

CENTRO UNIVERSITÁRIO FEI

PAULO HENRIQUE DA ROCHA ALVIM
THIAGO LUIZ DE OLIVEIRA GREGORIO
TIAGO OLIVEIRA VIDAL DE PAULA

TOKENIZAÇÃO DE SEGUROS MASSIFICADOS EM *BLOCKCHAIN* PRIVADA

São Bernardo do Campo

2024

PAULO HENRIQUE DA ROCHA ALVIM
THIAGO LUIZ DE OLIVEIRA GREGORIO
TIAGO OLIVEIRA VIDAL DE PAULA

TOKENIZAÇÃO DE SEGUROS MASSIFICADOS EM *BLOCKCHAIN* PRIVADA

Trabalho de Conclusão de Curso apresentado ao Centro Universitário FEI, como parte dos requisitos necessários para obtenção do título de Bacharel em Engenharia Elétrica. Orientado pelo Prof. Dr. Ricardo de Carvalho Destro.

São Bernardo do Campo

2024

Oliveira Gregorio, Thiago Luiz de.

TOKENIZAÇÃO DE SEGUROS MASSIFICADOS EM
BLOCKCHAIN PRIVADA / Thiago Luiz de Oliveira Gregorio, Tiago
Oliveira Vidal de Paula, Paulo Henrique da Rocha Alvim. São Bernardo
do Campo, 2024.

61 f. : il.

Trabalho de Conclusão de Curso - Centro Universitário FEI.
Orientador: Prof. Dr. Ricardo de Carvalho Destro.

1. Seguros massificados. 2. Tokenização. 3. Blockchain privada. 4.
Smart Contracts. 5. Prova de conceito. I. Oliveira Vidal de Paula, Tiago.
II. Rocha Alvim, Paulo Henrique da. III. Carvalho Destro, Ricardo de,
orient. IV. Título.

Elaborada pelo sistema de geração automática de ficha catalográfica da FEI com os
dados fornecidos pelo(a) autor(a).

PAULO HENRIQUE DA ROCHA ALVIM
THIAGO LUIZ DE OLIVEIRA GREGORIO
TIAGO OLIVEIRA VIDAL DE PAULA

TOKENIZAÇÃO DE SEGUROS MASSIFICADOS EM *BLOCKCHAIN* PRIVADA

Trabalho de Conclusão de Curso, apresentado
ao Centro Universitário FEI, como parte dos
requisitos necessários para obtenção do título
de Bacharel em Engenharia Elétrica.

Comissão julgadora

Orientador e presidente

Examinador (1)

Examinador (2)

São Bernardo do Campo

Dedicamos este trabalho à nossas famílias e as
pessoas que nos apoiaram durante este período.

AGRADECIMENTOS

Gostaríamos de expressar nossa sincera gratidão ao nosso orientador, Prof. Dr. Ricardo de Carvalho Destro, por seu inestimável suporte e orientação ao longo do desenvolvimento deste trabalho.

RESUMO

Os seguros massificados, amplamente utilizados pela população de baixa renda no Brasil por seus custos acessíveis e cobertura eficiente, demandam soluções tecnológicas que ampliem e melhorem sua oferta. Este trabalho explora uma solução com *smart contracts* baseados em *blockchain* privada com a plataforma *Hyperledger Fabric* para o mercado de seguros massificados, implementando uma prova de conceito que permite registrar operações de um contrato de seguro massificado, como contratação, acionamento e aprovação/rejeição. A prova de conceito demonstrou redução no compartilhamento de informações entre os atores e viabilizou um modelo de rede que promove a descentralização das informações, ainda que modular o suficiente para ajustar a autoridade entre os participantes. Verificou-se também que dados sensíveis do segurado podem ser mantidos fora da *blockchain*, com alternativas de armazenamento *on-chain* e *off-chain*, promovendo maior segurança e conformidade. Além disso, a tokenização dos contratos permite novos modelos de negócios mediante fracionamento dos seguros massificados, possibilitando maior flexibilidade na distribuição. Esses resultados indicam que a tokenização de contratos massificados e a adoção de *blockchain* representam um caminho promissor para centralizar informações de maneira descentralizada, contribuindo para a transparência e integridade dos dados no setor de seguros.

Palavras-chave: Seguros massificados. Tokenização. *Blockchain* privada. *Smart Contracts*.

Prova de conceito.

ABSTRACT

Massified insurances, widely used by low-income populations in Brazil due to its affordable costs and efficient coverage, requires technological solutions that can expand and enhance its offerings. This study explores a solution with smart contracts based on private blockchain technology, using the Hyperledger Fabric platform for the massified insurance sector. It implements a proof of concept that enables the registration of various operations in a massified insurance contract, such as issuance, activation, and approval/rejection. The proof of concept demonstrated a reduction in information sharing between stakeholders and enabled a network model that promotes decentralized information sharing while remaining modular enough to adjust the authority among participants. It was also found that sensitive policyholder data can be kept off the blockchain, with both on-chain and off-chain storage options available, enhancing security and compliance. Additionally, contract tokenization enables new business models by fragmenting massified insurance, allowing greater flexibility in distribution. These results suggest that tokenizing massified insurance contracts and adopting blockchain technology represent a promising path toward decentralized information centralization, contributing to data transparency and integrity in the insurance sector.

Keywords: Massified insurance. Tokenization. Private blockchain. Smart contracts. Proof of concept.

LISTA DE ILUSTRAÇÕES

Figura 1 - Diagrama de uma rede P2P	17
Figura 2 - Diagrama do fluxo de proposta transacional	23
Figura 3 - Fluxo de verificação do sinistro de celular danificado	28
Figura 4 - Representação da distribuição de seguros massificados	30
Figura 5 - Processo atual de comunicação de contratação entre parceiros e seguradora	31
Figura 6 - Informação transparente para os participantes da rede	32
Figura 7 - Diagrama de fluxo da aplicação	34
Figura 8 - Fluxo de contratação do seguro	35
Figura 9 - Fluxo de avaliação do acionamento do seguro	36
Figura 10 - Diagrama dos participantes da rede de testes	37
Figura 11 - Listagem dos contêineres ativos que compõem a rede	38
Figura 12 - Comunicação entre aplicações	39
Figura 13 - Oferta de celular da Apple	43
Figura 14 - Oferta de celular da Samsung	43
Figura 15 - Opção de contratação do seguro para o celular	44
Figura 16 - Contratação do seguro	45
Figura 17 - Credenciais geradas	45
Figura 18 - Página de login da seguradora	46
Figura 19 - Página de detalhe do seguro	47
Figura 20 - Aguardando upload dos arquivos	48
Figura 21 - Upload de arquivos realizado com sucesso	48
Figura 22 – Detalhe do seguro após ser acionado	49
Figura 23 - Página dos seguros aguardando análise das evidências	50
Figura 24 - Página de detalhe de um seguro em análise de evidências	51
Figura 25 - Detalhe de um seguro na página da decisão final	52
Figura 26 - Consulta do histórico do token, últimos estados	53

LISTA DE ABREVIATURAS E SIGLAS

API	<i>Application Programming Interface</i>
B2B2C	<i>Business to Business to Consumer</i>
CLI	<i>Command-Line Interface</i>
CNSP	Resolução do Conselho Nacional de Seguros Privados, Conselho Nacional de Seguros Privados
HTTP	<i>Hypertext Transfer Protocol</i>
LGPD	Lei Geral de Proteção de Dados Pessoais
P2P	<i>Peer-to-Peer</i>
PKI	<i>Public Key Infrastructure</i>
PoC	<i>Proof of Concept</i>
REST	<i>Representational State Transfer</i>
RPC	<i>Remote Procedure Call</i>
TLS	<i>Transport Layer Security</i>
UI	<i>User Interface</i>

SUMÁRIO

1 INTRODUÇÃO	13
1.1 MOTIVAÇÃO	13
1.2 OBJETIVO	14
1.2.1 Objetivo geral	14
1.2.2 Objetivos específicos	14
1.3 JUSTIFICATIVA	15
1.4 TRABALHOS RELACIONADOS	15
2 REVISÃO BIBLIOGRÁFICA	16
2.1 SISTEMAS DISTRIBUÍDOS	16
2.1.1 <i>Peer-to-Peer</i>	16
2.2 <i>BLOCKCHAIN</i>	17
2.2.1 Visibilidade da <i>blockchain</i>	17
2.2.1.1 Pública	18
2.2.1.2 Privada	18
2.2.2 Tokenização	19
2.3 <i>SMART CONTRACTS</i>	19
2.3.1 <i>Smart Contracts</i> baseados em <i>blockchain</i>	20
2.3.2 <i>Hyperledger Fabric</i>: Uma abordagem privada	21
2.3.3 <i>Ethereum</i>: Uma abordagem pública	23
2.4 AMBIENTE DE TESTES PARA REDES BLOCKCHAIN	24
2.4.1 Interação com a rede	24
2.4.2 Contêineres	25
2.4.3 Automação com <i>Bash</i>	25
2.5 TECNOLOGIAS <i>WEB</i>	26
2.6 O MERCADO DE SEGUROS	27
2.6.1 Seguros massificados	30
3 METODOLOGIA	32
3.1 DEFINIÇÃO DO ESCOPO	32

3.2 PROVA DE CONCEITO	33
3.3 DESENVOLVIMENTO	37
3.3.1 Configuração da rede de testes	37
3.3.2 Aplicação cliente	39
3.3.2.1 <i>Servidor</i>	40
3.3.2.2 <i>Cliente</i>	41
4 RESULTADOS	43
4.1 CONTRATAÇÃO	43
4.2 ACIONAMENTO DO SEGURO	46
4.3 ANÁLISE DAS EVIDÊNCIAS	49
4.4 ANÁLISE FINAL DA SOLICITAÇÃO	51
5 CONCLUSÃO	54
5.1 TRABALHOS FUTUROS	55
5.2 CONSIDERAÇÕES FINAIS	55
REFERÊNCIAS	57
APÊNDICE A – REPOSITÓRIO	60

1 INTRODUÇÃO

A *blockchain* desponta como a principal tecnologia da próxima geração de empresas de serviços financeiros e seguradoras que utilizem os canais digitais. Essa tecnologia garante que as transações sejam processadas de maneira transparente, com maior disponibilidade de dados, segurança e diminuição dos custos operacionais. A previsão é de que o valor gerado ao negócio pela tecnologia *blockchain* chegará a 177 bilhões de dólares em 2025, aumentando para 3,1 trilhões de dólares até 2030 (ZAND; WUN; MORRIS, 2021).

Após a incorporação dos *smart contracts* na *Ethereum*, iniciou-se o período denominado *Blockchain 2.0*, representando um marco para a tecnologia *blockchain* ao possibilitar a execução de transações complexas de forma inteligente e autônoma, expandindo as capacidades da *blockchain* para além da troca de valor representada pelo *Bitcoin*, na *Blockchain 1.0*. Esse avanço tecnológico não apenas impulsionou a revolução *blockchain*, mas também despertou o interesse de grandes empresas e organizações. Empresas como *IBM*, *Intel*, *Oracle*, *Amazon*, *Microsoft* e outras começaram a perceber o potencial dos *smart contracts* para otimizar processos e possibilitar novas soluções em diversos setores (ZAND; WUN; MORRIS, 2021).

O mercado de seguros é um setor conhecido por sua complexidade, burocracia e pela presença de regulamentações (OUTREVILLE, 1998). As seguradoras enfrentam desafios significativos em relação à transparência das informações, eficiência operacional e conformidade regulatória. A necessidade de intermediários, a falta de transparência na comunicação entre as partes e a centralização das operações são apenas algumas das barreiras que limitam a eficiência e a agilidade nesse mercado (SANTOS, 2023).

Nesse contexto, a tecnologia *blockchain*, aliada aos *smart contracts*, surge como uma solução promissora para otimizar os processos no setor de seguros. Ao possibilitar o registro transparente e imutável de transações, a *blockchain* permite maior confiabilidade e segurança na troca de informações entre seguradoras, parceiros, segurados e outros participantes do mercado.

1.1 MOTIVAÇÃO

Segundo Santos (2023), no caso específico dos seguros massificados, a transparência das informações é limitada devido a oferta ser realizada por meio do modelo estratégico Empresa para Empresa para Consumidor – *Business to Business to Consumer* (B2B2C).

Diante disso, torna-se evidente que os intermediários são atores essenciais para que a seguradora consiga ofertar seus produtos para uma ampla base de consumidores em potencial, não sendo viável a oferta direta de seguros massificados entre seguradora e consumidor. Com isso, o presente estudo busca otimizar o processo de comunicação entre os atores envolvidos na operação dos segurados massificados.

A transparência oferecida pela *blockchain* permite a gestão eficiente e segura das transações, garantindo que todas as partes envolvidas tenham acesso igualitário às informações e processos (NAKAMOTO, 2008). Isso pode resultar em uma melhoria significativa na experiência do cliente, redução de custos operacionais, maior conformidade com regulamentações governamentais e agilidade no faturamento de prêmios.

1.2 OBJETIVO

Esta seção estabelece os objetivos deste trabalho de conclusão de curso.

1.2.1 Objetivo geral

O objetivo geral é demonstrar a viabilidade e os benefícios de uma solução baseada em *blockchain* privada para o mercado de seguros massificados, através de uma implementação modelo em que será possível registrar a contratação, o acionamento, a aprovação/rejeição das evidências e a aprovação/rejeição da solicitação de sinistro de um seguro.

1.2.2 Objetivos específicos

- a) Analisar o mercado de seguros, com foco nos seguros massificados;
- b) Desenvolver uma Prova de Conceito – *Proof of Concept* (PoC), em um ambiente de testes, utilizando as tecnologias do ecossistema *blockchain*, a fim de distribuir a informação, de forma descentralizada, entre os participantes das operações existentes no mercado de seguros massificados;
- c) Analisar os resultados obtidos da PoC e possibilidade de sua aplicação em produção, cenário real, no mercado de seguros massificados.

1.3 JUSTIFICATIVA

Os seguros massificados possuem forte adoção entre as pessoas de baixa renda, maioria da população brasileira, por possuírem valores acessíveis, mas com cobertura eficaz. Com isso, mais de 70 milhões de brasileiros tornaram-se consumidores ativos (FELIX, 2020). Diante deste cenário, é essencial o desenvolvimento de uma solução que aprimore e amplie a cobertura dos seguros massificados oferecidos.

A introdução de *smart contracts* baseados em *blockchain* pode otimizar os procedimentos associados a esses seguros, facilitando a expansão da oferta ao público de forma tecnologicamente avançada e acessível. Tal abordagem não apenas simplifica processos e diminui custos operacionais, mas também fomenta uma experiência mais transparente e segura para todos os participantes, impulsionando o crescimento sustentável e inclusivo do mercado de seguros massificados.

1.4 TRABALHOS RELACIONADOS

Diversos estudos e soluções têm explorado a aplicação da tecnologia *blockchain* no mercado de seguros, com foco significativo nos seguros paramétricos. Esta categoria de seguro utiliza *smart contracts* para automatizar processos de pagamento, reduzindo a necessidade de intervenção manual.

Um exemplo notável é a *Etherisc*, uma plataforma de *blockchain* pública que oferece soluções para seguros paramétricos, utilizando-se de *smart contracts* para automatizar a indenização do segurado quando determinados parâmetros pré-definidos são atingidos, eliminando a necessidade de intermediários e agilizando o processo de indenização.

Outro projeto relevante é a *Chainlink*, que fornece a infraestrutura para conectar *smart contracts* a fontes de dados externas, essenciais para a execução automática de seguros paramétricos.

Apesar desses avanços, tanto a *Etherisc* quanto o *Chainlink* utilizam *blockchain* pública, diferindo do enfoque deste trabalho. Este trabalho de conclusão de curso concentra-se em soluções corporativas para seguros massificados, não-paramétricos, utilizando *blockchain* privada, visando atender às exigências de segurança, privacidade e controle das empresas do setor de seguros. Essa distinção é crucial, pois a adoção de *blockchain* privada pode atender as necessidades específicas de segurança e conformidade regulatória.

2 REVISÃO BIBLIOGRÁFICA

Nesta seção, é apresentada a revisão bibliográfica que fundamenta conceitualmente a execução da metodologia proposta. O escopo abrange desde os fundamentos da tecnologia *blockchain* até as aplicações no setor de seguros. São discutidos conceitos-chave, como *smart contracts* baseados em *blockchain*, seguros massificados e suas interseções.

2.1 SISTEMAS DISTRIBUÍDOS

Os sistemas distribuídos são compostos por máquinas autônomas conectadas por redes de comunicação, visando criar um ambiente de computação integrado e eficiente. Eles facilitam a cooperação entre usuários e têm objetivos como compartilhamento de recursos, abertura, concorrência, escalabilidade, tolerância a falhas e transparência (JIA; ZHOU, 2004).

Esses sistemas permitem compartilhar recursos como hardware e software entre usuários, estendendo suas funcionalidades por meio de interfaces de software definidas. Eles processam solicitações simultaneamente em várias máquinas, garantindo escalabilidade ao aumentar a capacidade de processamento conforme necessário. Além disso, são projetados para tolerar falhas, replicando o software em múltiplas máquinas para mitigar problemas. Por fim, oferecem transparência, permitindo acesso unificado a informações locais e remotas, além de mascarar automaticamente falhas e replicar dados de forma invisível em várias máquinas.

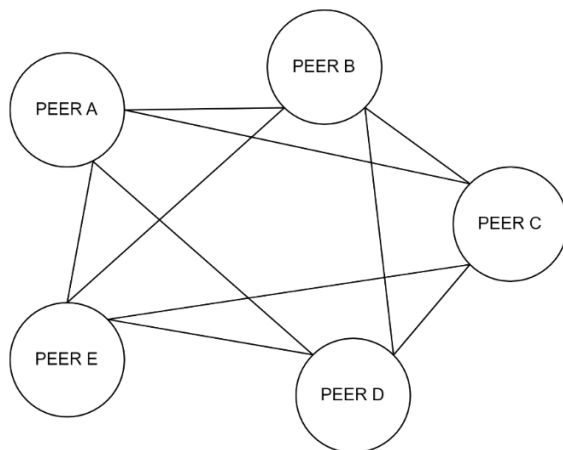
2.1.1 *Peer-to-Peer*

O termo "*peer*" é definido como um indivíduo de igual posição ou status em relação a outro. Dessa forma, a computação ponto a ponto – *Peer-to-Peer* (P2P) pode ser entendida como um modelo no qual os participantes têm igualdade de condições (JIA; ZHOU, 2004).

O conceito de igualdade de participação é compartilhado com os sistemas de registro distribuído, nos quais múltiplos pontos na rede têm a mesma capacidade de participar na validação e no registro das transações, sem a necessidade de uma autoridade central.

Os participantes são geralmente não confiáveis e podem entrar e sair dinamicamente do sistema, além de enfrentar falhas tanto nos *peers* quanto nos links de comunicação (ANDROULAKI et al., 2018). Isso torna o desenvolvimento de aplicações P2P um desafio, especialmente em termos de segurança, escalabilidade e desempenho.

Figura 1 - Diagrama de uma rede P2P



Fonte: Autores

2.2 BLOCKCHAIN

A *blockchain* é um sistema de registro imutável e distribuído que mantém uma lista contínua de registros, chamados blocos, interligados e protegidos por criptografia. Cada *peer* da rede contém uma cópia do registro de transações e um *hash*¹ do bloco anterior, garantindo a integridade e a imutabilidade dos dados. A rede, formada pelos *peers*, coleta, valida e executa a transação por intermédio de um protocolo de consenso, gerando uma cadeia de blocos (ANDROULAKI et al., 2018), em tradução direta *blockchain*. Os *peers* que validam as transações e, conseqüentemente, formam os blocos são denominados “validadores”.

O primeiro caso de uso da tecnologia *blockchain* foi o *Bitcoin*, um sistema de dinheiro eletrônico P2P (NAKAMOTO, 2008), de natureza descentralizada e segura.

2.2.1 Visibilidade da *blockchain*

Uma questão recorrente nas redes *blockchain* é sobre como assegurar a honestidade dos participantes ao protocolo, garantindo que a rede se mantenha íntegra. Diversas *blockchains* adotam mecanismos distintos para garantir a integridade da rede. Uma classificação comum nesse sentido é a divisão entre *blockchains* públicas e privadas, cada qual com abordagens específicas para a seleção de participantes confiáveis (SHETTY; KAMHOUA; NJILLA, 2019).

¹ Saída de uma função *Hash*, utilizada para garantir a integridade dos dados em questão, sem expô-los.

2.2.1.1 Pública

Uma *blockchain* pública, também conhecida como sem permissão, permite a participação irrestrita de qualquer indivíduo. Além disso, a identificação pessoal do usuário não é exigida, o que potencialmente permite que uma única pessoa controle múltiplas identidades de forma anônima (BAKOS; HALABURDA, 2023).

Em *blockchains* públicas, não existe o conceito de autoridade central responsável por deter o poder final no que tange às validações da rede. Na ausência dessa autoridade, todos os participantes possuem direitos iguais para validar as transações (SANKAR; SINDHU; SETHUMADHAVAN, 2017).

Devido à natureza descentralizada e anônima em que as transações são executadas, para garantir a integridade da rede quanto ao consenso, é necessário que um recurso do participante seja gasto, sendo ele computacional ou monetário, de forma que haja um incentivo ao comportamento honesto relativo aos protocolos da rede (SHETTY; KAMHOUA; NJILLA, 2019).

Por outro lado, a necessidade de gastos de recursos pode resultar em desempenho reduzido das transações na rede e custos significativos aos participantes. Esses obstáculos podem tornar a operação inviável em certos cenários onde alta capacidade de velocidade e baixo custo sejam primordiais (BAKOS; HALABURDA, 2023).

2.2.1.2 Privada

Uma *blockchain* privada é definida pela capacidade de qualificar os participantes da rede. Comumente, *blockchains* privadas exigem que ao menos a identidade pessoal dos validadores seja conhecida, haja visto que o processo exige um nível de confiança das partes com relação ao validador (BAKOS; HALABURDA, 2023).

Em função da necessidade de validações por uma autoridade central, o protocolo é guiado por processos que ocorrem externamente à rede, como contratos. Em contrapartida às redes públicas, onde o consenso é alcançado mediante gasto de recursos pela maioria dos participantes, as redes privadas têm uma tendência a serem mais eficientes, já que um reduzido número de validadores pode processar uma transação de forma direta. No entanto, as operações em uma rede privada estão mais suscetíveis a ataques direcionados aos validadores, os quais, por serem poucos, facilitam o controle sobre a rede (BAKOS; HALABURDA, 2023).

2.2.2 Tokenização

A tokenização de ativos é o processo de representar digitalmente o valor econômico e os direitos associados a um ativo real, permitindo que ele seja transacionado de forma eficiente em uma rede *blockchain* (ANBIMA, 2022). No contexto de seguros, essa abordagem possibilita que contratos de seguro, tradicionalmente vinculados a processos burocráticos e intermediários, sejam convertidos em *tokens*, que representam os direitos e obrigações desses contratos em formato digital.

Além dos benefícios inerentes do *token* ser parte de uma rede *blockchain*, essa tecnologia tem o potencial de gerar oportunidades de negócios, como a negociação de frações do ativo em mercados secundários, aumentando a liquidez e o acesso a produtos financeiros relacionados (ANBIMA, 2022). Com isso, o setor financeiro não apenas moderniza a forma de emissão e transação desses ativos, mas também abre novas possibilidades para a criação de mercados mais dinâmicos e acessíveis.

2.3 SMART CONTRACTS

No âmbito da exploração dos *smart contracts*, é necessário definir os contratos convencionais. Segundo Szabo (1997) um contrato é a maneira tradicional de formalizar uma relação de negócio e possui cinco etapas:

- a) pesquisa: a fase inicial de pesquisa envolve a identificação e especificação dos termos e condições que serão cobertos no contrato;
- b) negociação: resolução das divergências entre as partes em relação aos termos do contrato;
- c) comprometimento: ambas as partes concordam com os termos do contrato e prometem honrar o contrato;
- d) execução: cumprimento dos termos do contrato;
- e) adjudicação: processo legal de resolução de disputas decorrentes da falta de cumprimento dos termos do contrato.

Os *smart contracts* representam uma evolução significativa no processo de formalização de relações, proporcionando uma redução na carga cognitiva e nos custos computacionais

associados (SZABO, 1997). Além disso, são sistemas que transferem recursos digitais automaticamente em função de regras pré-definidas (BUTERIN, 2014).

Ao contrário dos contratos tradicionais, os *smart contracts* possibilitam a remoção do intermediário, caso sejam autoexecutáveis, simplificando e agilizando cada fase do processo contratual.

2.3.1 *Smart Contracts* baseados em *blockchain*

Os *smart contracts* baseados em *blockchain* são códigos de programas que implementam a lógica da aplicação e são executados dentro da rede *blockchain* (ANDROULAKI et al., 2018). Neste ambiente, aplicações *off-chain*² invocam o *smart contract* para criar transações que são registradas na rede *blockchain*.

As cinco etapas contratuais descritas por Szabo (1997) são integralmente incorporadas de maneira transparente nos *smart contracts*:

- a) pesquisa:
 - a fase inicial de pesquisa envolve a identificação e especificação dos termos e condições que serão codificados no contrato;
- b) negociação:
 - as partes podem utilizar algoritmos e protocolos para facilitar as interações e resolver divergências de forma eficaz;
 - os *smart contracts* podem incluir mecanismos de negociação automatizados que permitem que as partes cheguem a um acordo sem a necessidade de intervenção humana;
- c) comprometimento:
 - uma vez que os termos do contrato são finalizados as partes se comprometem a honrar esses termos dando origem a um *smart contract*;
 - o compromisso é registrado e codificado de forma imutável na *blockchain*;
- d) execução:
 - o *smart contract* pode ser executado de forma automática conforme estipulado em seus termos;

² Simboliza algo externo à *blockchain*

- por meio de código pré-programado os *smart contracts* podem acionar operações e executar outras ações automaticamente sem a necessidade de intervenção humana;
- e) adjudicação:
 - os *smart contracts* podem incluir mecanismos de resolução de disputas automatizados;
 - mecanismos automatizados podem ser programados para seguir uma série de regras pré-definidas para resolver a disputa de forma justa e transparente.

Essa abordagem proporciona novas formas de formalizar e garantir relacionamentos digitais, destacando-se pela transparência e automação que os *smart contracts* oferecem sobre os contratos digitalizados tradicionais. Ao possibilitar a eliminação de intermediários e prover imutabilidade, os *smart contracts* oferecem uma solução eficiente e transparente para todos envolvidos no contrato.

2.3.2 *Hyperledger Fabric*: Uma abordagem privada

A *Hyperledger Fabric*, desenvolvida pela *Linux Foundation*, visa facilitar a implementação de aplicações *blockchain* no ambiente corporativo, adaptando-se às necessidades específicas de cada empresa (ALEKSIEVA; VALCHANOV; HULIYAN, 2020).

Devido ao fato de se tratar de uma plataforma privada, a *Hyperledger Fabric* possui autoridades centrais que certificam os participantes da rede, denominadas autoridades certificadoras. Cada participante deve possuir uma identidade digital encapsulada em um certificado digital. Por meio dessa identidade é possível determinar as permissões e acessos do agente na rede. O componente padrão da *Hyperledger Fabric* utiliza a tradicional *Public Key Infrastructure* (PKI), uma coleção de tecnologias que fornecem comunicação segura em uma rede (HYPERLEDGER, 2023).

A fim de estabelecer uma comunicação segura, o mecanismo de assinatura digital requer que cada parte possua duas chaves conectadas por criptografia: as chaves pública e privada. A chave privada é utilizada para produzir a assinatura digital nas mensagens. O destinatário da mensagem pode verificar a origem e integridade utilizando a chave pública do remetente (HYPERLEDGER, 2023).

Além disso, a tecnologia introduz o conceito de canais, que separa diferentes contextos dentro da rede, facilitando a modelagem de empresas com diversos clientes e circunstâncias. Dessa forma, integrantes de um canal conhecem apenas as transações registradas neste mesmo canal (ANDROULAKI et al., 2018).

Os *smart contracts* na *Hyperledger Fabric* definem a lógica executável para transações na rede *blockchain*. Uma característica distintiva é a presença de políticas de endosso, que determinam quais organizações devem aprovar uma transação para que ela seja considerada válida (HYPERLEDGER, 2023). Essas políticas oferecem alto grau de controle sobre quem pode participar de transações específicas, garantindo a integridade e segurança das operações.

Além disso, os *smart contracts* operam dentro dos canais, garantindo a separação de contextos e mantendo a privacidade e confidencialidade das transações (HYPERLEDGER, 2023). Por exemplo, uma empresa pode ter um canal específico para transações financeiras internas e outro para interações com fornecedores externos.

Outro aspecto importante é a validação das transações e sua relação com o registro na *blockchain*. Embora todas as transações sejam registradas na *blockchain*, somente as válidas são incorporadas ao estado atual da rede, conhecido como *world state* (HYPERLEDGER, 2023). Assim, garante-se que apenas transações legítimas e autorizadas tenham impacto no estado atual do sistema, mantendo a consistência e precisão dos dados.

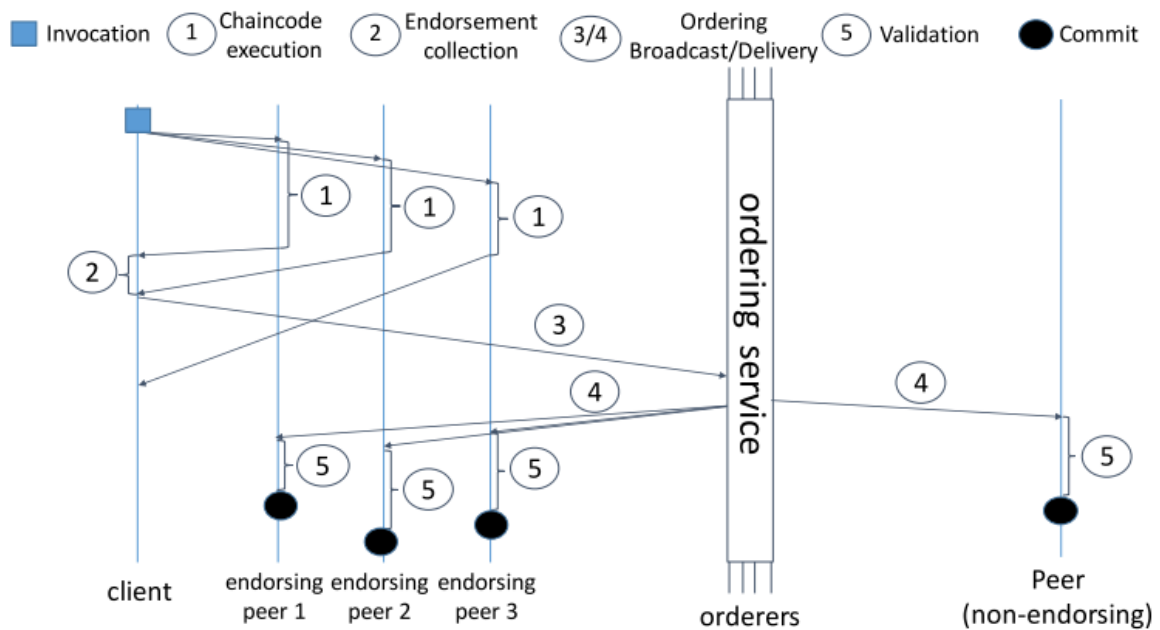
As políticas de endosso diferenciam a *Hyperledger Fabric* em comparação com *blockchain* públicas, em que as transações podem ser validadas por qualquer *peer* presente na rede. A abordagem da *Hyperledger Fabric* espelha de forma fiel os procedimentos do mundo real, onde transações requerem validação por entidades de confiança dentro de uma rede (HYPERLEDGER, 2023). Um exemplo dessa modelagem na prática é encontrado em contratos de seguro, nos quais a ocorrência de um evento demanda a verificação por validadores especializados para autorizar a transação.

Na Figura 2 são ilustradas as três fases do processo de proposta de transação (ANDROULAKI et al., 2018):

- a) execução: os *smart contracts* são invocados pela aplicação cliente para processar uma transação específica;
- b) consenso:
 - endosso: garante que a transação seja aprovada pelas organizações relevantes de acordo com a política de endosso do *smart contract* associado;

- ordenação: assegura que as transações sejam ordenadas e agrupadas em blocos para serem distribuídas para os *peers*;
 - validação: cada *peer* verifica a transação para validá-la em função das regras de consenso da rede;
- c) comprometimento: confirmação e registro permanente na *blockchain*.

Figura 2 - Diagrama do fluxo de proposta transacional



Fonte: Androuraki et al., 2018

2.3.3 Ethereum: Uma abordagem pública

A *Ethereum* é uma plataforma *blockchain* pública, sem permissão, que permite a execução de *smart contracts*. Proposta em 2013 por Vitalik Buterin e desenvolvida de forma *Open Source*³, trouxe inovações em relação à tecnologia *blockchain*, tornando-se uma plataforma popular para implementação de *smart contracts* e aplicações descentralizadas (BUTERIN, 2014).

Ao contrário da *Hyperledger Fabric*, a *Ethereum* permite a participação de qualquer usuário. Isso significa que não é necessário um convite ou aprovação para ingressar na rede,

³ Código-fonte desenvolvido de maneira pública, disponível para uso e modificação.

tornando-a aberta e acessível a todos os usuários. Além disso, uma transação pode ser validada por qualquer *peer* da rede, característica de uma *blockchain* pública (ETHEREUM, [s.d.]).

Os *smart contracts* na rede *Ethereum* oferecem vantagens, como automação de processos, transparência, imutabilidade e segurança. No entanto, também apresentam a desvantagem de possuir custos de transação variáveis. Além disso, por ser pública, pode não ser a escolha ideal para soluções corporativas que requerem controle sobre os participantes da rede e a confidencialidade das transações. Empresas que operam em setores altamente regulamentados ou que necessitam de uma rede com permissões específicas podem encontrar desafios ao utilizar a plataforma para suas aplicações *blockchain*.

2.4 AMBIENTE DE TESTES PARA REDES BLOCKCHAIN

O desenvolvimento e implementação de redes *blockchain*, especialmente em ambiente de teste, exige a adoção de diversas tecnologias que proporcionem isolamento de processos, eficiência e escalabilidade. Neste capítulo, serão discutidas as tecnologias essenciais utilizadas em ambientes de testes de redes distribuídas, com foco em *blockchain*.

2.4.1 Interação com a rede

As plataformas *blockchain* fornecem interfaces de comunicação para interação com a rede. Com objetivo de exemplificar uma dessas interfaces descreve-se a seguir a interface fornecida pela *Hyperledger Fabric* que disponibiliza binários pré-compilados de uma Interface de Linha de Comandos – *Command-Line Interface* (CLI), que suportam a interação com a rede. Os binários são (HYPERLEDGER, 2023):

- a) *configtxgen*: criação e consulta de artefatos relacionados à configuração do canal;
- b) *configtxlator*: ferramenta para *decoding* e *encoding* de estruturas de dados nos formatos *protobuf*⁴ e *JSON*⁵;
- c) *cryptogen*: ferramenta para criação de chaves criptográficas;
- d) *discover*: serviço utilizado para armazenar certificados e caminhos de chaves privadas;

⁴ *Protocol buffers*: ferramenta de serialização de dados estruturados.

⁵ Padrão de formatação utilizado para troca de dados.

- e) *osnadmin*: manipulação do *peer* ordenador pelo administrador da rede;
- f) *peer*: gerenciamento de *peers* pelo administrador da rede;
- g) *fabric-ca-client*: permite gerenciar identidades e certificados;
- h) *fabric-ca-server*: inicialização do servidor da Autoridade Certificadora.

2.4.2 Contêineres

Um contêiner pode ser descrito como um processo isolado em execução em uma máquina hospedeira, utilizando recursos do *kernel*⁶ *Linux* para garantir o isolamento de outros processos no sistema. Além disso, é uma instância executável de uma imagem, que fornece um sistema de arquivos isolado contendo todos os elementos necessários para a execução de uma aplicação, incluindo dependências, configurações, *scripts* e binários. Essa estrutura garante portabilidade e isolamento, sendo possível executá-los em máquinas locais, máquinas virtuais ou na nuvem (DOCKER, [s.d.]).

Soluções, como a tecnologia *Docker*, têm transformado o desenvolvimento de software ao oferecer um ambiente isolado e portátil para execução de aplicações. De acordo com Merkel (2014), contêineres permitem que desenvolvedores construam, testem e implantem aplicações em diferentes sistemas com consistência.

No contexto da tecnologia *blockchain*, contêineres têm se mostrado essenciais. Eles permitem o isolamento de componentes críticos, cada um operando de maneira independente. Este isolamento evita conflitos de dependências e permite que múltiplos componentes de uma rede *blockchain* sejam configurados de forma ágil e replicável, o que é crucial em ambientes de testes que exigem flexibilidade para diferentes configurações e topologias de rede (PAHL et al., 2019).

2.4.3 Automação com *Bash*

O *Bash* é um interpretador de comandos, ou *shell*, utilizado no sistema operacional *GNU*, também conhecido como *Unix*. Além de atuar como *shell*, destaca-se por suas capacidades avançadas no desenvolvimento de *scripts*. Os *scripts* permitem a automação de tarefas, combinando diversos comandos do *Unix* em um único arquivo executável. Esses

⁶ Principal componente do Sistema Operacional, responsável por comunicar hardware e processos.

arquivos de *script* podem realizar uma ampla gama de operações, desde manipulação de arquivos e diretórios até o controle de processos e redes (GNU OPERATION SYSTEM, [s.d.]).

Por intermédio de *scripts*, é possível criar soluções personalizadas para automatizar tarefas recorrentes e processos complexos, como a configuração de redes de teste em sistemas distribuídos.

Automatizar processos é uma prática necessária em ambientes de desenvolvimento e teste, e *Bash Scripts* são utilizados com essa finalidade. O projeto *Hyperledger Fabric*, por exemplo, disponibiliza *Bash scripts* para facilitar a criação de redes de teste. Esses *scripts* podem ser ajustados de acordo com as necessidades específicas de cada rede, possibilitando o controle sobre a topologia. A automação via *Bash* proporciona, além de agilidade, a consistência no comportamento do ambiente, permitindo que a mesma configuração seja repetida.

2.5 TECNOLOGIAS *WEB*

As tecnologias *web* são um conjunto de ferramentas e padrões amplamente utilizados para o desenvolvimento de aplicações acessíveis via *internet*. A adoção, em massa, dessas tecnologias transformou a forma com que as pessoas interagem com serviços, negócios e informações. Navegadores, como o *Google Chrome*, *Mozilla Firefox*, *Safari etc.*, são fundamentais na execução dessas tecnologias, permitindo que os usuários naveguem e interajam com interfaces dinâmicas de maneira eficiente (AMAZON AWS, [s.d.]).

A arquitetura de aplicações *web* é composta por duas entidades: cliente e servidor. Essa segmentação ocorre, pois existem códigos que são executados no navegador do usuário final, o lado do cliente, e códigos executados externamente ao navegador do cliente, no servidor.

No contexto atual, o cliente refere-se à interface visual com a qual o usuário final interage. Diversas ferramentas suportam o desenvolvimento das interfaces *web*, como *React*, *Vue.js* e *Angular*, permitindo a criação de páginas interativas e dinâmicas. Dentre as diversas funcionalidades ofertada por essas tecnologias, destaca-se a reatividade que possibilita atualizações em tempo real, em função dos estados da aplicação, melhorando a experiência do usuário sem a necessidade de recarregar a página.

Por outro lado, o servidor é responsável por processar as requisições enviadas pelo cliente, além de gerenciar as regras de negócios, autenticação e persistência dos dados. Basicamente, todas linguagens de programação podem ser utilizadas para desenvolvimento de

back-end, visto que sua execução será no servidor, permitindo o desenvolvimento de aplicações utilizando linguagens com maior aderência ao domínio da solução.

A comunicação entre o cliente e o servidor pode ocorrer de várias formas, as mais comuns são com *REST*, *GraphQL* e *gRPC*. A Transferência Representacional de Estado – *Representational State Transfer* (REST) utiliza as operações do Protocolo de Transferência de Hipertexto – *Hypertext Transfer Protocol* (HTTP) para realizar a manipulação de dados de maneira escalável e eficiente. Alternativamente, o *gRPC*, uma implementação de Chamada de Procedimento Remoto – *Remote Procedure Call* (RPC), do *Google*, oferece maior performance sendo adequado para cenários onde a baixa latência é um requisito, como *streaming* e na interação com *blockchain* (AMAZON AWS, [s.d.]).

Por fim, a comunicação entre as aplicações *web* e a *blockchain* apresenta desafios específicos de segurança. A proteção das trocas de dados é garantida pela utilização da Segurança da Camada de Transporte – *Transport Layer Security* (TLS) e de certificados digitais, que asseguram a autenticidade e a criptografia das informações trafegadas (STALLINGS, 2017). No caso da rede *Hyperledger Fabric*, a interação entre o *back-end* e a *blockchain* é feita mediante conexão *gRPC*, utilizando o conjunto de chaves pública e privada para autenticação, denominada *gateway*.

2.6 O MERCADO DE SEGUROS

O setor de seguros no Brasil é marcado pela presença de grandes empresas seguradoras, muitas delas associadas aos principais grupos econômicos do país, o que evidencia a interseção entre o mercado de seguros e o setor bancário. Em 2017, os bancos concentravam 80% do total de ativos do setor de seguros, representando um montante de R\$ 5,7 trilhões (CHAVES; FERRAZ; FERRAZ, 2024). Essa concentração de ativos demonstra a significativa participação dessas empresas no mercado segurador brasileiro, o que evidencia o alto capital presente no setor de seguros, reforçando sua influência e importância no cenário econômico nacional.

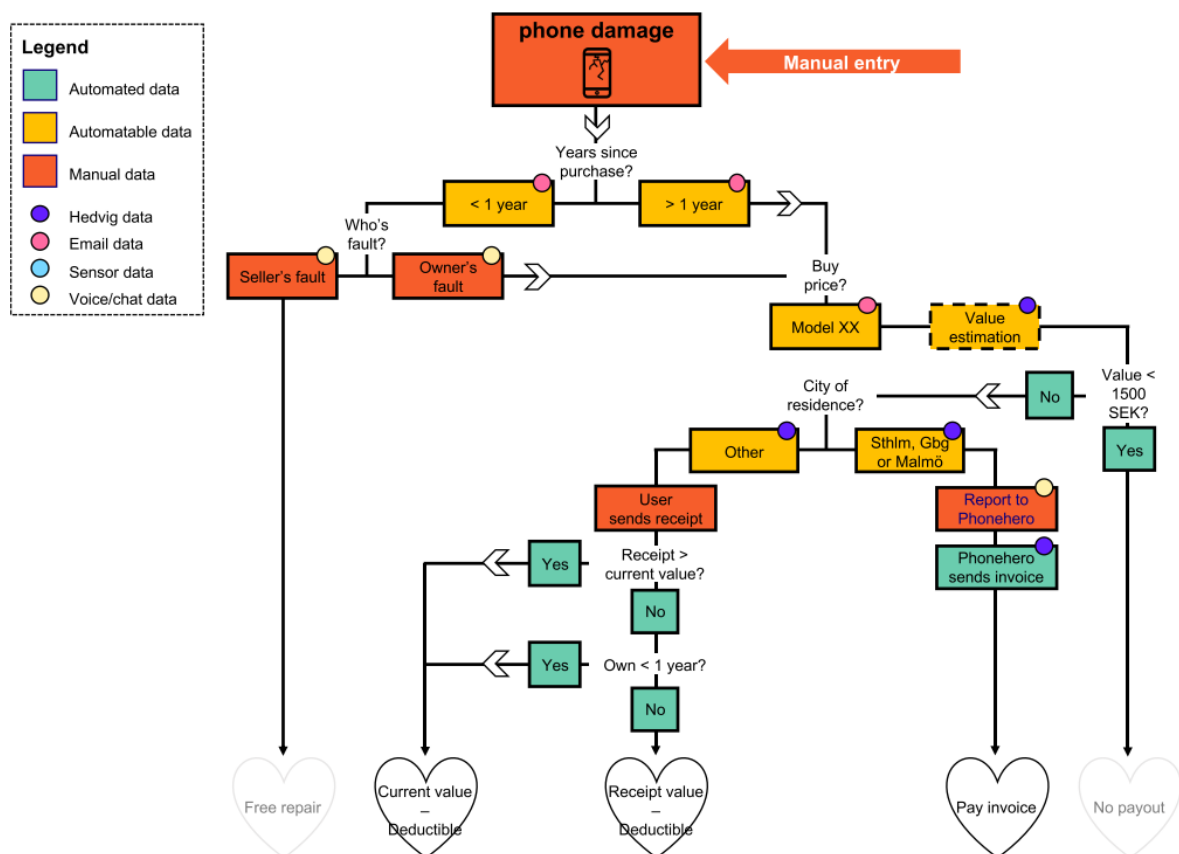
O surgimento e desenvolvimento do seguro estão profundamente enraizados na necessidade da sociedade em se proteger contra eventos futuros que possam afetar indivíduos ou bens, visando restaurar o equilíbrio diante de situações adversas, sejam elas previsíveis ou incertas. Nesse contexto, os princípios do mutualismo e da probabilidade guiam a estruturação dos contratos de seguro. O mutualismo implica a redistribuição dos prejuízos entre os participantes do grupo segurado, enquanto a probabilidade está relacionada à habilidade de

prever antecipadamente os pagamentos necessários para cobertura dos riscos previstos (SANTOS, 2023).

De acordo com Outreville (1998), o contrato de seguro é estabelecido entre o segurador e o segurado. Nele, o segurador se compromete a indenizar o segurado pelos prejuízos decorrentes de riscos futuros, mediante o pagamento do prêmio pelo segurado. Esse prêmio é essencial para a operação do seguro, representando o valor cobrado pela seguradora para assumir os riscos. O sinistro, por sua vez, corresponde à ocorrência do evento previsto no contrato, enquanto a indenização é o pagamento efetuado pela seguradora ao segurado ou beneficiário em caso de sinistro.

Um exemplo do fluxo de análise do sinistro, utilizado pela empresa sueca Hedvig, pode ser visualizado na Figura 3, conforme demonstrado por Salahshor e Scherrer (2020). Neste fluxo, é detalhado o processo de verificação do evento previsto, em que a seguradora analisa as evidências apresentadas pelo segurado para determinar a legitimidade do sinistro antes de aprovar a indenização.

Figura 3 - Fluxo de verificação do sinistro de celular danificado



Fonte: Salahshor e Scherrer (2020)

Apesar da regulação governamental significativa, o mercado segurador brasileiro tem experimentado maior flexibilidade regulatória desde 2020, possibilitando a configuração de coberturas mais diversificadas nos contratos (SANTOS, 2023). Além disso, as seguradoras têm a opção de recorrer a operações de resseguro para transferir parte dos riscos a terceiros, reduzindo sua exposição.

Santos (2023) explicita que os parceiros de distribuição são categorizados como estipulantes ou representantes de seguros. Esses atuam oferecendo o seguro de forma acessória à sua atividade principal, mediante remuneração. O estipulante de seguro é a entidade que propõe a contratação de um plano coletivo de seguro, assumindo poderes de representação do segurado, conforme estabelecido na Resolução do Conselho Nacional de Seguros Privados (CNSP) nº 348/2017 (2017). Por outro lado, o representante de seguros é uma pessoa jurídica que se compromete a promover, oferecer ou distribuir contratos de seguros em nome da seguradora, sem possuir poderes de representação dos segurados, sendo considerado um intermediário da seguradora, conforme a mesma resolução.

Quanto à distribuição de seguros, prevalece a venda mediante corretores, representantes e estipulantes. No caso das seguradoras vinculadas a grandes bancos, estes desempenham o papel de estipulantes de seguro. Observa-se também uma tendência crescente de expansão da distribuição de seguros por meios digitais, com processos de venda autoexplicativos, indicando a adaptação do setor às novas tecnologias e preferências do cliente (SANTOS, 2023).

No mercado de seguros brasileiro, uma ampla variedade de tipos de seguros está disponível para atender às necessidades diversificadas dos clientes. Desde seguros de vida e saúde até seguros patrimoniais e de responsabilidade civil, há opções para proteger os indivíduos, suas famílias e seus bens contra uma série de riscos.

Dentre os diversos produtos ofertados no Brasil, destacam-se os seguros massificados, por conta de sua comercialização para as classes C e D/E (FELIX, 2020), que na estratificação dos domicílios em 2022 representavam aproximadamente 84% da população do país (INFOMONEY, 2022). O desenvolvimento e a expansão dos seguros massificados não apenas fortalecem o mercado segurador, mas também promovem a resiliência econômica e social do Brasil.

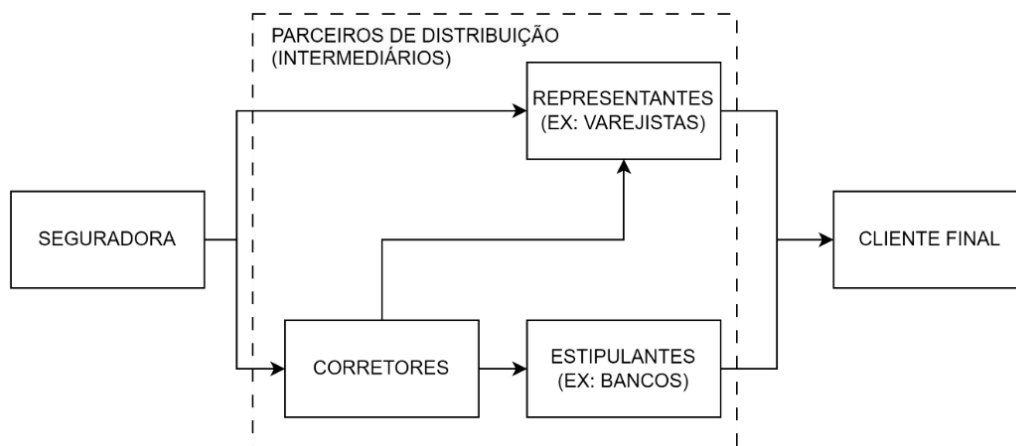
2.6.1 Seguros massificados

Os seguros massificados constituem contratos caracterizados por baixo preço, baixo valor de cobertura e simplicidade de contratação, destacando-se como uma modalidade acessível. Comumente, esses seguros são comercializados através do modelo de negócios B2B2C e marketing por afinidade, nos quais parceiros-chave aproveitam suas bases de clientes para ofertar soluções de seguros (SANTOS, 2023).

Exemplos clássicos de seguros massificados incluem garantia estendida de eletroportáteis, proteção contra roubo, furto e quebra de eletrônicos, cobertura de acidentes pessoais e seguros de vida em grupo, frequentemente comercializados por companhias varejistas (SANTOS, 2023).

Nesse contexto, o cliente final adquire os contratos principalmente por intermédio de companhias varejistas, financeiras, bancos e operadoras de crédito. Além dos clientes finais, os parceiros e intermediários são também considerados clientes, pois podem contar com diversas seguradoras para ofertar soluções de seguro aos seus clientes, buscando sempre as melhores condições para atender suas necessidades (SANTOS, 2023).

Figura 4 - Representação da distribuição de seguros massificados



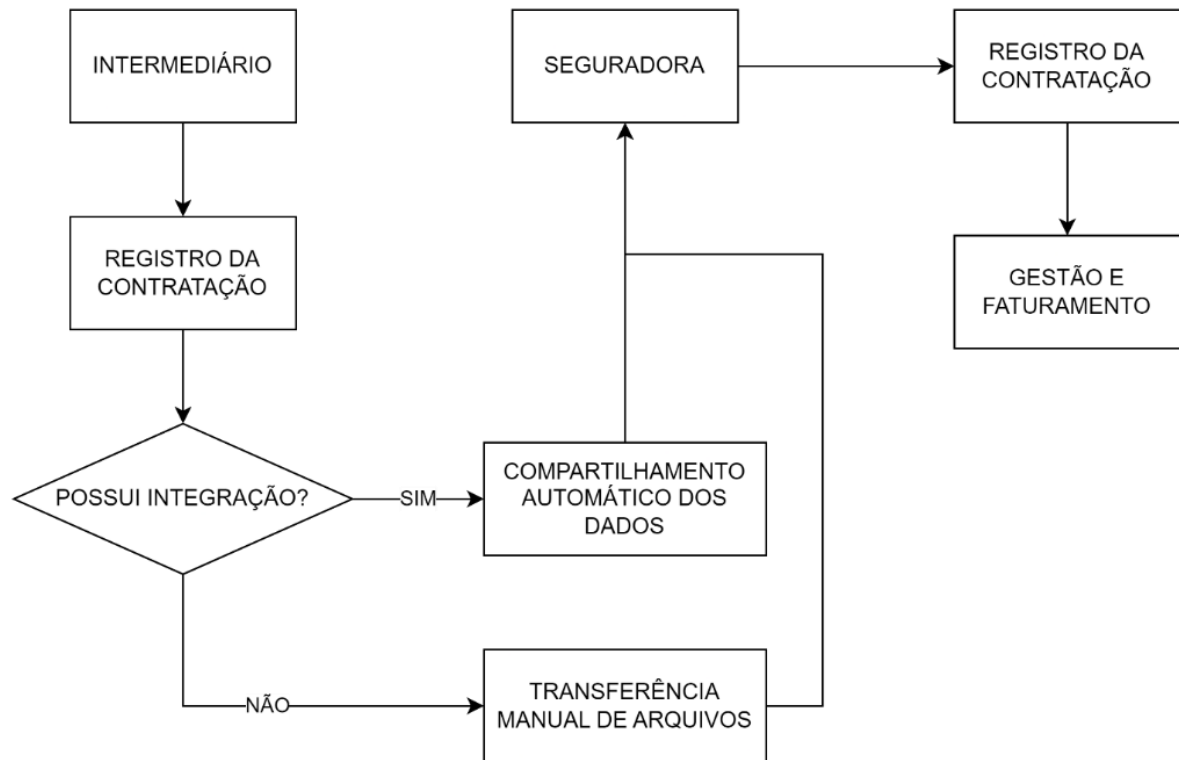
Fonte: Adaptado de Santos, 2023

A distribuição dos seguros massificados ocorre por intermédio de representantes e estipulantes de seguro, que utilizam suas equipes de vendas para promover os seguros de forma acessória ao *core business*⁷ do parceiro de distribuição. As vendas são registradas inicialmente

⁷ Atividade principal de uma empresa

nos sistemas de venda do parceiro de distribuição e, posteriormente, os dados são comunicados mediante transferência de arquivos. Em algumas operações, há integração de dados na seguradora, proporcionando agilidade na gestão e faturamento dos prêmios comerciais (SANTOS, 2023).

Figura 5 - Processo atual de comunicação de contratação entre parceiros e seguradora



Fonte: Autores

Em um ambiente de seguros massificados, diversos elementos são identificados como fatores-chave de sucesso, incluindo a reputação da seguradora e de seus colaboradores, o relacionamento com o mercado (corretores, representantes e estipulantes), o entendimento dos riscos envolvidos, a precificação adequada, a rapidez e agilidade no atendimento ao cliente, a capacidade tecnológica para rápida implementação, a qualidade do atendimento e a clareza do contrato oferecido ao cliente (SANTOS, 2023). Esses elementos são essenciais para garantir a eficácia e a competitividade das operações de seguros massificados no mercado brasileiro.

3 METODOLOGIA

Embasando-se nos conceitos fundamentados na revisão bibliográfica, desenvolveu-se uma PoC acerca da viabilidade da implementação de *smart contracts* baseados em *blockchain* para o mercado de seguros massificados.

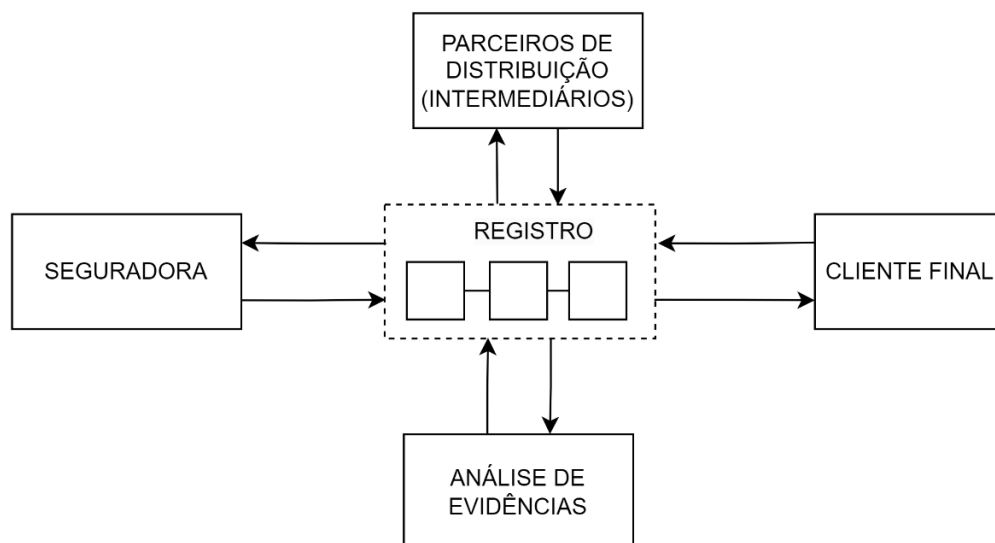
3.1 DEFINIÇÃO DO ESCOPO

Considerando as regulamentações impostas pelo CNSP e a necessidade de gerenciar permissões dos usuários, optou-se pela utilização de uma plataforma privada para realização da PoC. Essa escolha permitiu controlar a função de cada participante da rede e garantir a privacidade de processos específicos.

No que tange ao foco da implantação, direcionou-se aos seguros massificados, em virtude de sua relevância econômica e social no Brasil, evidenciada na seção 2.6.

Além disso, ressalta-se que no processo atual de contratação de seguros massificados (Figura 5) os parceiros precisam comunicar, posteriormente, a seguradora sobre as vendas realizadas. Com a solução proposta (Figura 6), a informação foi centralizada na *blockchain*, acessível a todos os participantes da rede com permissão, promovendo transparência e agilidade.

Figura 6 - Informação transparente para os participantes da rede



Fonte: Autores

Na seleção dos processos, foram escolhidas as operações relacionadas ao seguro de celular devido à sua natureza massificada e comum, amplamente oferecido tanto por representantes no momento da compra quanto por estipulantes em momentos posteriores.

Comumente, o seguro de celular é oferecido com cobertura contra roubo/furto e danos acidentais. Para facilitar a implementação da PoC, apenas o cenário de roubo/furto foi abordado. Assim, os processos estudados incluem:

- a) contratação: o consumidor final adquire o seguro por intermédio de um parceiro de distribuição (Figura 5);
- b) acionamento do seguro: ao solicitá-lo o segurado deverá apresentar a nota fiscal do celular e o boletim de ocorrência do furto/roubo;
- c) aprovação/rejeição das evidências de sinistro: após acionamento do seguro a ocorrência do evento será verificada, sendo aprovada ou rejeitada;
- d) aprovação/rejeição da solicitação: decisão final de aprovação ou rejeição da solicitação de sinistro.

Assim, em função do objetivo deste trabalho, definido na seção 1.2, busca-se promover transparência, eficiência e conformidade regulatória nas operações realizadas.

3.2 PROVA DE CONCEITO

A disposição dos usuários e das organizações envolvidas no processo é pautada na arquitetura representada na Figura 7. Nesta arquitetura, grupos de usuários distintos se conectam por meio de uma aplicação cliente, que por sua vez, se comunica com os *smart contracts* estabelecidos dentro de um canal na rede *blockchain*. O *peer* ordenador será encarregado de ordenar e gerar blocos de transação, os quais são validados e armazenados em cada *peer* da rede.

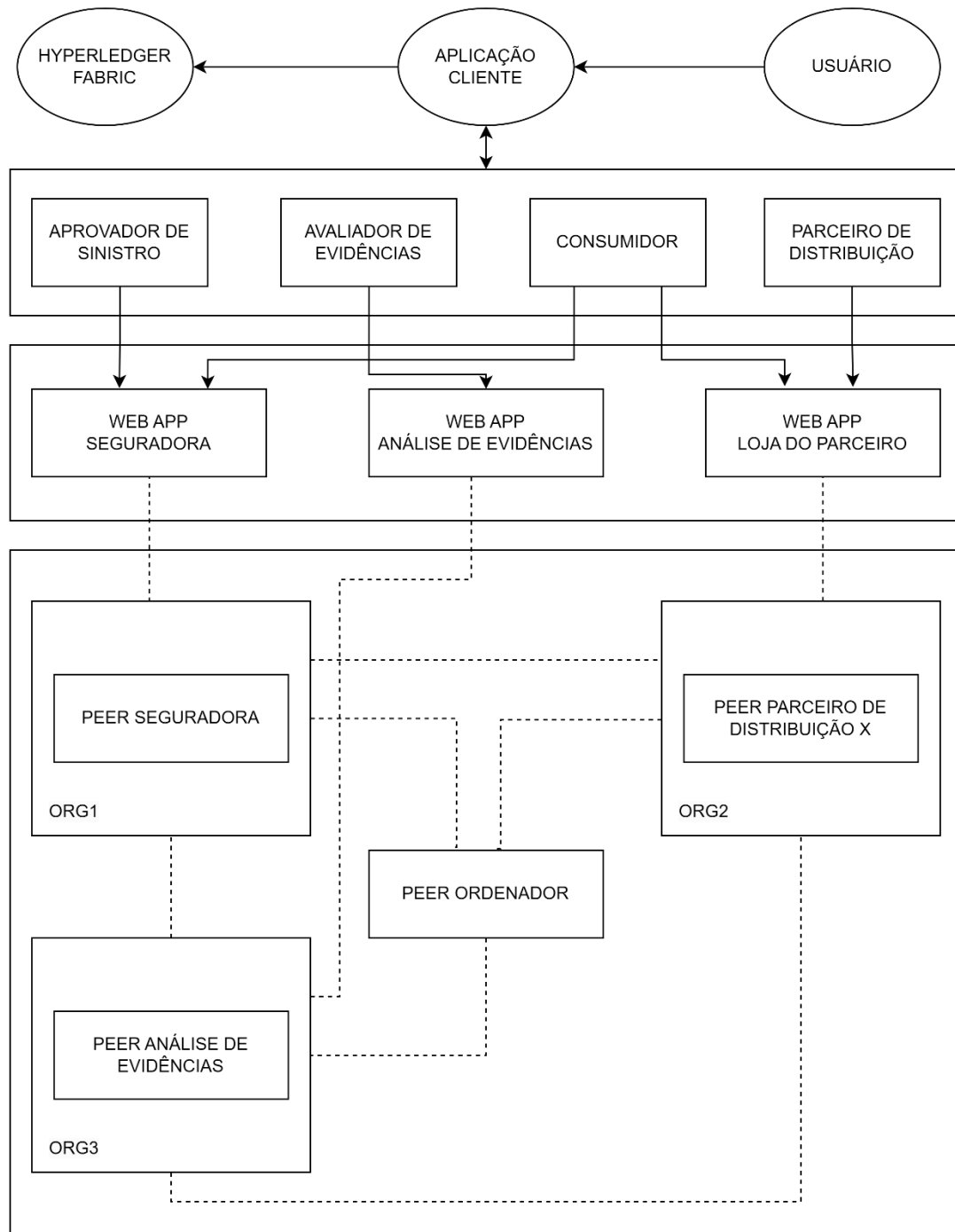
Dentro dessa rede estão presentes três organizações:

- a) seguradora: responsável pela gestão do seguro do celular e pela aprovação da indenização em função da ocorrência do sinistro;
- b) parceiro de distribuição: encarregado da venda do celular, oferta e contratação do seguro;

- c) empresa externa ou departamento da seguradora de avaliação de documentos comprobatórios: responsável pela análise de evidências.

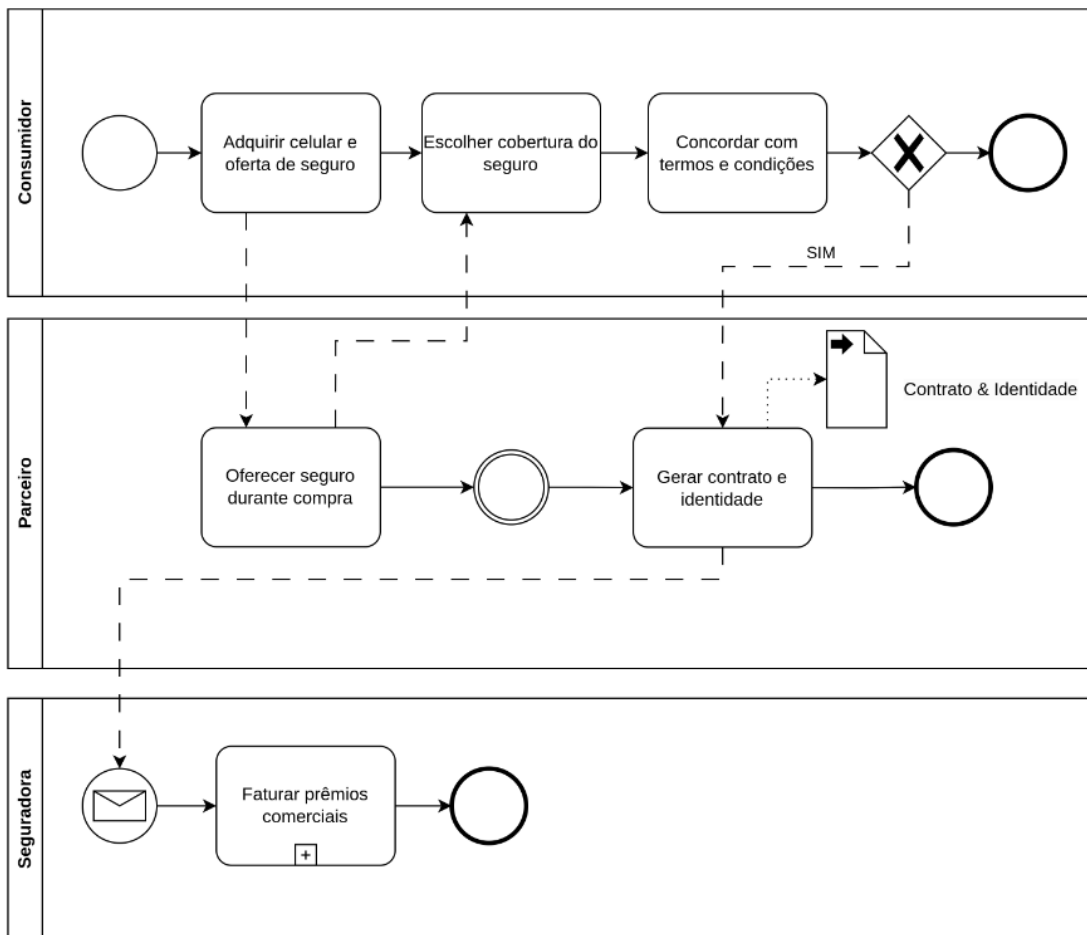
Cada organização possui um *peer* capaz de invocar *smart contracts*.

Figura 7 - Diagrama de fluxo da aplicação



O primeiro processo a ser abordado é a contratação do seguro, exemplificado na Figura 8. Neste procedimento, o consumidor acessa a aplicação cliente do parceiro de distribuição e adquire um celular.

Figura 8 - Fluxo de contratação do seguro



Fonte: Autores

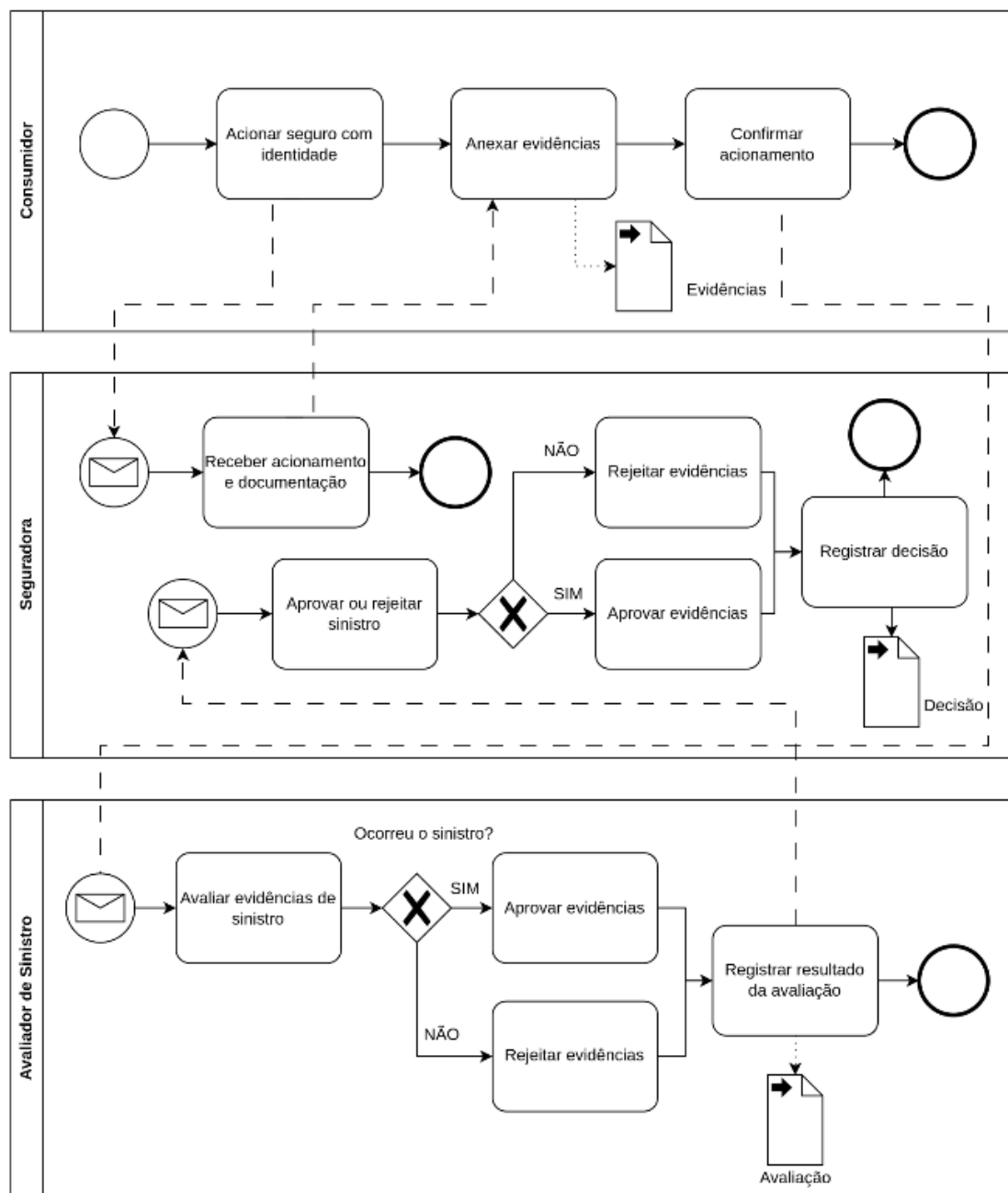
Durante a aquisição, é oferecido um seguro contra roubo/furto por um período específico, junto com o prêmio a ser pago. Se o consumidor concordar com os termos e condições, um *token*, representando o contrato, é gerado na *blockchain* e as credenciais são emitidas para autenticar o segurado em processos futuros com a seguradora, como o acionamento do seguro.

Para acionar o seguro, o segurado acessa a aplicação cliente da seguradora utilizando as credenciais referentes ao celular e seguro adquiridos. Além disso, neste momento o segurado deve anexar a documentação comprobatória da ocorrência do evento. A solicitação é registrada na rede e torna-se disponível para análise.

Em seguida, o avaliador possui a opção de aprovar ou rejeitar a solicitação em função da análise das evidências enviadas pelo segurado. Se for rejeitada, a solicitação recebe a situação de rejeitada. Caso contrário, se for aprovada, a decisão final de indenizar ou rejeitar a solicitação cabe à seguradora. Por fim, o responsável por aprovar a solicitação de sinistro, adiciona um registro na rede informando se a solicitação foi aprovada ou rejeitada.

Esses processos são descritos na figura a seguir.

Figura 9 - Fluxo de avaliação do acionamento do seguro



3.3 DESENVOLVIMENTO

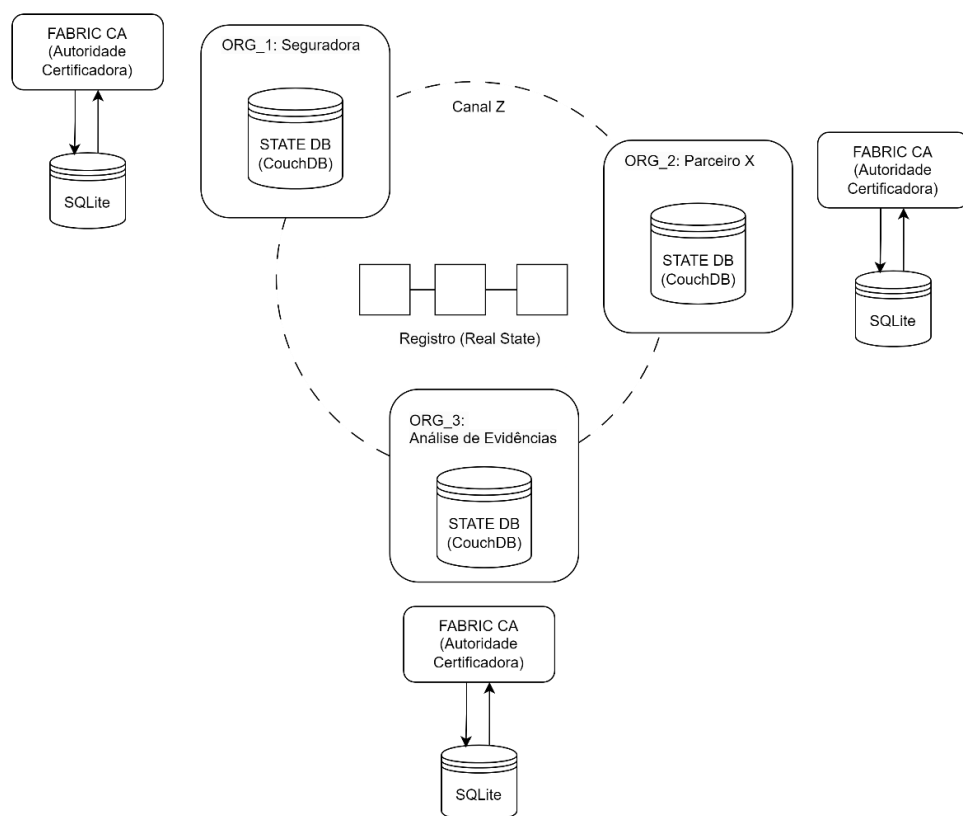
Em função do escopo definido para a PoC, o desenvolvimento foi dividido em dois domínios principais: configuração da rede de testes e implementação da aplicação cliente.

A referência ao repositório que contém a implementação da PoC encontra-se no Apêndice A.

3.3.1 Configuração da rede de testes

A rede de testes descentralizada, Figura 10, foi configurada de acordo com o diagrama apresentado na Figura 7, sendo composta por três organizações: seguradora, parceiro de negócios e análise de evidências. Para a implantação, utilizou-se a rede de teste pré-configurada fornecida pela *Hyperledger Fabric*, que originalmente incluía duas organizações, cada uma com seu próprio *peer*, além de um *peer* ordenador. Com base nessa estrutura inicial, adaptou-se a rede para suportar três organizações.

Figura 10 - Diagrama dos participantes da rede de testes



Fonte: Autores

Embora fosse possível criar uma rede com apenas um *peer* ordenador e uma única organização com seu *peer*, isso comprometeria a descentralização entre os participantes, uma vez que a única organização seria soberana no controle da rede. Portanto, a escolha por três organizações visa garantir a descentralização.

A configuração da rede foi facilitada por diversos *Bash scripts* auxiliares, além de um *script* principal que gerencia a criação da rede de forma personalizada, suportando diferentes *flags*⁸. Os *Bash scripts* possibilitam a execução de diversas operações, como levantar uma rede sem uma autoridade central, selecionar um algoritmo de consenso específico, criar canais e fazer *deploy* de *smart contracts* nesses canais.

A infraestrutura da rede é composta por múltiplos contêineres, com cada *peer* ou serviço executado em seu próprio contêiner, conforme ilustrado na Figura 11.

Figura 11 - Listagem dos contêineres ativos que compõem a rede

```
thiago@debian: ~/go/src/github.com/thiagore/fabric-massified-insurances/test-network$ docker ps --format "{{.Names}}: {{.Ports}}"
dev-peer0.org2.example.com-basic_1.0.1-7be248d097991a9bf65863e45376b2c204096ea5666fee101b9c4d39cfca8a74:
dev-peer0.org3.example.com-basic_1.0.1-7be248d097991a9bf65863e45376b2c204096ea5666fee101b9c4d39cfca8a74:
dev-peer0.org1.example.com-basic_1.0.1-7be248d097991a9bf65863e45376b2c204096ea5666fee101b9c4d39cfca8a74:
logspout: 127.0.0.1:8000->80/tcp
peer0.org3.example.com: 0.0.0.0:11051->11051/tcp, :::11051->11051/tcp, 7051/tcp, 0.0.0.0:11445->11445/tcp, :::11445->11445/tcp
peer0.org2.example.com: 0.0.0.0:9051->9051/tcp, :::9051->9051/tcp, 7051/tcp, 0.0.0.0:9445->9445/tcp, :::9445->9445/tcp
peer0.org1.example.com: 0.0.0.0:7051->7051/tcp, :::7051->7051/tcp, 0.0.0.0:9444->9444/tcp, :::9444->9444/tcp
couchdb2: 4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp, :::7984->5984/tcp
couchdb3: 4369/tcp, 9100/tcp, 0.0.0.0:9984->5984/tcp, :::9984->5984/tcp
orderer.example.com: 0.0.0.0:7050->7050/tcp, :::7050->7050/tcp, 0.0.0.0:7053->7053/tcp, :::7053->7053/tcp, 0.0.0.0:9443->9443/tcp, :::9443->9443/tcp
couchdb1: 4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp, :::5984->5984/tcp
ca_orderer: 0.0.0.0:9054->9054/tcp, :::9054->9054/tcp, 7054/tcp, 0.0.0.0:19054->19054/tcp, :::19054->19054/tcp
ca_org1: 0.0.0.0:7054->7054/tcp, :::7054->7054/tcp, 0.0.0.0:17054->17054/tcp, :::17054->17054/tcp
ca_org2: 0.0.0.0:8054->8054/tcp, :::8054->8054/tcp, 7054/tcp, 0.0.0.0:18054->18054/tcp, :::18054->18054/tcp
ca_org3: 0.0.0.0:11054->11054/tcp, :::11054->11054/tcp, 7054/tcp, 0.0.0.0:21054->21054/tcp, :::21054->21054/tcp
thiago@debian:~/go/src/github.com/thiagore/fabric-massified-insurances/test-network$
```

Fonte: Autores

Em relação aos *smart contracts*, optou-se por implementar apenas um, abrangendo todas as transações sobre o *token* do contrato de seguro. As transações suportadas pelo *smart contract* são:

- criação: emite uma novo *token* em função dos dados recebidos;
- consulta: retorna os dados do *token* consultado;
- atualização: atualiza informações do *token*;
- exclusão: remove o *token* do banco de dados de cada *peer*, mas não exclui do registro;
- listagem: lista todos os *tokens* ativos;
- consulta de histórico: lista todos os estados que o *token* já possuiu;

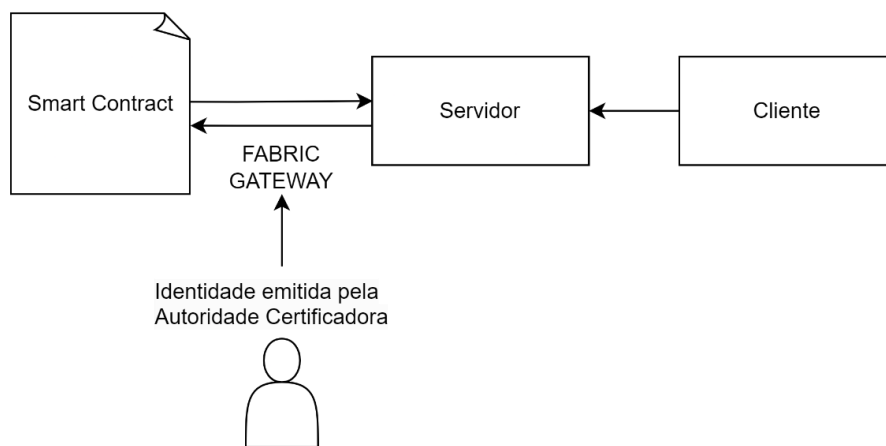
⁸ Parâmetros para execução de um *script*

g) listagem por *rich query*⁹: lista todos os *tokens* encontrados.

Apesar da possibilidade de desassociar as transações em diferentes *smart contracts*, a escolha por centralizar todas as transações em apenas um *smart contract* visa simplificar a usabilidade da PoC. No entanto, em um ambiente de produção, recomenda-se a segregação de transações em *smart contracts* distintos, a fim de facilitar a manutenção e adições de novas transações.

Por fim, ao concluir a configuração da rede, são geradas identidades certificadas padrão para cada organização, necessárias para a aplicação cliente, pois são utilizadas para estabelecer a conexão com o *gateway* da rede *blockchain*, vide Figura 12.

Figura 12 - Comunicação entre aplicações



Fonte: Autores

3.3.2 Aplicação cliente

A aplicação cliente foi projetada com o objetivo de permitir que o usuário final interaja diretamente com os *smart contracts* da rede *blockchain*. Para isso, sua arquitetura foi dividida em duas partes: servidor e cliente, como descrito na seção 2.5.

É importante destacar que, por se tratar de uma PoC, a arquitetura, as ferramentas utilizadas e os padrões de comunicação não foram desenvolvidos com o intuito de serem aplicados em um ambiente de produção. O principal foco da PoC foi atestar a viabilidade da ideia, e por essa razão, diversas convenções e boas práticas de desenvolvimento foram

⁹ Query complexa suportada pelo banco de dados, com capacidade de busca avançada e filtragem.

propositalmente ignoradas. Por exemplo, padrões de segurança mais robustos e a otimização da escalabilidade, visando simplificar o desenvolvimento e acelerar a implementação da PoC.

Dessa forma, a aplicação cliente, embora funcional para os propósitos da PoC, não deve ser considerada como modelo para ambientes de produção, onde aspectos como segurança, performance e manutenção são críticos.

3.3.2.1 Servidor

O servidor da aplicação foi desenvolvido em *Golang*, decisão tomada devido à proximidade com a plataforma *Hyperledger Fabric*, também desenvolvida nessa linguagem. Tal escolha oferece uma documentação mais rica e exemplos mais detalhados, o que facilitou a implementação de funcionalidades essenciais, quando comparado com outras opções como *JavaScript* e *Java*.

As responsabilidades centrais deste servidor envolvem executar invocações do *smart contract*, manipular os dados persistidos e expor *endpoints*¹⁰ HTTP para facilitar a comunicação com o cliente. Além disso, executar *Bash scripts*, como o *script* de criação de identidades. Essas funções são essenciais para garantir a interação entre o cliente e a rede *blockchain*.

As rotas da aplicação foram organizadas de modo a segmentar diferentes funcionalidades em *endpoints* específicos, assegurando modularidade e escalabilidade. Isso permite que a aplicação seja facilmente expandida à medida que novas funcionalidades são adicionadas, ou que novos serviços sejam integrados. Os principais grupos de rotas são:

- a) autenticação: responsável por autenticar o usuário com base nas credenciais geradas pela Autoridade Certificadora;
- b) eventos: permite a consulta aos blocos do registro, fornecendo visibilidade dos eventos transacionais registrados na *blockchain*;
- c) identidades: encarregado da emissão de novas identidades digitais;
- d) *smart contracts*: engloba a invocação do *smart contract*, permitindo tanto mutações quanto consultas sobre os dados da rede;
- e) acionamento do seguro: gerencia todo o fluxo de acionamento do seguro.

¹⁰ Localização exposta pela *API* para receber e responder consultas

Todas essas rotas foram configuradas seguindo o padrão REST, que padroniza a troca de dados entre o cliente e o servidor, permitindo uma comunicação eficiente. A escolha se deu em função de sua ampla utilização, além de ser uma forma de transferência de dados leve e eficaz.

Por fim, em um cenário real, cada participante da rede *blockchain* operaria seu próprio servidor, implementando suas próprias regras de negócios e atendendo aos requisitos específicos de seu domínio. Através da personalização garante-se que cada organização pode manter sua independência e controle sobre seus processos internos, ao mesmo tempo em que participa da rede descentralizada. Para efeito de demonstração na PoC, configurou-se três instâncias do mesmo servidor, cada um representando um participante da rede, e cada um com sua respectiva identidade para se conectar à *blockchain*. Essa configuração simplificada permite simular a comunicação entre diferentes entidades, porém, evidencia-se que em um ambiente de produção, a complexidade seria maior, com servidores ajustados às necessidades individuais de cada organização.

3.3.2.2 *Cliente*

A interface que o usuário final utiliza para interagir com o servidor foi implementada utilizando a biblioteca para desenvolvimento da Interface do Usuário – *User Interface* (UI) *React* em conjunto com *Next.js*¹¹. A escolha dessas ferramentas se deu pela experiência prévia com a tecnologia, além da sua robustez no desenvolvimento de interfaces modernas, ecossistema rico que acelera o desenvolvimento, como componentização, estilização modular e roteamento eficiente.

A principal função dessa aplicação foi possibilitar a simulação da interação dos diversos agentes da rede com o servidor, oferecendo uma interface simplificada para testes e validação da PoC. É importante destacar que, no cenário real, cada participante da rede *blockchain* teria sua própria aplicação. Entretanto, com objetivo de agilizar o desenvolvimento e para facilitar a visualização do fluxo geral do processo, optou-se por implementar uma única aplicação capaz de simular diferentes agentes.

Essa abordagem facilitou o desenvolvimento e permitiu que o foco da PoC permanecesse na validade funcional do sistema, ao invés de replicar a complexidade de

¹¹ Biblioteca do ecossistema React

múltiplas interfaces. A aplicação desenvolvida permitiu ao usuário final realizar ações como consulta de eventos, autenticação, operações do negócio e execução de transações do *smart contract*, acessando diretamente os *endpoints* expostos pela Interface de Programação de Aplicação – *Application Programming Interface* (API), descritos no capítulo anterior. Por meio dessa interface, pode-se demonstrar de forma mais concreta a operação do *smart contract* na *Hyperledger Fabric*, embora o desenvolvimento de um cliente exclusivo para cada agente seja essencial em um ambiente de produção.

Com isso, o cliente não só simplifica a interação com o servidor, como também viabiliza a visualização dos casos de uso propostos pela PoC. Mesmo não sendo essencial para a validação da viabilidade técnica, ele proporciona uma interface visual tangível para que os processos sejam avaliados de forma prática.

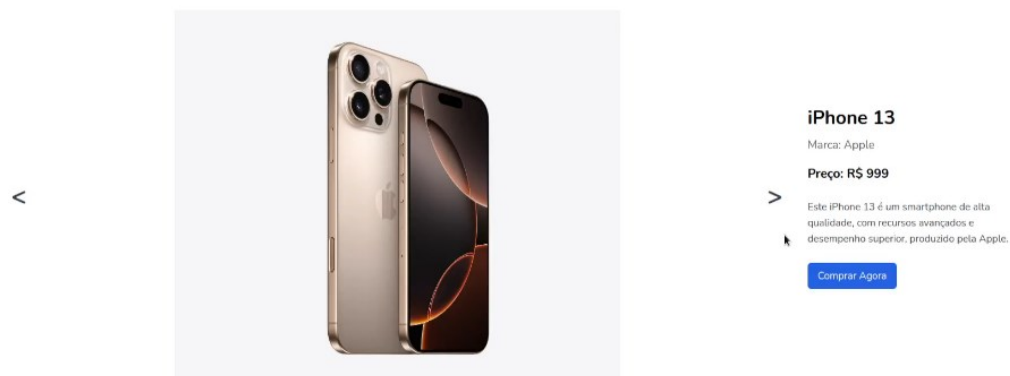
4 RESULTADOS

Este capítulo apresenta os casos de uso definidos no escopo desta PoC, seção 3.1. Os processos foram projetados para simular um ambiente real de contratação de seguro, com base em interações no *e-commerce*¹² e a tokenização do contrato de seguro na rede *blockchain*. As etapas a seguir detalham o funcionamento de cada parte do sistema e os resultados obtidos.

4.1 CONTRATAÇÃO

O fluxo tem início no processo de compra de um celular por intermédio do *e-commerce* de um parceiro de distribuição, como ilustrado na Figura 13, com a oferta de modelos distintos de celular (Figura 14).

Figura 13 - Oferta de celular da *Apple*



Fonte: Autores

Figura 14 - Oferta de celular da *Samsung*

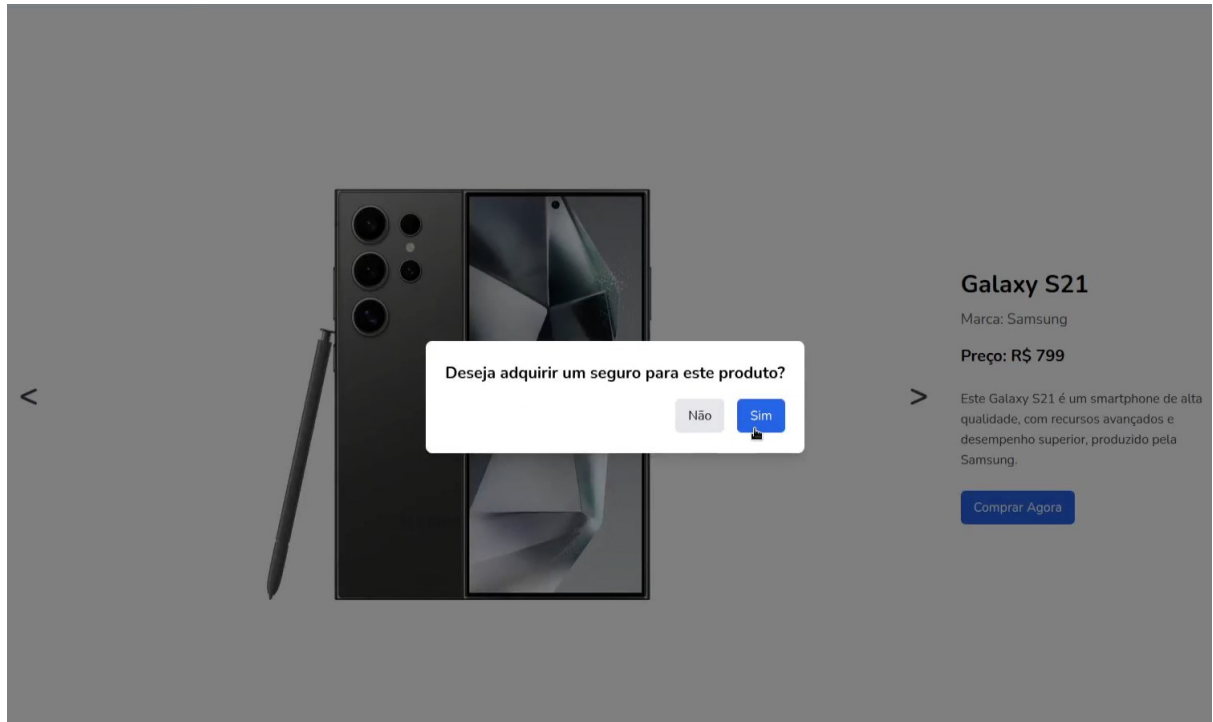


Fonte: Autores

¹² Comércio eletrônico caracterizado pela compra e venda realizada via *internet*

Após o consumidor escolher o produto desejado e clicar no botão "Comprar Agora", um modal é exibido, oferecendo a opção de adquirir um seguro para o celular (Figura 15).

Figura 15 - Opção de contratação do seguro para o celular




Fonte: Autores

Neste protótipo, apenas a opção positiva foi considerada. Em caso de negativa, o processo de finalização da compra continua pelo parceiro de distribuição. No entanto, ao optar pela contratação do seguro, inicia-se o processo de contratação descrito na Figura 8. A fim de ilustrar uma situação fidedigna ao cenário real, Figura 16, nessa página o parceiro solicita informações sensíveis do consumidor. Estas informações, podem ser armazenadas em um banco de dados *off-chain*, e depois consultadas pela seguradora e pelo responsável por analisar as evidências, garantindo a veracidade dos dados fornecidos. Apenas as informações essenciais para a emissão do *token* do seguro são registradas na *blockchain*.

Figura 16 - Contratação do seguro

Contratar Seguro

Galaxy S21



Smartphone avançado da Samsung.

Valor Coberto pelo Seguro:	R\$ 1000.00
Tipo de Cobertura:	Contra furto e roubo
Valor do Prêmio:	R\$ 55.00 por mês
Prazo do Seguro:	12 meses

Informações pessoais


Documento de identificação

Fonte: Autores

Figura 17 - Credenciais geradas

Contratar Seguro

Galaxy S21



Smartphone avançado da Samsung.

Valor Coberto pelo Seguro:	R\$ 1000.00
Tipo de Cobertura:	Contra furto e roubo
Valor do Prêmio:	R\$ 55.00 por mês
Prazo do Seguro:	12 meses

Informações pessoais

Documento de identificação

Usuário: Kx8suTtGpXSohbft
Senha: yEnYCHDqtC5PxsfxC6QxBm1N

Fonte: Autores

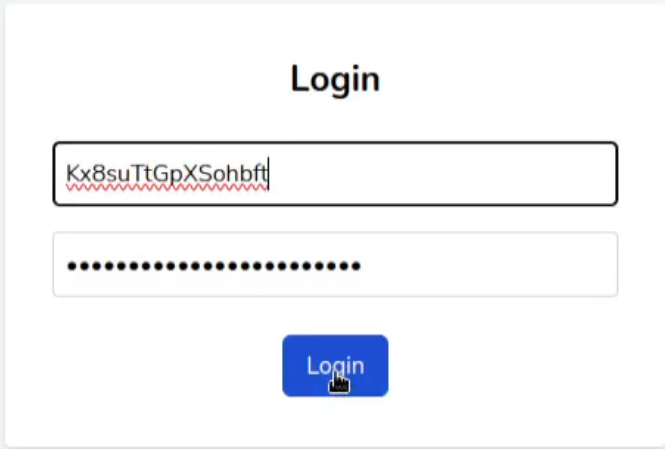
Ao finalizar a contratação, uma identidade digital é gerada para o segurado, vide Figura 17. Esta identidade, vinculada ao *token* do seguro, serve para autenticação futura no sistema da seguradora. O relacionamento entre o *token* e o segurado é estabelecido por meio da *string* “Usuário”, garantindo a associação clara e segura entre as partes envolvidas.

4.2 ACIONAMENTO DO SEGURO

Uma vez que o segurado esteja de posse de suas credenciais, ele acessa a página da seguradora e realiza a autenticação (Figura 18). Como cada identidade digital é única e vinculada a um único contrato de seguro, o sistema exibirá apenas o seguro correspondente ao par de credenciais inserido. Se o consumidor possuir mais de um seguro, ele terá múltiplas credenciais correspondentes.

A autenticação é realizada mediante busca pelo identificador do usuário e pela comparação do *hash* da senha fornecida com a armazenada no banco de dados da Autoridade Certificadora. Após a validação, o usuário é redirecionado para a página de detalhes do seguro (Figura 19), onde poderá visualizar as informações do contrato e acionar o seguro, quando necessário.

Figura 18 - Página de login da seguradora



Fonte: Autores

Figura 19 - Página de detalhe do seguro

Galaxy S21

Ativo



Smartphone avançado da Samsung.

Valor Coberto pelo Seguro:	R\$ 1000.00
Tipo de Cobertura:	Contra furto e roubo
Valor do Prêmio:	R\$ 55.00 por mês
Prazo do Seguro:	12 meses

Acionar seguro

Fonte: Autores

Na página de acionamento, o segurado anexa os documentos comprobatórios do sinistro, podendo incluir mais de um arquivo, como ilustrado na Figura 20. Após o envio dos documentos, o sistema realiza o *upload* e exibe uma mensagem de confirmação da conclusão do processo (Figura 21). Após o segurado clicar no botão “OK” ocorre o redirecionamento para a página atualizada de detalhe do seguro, com exibição da situação "Em Análise", indicando que o pedido de acionamento foi realizado (Figura 22).

Figura 20 - Aguardando *upload* dos arquivos

Envio de Evidências

Descreva o evento

test

Arraste ou clique e selecione os arquivos.

Arquivos selecionados:

test.pdf [Remover](#)

TIAGO VIDAL.pdf [Remover](#)

[Enviar](#)

Fonte: Autores

Figura 21 - *Upload* de arquivos realizado com sucesso

Claim in analysis

OK

test

Arraste ou clique e selecione os arquivos.

Arquivos selecionados:

test.pdf [Remover](#)

TIAGO VIDAL.pdf [Remover](#)

[Enviar](#)

Fonte: Autores

Figura 22 – Detalhe do seguro após ser acionado

Galaxy S21

Em Análise



Smartphone avançado da Samsung.

Valor Coberto pelo Seguro:	R\$ 1000.00
Tipo de Cobertura:	Contra furto e roubo
Valor do Prêmio:	R\$ 55.00 por mês
Prazo do Seguro:	12 meses

Fonte: Autores

4.3 ANÁLISE DAS EVIDÊNCIAS

A análise de evidências é realizada pelo analista da seguradora, que acessa a página de pedidos pendentes (Figura 23). Ao clicar em "Analisar", o analista é direcionado para a página de detalhes do pedido (Figura 24), em que visualiza as informações do contrato e as evidências.

Figura 23 - Página dos seguros aguardando análise das evidências

Pedidos para análise

Galaxy S21

Em Análise

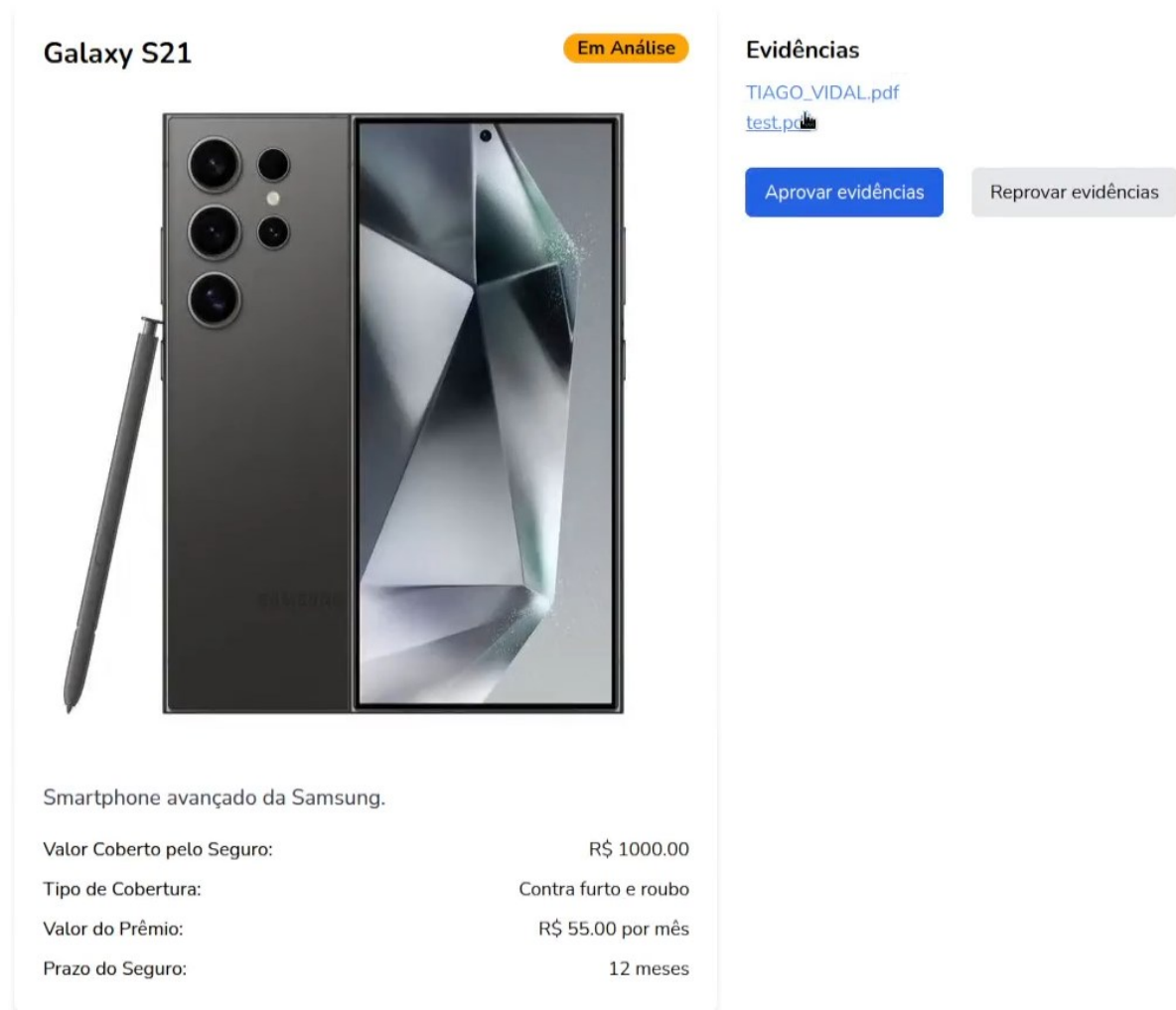
Smartphone avançado da Samsung.

Valor Coberto pelo Seguro:	R\$ 1000.00
Tipo de Cobertura:	Contra furto e roubo
Valor do Prêmio:	R\$ 55.00 por mês
Prazo do Seguro:	12 meses

Analisar

Fonte: Autores

Figura 24 - Página de detalhe de um seguro em análise de evidências



Fonte: Autores

Os documentos são exibidos individualmente no navegador, permitindo uma análise detalhada diretamente no sistema. Após a revisão dos documentos, o analista escolhe uma das opções: "Aprovar evidências" ou "Reprovar evidências". A escolha atualiza a situação do *token* de seguro. O analista é então redirecionado para a lista de pedidos, em que pode prosseguir com a análise de outras solicitações, quando houver mais pedidos para análise.


4.4 ANÁLISE FINAL DA SOLICITAÇÃO

Após a análise das evidências, a decisão final da solicitação está sob o controle da seguradora. A seguradora acessa uma página similar à de análise de evidências, conforme

mostrado na Figura 25, onde a decisão sobre o pedido de sinistro é formalizada. A análise final garante que todas as etapas foram seguidas corretamente antes de aprovar o pagamento da indenização ou encerrar o pedido.

Figura 25 - Detalhe de um seguro na página da decisão final

Galaxy S21



Evidências aprovadas

Evidências

TIAGO VIDAL.pdf
test.pdf

Aprovar

Reprovar

Smartphone avançado da Samsung.

Valor Coberto pelo Seguro:	R\$ 1000.00
Tipo de Cobertura:	Contra furto e roubo
Valor do Prêmio:	R\$ 55.00 por mês
Prazo do Seguro:	12 meses

Fonte: Autores

Por fim, através da API e da transação consulta de histórico, disponibiliza-se o histórico dos estados de um *token* específico, conforme ilustrado na Figura 26.

Figura 26 - Consulta do histórico do *token*, últimos estados

GET `http://localhost:3001/smartcontract/query` Send 200 OK 4.23 ms 1408 B 3 Days Ago

Params (4) Body Auth Headers (3) Scripts Docs

URL PREVIEW
`http://localhost:3001/smartcontract/query?channelid=mychannel&chaincodeid=basic&function=GetAssetRecords&args=cae47d65-208e-4647-bd02-83029e3693f0`

QUERY PARAMETERS

channelid	mychannel		
chaincodeid	basic		
function	GetAssetRecords		
args	5-208e-4647-bd02-83029e3693f0		

PATH PARAMETERS

Path parameters are url path segments that start with a colon ':'
 e.g. ':id'

Preview

```

1 {
2   "success": true,
3   "data": {
4     "docs": [
5       {
6         "isDelete": false,
7         "record": {
8           "claimStatus": "Approved",
9           "coverageDuration": 12,
10          "coverageType": 1,
11          "coverageValue": 1000,
12          "ID": "cae47d65-208e-4647-bd02-83029e3693f0",
13          "Insured": "ybrV40NdtPaxSg7c",
14          "Partner": "Varejista",
15          "Premium": 55
16        },
17        "timestamp": "2024-09-24T21:23:27.664861475Z",
18        "txId":
19          "9f6bd32a2f8ba357c85515c1bf2c868b93d169ef46355fbf1201ae13a36bb070"
20      },
21      {
22        "isDelete": false,
23        "record": {
24          "claimStatus": "EvidencesApproved",
25          "coverageDuration": 12,
26          "coverageType": 1,
27          "coverageValue": 1000,
28          "ID": "cae47d65-208e-4647-bd02-83029e3693f0",
29          "Insured": "ybrV40NdtPaxSg7c",
30          "Partner": "Varejista",
31          "Premium": 55
32        },
33        "timestamp": "2024-09-24T21:22:10.093752223Z",
34        "txId":
35          "7688419218d011f6b402086c630ca0ce82e96b162c69e64899800a3db67949dc"
36      },
37      {
38        "isDelete": false,
39        "record": {
40          "claimStatus": "Pending",
41          "coverageDuration": 12,
42          "coverageType": 1,
43          "coverageValue": 1000,
44          "ID": "cae47d65-208e-4647-bd02-83029e3693f0",
45          "Insured": "ybrV40NdtPaxSg7c",
46          "Partner": "Varejista",
47          "Premium": 55
48        },
49        "timestamp": "2024-09-24T21:16:56.481688146Z"
50      }
51    ]
52  }
53 }
  
```

\$.store.books[*].author

Fonte: Autores

5 CONCLUSÃO

Por meio da metodologia explicitada e dos resultados apresentados no capítulo anterior, observa-se que a necessidade de compartilhamento de informações entre os atores envolvidos no contrato de seguro foi reduzida. A implementação de soluções baseadas em *blockchain*, especialmente na PoC, conseguiu alcançar o objetivo proposto dentro do escopo definido. No entanto, para garantir a implementação, algumas abstrações precisaram ser feitas, as quais devem ser consideradas em cenários reais.

É importante destacar que o modelo topológico da rede utilizado foi escolhido pelos autores com o intuito de garantir a descentralização da informação entre os participantes da rede. Contudo, devido à modularidade das ferramentas utilizadas, seria possível adotar diversos modelos topológicos. Com isso, possibilita-se a redução da descentralização e aumento da autoridade da seguradora em relação aos demais atores.

Uma constatação que surgiu após a implementação da PoC foi que não é necessário armazenar os dados do segurado no *token* do contrato de seguro na *blockchain*. O uso das credenciais do segurado, que o validam como a pessoa segurada, pode substituir a necessidade de armazenar essas informações no contrato tokenizado. Isso se assemelha ao funcionamento das carteiras de criptomoedas, em que o portador das *seeds*¹³ é o portador da carteira, sem vínculo com sua identidade pessoal. No entanto, existem diferentes soluções possíveis para o tratamento desses dados:

- a) solução personalizada *on-chain*: armazenamento do *hash* dos dados na *blockchain*, com o uso de uma chave simétrica para obter os dados quando necessário;
- b) solução padrão *on-chain*: utilização da funcionalidade "*Private Data*", que possibilita a eliminação de dados privados, mantendo apenas o *hash* para comprovar a existência desses dados na rede em um momento específico;
- c) solução personalizada *off-chain*: armazenamento e gerenciamento dos dados em bancos de dados externos à *blockchain*, solução mais próxima ao que já é adotado atualmente para lidar com dados sensíveis.

¹³ Palavras geradas aleatoriamente que representam todas as chaves privadas associadas a uma determinada carteira

Além disso, a tokenização do contrato de seguro, especialmente na categoria de seguros massificados, possibilita o fracionamento do seguro oferecido pelo parceiro de distribuição ao consumidor final, abrindo espaço para o surgimento de novos modelos de negócios.

5.1 TRABALHOS FUTUROS

Em razão das novas possibilidades de modelos de negócios no setor de seguros, especialmente no contexto dos seguros massificados, diversas lacunas precisam ser preenchidas para garantir a conformidade com as regulamentações. Algumas sugestões para o avanço nesse campo incluem:

- a) exploração de soluções para o tratamento de dados sensíveis: buscar a melhor estratégia para garantir a proteção e a conformidade com regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD);
- b) desenvolvimento de modelos hierárquicos de rede: construção de modelos que equilibrem descentralização e autoridade, levando em consideração a diversidade de atores na rede;
- c) ferramentas para auditoria do registro: desenvolvimento de ferramentas de auditoria para usuários não técnicos, facilitando o acompanhamento do processo de forma transparente;
- d) estudos comparativos de ambientes *on-premise*¹⁴ e em nuvem: realização de estudos para comparar o desempenho, a segurança e a eficiência econômica entre servidores *on-premise* e soluções em nuvem.

5.2 CONSIDERAÇÕES FINAIS

A análise preliminar do mercado de seguros massificados no Brasil revela a crescente adesão entre a população de baixa renda, impulsionada pela acessibilidade dos custos e pela eficácia da cobertura oferecida. Esse cenário reforça a necessidade de soluções tecnológicas que possam ampliar e melhorar a oferta desses seguros, dado o grande mercado disponível.

O presente trabalho foi iniciado com a hipótese de que seria viável a tokenização de contratos de seguros massificados com o objetivo de centralizar, de forma descentralizada, a

¹⁴ Modelo em que a infraestrutura de *hardware* é gerenciada localmente

informação entre os participantes da rede, promovendo a transparência e a integridade dos dados. A solução proposta, baseada em *blockchain* privada, foi aplicada ao mercado de seguros massificados, oferecendo um caminho promissor para a transformação digital deste segmento.

REFERÊNCIAS

ALEKSIEVA, V.; VALCHANOV, H.; HULIYAN, A. **Implementation of Smart Contracts based on Hyperledger Fabric Blockchain for the Purpose of Insurance Services**. [s.l: s.n.]. Disponível em: <<https://ieeexplore.ieee.org/document/9244500>>. Acesso em: 23 abr. 2024.

AMAZON AWS. **What is a Web Application?** Disponível em: <<https://aws.amazon.com/what-is/web-application/>>. Acesso em: 23 ago. 2024a.

AMAZON AWS. **What's the Difference Between RPC and REST?** Disponível em: <<https://aws.amazon.com/compare/the-difference-between-rpc-and-rest/>>. Acesso em: 23 ago. 2024b.

ANBIMA. **Tokenização de Ativos**. [s.l: s.n.]. Disponível em: <<https://www.anbima.com.br/data/files/02/30/82/CB/68001810C27A8F08882BA2A8/Tokenizacao%20de%20ativos.pdf>>. Acesso em: 8 out. 2024.

ANDROULAKI, E. et al. **Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains**. Proceedings of the 13th EuroSys Conference, EuroSys 2018. Anais...Association for Computing Machinery, Inc, 23 abr. 2018.

BAKOS, Y.; HALABURDA, H. **Permissioned vs Permissionless Blockchain Platforms: Tradeoffs in Trust and Performance**. [s.l: s.n.]. Disponível em: <<https://ssrn.com/abstract=3789425>>.

BRASIL. **Resolução CNSP nº 348, de 25 de setembro de 2017**. Seção 1, n. 186, p. 23, , 25 set. 2017. Disponível em: <<https://www2.susep.gov.br/safe/scripts/bnweb/bnmapa.exe?router=upload/18574>>. Acesso em: 2 maio. 2024

BUTERIN, V. **Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform**. [s.l: s.n.]. Disponível em:

<https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf>. Acesso em: 1 maio. 2024.

CHAVES, R. H. S.; FERRAZ, D. L. DA S.; FERRAZ, J. DE M. Capital-imperialismo e a expansão do setor de seguros brasileiro no século XXI. **Argumentum**, v. 16, n. 1, p. 98–113, 1 maio 2024.

DOCKER. **Docker Docs**. Disponível em: <<https://docs.docker.com/get-started/workshop/>>. Acesso em: 3 out. 2024.

ETHEREUM. **Ethereum Development Documentation**. Disponível em: <<https://ethereum.org/en/developers/docs/>>. Acesso em: 9 abr. 2024.

FELIX, A. A. **Educação corporativa no varejo de eletrodomésticos e seguros massificados**. São Paulo: [s.n.].

GNU OPERATION SYSTEM. **Bash Reference Manual**. Disponível em: <<https://www.gnu.org/software/bash/manual/bash.html>>. Acesso em: 13 ago. 2024.

HYPERLEDGER. **Hyperledger Fabric Docs**. Disponível em: <<https://hyperledger-fabric.readthedocs.io/en/release-2.5/>>. Acesso em: 19 abr. 2024.

INFOMONEY. **Classes D e E continuarão a ser mais da metade da população até 2024, projeta consultoria**. Disponível em: <<https://www.infomoney.com.br/minhas-financas/classes-d-e-e-continuarao-a-ser-mais-da-metade-da-populacao-ate-2024-projeta-consultoria/>>. Acesso em: 6 maio. 2024.

JIA, W.; ZHOU, W. **Distributed Network Systems: From Concepts to Implementations**. [s.l.] Springer, 2004. v. 15

MERKEL, D. Docker: Lightweight Linux Containers for Consistent Development and Deployment. **Linux Journal**, 19 maio 2014.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. [s.l: s.n.]. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 26 abr. 2024.

OUTREVILLE, J. F. **Theory and Practice of Insurance**. [s.l.] Springer US, 1998.

PAHL, C. et al. Cloud Container Technologies: A State-of-the-Art Review. **IEEE Transactions on Cloud Computing**, v. 7, n. 3, p. 677–692, 1 jul. 2019.

SALAHSHOR, A.; SCHERRER, J. **Smart Contracts, Insurtechs and the Future of Insurance**. [s.l: s.n.]. Disponível em: <<http://lup.lub.lu.se/student-papers/record/9001985>>. Acesso em: 23 abr. 2024.

SANKAR, L. S.; SINDHU, M.; SETHUMADHAVAN, M. **Survey of consensus protocols on blockchain applications**. [s.l: s.n.]. Disponível em: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8014672&isnumber=8014556>>. Acesso em: 4 maio. 2024.

SANTOS, G. L. DOS. **Agilização de Processo de Negociação de Seguros Massificados com Parceiros em Empresa Seguradora**. São Paulo: [s.n.].

SHETTY, S. S.; KAMHOUA, C. A.; NJILLA, L. L. **Blockchain for Distributed Systems Security**. [s.l: s.n.].

STALLINGS, WILLIAM. **Cryptography and Network Security: Principles and Practice**. [s.l.] Pearson Education Limited, 2017.

SZABO, N. Smart Contracts: Formalizing and Securing Relationships on Public Networks. **First Monday**, v. 2, n. 9, 1 set. 1997.

ZAND, M.; WUN, X.; MORRIS, M. A. **Hands-On Smart Contract Development with Hyperledger Fabric V2 Building Enterprise Blockchain Applications**. 1. ed. [s.l.] O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2021.

APÊNDICE A – REPOSITÓRIO

Os códigos-fonte e binários utilizados para implementação da PoC encontram-se no repositório <<https://github.com/thiagogre/fabric-massified-insurances>>.

Os principais códigos-fonte desenvolvidos podem ser diretamente acessados nos endereços:

- a) Cliente: < <https://github.com/thiagogre/fabric-massified-insurances/tree/main/test-network/frontend-react> >;
- b) Servidor: <<https://github.com/thiagogre/fabric-massified-insurances/tree/main/test-network/rest-api-go>>;
- c) Script principal: <<https://github.com/thiagogre/fabric-massified-insurances/blob/main/test-network/run-test-network.sh>>.