colaborador da empresa Coover.



Figura 5 - Mariana Trindade, segunda persona desenvolvida, para representar um cliente da empresa Coover.

## 4.2. Jornadas do Usuário e/ou Storyboard.

A jornada do usuário é uma representação visual da interação que um usuário tem ao interagir com um sistema ao longo do tempo. Com isso é possível verificar possíveis melhorias para melhorar a experiência geral do usuário.

Além disso, a jornada do usuário também alinha as expectativas durante o desenvolvimento de um sistema, garantindo que os desenvolvedores estejam trabalhando em direção dos mesmos objetivos.

A seguir a jornada do usuário desenvolvida para este projeto:

- Deploy manual do smart contract;
- Adicionar usuário através do pedido de adesão do cliente, aprovado pelo administrador;
- Depósito inicial feito pelo usuário cliente;
- Usuário cliente verificar o valor do contrato;
- Fazer o pedido de indenização, que pode ser aprovado por um administrador.

## 4.3. User Story

As User Stories são uma técnica de gerenciamento de projetos que se concentra em descrever o comportamento desejado do usuário em relação ao software. Elas fornecem uma visão geral do que o usuário final espera do sistema e ajudam a equipe de desenvolvimento a compreender as necessidades e expectativas do público-alvo. As User Stories são escritas de uma perspectiva do usuário e descrevem, de maneira simples e direta, o que o usuário quer fazer com o software.

Para estas User Stories, utilizamos uma estrutura que inclui a persona, critérios de aceitação e exemplos de teste de aceitação, para facilitar a compreensão e o aprofundamento das ações no sistema.

<b>Número</b>	<b>1.0</b>
<b>Título</b>	Solicitar adesão
<b>Personas</b>	Estudante de TI
<b>História</b>	Como estudante de TI, gostaria de solicitar a adesão ao grupo de seguro mútuo para me proteger contra gastos imprevistos com celular.
<b>Critérios de aceitação</b>	<p>CR-01: Ter um smart contract válido;</p> <p>CR-02: Ter saldo maior ou igual à porcentagem do smart contract.</p>
<b>Testes de aceitação</b>	<p>Testes de aceitação: <b>CR-01</b></p> <p>a) Estudante tem um smart contract</p> <ul style="list-style-type: none"> <li>- Aceitou = correto</li> <li>- Recusou = errado, revisar processo</li> </ul> <p>Testes de aceitação: <b>CR-02</b></p> <p>a) Estudante informa no momento da adesão smart contract com saldo R\$ 0,00</p> <ul style="list-style-type: none"> <li>- Aceitou = errado, corrigir o processo</li> <li>- Recusou = correto</li> </ul> <p>b) Estudante informa um valor menor a porcentagem desejada</p> <ul style="list-style-type: none"> <li>- Aceitou = errado, corrigir o processo</li> <li>- Recusou = correto</li> </ul> <p>c) Estudante informa valor maior ou igual a porcentagem desejada</p> <ul style="list-style-type: none"> <li>- Aceitou = correto</li> <li>- Recusou = errado, revisar o processo</li> </ul>



<b>Número</b>	<b>2.0</b>
<b>Título</b>	Ingressar num grupo de seguro mútuo
<b>Personas</b>	Estudante de TI & Colaborador Coover
<b>História</b>	Como Colaborador Coover, gostaria de poder entrar em contato com o segurado, para manter estabelecida uma relação de confiança.
<b>Crítérios de aceitação</b>	<p>CR-01: O Colaborador Coover envia o link para o segurado(estudante);</p> <p>CR-02: O segurado entra no grupo através do link.</p>
<b>Testes de aceitação</b>	<p>Testes de aceitação: <b>CR-01</b></p> <p>a) O segurado recebeu o link enviado pelo gerente.</p> <ul style="list-style-type: none"> <li>- Recebeu = correto</li> <li>- Não recebeu = errado, revisar o processo.</li> </ul> <p>Testes de aceitação: <b>CR-02</b></p> <p>a) O segurado acessou o link e entrou no grupo de seguro mútuo.</p> <ul style="list-style-type: none"> <li>- Acessou = correto</li> <li>- Não Acessou = errado, revisar o processo</li> </ul>

<b>Número</b>	<b>3.0</b>
<b>Título</b>	Pedir indenização
<b>Personas</b>	Estudante de TI & Colaborador Coover
<b>História</b>	Como estudante de TI, gostaria de poder contar com uma interface visual para poder realizar o pedido de indenização do meu celular em caso de furto ou roubo.
<b>Crítérios de aceitação</b>	<p>CR-01: Pedido de indenização pelo estudante;</p> <p>CR-02: O Smart Contract valida automaticamente os termos estabelecidos;</p> <p>CR-03: Colaborador Coover entra em contato para realizar o processo de indenização.</p>

<b>3.0</b>	
Pedir indenização	
<b>Personas</b>	Estudante de TI & Colaborador Coover
<b>Testes de aceitação</b>	<p>Testes de aceitação: <b>CR-01</b></p> <p>a) O smart contract estava válido no momento do pedido de indenização</p> <ul style="list-style-type: none"> <li>- Aceitou = correto</li> <li>- Recusou = errado, revisar o processo</li> </ul> <p>Testes de aceitação: <b>CR-02</b></p> <p>a) Os termos do smart contract estão válidos</p> <ul style="list-style-type: none"> <li>- Aceitou = correto</li> <li>- Recusou = errado, revisar o processo</li> </ul> <p>b) Os termos do smart contract não estão válidos</p> <ul style="list-style-type: none"> <li>- Aceitou = errado, revisar o processo</li> <li>- Recusou = correto</li> </ul> <p>Teste de aceitação: <b>CR-03</b></p> <p>a) Contato com cliente foi bem sucedido</p> <ul style="list-style-type: none"> <li>- Contatou = correto</li> <li>- Não contatou = errado, tentar novamente</li> </ul>

<b>Número</b>	<b>4.0</b>
<b>Título</b>	Repor reserva de risco
<b>Personas</b>	Colaborador Coover
<b>História</b>	Como Colaborador Coover, gostaria que as reservas de risco sejam repostas para estar preparado para indenizar possíveis sinistros.
<b>Critérios de aceitação</b>	<p><b>CR-01:</b> A reserva estar menor que o valor total do seguro mútuo;</p> <p><b>CR-02:</b> Solicitar que os integrantes já indenizados, depositem novamente no contrato a porcentagem correspondente ao seguro do seu dispositivo.</p> <p><b>CR-03:</b> Usar o dashboard para garantir que a reserva de risco foi reposta.</p>
<b>Testes de aceitação</b>	<p>Testes de aceitação: <b>CR-01</b></p> <p>a) A reserva ultrapassa o valor total do seguro mútuo.</p> <ul style="list-style-type: none"> <li>- Aceitou = correto.</li> <li>- Recusou = errado, revisar o processo.</li> </ul> <p>b) A reserva está abaixo do valor total do seguro mútuo.</p> <ul style="list-style-type: none"> <li>- Aceitou = errado, revisar o processo.</li> <li>- Recusou = correto.</li> </ul>

## 4.0

Repor reserva de risco

### Personas

Colaborador Coover

Testes de aceitação: **CR-02**

- a) O valor depositado não foi correspondente à percentagem do seguro do dispositivo.
  - Aceitou = errado, revisar o processo.
  - Recusou = correto
- b) O valor não foi depositado.
  - Aceitou = errado, revisar o processo
  - Recusou = correto
- c) O valor foi depositado referente a percentagem do seguro do dispositivo.
  - Aceitou = correto
  - Recusou = errado, revisar o processo.
  -

Testes de aceitação: **CR-03**

- a) O Colaborador Coover checa o dashboard.
  - Aceitou = correto
  - Recusou = errado, revisar o processo.
- b) Há reserva de risco suficiente para as indenizações.
  - Aceitou = correto
  - Recusou = errado, revisar o processo.
- c) Não há reserva de risco suficiente para as indenizações.
  - Aceitou = errado, revisar o processo
  - Recusou = correto

## 5. Solução Proposta

### 5.1. Solução

Para atender às regras de negócio do parceiro de projeto, a Coover, a solução será criar um Smart Contract de seguro mútuo de smartphones. Para a adesão neste Smart Contract, o usuário deve depositar um valor que corresponde a uma porcentagem do valor total do smartphone a ser protegido, acrescido uma taxa administrativa neste depósito.

Em caso de sinistro, o processo de indenização será iniciado, e o valor correspondente do aparelho protegido será pago ao usuário solicitante, após avaliação da seguradora, dona do contrato, utilizando o valor total depositado pelo usuário solicitante, e uma parte do valor depositado por cada usuário que compartilha este contrato.

Para manter o montante de recursos da reserva de risco e a cobertura total do seu aparelho, cada usuário deverá repor o valor que foi debitado de suas reservas do contrato.

A partir da solução desenvolvida, a seguradora Coover poderá oferecer um serviço de seguro de uma forma mais eficiente, sem a dependência de tantos intermediários, com mais transparência, por registrar as ações realizadas no Smart Contract, e segurança, por todo o aspecto que o blockchain e a Web 3.0 fornece.

### 5.2. Arquitetura Proposta

A arquitetura a seguir apresenta uma visão de alto nível do sistema, com seus componentes, interações e estratégias para atender aos requisitos do sistema. Ela descreve as entidades e seus comportamentos.

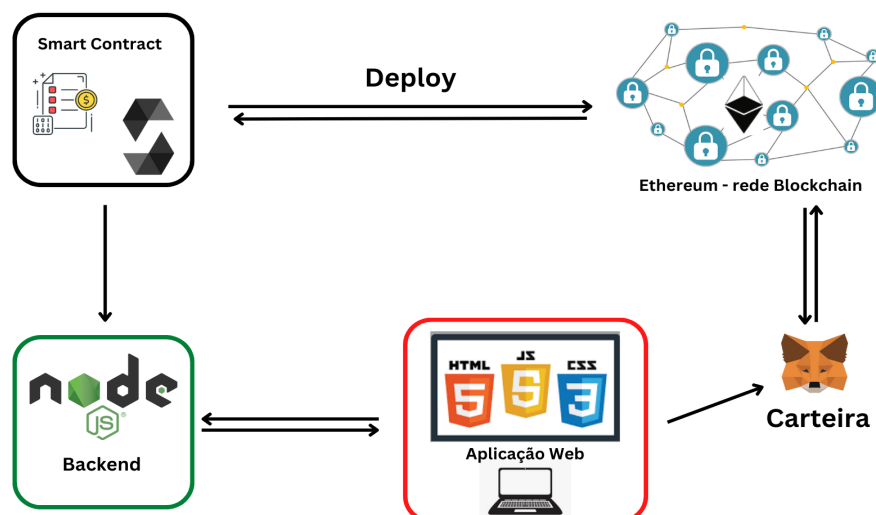


Figura 6 - Arquitetura da Solução proposta pelo projeto, com as ferramentas utilizadas pela solução.

### 5.3. Diagrama Macro da Solução

A partir de uma representação visual de alto nível de um sistema, o Diagrama Macro da Solução fornece uma visão geral dos principais componentes e fluxos de dados da solução, facilitando o entendimento da arquitetura e funcionalidade geral do sistema.

Um diagrama de blocos ilustra a estrutura e o fluxo de um sistema com seus processos, onde cada bloco representa um componente. Assim é possível representar objetivamente as interações entre os blocos e suas interdependências para o funcionamento do sistema.

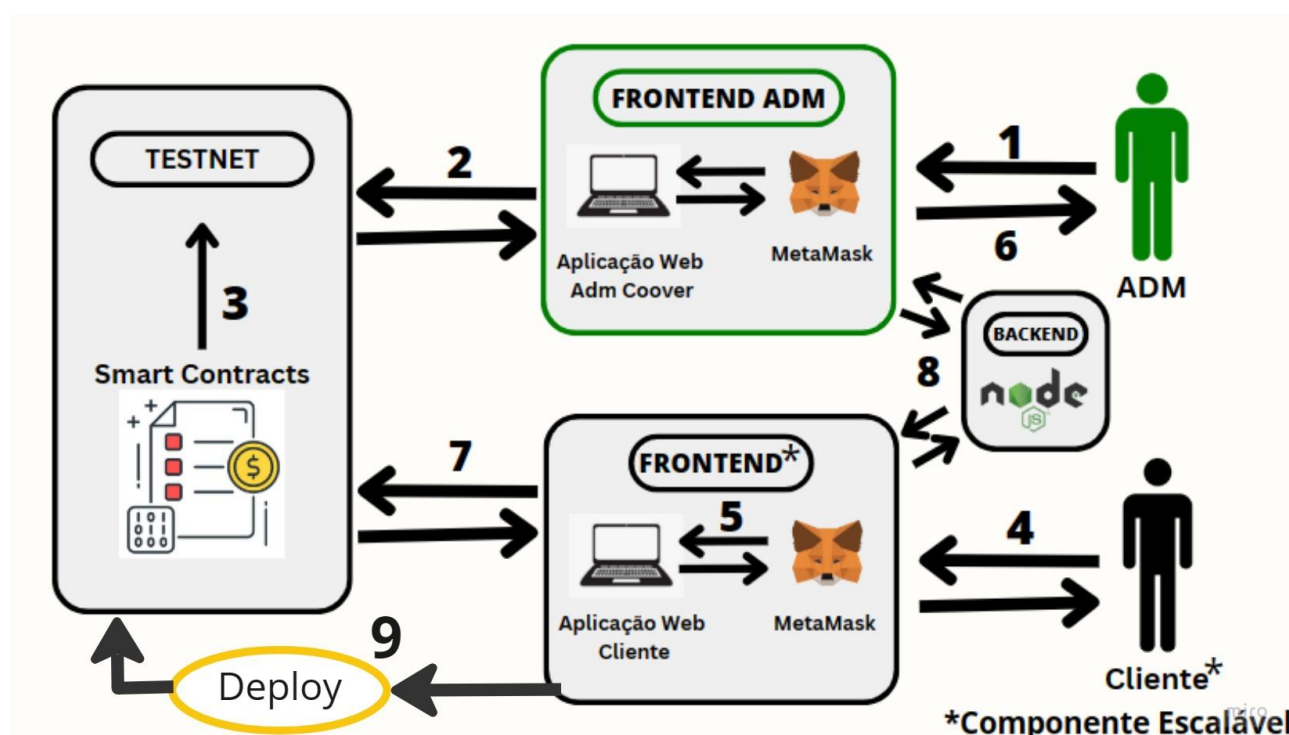


Figura 7 - Diagrama de blocos da solução deste projeto, com a interação entre os atores do sistema, como Cliente, Administrador, Interface Web, etc.

Com base no diagrama de blocos (Figura 7), é possível ver a interdependência entre os componentes, onde primeiramente o administrador acessa a interface web (1) para acessar o TestNet (2), e fazer o deploy de um Smart Contract (3).

Isso possibilita o Cliente acessar o FrontEnd (4), autenticando sua identidade através do MetaMask com a interface web (5), conseguindo realizar solicitações através dessa interface, que serão avaliadas pelo administrador com o FrontEnd de administrador (6), permitindo por exemplo a adesão de um cliente que vai ser registrado no blockchain do Smart Contract (7), e armazenando informações sensíveis em um BackEnd da Coover (8). Todas as funcionalidades do Smart Contract dependem de um deploy (9), onde o contrato estará disponível. O Administrador Coover é o responsável por realizar esta ação.

Reforçando que os componentes dos clientes e o FrontEnd dos clientes são escaláveis, possibilitando a entrada de vários clientes no sistema desenvolvido.

## 5.4. Descrição da Solução

A solução desenvolvida em blockchain oferece uma alternativa segura e transparente para contratos de seguro mútuo. O sistema é dividido em duas partes, sendo uma para o usuário cliente, e outra para o usuário administrador.

Para melhor representar o sistema, foi desenvolvido um fluxo de controle, que permite visualizar o caminho que o usuário do sistema vai seguir para realizar tarefas dentro do sistema, que pode ser visto a seguir:

Para o usuário cliente, o fluxo de controle começa com o acesso à página de cadastro, onde serão fornecidas informações para solicitar a adesão a um dos contratos de seguro mútuo disponíveis no sistema. Após a aprovação de um administrador, o cliente realiza um depósito inicial que representa a porcentagem do ativo que será segurado, mais o valor da taxa administrativa. Uma vez confirmado o depósito, o cliente é adicionado ao grupo do contrato correspondente. O acesso à página de autenticação da carteira digital por meio da extensão de navegador MetaMask é necessário para realizar transações no sistema. O cliente pode solicitar uma indenização, fornecendo as informações do Boletim de Ocorrência, ou repor a reserva de seguro, se estiver menor que o valor da porcentagem do ativo segurado.

Para o usuário administrador, o fluxo de controle começa com o acesso à página de autenticação da carteira digital por meio da extensão de navegador MetaMask, que possibilita o acesso às demais funcionalidades do sistema. O administrador tem a opção de criar um grupo novo de um SmartContract. Além disso, é responsável por avaliar e aceitar as solicitações de adesão dos clientes e avaliar e aceitar as solicitações de indenização. Também pode verificar os grupos que foram criados e a situação dos recursos disponíveis nestes grupos.

## 5.5. Diagrama de Implantação UML

Utilizado para representar como os componentes de um sistema de software são implementados em redes físicas, o diagrama de implantação UML mostra a relação entre os diferentes nós do sistema, como computadores, servidores e o próprio Smart Contract. Ele pode ajudar a identificar problemas de segurança e desempenho, além de ser usado como uma ferramenta de comunicação em relação à arquitetura e as outras partes interessadas do projeto.

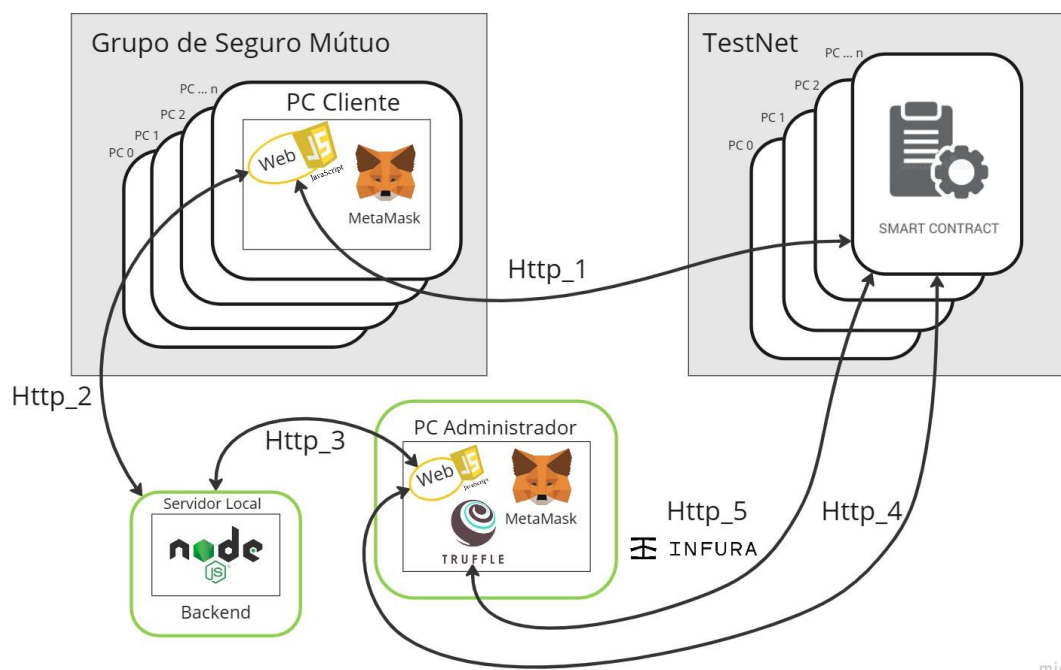


Figura 8 - Diagrama de Implantação UML desenvolvido para o projeto, que apresenta a arquitetura física do sistema, e as relações entre os componentes físicos e os componentes de software.

A representação da infraestrutura do projeto pode ser observada no Diagrama de Implantação UML (Figura 14), que apresenta os quatro blocos responsáveis por diferentes aspectos da solução.

O primeiro bloco representa o PC (Personal Computer) do Cliente, em um grupo de seguro mútuo, com vários clientes, cada um com seu computador pessoal, sendo indicados pela sequência PC 0, PC 1, PC 2, ..., PC N. Este bloco utiliza softwares como o Web JS (web services em Javascript) e MetaMask.

Os Web Services permitem que aplicativos e serviços possam interagir entre si e usaremos Web Services em Javascript pois a linguagem é altamente flexível, podendo ser executada tanto no cliente (navegador) quanto no servidor (Node.js), tem uma comunicação assíncrona e possui diversas Bibliotecas e Frameworks, o que facilita na criação e no consumo de Web Services.

Já a MetaMask é uma carteira de criptomoedas que por meio de uma extensão do navegador ou aplicativo móvel, permite a interação com aplicativos descentralizados (dApps) e com a rede Ethereum de forma segura. É preciso enfatizar que para a utilização do Web JS pelo cliente, a carteira do mesmo deve ter sido autenticada pela MetaMask.

O segundo bloco representa o PC (Personal Computer) Administrador, que além dos softwares utilizados pelo PC do cliente, onde é necessário destacar que assim como no PC do cliente, a carteira também deve ter sido autenticada pelo MetaMask, também possui o Truffle, que é uma

ferramenta de desenvolvimento que permite a compilação, implantação e o teste de Smart Contracts, presentes no bloco TestNet.

No terceiro bloco está presente o servidor Backend, para armazenar informações sensíveis dos clientes, utilizando o Node.js, uma plataforma de software de código aberto que permite a execução de código JavaScript fora de um navegador.

O TestNet está no quarto e último bloco, que é uma rede de testes com os Smart Contracts que foram publicados na blockchain, sendo estes representados por uma sequência de blocos no diagrama.

Quanto às conexões entre os blocos, o Web JS do PC do cliente se conecta ao Smart Contract e ao Node.js do Backend por meio de um protocolo HTTP (Http\_1 e Http\_2, respectivamente). O PC do Administrador se conecta ao Backend com o Node.js e ao Smart Contract também utilizando um protocolo HTTP (Http\_3 e Http\_4, respectivamente). Utilizando o Truffle e o Infura na conexão HTTP (Http\_5), o administrador passa a ter acesso às redes Ethereum hospedadas no TestNet através de uma conexão direta e remota, para a compilação de contratos, testes automatizados e executar transações de forma segura sem a necessidade de manter um nó local em funcionamento.

Cabe salientar que as conexões representadas no Diagrama de Implantação UML validam os caminhos lógicos da comunicação entre os blocos, apresentados nos Diagramas Sequenciais, bem como uma visão geral do comportamento do sistema nos exemplos que foram modelados nos Diagramas Sequenciais. No caso do Diagrama de Implantação UML, a ênfase foi nos componentes físicos e a relação entre os softwares utilizados, sendo que nos Diagramas Sequenciais os exemplos trazidos mostram, em cadeia, as condições para a execução de funcionalidades específicas implementadas no Smart Contract.

## 5.6. Diagrama de Sequência de Integração FrontEnd com Smart Contract

A descrição da solução é útil para comunicar como os módulos se encaixam logicamente, e como o MVP do projeto funciona em relação aos processos de negócios. Para representar a sequência de ações de uma forma visual e lógica, os diagramas sequenciais são uma ferramenta interessante para representar os fluxos entre a interação do usuário, as requisições feitas e as respostas do sistema.

Esses diagramas mostram a ordem das interações e as condições de entrada e saída, permitindo a visualização das etapas necessárias para a conclusão de uma tarefa ou processo, sendo úteis para criar uma documentação mais clara para os desenvolvedores do projeto. Também são usados para identificar problemas potenciais, como por exemplo, falhas de comunicação e gargalos de processo.

O diagrama de sequência a seguir (Figura 9) descreve o processo de integração do botão de conexão e depósito inicial, que utilizam o sistema web2.0, em uma plataforma que utiliza a tecnologia blockchain, ou seja, web3.0.



## Integração do Botão de Conexão e Depósito Inicial

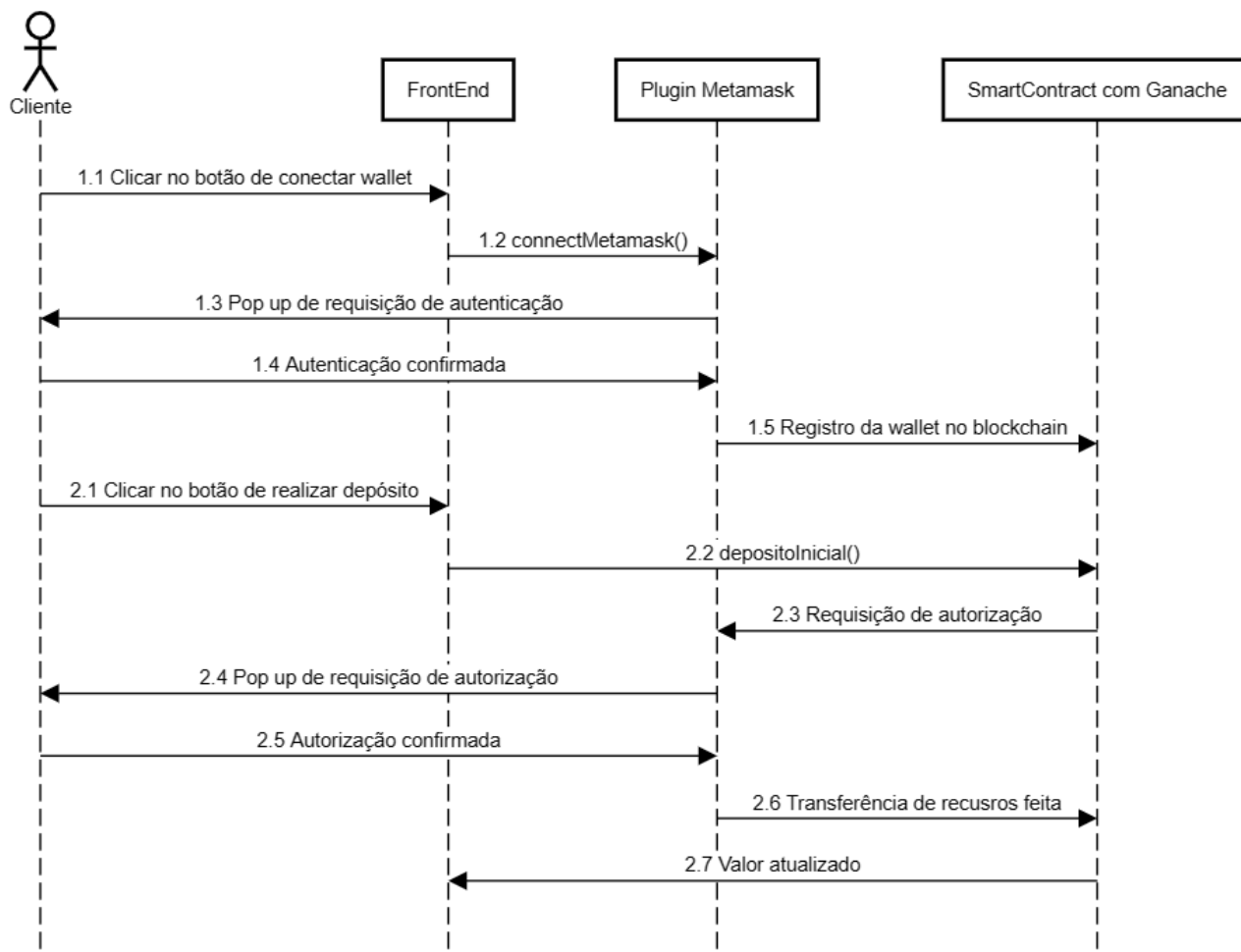


Figura 9 - Diagrama sequencial que mostra a integração entre o frontend do sistema com o smartcontract em blockchain, em um evento de conexão com a carteira (wallet) utilizando MetaMask e realizando o depósito inicial de recursos.

O processo se inicia quando o usuário cliente clica no botão de conectar wallet no frontend da plataforma (1.1). Com isso, o plugin MetaMask é acionado através da função javascript `connectMetamask()` (1.2), abrindo um pop-up na tela do usuário (1.3), onde o cliente confirma e autentica a sua carteira (1.4) que é registrada no blockchain do smart contract (1.5).

Com o encerramento do primeiro evento, o segundo se inicia com o cliente clicando no botão de realizar o depósito inicial (2.1) no frontend da plataforma, que envia uma solicitação para o smart contract com a função `depositInicial()` (2.2). O smart contract solicita autorização ao plugin do MetaMask do usuário (2.3), com outro pop-up na tela (2.4). Após a confirmação da transação (2.5) o smart contract recebe os recursos da carteira do usuário pelo próprio plugin do MetaMask (2.6), retornando para o frontend o valor atualizado dos recursos disponíveis para o usuário em seu contrato (2.7).

## 6. Desenvolvimento e Resultados

### 6.1. Usuário Cliente

#### 6.1.1. Descrição

Esta seção se trata do sistema voltado ao usuário cliente dentro de um sistema blockchain para um Smart Contract de seguro mútuo. Dentre as funções do usuário, será possível o pedido de adesão ao grupo mútuo por meio do preenchimento das informações solicitadas na interface, a requisição de indenizações, a visualização do contrato do grupo em que está inserido e as aprovações feitas pelo administrador, além da opção de sair do grupo ou entrar em outros. Portanto, o usuário tem a responsabilidade de fazer sua conexão com a Metamask e preencher todos os dados necessários.

#### 6.1.2. Tecnologia adotada

A fim de facilitar o processo de desenvolvimento do projeto, utilizamos uma combinação de tecnologias para garantir a integridade e eficácia dos contratos inteligentes.

Por meio de tecnologias como IDEs, bibliotecas externas, ferramentas de análise de segurança, frameworks como Truffle e tecnologias como o Ganache, foi possível a criação de um ambiente de desenvolvimento completo e eficiente para a criação de smart contracts em Solidity.

A seguir serão apresentadas as tecnologias adotadas usadas tanto para o cliente quanto para o administrador, onde cada uma possui seus objetivos e suas aplicações específicas:

##### 6.1.2.1. Carteira MetaMask

Para testar funcionalidades do Smart Contract desenvolvido no projeto, em um ambiente controlado, foi criada uma carteira no MetaMask (Figura 15) a fim de simular o comportamento de um usuário que utiliza o sistema de seguro mútuo. O MetaMask é necessário para autenticar usuários, permitindo a interação com aplicativos descentralizados (dApps).

Para a criação da carteira no MetaMask, foi gerada uma chave privada para acessar os recursos da carteira, tendo assim que deve ser mantida em segurança.

##### 6.1.2.2. Truffle-cli

O Truffle é um framework de desenvolvimento para blockchain, que possibilita a compilação de Smart Contracts, testes automatizados, entre outros. Além de suas funções básicas, o Truffle permite a criação, gerenciamento e deploy de Smart Contracts, que foi a principal utilização deste framework neste projeto.

A partir do comando “npm install -g truffle” no terminal do computador, é possível verificar a versão instalada (Figura 16) e garantir que foi utilizada a versão mais recente, até o momento de desenvolvimento do projeto.

### 6.1.2.3. Infura

O Infura é uma plataforma que reúne APIs (Application Programming Interface) de Blockchain, a fim de auxiliar desenvolvedores no desenvolvimento de ativos na rede.

Ao criar uma conta, o desenvolvedor pode nomear o projeto que está desenvolvendo e ter a chave da API.

API key é de fundamental importância para o deploy do Smart Contract, visto que, é a partir desse fator que é possível identificar o dono do contrato e autorizar a publicação (Figura 17).

### 6.1.2.4. Ganache-cli

O Ganache-cli é um emulador de uma rede blockchain local, executada dentro do próprio computador. Com isso é possível realizar o deploy de forma rápida (Figura 18), através da integração com o Truffle, e testar seu funcionamento antes de realizar o deploy em uma rede pública, por exemplo.

## 6.1.3. User Stories

Coloque aqui a lista das user stories relacionadas ao módulo.

Informe apenas o Número das user stories (não duplique as user stories).

Segue abaixo as user stories referentes ao Usuário Cliente (estudante de TI):

User story 1.0: Solicitar adesão;

User story 2.0: Ingressar num grupo de seguro mútuo;

User story 3.0: Pedir Indenização.

## 6.1.4. Prototipação

A seguir, as telas do frontend da plataforma do sistema de usuários clientes.

As imagens das telas do frontend estão no Anexo IV deste arquivo.

Figura 22: Login do Cliente;

Figura 22: Visualização do contrato do grupo em que está inserido;

Figura 22: Pedido de indenização.

## 6.1.5. Diagramas

### 6.1.5.1 Diagrama Sequencial - Pedido de Adesão

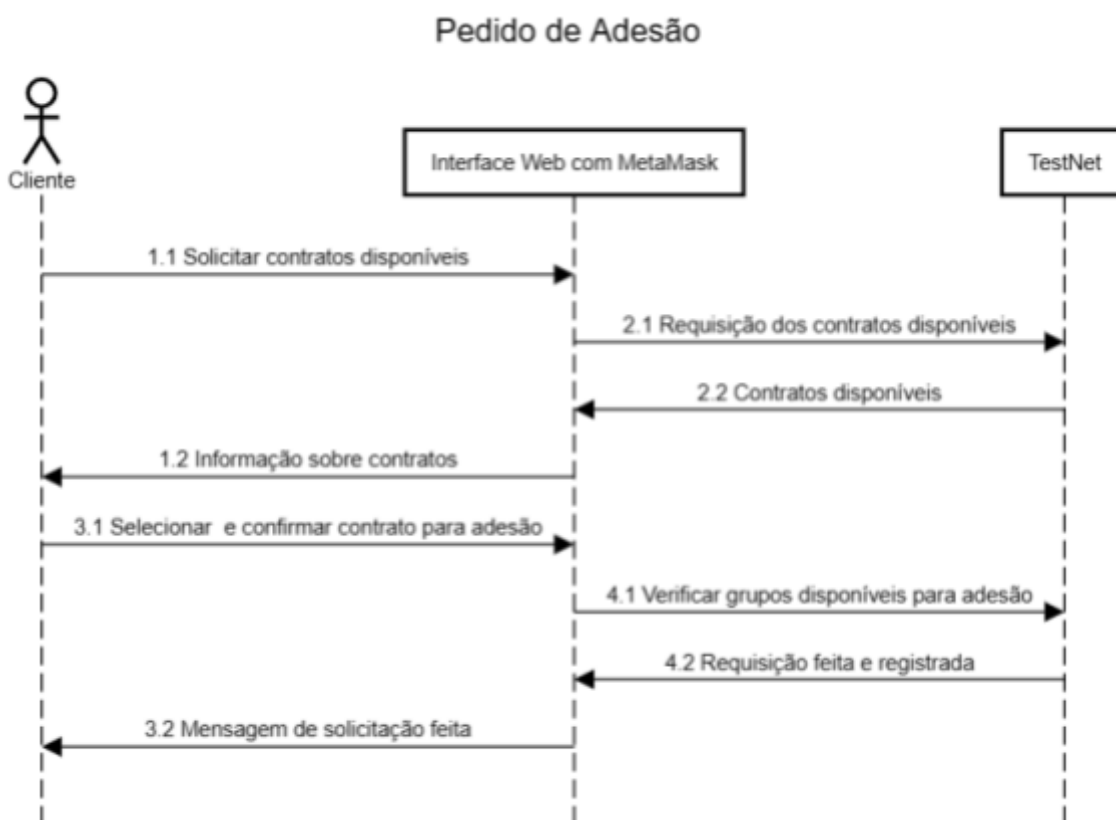


Figura 10 - Diagrama sequencial do processo de pedido de adesão, mostrando as interações entre o Cliente e a Interface Web com MetaMask e o Smart Contract (TestNet). Atenção: O diagrama considera a autenticação da identificação do usuário na Interface Web com MetaMask como bem sucedida.

Com o fluxo para o pedido de adesão de um cliente (Figura 10), o sistema permite que o cliente solicite a adesão de um contrato através de uma Interface Web contactada à MetaMask. O cliente solicita os contratos disponíveis para o sistema utilizando uma Interface Web (1.1), que requisita ao Smart Contract no servidor de teste TestNet (2.1), retornando os contratos disponíveis para a Interface (2.2), mostrando na tela para o Cliente visualizar (1.2).

Com isso o usuário pode selecionar um contrato dentre os disponíveis, confirmar a seleção (3.1), e o sistema verifica os grupos disponíveis para este contrato no Smart Contract (4.1), retornando para a Interface o registro e a confirmação da requisição (4.2), mostrando uma mensagem para o usuário do sucesso da requisição feita (3.2).

Todo esse processo é realizado de forma sequencial, onde o sistema deve garantir que as interações do Cliente com a Interface Web sejam registradas corretamente.

## 6.1.5.2. Diagrama Sequencial - Pedido de Indenização

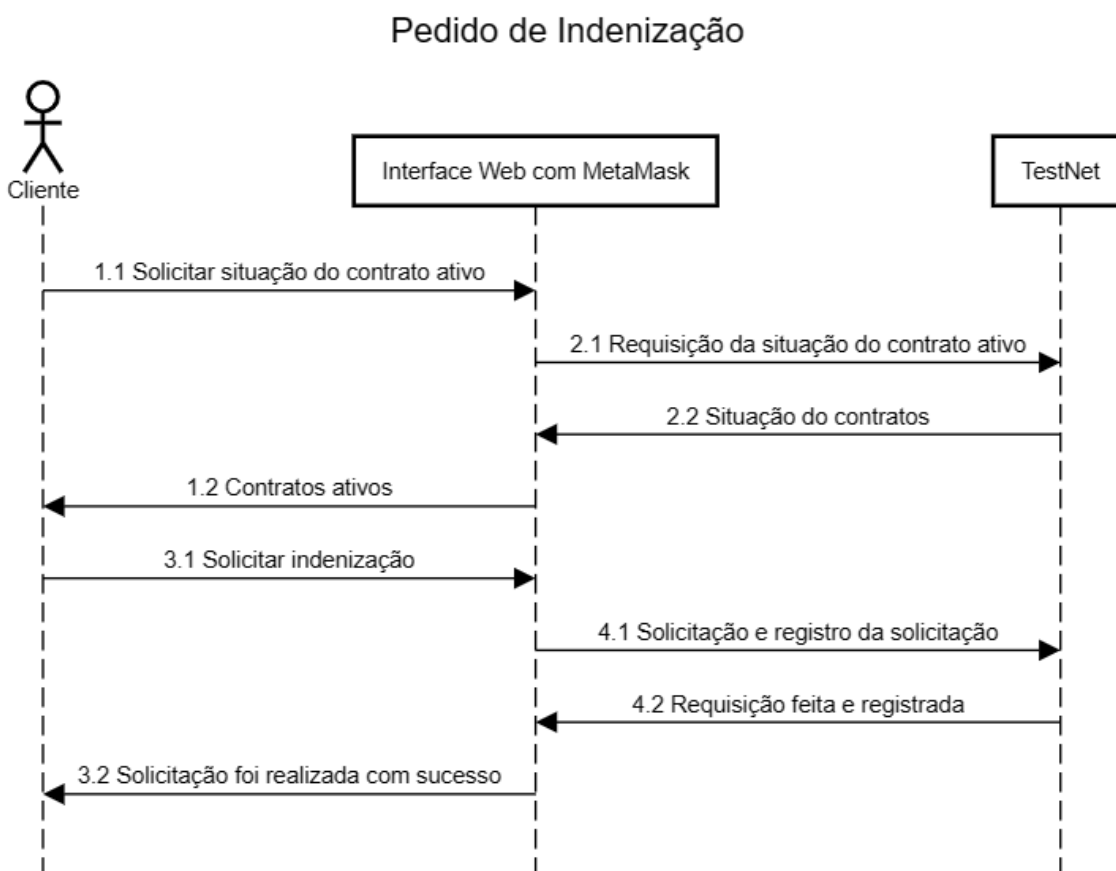


Figura 11 - Diagrama sequencial do processo de pedido de indenização, mostrando as interações entre o Cliente e a Interface Web com MetaMask e o Smart Contract (TestNet). Atenção: O diagrama considera a autenticação da identificação do usuário na Interface Web com MetaMask como bem sucedida.

A partir de um contrato ativo, o diagrama (Figura 11) ilustra o processo de um pedido de indenização de um cliente.

Neste processo, o Cliente inicia solicitando a situação de seus contratos ativos por meio da Interface Web com MetaMask (1.1), onde a requisição é feita para o Smart Contract (2.1), onde a informação é retornada para a Interface (2.2) permitindo a análise da situação dos contratos em que o usuário faz parte (1.2).

Quando o cliente decide fazer a solicitação de uma indenização (3.1), a Interface Web envia a requisição e registra esse pedido no Smart Contract (4.1), que sendo bem sucedida, retorna para a Interface que a solicitação foi feita (4.2), mostrando para o usuário que a solicitação foi realizada (3.2).

Para ressaltar a importância das etapas, foi desenvolvido um diagrama de sequência alternativo para um caso que será descrito a seguir:

## Pedido de Indenização com Negação por Falta de Recursos

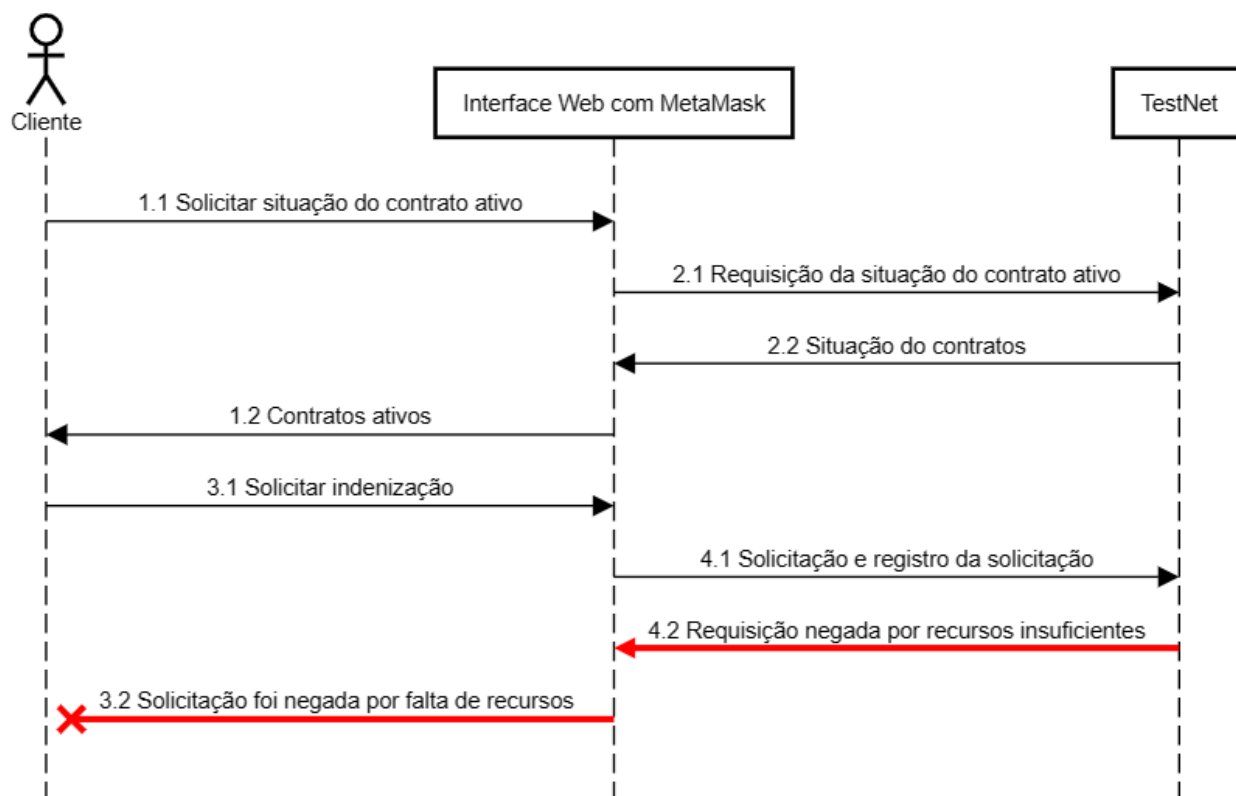


Figura 12 - Diagrama sequencial do processo de pedido de indenização, mostrando as interações entre o Cliente e a Interface Web com MetaMask e o Smart Contract (TestNet). Atenção: O diagrama considera a autenticação da identificação do usuário na Interface Web com MetaMask como bem sucedida.

A partir de um contrato ativo, o diagrama (Figura 12) ilustra a negação de um processo de um pedido de indenização de um cliente, por falta de recursos disponíveis.

O Cliente inicia solicitando a situação de seus contratos ativos por meio da Interface Web com MetaMask (1.1), com a requisição é indo até o Smart Contract (2.1), onde a informação é retornada para a Interface (2.2) para que a análise da situação dos contratos possa ser feita pelo usuário (1.2).

Quando o cliente decide fazer a solicitação de uma indenização (3.1), a Interface Web envia a requisição e registra esse pedido no Smart Contract (4.1), que ao identificar a falta dos recursos necessários, nega a requisição e retorna para a Interface que a solicitação não foi feita (4.2), mostrando para o usuário que a solicitação foi negada com o motivo de falta de recursos disponíveis (3.2).

### 6.1.5.3. Diagrama Sequencial - Reposição de Reserva de Risco

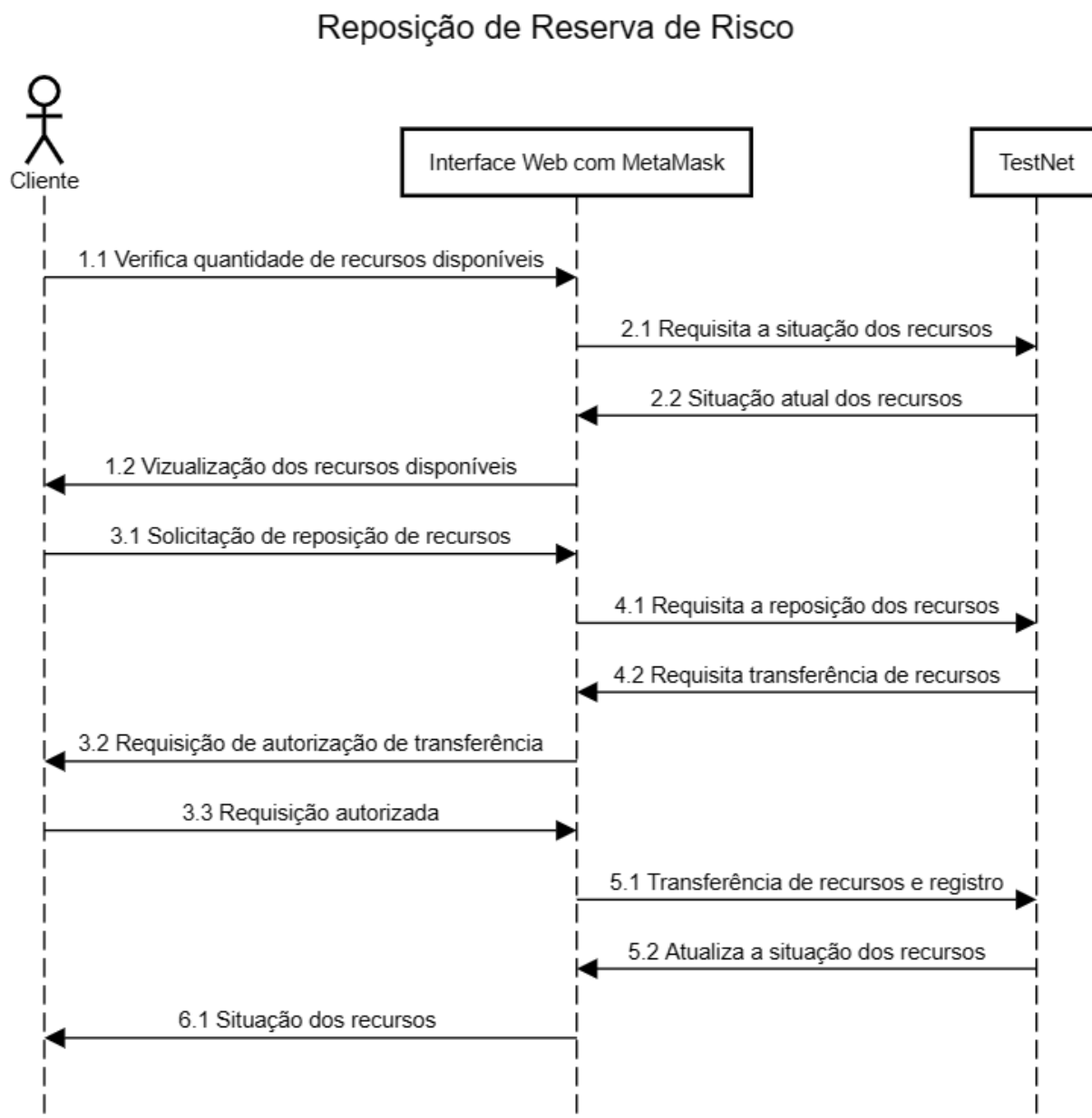


Figura 13 - Diagrama sequencial que descreve o processo de reposição de recursos da reserva de risco de um cliente, mostrando as interações entre o Cliente e a Interface Web com MetaMask e o Smart Contract (TestNet). Atenção: O diagrama considera a autenticação da identificação do usuário na Interface Web com MetaMask como bem sucedida.

Este diagrama sequencial (Figura 12) descreve o comportamento esperado do sistema em uma operação de reposição de reserva de risco por parte do cliente. O processo se inicia com a verificação do Cliente pela quantidade de recursos disponíveis a partir da Interface Web (1.1). A seguir a Interface requisita do Smart Contract a situação atual dos recursos (2.1), que retorna para a Interface a informação solicitada (2.2), que permite sua visualização por parte do cliente (1.2).

Considerando que os recursos não estejam no seu valor total, o Cliente faz uma solicitação de reposição de recursos utilizando a Interface Web (3.1), que envia a solicitação para o Smart Contract (4.1), que calcula a diferença no valor depositado com o valor total, retornando uma requisição de transferência para a Interface Web que está ligada ao MetaMask do Cliente (4.2). O MetaMask através da Interface Web solicita uma autorização de transferência de recursos (3.2), e assim que for aprovada pelo Cliente (3.3), Transfere os recursos para o Smart Contract e registra essa transferência (5.1).

Com isso, o Smart Contract retorna para a Interface Web a atualização da situação dos recursos do usuário (5.2), que pode ver na tela os recursos atuais disponíveis (6.1).

O processo de reposição de recursos da reserva de risco é fundamental para garantir a cobertura total do serviço contratado, ajudando a manter a solvência da empresa, permitindo recursos disponíveis para cobrir riscos e indenizações do grupo de seguro mútuo. O diagrama ainda destaca a importância de registrar a transferência bem sucedida, assim que for efetuada, trazendo mais segurança e transparência no processo.

## 6.2. Usuário Administrador

### 6.2.1. Descrição

Esta seção trata da parte do sistema voltado ao usuário administrador de um sistema de blockchain para um smartcontract de seguro mútuo. Dentre as funções deste usuário, estão criação e gerenciamento de grupos de clientes, avaliação e aprovação de solicitações feitas para o cliente, entre outros.

### 6.2.2. Tecnologia adotada

A fim de facilitar o processo de desenvolvimento do projeto, utilizamos uma combinação de tecnologias para garantir a integridade e eficácia dos contratos inteligentes.

Por meio de tecnologias como IDEs, bibliotecas externas, ferramentas de análise de segurança, frameworks como Truffle e tecnologias como o Ganache, foi possível a criação de um ambiente de desenvolvimento completo e eficiente para a criação de smart contracts em Solidity.

### 6.2.3. User Stories

Segue abaixo as user stories referentes ao Usuário Administrador (Coover):

User story 2.0: Ingressar num grupo de seguro mútuo;

User story 3.0: Pedir Indenização;

User story 4.0: Repor reserva de risco.

### 6.2.4. Prototipação

A seguir, as telas do frontend da plataforma do sistema do usuário administrador.



As imagens das telas do frontend estão no Anexo IV deste arquivo.

Figura 20: Login do Administrador;

Figura 20: Criação de um novo grupo;

Figura 20: Adicionar usuários no Smart Contract;

Figura 21: Definição da taxa administrativa do contrato.

Figura 21: Visualização do contrato e dos usuários inseridos nele.

## 6.2.5. Diagramas

### 6.2.5.1 Diagrama Sequencial - Aceitar Pedido de Adesão

Após o Cliente realizar o pedido de adesão, o processo continua com a avaliação de um administrador do parceiro de projeto Coover, que pode aprovar ou rejeitar a solicitação. O diagrama a seguir apresenta as etapas do processo de avaliação e aprovação do administrador Coover.

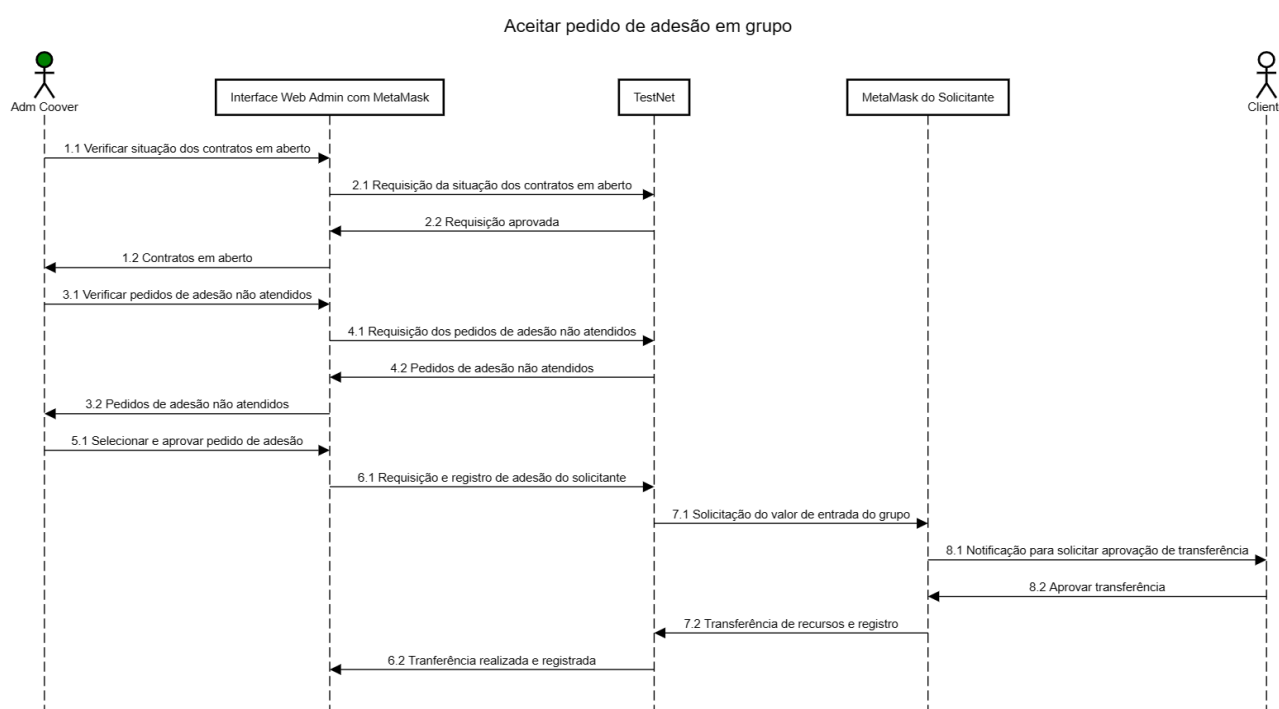


Figura 14 - Diagrama sequencial do processo de aceitação de um pedido de adesão feito por um cliente, mostrando as interações entre um administrador (Adm Coover) e a Interface Web Admin com MetaMask e o Smart Contract (TestNet). Atenção: O diagrama considera a autenticação da identificação do usuário na Interface Web Admin com MetaMask e MetaMask do Solicitante como bem sucedida..

O diagrama (Figura 14) ilustra o fluxo do administrador, que possui várias etapas do processo de análise de um pedido de adesão, até sua aprovação.

A primeira etapa é a requisição para visualização da situação dos contratos em aberto a partir do administrador (1.1), através da Interface Web de Administrador que requisita no Smart Contract a situação dos contratos em aberto (2.1). O retorno bem-sucedido da requisição permite que o Smart Contract forneça a informação na tela da Interface Web (2.2),

possibilitando a visualização pelo usuário deste sistema (1.2) permitindo a avaliação dos contratos em aberto.

A segunda etapa se assemelha à primeira, onde o usuário solicita os pedidos de adesão não atendidos através da Interface Web de administrador (3.1), que por sua vez requisita a informação do Smart Contract no TestNet (4.1), que retorna à Interface as informações requisitadas (4.2), possibilitando a análise das informações pelo usuário (3.2).

Com essas informações, o administrador pode selecionar e aprovar um pedido de adesão de um cliente, utilizando a Interface Web de administrador (5.1), que envia a aprovação do pedido ao Smart Contract (6.1), onde um código será executado para fazer uma solicitação de transferência de recursos ao Smart Contract, a partir da carteira do usuário solicitante através do MetaMask (7.1), que por sua vez irá notificar o Cliente para aprovação ou rejeição da transferência (8.1). Ao aprovar (8.2), os recursos saem do MetaMask para o Smart Contract com o valor de entrada do contrato, registrando na rede a adesão do Cliente solicitante e a transferência dos recursos (7.2), retornando à Interface Web de administrador que a transferência foi realizada e registrada no Smart Contract (6.2).

Cada uma das etapas é importante para garantir a segurança e eficiência do processo de adesão de clientes no Smart Contract. O administrador podendo aceitar ou rejeitar pedidos de adesão permite a atribuição de critérios próprios para essas decisões, antes de solicitar a transferência de recursos do usuário, caso este seja rejeitado. A transferência do valor, por sua vez, garante que o membro está comprometido financeiramente com os recursos do seguro mútuo do grupo, que apenas finaliza sua aprovação de entrada após o pagamento.

#### **6.1.5.2. Diagrama Sequencial - Pedido de Indenização**

A avaliação do pedido de indenização é realizada por um administrador que verifica os pedidos de indenização não atendidos. O processo de aceitação de um pedido de indenização está ilustrado no diagrama a seguir:

### Aceitar pedido de indenização

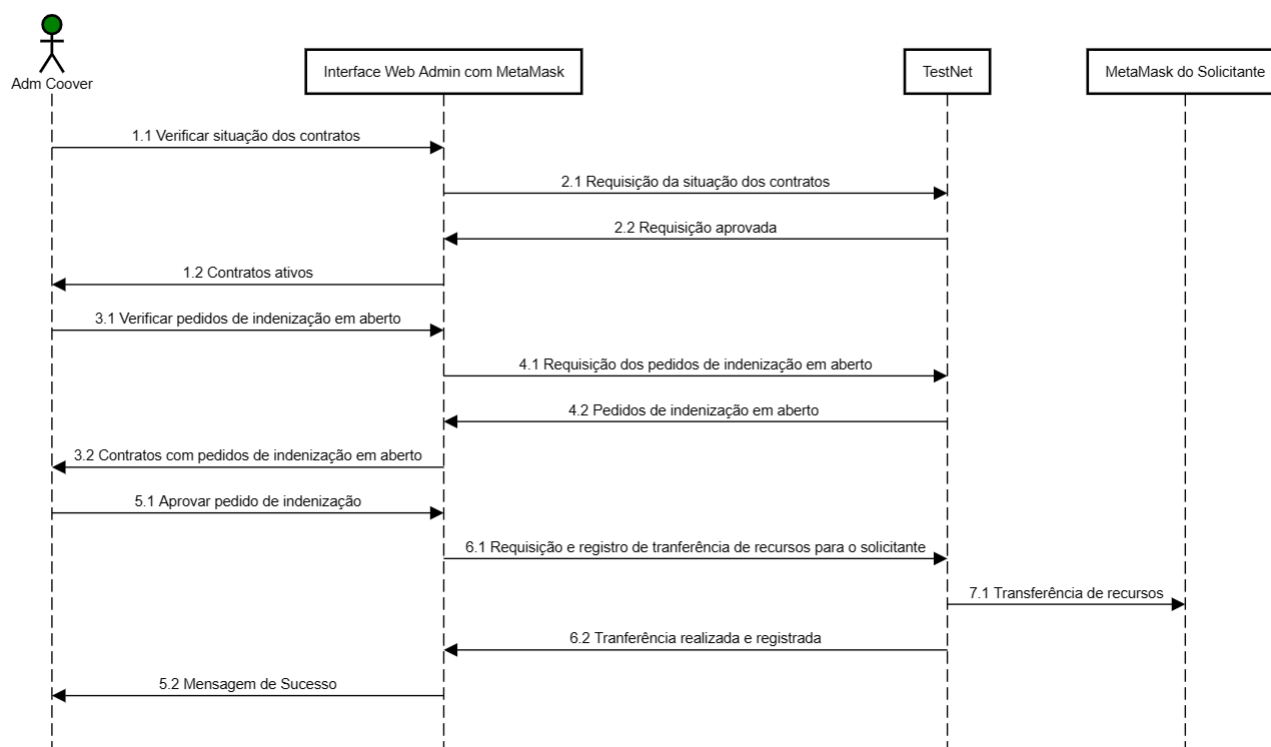


Figura 15 - Diagrama sequencial que descreve o processo de aceitação de pedido de indenização por um administrador (Adm Coover) por meio de uma Interface Web Admin com MetaMask e o Smart Contract (TestNet). Atenção: O diagrama considera a autenticação da identificação do usuário na Interface Web Admin com MetaMask e MetaMask do Solicitante como bem sucedida..

O comportamento esperado do sistema descrito no diagrama (Figura 15) é que, ao receber a solicitação de indenização feito por um cliente, o administrador (Adm Coover) deve verificar a situação dos contratos ativos (1.1), através da Interface Web de administrador, que requisita a informação ao Smart Contract (TestNet) (2.1), retornando a informação na tela (2.2) para o administrador visualizar os contratos ativos (1.2).

Em seguida, devem ser verificados os pedidos de indenização em aberto com solicitações pendentes, pelo usuário administrador utilizando a Interface Web de administrador (3.1), que também requisita a informação ao Smart Contract (4.1), retornando à Interface (4.2) as informações para o usuário (3.2).

Caso o pedido seja aprovado pelo usuário administrador através da Interface Web de administrador (5.1), a requisição de transferência de recursos para o solicitante é feita e registrada na blockchain (6.1), que transfere esses recursos diretamente para a carteira do MetaMask (7.1). Após a transferência, o Smart Contract registra que a transferência foi realizada e devolve a informação de sucesso para a Interface Web de administrador (6.2) que visualiza a mensagem de sucesso na tela (5.2).

Vale destacar que a ordem das etapas é muito importante, pois o registro da aprovação da transferência e o registro da transferência efetuada garantem a segurança do que foi realizado, podendo identificar problemas caso a transferência tenha sido aprovada e registrada, mas não tenha sido realizada, e registrando apenas após a transferência ter sido feita, e não antes. Além de maior segurança, também garante a transparência das transações, reduzindo custos e intermediários nos processos na forma tradicional.

## 6.3. Avaliação

USER STORY	CRITÉRIO DE ACEITAÇÃO	STATUS
Solicitar adesão	Ter um smart contract válido	Smart contract construído com sucesso
Solicitar adesão	Ter saldo maior ou igual à porcentagem do smart contract	Há função no smart contract para conferir se há saldo na wallet
Ingressar num grupo de seguro mútuo	O Colaborador Coover envia o link para o segurado	Função substituída, comunicação com o usuário será via interface web3
Ingressar num grupo de seguro mútuo	O segurado entra no grupo através do link	Função substituída
Pedir indenização	Pedido de indenização	Função existente no contrato e executada ao preencher BO, IMEI e motivo
Pedir indenização	O Smart Contract valida automaticamente os termos estabelecidos	Smart contract se autoexecuta com sucesso
Pedir indenização	Colaborador Coover entra em contato para realizar o processo de indenização	O processo ocorre diretamente via interface web3
Repor reserva de risco	A reserva estar menor que o valor total do seguro mútuo	A função existe no smart contract mas não foi integrada com a interface web3

	Repor reserva de risco	Solicitar que os integrantes já indenizados, depositem novamente no contrato a porcentagem correspondente ao seguro do seu dispositivo	“
Repor reserva de risco	Usar o dashboard para garantir que a reserva de risco foi repostada	Função substituída pela tela “indenizações”	

## 7. Conclusões e Recomendações

Durante o desenvolvimento do projeto, foi notada a oportunidade de novas soluções que o uso de tecnologias web3.0 podem trazer aos negócios, no caso, o uso de Smart Contracts para uma empresa de seguros, em grupos de seguros mútuos.

Este tipo de tecnologia traz uma camada de segurança mais profunda, com a redução de intermediários, e o aumento da eficiência pela automatização de funções e tarefas.

Porém por ser uma tecnologia nova, que utiliza outros tipos de softwares para sua implementação e integração com sistemas web2.0, como páginas web http, o desafio de manter todas as funcionalidades do Smart Contract presentes em um frontend que utiliza html e javascript se mostrou um grande desafio para a equipe de desenvolvedores, que decidiram reduzir a quantidade de páginas, para manter o mais importante neste projeto, que são as regras de negócio do parceiro deste projeto.

Com isso, vale dizer que durante o desenvolvimento deste projeto, toda a equipe de desenvolvedores, estudantes do Inteli, se beneficiaram desta oportunidade para o aprendizado, enquanto estudantes, enquanto time, e profissionais de sistemas de informação.

Como recomendação, o time sugere uma ênfase maior de desenvolvedores que estão aprendendo a desenvolver em sistemas que utilizam blockchain que realizem provas de conceito de sistemas feitos em web3.0 na integração com páginas html, de forma mais simplificadas, antes de crescer o Smart Contract, por exemplo, ou as páginas front end com suas funcionalidades.

## 8. Referências

Castilho, S. D. e Fonte, M. F. (2012). Política de segurança da informação aplicada em uma instituição de ensino mediante análise de Risco. RETEC-Revista de Tecnologias.

Nakamura, A. M. (2011). Comércio eletrônico riscos nas compras pela internet. Faculdade de Tecnologia de São Paulo.

# Anexos

Utilize esta seção para anexar materiais como manuais de usuário, documentos complementares que ficaram grandes e não couberam no corpo do texto etc.

**Sugestão:**

*Documentos que são alterados por cada sprint, como a Matriz de Riscos, devem ser movidas para a seção de anexo.*

*No corpo do documento deve permanecer o documento atual.*

*Separar os documentos por sprints.*

**Sugestão de divisão da seção Anexo:**

## ANEXO I – Sprint 1

[Matriz de Risco](#)

[Matriz Oceano Azul](#)

Mova para essa seção os documentos produzidos na Sprint 1 que sofreram alterações na Sprint 2.

## ANEXO II – Sprint 2

Mova para essa seção os documentos produzidos na Sprint 2 que sofreram alterações na Sprint 3.



## ANEXO III – Sprint 3

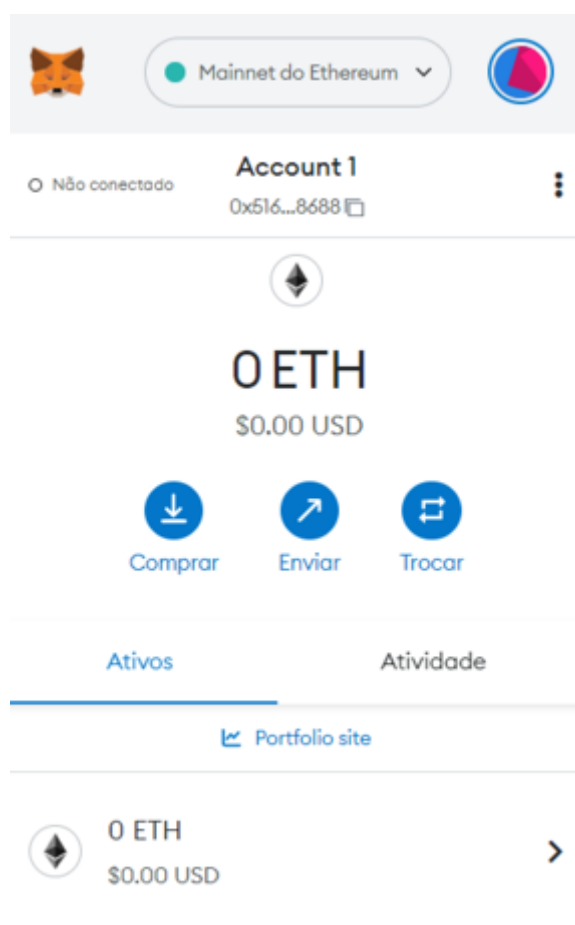


Figura 16 - Imagem da interface da carteira virtual MetaMask utilizada para realizar testes do Smart Contract desenvolvido no projeto.

```
C:\Users\Inteli\Documents\solidity_vs>npm truffle --version
9.5.0
```

Figura 17 - Captura de tela do prompt de comando do computador mostrando a versão instalada do Truffle.


API Keys				All Products		All Roles		CREATE NEW API KEY
Name	Created	Role	Requests Today					
 VanCoover	2023-03-07	Owner	0					<a href="#">VIEW STATS</a>

Figura 18 - API Key para o deploy do contrato. Observa-se a data de criação, o nome do time e a publicação identificação da publicação pelo dono do contrato.

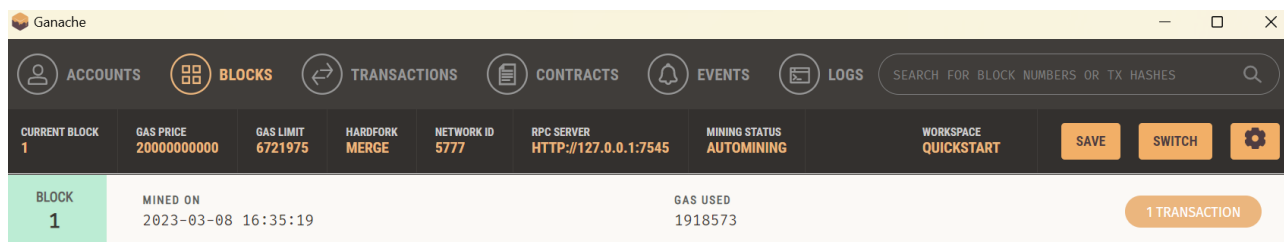


Figura 19 - Captura de tela do Ganache mostrando o deploy bem-sucedido do Smart Contract. Os endereços locais de contrato e transação são exibidos na imagem.

## ANEXO IV – Sprint 5

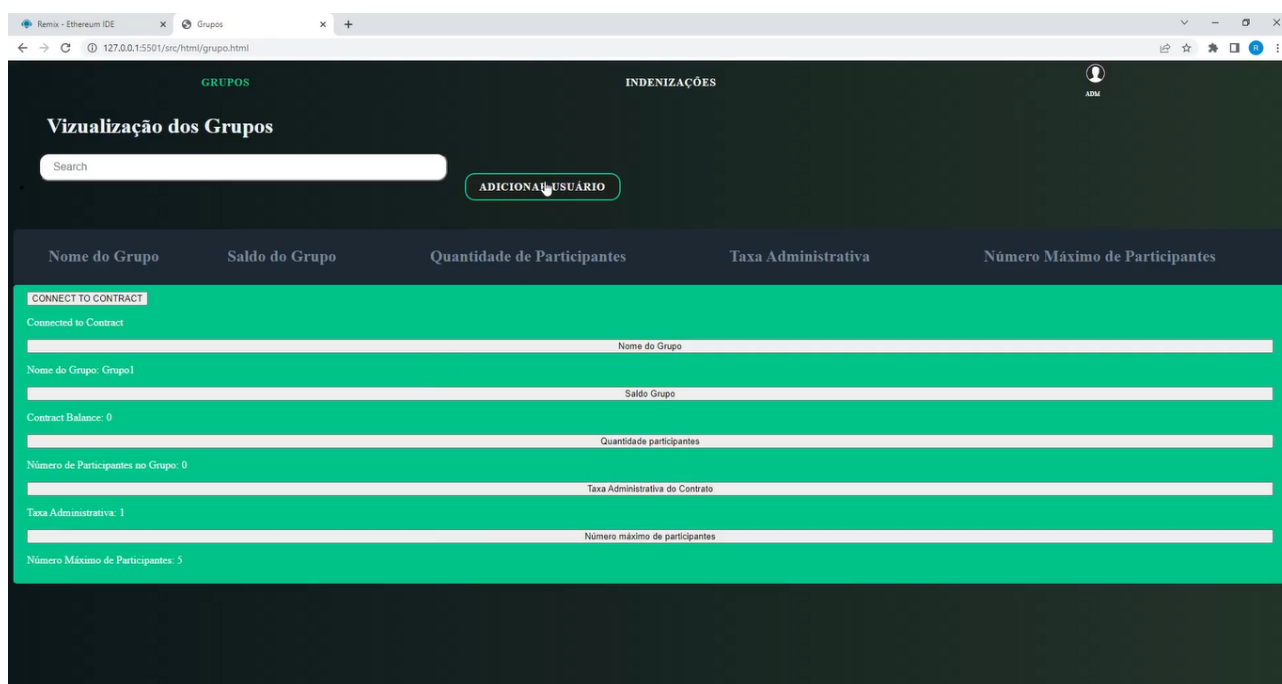


Figura 20 - Frontend do usuário administrador com as respectivas funções para gerenciamento do smart contract.

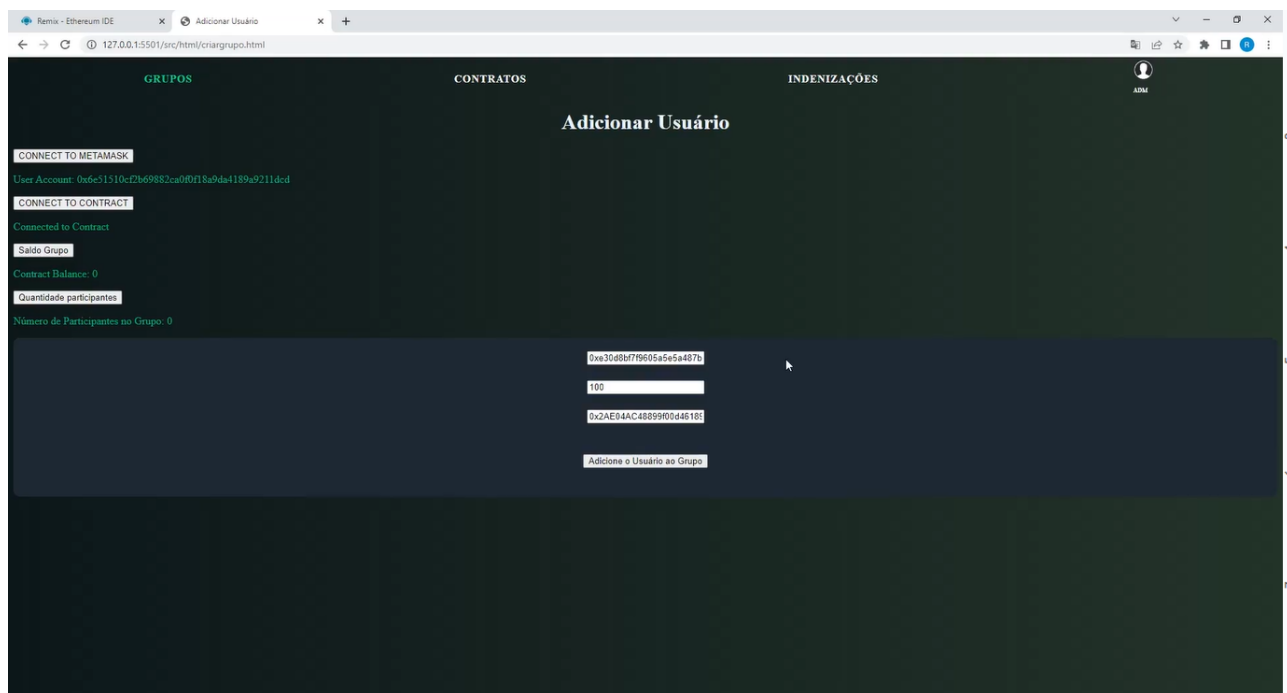


Figura 21 - Frontend do usuário administrador com as respectivas funções para adicionar usuários no smart contract.

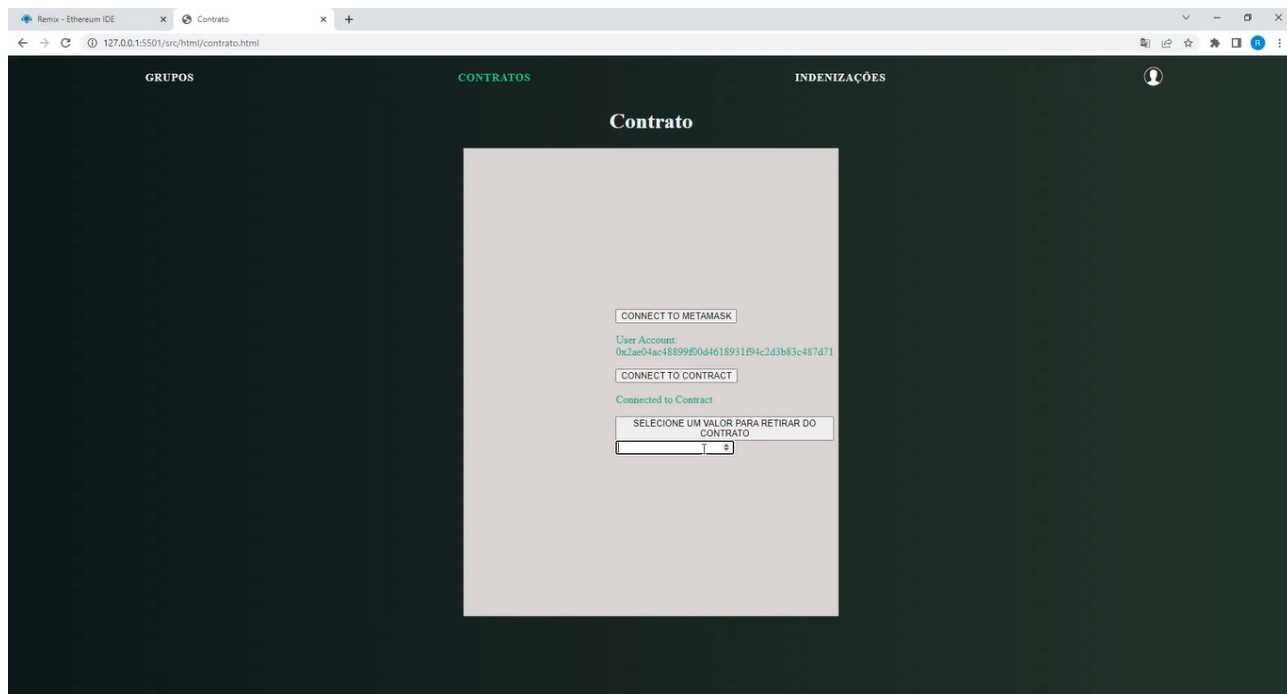


Figura 22 - Frontend do usuário cliente com as respectivas funções para conexão no metamask e solicitar indenização.